Secret key sharing and secret key generation

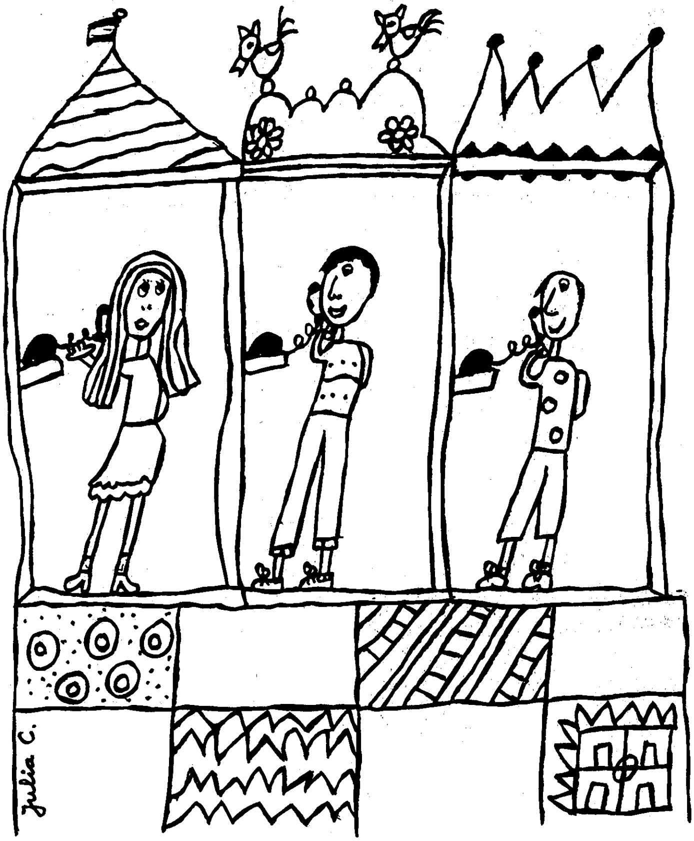
DOI:
10.6100/IR501451

Document status and date:
Published: 01/01/1997

Document Version:
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Secret Key Sharing and Secret Key Generation

Marten van Dijk



Secret Key Sharing
and
Secret Key Generation

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, prof.dr. M. Rem, voor een commissie aangewezen door het College voor Promoties in het openbaar te verdedigen op

dinsdag 9 december 1997 om 16.00 uur

door

Marten van Dijk

geboren te Amsterdam

Dit proefschrift is goedgekeurd door de promotoren:

prof.dr.ir. H.C.A. van Tilborg
en
prof.dr.ir. B.J.M. Smeets

Druk: Boek- en Offsetdrukkerij Letru, Helmond, (0492) 59 07 60

Voorplaat getekend door Julia Claassen

CIP-data library Technische Universiteit Eindhoven

Dijk, Marten van

Secret key sharing and secret key generation / by Marten van Dijk. -
Eindhoven : Eindhoven University of Technology, 1997.
Proefschrift. - ISBN 90-386-0591-9
Nugi 811
Subject headings: cryptology
1991 Mathematics Subject Classification: 94A60 / 11T71

Voor Wim, Tineke, en Jackie.

Preface

This thesis consists of two parts. The first one deals with the problem how to share efficiently a secret key among a group of people. The second part addresses the problem how two persons can generate a secret key while having at their disposal a noisy communication channel eavesdropped by an adversary. The following preprints and papers are included in this thesis (in order of their appearance as preprint):

[A] "On the information rate of perfect secret sharing schemes". *Designs, Codes and Cryptography*, 6:143–169, 1995.

[B] "A linear construction of secret sharing schemes". *Designs, Codes and Cryptography*, 12:161–201, 1997. A preliminary version titled "A linear construction of perfect secret sharing schemes" appeared in the Proceedings of EUROCRYPT '94, Lecture Notes in Comput. Sci., volume 950, pages 23–34, 1995.

[C] "Coding gain strategies for the binary symmetric broadcast channel with confidential messages". In *Proceedings of the 16th Symposium on Information Theory in the Benelux, May 18 - 19*, pages 53–60, 1995.

[D] "On a special class of broadcast channels with confidential messages". *IEEE Inform. Theory*, 43:712–714, 1997.

[E] "The binary symmetric broadcast channels with confidential messages, with tampering". In *Proceedings of ISIT'95, September 17-22*, page 487, 1995.

[F] with Christian Gehrmann and Ben Smeets. "Unconditionally secure group authentication". Submitted to Designs, Codes and Cryptography (in November 95).

[G] with Wen-Ai Jackson and Keith M. Martin. "A general decomposition construction for incomplete secret sharing schemes". Submitted to Designs, Codes and Cryptography (in November 95).

[H] with Wen-Ai Jackson and Keith M. Martin. "A note on duality in linear secret sharing schemes". *Bulletin of the Institute of Combinatorics and its Application*, Vol. 19:93–101, 1997.

[I] "The optimal linear worst-case information rate". In *Proceedings of ISIT'97, June 28 - July 4*, page 89, 1997. Extended version submitted to Designs, Codes and Cryptography (in July 1996).

[J] "More information theoretical inequalities to be used in secret sharing?". *Information Processing Letters*, 63:41–44, 1997.

[K] with Arie Koppelaar. "Quantum key agreement". In *Proceedings of the 18th Symposium on Information Theory in the Benelux, May 15 - 16*, pages 97–104, 1997.

We shortly summarize the results on which this thesis is based.

Part I (Chapters 1–6): A secret sharing scheme is a method which distributes shares to a set of participants in such a way that only specified groups of participants (collectively called the access structure) can reconstruct the secret by pooling their shares. The individual information rate of a participant is the size of its share divided by the size of the secret. The fundamental problem in secret sharing is to construct optimal schemes in the sense that the worst-case (greatest) individual information rate is as small as possible. This is for reasons of security and efficiency. Chapter 1 introduces the basic definitions and concepts.

We develop a method to lower bound individual information rates [A,J] in Chapter 2. For a special class of access structures, the so called graph-based access structures, we prove a tight bound in terms of the maximal degree of the graph. From this we obtain that shares may *need* to be impractically large.

Construction results can be split into two types: basic constructions and decomposition constructions. Basic constructions are methods to construct secret sharing schemes without using existing ones. In Chapter 3 we give a description of linear basic constructions by means of a matrix approach [B]. It leads to a duality result, which is joint work with Wen-Ai Jackson and Keith Martin [H], a lower bound on the individual information rate for linear schemes [I], and to an algorithm for finding secret sharing schemes. Optimal schemes for access structures based on connected graphs on six vertices constructed by this algorithm are presented in Chapter 4 (Perry Moerland implemented the algorithm) [A].

Decomposition constructions are methods to construct secret sharing schemes using existing ones. In Chapter 5, joint work with Wen-Ai Jackson and Keith Martin [G] we generalize all known decomposition constructions.

We also discuss an application of secret sharing in authentication theory in Chapter 6. In joint work with Christian Gehrmann and Ben Smeets

[F] we deal with a scenario where among a group of participants only certain subsets of participants are able to authenticate a message in order to send it to a trustable receiver. We use an approach where we extend existing linear secret sharing schemes to unconditionally secure group authentication schemes.

Part II (Chapters 7–10): The second part of the thesis is about secret key generation by two persons, Alice and Bob, who communicate to each other by means of a noisy channel. The situation gets complicated by an adversary, Eve, who eavesdrops this noisy channel. Fortunately for Alice and Bob, the eavesdropping channel is noisy as well, which enables them to generate a secret key. Chapter 7 introduces the basic definitions and concepts, and also discusses the situation in which in addition Alice and Bob use a public channel.

In Chapter 8 we allow Eve to tamper the communication over the noisy channel between Alice and Bob. We treat two examples. In the first one Eve tampers passively (joint work with Arie Koppelaar) [K] and in the second one Eve tampers actively [E].

For a special class of noisy channels we show in Chapter 9 how to determine the maximal rate at which Alice and Bob can generate a secret key without using a public channel (and without tampering by Eve) [D].

In Chapter 10 we consider the following special situation. Alice and Bob, communicate to each other by means of a binary symmetric main channel and a noiseless public channel. The only facility Eve has is to tap the main channel using a binary symmetric wire-tap channel. Alice and Bob want to generate a secret key such that Eve can only obtain a negligible amount of information about it. In general for this case, the generation of the secret key can be split into three phases; the advantage distillation phase, the reconciliation phase, and the privacy amplification phase. We discuss the advantage distillation phase, where we generalize Maurer's reliability estimation technique and we generalize Gander and Maurer's improvement of the reliability estimation technique [C].

Notice that Chapters 1 and 7 contain an outline of what is explained in their parts. Have fun reading :-)!

September 1997 Marten van Dijk

Acknowledgements

In the first place I would like to thank my parents, Wim and Tineke, who taught me to be curious throughout all my live. They supported me during my masters and PhD studies. I like to thank my supervisor Henk van Tilborg for giving me the opportunity to do a PhD-study in cryptology. Henk showed lots of patience and he taught me about technical English which improved my presentations enormously. Furthermore, I would like to thank the Discrete Mathematics group at the Eindhoven University of Technology for their stimulating working environment, where I learned about various aspects of discrete maths in general. I enjoyed the company of the members of this group very much. I like to thank my co-authors Keith Martin, Wen-Ai Jackson, Ben Smeets, Christian Gehrmann, and Arie Koppelaar. Special thanks go to Perry Moerland with whom I had interesting discussions and who implemented a first version of the search algorithm as described in Chapter 3. Finally, I like to thank Ben Smeets who encouraged me to work at the University of Lund for a few months, and I like to thank Victor Wei who offered me a position at the Chinese University of Hong Kong. In Hong Kong I met my wife Jackie to whom I give my special thanks for giving me lots of love during this last period of writing.

Contents

Part I

Secret Key Sharing

Chapter 1

Why Secret Sharing? A Brief Introduction

A secret sharing scheme is a method which distributes *shares* of a *secret* to a set of *participants* in such a way that only specified groups of participants (collectively called the *access structure*) can reconstruct the secret by pooling their shares. Secret sharing is related to key management and key distribution. These problems are common to all crypto systems. Secret sharing is also used in multi-party secure protocols. Further, secret sharing schemes have natural applications in access control and cryptographic key initialization. Let us introduce the concept of secret sharing by some examples.

1.1 Some Examples

Example 1.1.1 Let us consider the following situation. Suppose a computer selects a secret s in $\mathbb{Z}_m$ according to a probability distribution $p(s)$. The secret has to be shared by the computer among three participants 1, 2, and 3 subject to the following requirements. Groups $\{1,2\}$, $\{2,3\}$, and $\{1,2,3\}$ have to be able to reconstruct the secret, but all other combinations should not be able to obtain information about the secret. For example, if participants 2 and 3 sit together and exchange their shares they can reconstruct s. On the other hand if participants 1 and 3 sit together and pool their shares then they do not obtain any information about s (besides the information they already know). Thus participants 1 and 3 can do no better than guessing the secret s according to the probability distribution $p(s)$.

We call the groups who are allowed to reconstruct the secret *qualified*, and we call the groups who should not be able to obtain information about the secret *forbidden*. The collection of all qualified groups is denoted by Γ, and the collection of all forbidden groups is denoted by Δ. In this example

$$\begin{aligned}&\Gamma = \{\{1,2\},\{2,3\},\{1,2,3\}\} \text{ and}\\ &\Delta = \{\emptyset,\{1\},\{2\},\{3\},\{1,3\}\}.\end{aligned}$$

The tuple (Γ, Δ) is called the *access structure.* It describes all requirements we impose on our secret sharing scheme.

In Figure 1.1 an example is given of a secret sharing scheme meeting the requirements described by (Γ, Δ). The description of the scheme is public knowledge. For instance, 2 and 3 know how to compute s, namely by subtracting share a from $a+s$. Similarly, groups $\{1,2\}$ and $\{1,2,3\}$ can compute s.

What about the remaining groups? (Note that the remaining groups are all forbidden.) When 1 and 3 combine their shares they only obtain the value of the uniformly distributed random variable a. It tells them nothing about the secret s. Thus 1 and 3 can do no better than guessing s according to its probability distribution $p(s)$. Similarly all subgroups of $\{1,3\}$ can not obtain information about the secret. The last group we have to consider is $\{2\}$. Since a is randomly chosen in $\mathbb{Z}_m$ and since a is independent of s share $a+s$ is uniformly distributed over $\mathbb{Z}_m$. Share $a+s$ takes on every value with equal probability. This means that $a+s$ and s are statistically independent. Hence, $a+s$ gives no information about s. Therefore also 2 can do no better than guessing s according to its probability distribution $p(s)$. We conclude that the secret sharing scheme in Figure 1.1 satisfies all imposed requirements.

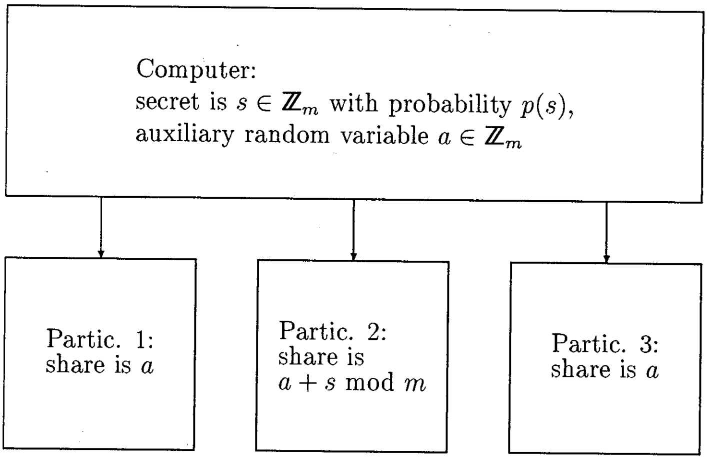

Computer:
secret is $s \in \mathbb{Z}_m$ with probability $p(s)$,
auxiliary random variable $a \in \mathbb{Z}_m$
Partic. 1:
share is a
Partic. 2:
share is
$a + s \bmod m$
Partic. 3:
share is a

Figure 1.1: A secret sharing scheme.

To give a formal definition of secret sharing schemes we like to describe secret sharing schemes by some mathematical structure. We do not like to do this by means of a figure as done in this example. Therefore we introduce the following approach to describe the secret sharing scheme of Figure 1.1. We will show that the scheme can be fully described by a probability mass function ν over four-tuples with entries in $\mathbb{Z}_m$ defined by

$$\nu(s, a, a + s, a) = p(s)/m. \tag{1.1}$$

Note that the first argument is the actual secret while the others correspond with the shares. For example suppose that $m = 2$ and $p(s) = 1/2$ for $s \in \mathbb{Z}_2$. Then the probability mass function ν evaluated in each of the four-tuples

$$(0,0,0,0), (0,1,1,1), (1,0,1,0), (1,1,0,1) \tag{1.2}$$

equals 1/4.

In Figure 1.2 a secret sharing scheme based on function ν is given. Let us explain why ν describes the secret sharing scheme of Figure 1.1. By using (1.1) we derive that the probability that the computer selects s as secret in the scheme of Figure 1.2 is equal to

$$\sum_{(\chi_1,\chi_2,\chi_3)\in\mathbb{Z}_m^3} \nu(s, \chi_1, \chi_2, \chi_3) = \sum_{a\in\mathbb{Z}_m} \nu(s, a, a + s, a) = \sum_{a\in\mathbb{Z}_m} p(s)/m = p(s),$$

as in the scheme of Figure 1.1. Further we notice that in the scheme of Figure 1.1 the probability that the computer selects secret s and random variable a is equal to $p(s)/m$. This shows that the probability that the secret is s and the shares of 1, 2, and 3 are a, $a + s$, and a respectively is equal to $p(s)/m = \nu(s, a, a + s, a)$ in both schemes. We conclude that ν describes the scheme of Figure 1.1 exactly. In the formal definition of secret sharing schemes in Section 1.2 we will make use of probability mass functions to mathematically describe how each share is produced.

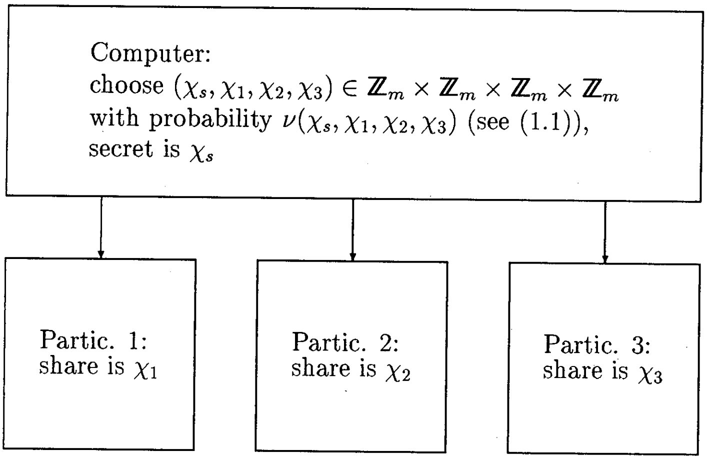

Computer:
choose $(\chi_s, \chi_1, \chi_2, \chi_3) \in \mathbb{Z}_m \times \mathbb{Z}_m \times \mathbb{Z}_m \times \mathbb{Z}_m$
with probability $\nu(\chi_s, \chi_1, \chi_2, \chi_3)$ (see (1.1)),
secret is χ_s
Partic. 1:
share is χ_1
Partic. 2:
share is χ_2
Partic. 3:
share is χ_3

Figure 1.2: Description by means of a probability mass function.

In the explanation of the scheme of Figure 1.1 we stated that its description is public knowledge. We finish this example by remarking that in secret sharing descriptions of schemes are public knowledge. In the scheme of Figure 1.2 ν is publicly available.

Example 1.1.2 Let the set of participants be $\mathcal{P} = \{1, 2, 3, 4\}$, the set of qualified groups be $\Gamma = \{X : \{1,2\} \subseteq X, \{1,3\} \subseteq X, \text{ or } \{2,3,4\} \subseteq X\}$, the set of forbidden groups be $\Delta = \{X : X \subseteq \{3,4\}, X \subseteq \{2,4\}, \text{ or } X \subseteq \{1\}\}$, and the set of possible secrets to be equal to $\mathbb{Z}_m^2$. In Figure 1.3 the access structure (Γ, Δ) is visualized.

To share a secret $(s_1, s_2) \in \mathbb{Z}_m^2$ according to a probability distribution $p(s_1, s_2)$ a mutually trusted authority first securely chooses random elements $a_1, a_2, a_3, a_4 \in \mathbb{Z}_m$. Secondly, the authority gives participant 1 share $(s_1 + a_1, s_2 + a_3, a_4) \in \mathbb{Z}_m^3$, participant 2 share $(s_1 + a_3, s_2 + a_4) \in \mathbb{Z}_m^2$, participant 3 share $(a_1, a_3) \in \mathbb{Z}_m^2$, and participant 4 share $a_1 + a_4 \in \mathbb{Z}_m$. We leave it to the reader to check that this is a secret sharing scheme for (Γ, Δ), that is that it meets the requirements described by (Γ, Δ). In this scheme $2^{\mathcal{P}} \setminus (\Gamma \cup \Delta)$ consists of the two subsets $\{1, 4\}$ and $\{2, 3\}$ (see Figure 1.3). Note that $\{1, 4\}$ can only reconstruct s_1 and note that $\{2, 3\}$ can only reconstruct s_1.

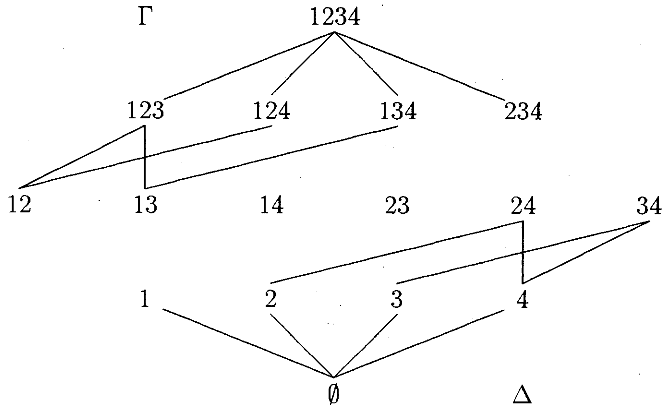


Figure 1.3: An access structure.

The probability mass function ν over five-tuples in $\mathcal{T} = \mathbb{Z}_m^2 \times \mathbb{Z}_m^3 \times \mathbb{Z}_m^2 \times \mathbb{Z}_m^2 \times \mathbb{Z}_m$ defined by

$$\nu((s_1, s_2), (s_1+a_1, s_2+a_3, a_4), (s_1+a_3, s_2+a_4), (a_1, a_3), a_1+a_4) = p(s_1, s_2)/m^4$$

describes our secret sharing scheme. Similarly to the previous example we index the entries of the five-tuples by s, 1, 2, 3, and 4. To share a secret selected from $\mathbb{Z}_m^2$ according to the probability distribution $p(s_1, s_2)$ a mutually trusted authority first selects a tuple $(\chi_s, \chi_1, \chi_2, \chi_3, \chi_4) \in \mathcal{T}$ according to the probability mass function ν. Secondly, the authority transmits χ_i to participant i, for $1 \leq i \leq 4$. The first entry χ_s will be the secret key.

Example 1.1.3 Another example of secret sharing is the following situation from [95, Chapter 9]. A bank may want to require the collaboration of at least two vice-presidents or of at least three senior tellers to be able to authenticate an electronic funds transfer (EFT) with the natural additional requirement that a vice-president should also be able to act as a senior teller. That is, any vice-president and any two senior tellers should also be able to authenticate an EFT. Let $1, \ldots, t$ be the senior tellers, and let $t+1, \ldots, t+v$ be the vice-presidents. Suppose that the president chooses randomly a secret authentication key $s \in GF(q)$, where $q \geq 1 + t + t(t-1)/2 + v$ is a prime power. To share s among the vice-presidents and senior tellers the president selects nonzero distinct elements $\alpha_1, \ldots, \alpha_{t+v} \in GF(q)$ as follows. He first selects $\alpha_1, \ldots, \alpha_t$. Then he selects the remaining $\alpha_{t+1}, \ldots, \alpha_{t+v}$ different from all values

$$\alpha_i \alpha_j (\alpha_i + \alpha_j)^{-1}, 1 \leq i < j \leq t.$$

Note that the president can select such elements since $q \geq 1+t+t(t-1)/2+v$. He stores these elements in a public directory. Next the president chooses random elements $a, b \in GF(q)$, and he transmits to i share

$$\begin{aligned} s_i &= s + a\alpha_i, \text{ if } t+1 \leq i \leq t+v \text{ (i is a vice-president), and} \\ s_i &= s + a\alpha_i + b(\alpha_i)^2, \text{ if } 1 \leq i \leq t \text{ (i is a senior teller).} \end{aligned}$$

The random elements a and b are kept secret by the president.

Suppose i, and j, two senior tellers, and k, a vice president, want to combine their shares in order to compute s, the authentication key. Using the public directory of the president they construct

$$G = \begin{pmatrix} 1 & 1 & 1 \\ \alpha_i & \alpha_j & \alpha_k \\ (\alpha_i)^2 & (\alpha_j)^2 & 0 \end{pmatrix}$$

and its inverse, which exists since $det(G) = [\alpha_k(\alpha_i + \alpha_j) - \alpha_i\alpha_j](\alpha_i - \alpha_j) \neq 0$. Then they compute

$$(s_i, s_j, s_k)G^{-1} = (s, a, b),$$

which reveals s. The combination of three senior tellers and the combination of two vice-presidents can be dealt with in a similar way and are left to the reader.

What does a combination of two senior tellers i and j know? Their shares are given by the entries of the vector

$$s(1,1) + (a,b) \begin{pmatrix} \alpha_i & \alpha_j \\ (\alpha_i)^2 & (\alpha_j)^2 \end{pmatrix}.$$

The knowledge about s contained in this vector equals the knowledge about s contained in the vector

$$s(1,1)\begin{pmatrix} \alpha_i & \alpha_j \\ (\alpha_i)^2 & (\alpha_j)^2 \end{pmatrix}^{-1} + (a,b).$$

Since s, a, and b are statistically independent, and a and b are uniformly chosen random variables a combination of two senior tellers can not obtain any information about s. The remaining case, a combination of one senior teller with a vice-president, can be dealt with in a similar way and is left to the reader.

Example 1.1.4 Cryptography is used by banks, authorities, and industries for protecting valuable data and ideas recorded in electronic documents. Criminals and terrorists on the other hand abuse cryptography to hide their illicit plans. This may pose a serious problem for the authorities during criminal investigations or when protecting the national security. Judges may give court-authorizations to the police to tap communication between persons with criminal behaviour. In the past the investigating authorities were able to interpret the tapped communication. Nowadays the communication is encrypted using (public and) secret keys. Decryption is only possible if all keys are known. Therefore the police can not obtain the meaning of the tapped messages. In other words the intention of the court-authorization is not met in practise. So, current legislation is not sufficient any more.

Micali [85] proposes to introduce a new law stating that only *fair crypto systems* are allowed to be used. Fair crypto systems are crypto systems having the properties that they can not be misused by any criminal organization and that they guarantee to citizens exactly the same rights to privacy they currently have under the law in democratic countries. For example industries want to keep complete freedom when choosing crypto systems. They do not want a limitation of their rights when choosing a crypto system. Thus limiting their freedom by introducing a law stating that one particular crypto system has to be used would hurt the principles of democracy (for example the clipper chip proposal put forward by the Clinton administration). A deep discussion on cryptology versus democracy can be found in [85].

As an example we describe Micali's fair Diffie-Hellman public key crypto system in which secret sharing plays a crucial role. Diffie-Hellman's scheme [40] can be used by a collection of person's to communicate securely to one another. Let us first explain their scheme. Let q be a prime power and let g generate $GF(q)$. In Diffie-Hellman's scheme each user i secretly selects an arbitrary non zero element $s_i \in GF(q)$ as private key and each user i publicly announces $p_i = g^{s_i}$ as public key. Suppose a pair of users x and y want to communicate securely. Then they compute $(p_y)^{s_x} = g^{s_y s_x}$ and $(p_x)^{s_y} = g^{s_x s_y}$ respectively. We call $g^{s_y s_x} = g^{s_x s_y}$ their common secret key

s_{xy}. To communicate a message they use s_{xy} as key for a conventional single-key crypto system. The security of Diffie-Hellman's scheme is based on the discrete logarithm problem. This is the problem of finding x such that $y = g^x$ given y and g. No efficient algorithm to compute a logarithm in a finite field is known. Therefore in general when q is sufficiently large it is infeasible for a person different from i to compute s_i.

Let us describe how Diffie-Hellman's scheme can be transformed into a fair crypto system. The idea is that the secret keys of each user have to be shared among trustees (for example judges). If the trustees combine their shares of a secret key of a certain user (because of a court order) then this secret key can be revealed by the trustees (to the police). We now give a detailed description, see Figure 1.4 as well. Each user i randomly chooses non-zero elements $s_{i,j} \in GF(q)$, $1 \leq j \leq n$, and computes $p_{i,j} = g^{s_{i,j}}$, $1 \leq j \leq n$. The private key will be $s_i = \sum_j s_{i,j}$ and the public key will be $p_i = \prod_j p_{i,j} = g^{s_i}$. The $p_{i,j}$'s are called the public shares of p_i and the $s_{i,j}$'s are called the private shares of p_i. Let $t_{i,j}$, $1 \leq j \leq n$, be the trustees of user i. Then i gives securely $(p_i, p_{i,j}, s_{i,j})$ to trustee $t_{i,j}$. Trustee $t_{i,j}$ verifies the correctness of his private share by checking the relation $g^{s_{i,j}} = p_{i,j}$. If so, pair $(p_i, s_{i,j})$ is stored and pair $(p_i, p_{i,j})$ is given to a key management center (trusted by all trustees). The key management center receives the public shares $p_{i,j}$, $1 \leq j \leq n$, of p_i, and verifies whether $p_i = \prod_j p_{i,j}$. If so, p_i is approved as a public key of user i.

Why does it work? Suppose that a group T with less than n trustees $t_{i,j}$ combine their private and public shares. All private shares are randomly chosen by user i. So $\sum_{j \notin T} s_{i,j}$ can take on any value in $GF(q)$. Hence, to the members of T the secret key $s_i = \sum_{j \in T} s_{i,j} + \sum_{j \notin T} s_{i,j}$ can be any value in $GF(q)$. We conclude that pooling the private shares of the trustees in T gives no additional information about s_i. Further if the key management center has validated the public key p_i then the corresponding private key is reconstructible by the government in case of a court order (by adding the corresponding private shares of all the trustees). Thus the new scheme can not be misused by any criminal organization. Also the privacy of communication offered by the system is the same as in the Diffie-Hellman scheme. We conclude that the new scheme is fair. In [85] a deeper discussion on Micali's fair Diffie-Hellman's public key crypto system can be found (for example it is shown that a user can not cheat his trustees).

1.2 The Mathematical Concept

1.2.1 Access Structures

We have demonstrated the concept of secret sharing. We will now give a more formal description of secret sharing schemes. If we want to apply secret

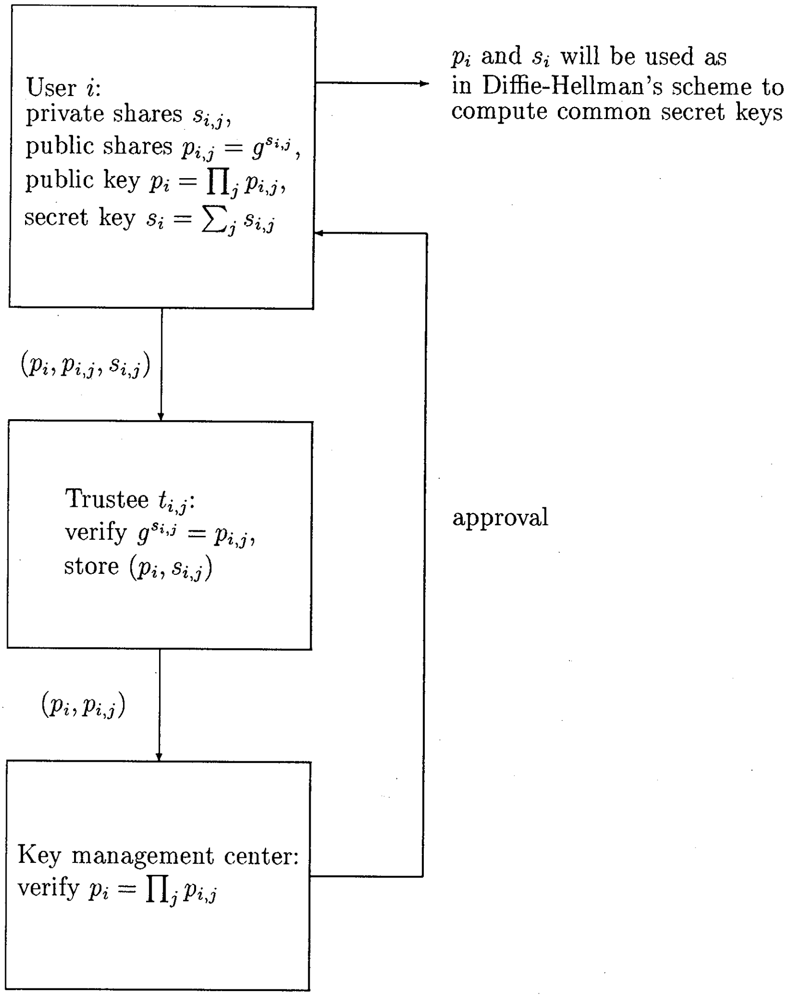

User i:
private shares $s_{i,j}$,
public shares $p_{i,j} = g^{s_{i,j}}$,
public key $p_i = \prod_j p_{i,j}$,
secret key $s_i = \sum_j s_{i,j}$
p_i and s_i will be used as in Diffie-Hellman's scheme to compute common secret keys
$(p_i, p_{i,j}, s_{i,j})$
Trustee $t_{i,j}$:
verify $g^{s_{i,j}} = p_{i,j}$,
store $(p_i, s_{i,j})$
approval
$(p_i, p_{i,j})$
Key management center:
verify $p_i = \prod_j p_{i,j}$

Figure 1.4: Micali's fair Diffie-Hellman's public key crypto system.

sharing schemes we first need to describe the set of participants in the scheme, those subsets of them who are *qualified* to reconstruct the secret, and those subsets of them who are *forbidden* to obtain additional knowledge about the secret by pooling their shares. Note that there can be groups of participants of which we do not mind whether they can obtain extra information about the secret by combining their shares. An *access structure* (or *concurrence scheme*) on the set of participants is a specification of those qualified and forbidden groups. The set of participants is denoted by $\mathcal{P}$, and an access structure on $\mathcal{P}$ is a pair (Γ, Δ), where Γ and Δ are collections of subsets of $\mathcal{P}$. Γ consists of all qualified groups and Δ consists of all forbidden groups. Let $2^{\mathcal{P}}$ denote the collection of subsets of $\mathcal{P}$. A subset Γ of $2^{\mathcal{P}}$ is called *monotone increasing* if with each set in Γ also each set containing it is in Γ (i.e., whenever $A \in \Gamma$ and $A \subseteq B \subseteq \mathcal{P}$ then $B \in \Gamma$). A subset Δ of $2^{\mathcal{P}}$ is called *monotone decreasing* if with each set in Δ also each subset is in Δ (i.e., whenever $A \in \Delta$ and $B \subseteq A$ then $B \in \Delta$). By $[\Gamma]^-$ we denote the collection of *minimal sets* of Γ and by $[\Delta]^+$ we denote the collection of *maximal sets* of Δ. We call (Γ, Δ) an *access structure* if Γ is monotone increasing, Δ is monotone decreasing and $\Gamma \cap \Delta = \emptyset$. This is a natural assumption: if a and b together are qualified to initiate an action, then a, b, and c should also be able to do so, and if the combination of a and b is forbidden to initiate an action, then a should also be forbidden. (We notice that non-monotone access structures have been considered in [11].) If $\Gamma = \emptyset$ then a secret sharing scheme meeting the requirements given by the access structure (Γ, Δ) can trivially be constructed. The secret will be kept secret and no one will receive a share. Further we notice that the secret would not be completely secret if $\emptyset \notin \Delta$. Therefore a *non-trivial* access structure (Γ, Δ) is an access structure for which $\Gamma \neq \emptyset$ and $\emptyset \in \Delta$. For the remainder of this thesis $\mathcal{P}$ is a set of participants and (Γ, Δ) is a non-trivial access structure on $\mathcal{P}$.

A *collusion* is defined to be any set of participants that does not include a qualified group. So the collusions in $\mathcal{P}$ are

$$\Gamma^c = \{A : A \notin \Gamma\}.$$

Γ^c is monotone decreasing; hence, $[\Gamma^c]^+$ denotes the collection of maximal collusions in $\mathcal{P}$. If $\Gamma \cup \Delta = 2^{\mathcal{P}}$ (that is $\Delta = \Gamma^c$), then we say that (Γ, Δ) is *complete* and we denote it by Γ. Otherwise we say that (Γ, Δ) is *incomplete.*

For an access structure (Γ, Δ), we define *core* Γ to be the set of participants which are in some minimal authorized set, that is

$$\text{core } \Gamma = \bigcup_{A \in [\Gamma]^-} A.$$

If core $\Gamma = \mathcal{P}$ then we say that (Γ, Δ) is *connected.* We may without loss of generality assume that access structures are connected (as will be explained by Lemma 1.2.7 in Section 1.2.4).

We call the person (or device) who selects and shares the secret the *dealer* or *mutually trusted authority* (*MTA*). The MTA chooses the secret, which we usually denote by s, according to a probability distribution $p(s)$. The set of possible secrets from which the secret has been selected is denoted by $\mathcal{S}$. It consists of all s with strict positive probability $p(s)$.

Example 1.2.1 In Example 1.1.2 the set of participants equals $\mathcal{P} = \{1, 2, 3, 4\}$, and, see Figure 1.3,

$$\begin{aligned} [\Gamma]^- &= \{\{1,2\},\{1,3\},\{2,3,4\}\}, \\ [\Delta]^+ &= \{\{1\},\{2,4\},\{3,4\}\}, \text{ and} \\ [\Gamma^c]^+ &= \{\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}. \end{aligned}$$

The access structure (Γ, Δ) is incomplete since $\Delta \neq \Gamma^c$. It is also connected. The set of possible secret is $\mathcal{S} = \mathbb{Z}_m^2$.

In Example 1.1.1 the mutually trusted authority is the computer and in Example 1.1.3 the MTA is the president of the bank. We leave as an exercise for the reader to determine $[\Gamma]^-$ and $[\Delta]^+$ in Examples 1.1.1 and 1.1.3. In both examples the access structure is complete and connected.

In Micali's fair Diffie-Hellman public key crypto system the concept of secret sharing is an underlying concept. Here each user i is the dealer for his own complete access structure Γ defined by

$$[\Gamma]^- = \{\{t_{i,j} : 1 \leq j \leq n\}\}.$$

The set of participants are all the trustees of user i (thus $[\Gamma]^- = \{\mathcal{P}\}$).

1.2.2 A Description of Secret Sharing Schemes by means of Probability Functions

As explained in Examples 1.1.1 and 1.1.2 we will describe secret sharing schemes by means of probability mass functions ν. We say that ν *describes a secret sharing scheme with set of participants* $\mathcal{P}$ if ν is a probability measure on some finite set $\mathcal{A} = \mathcal{A}_s \times \mathcal{A}_1 \times \mathcal{A}_2 \times \ldots \times \mathcal{A}_{|\mathcal{P}|}$ consisting of tuples of length $|\mathcal{P}| + 1$. Usually, alphabets $\mathcal{A}_i$, $i \in \{s\} \cup \mathcal{P}$, are equal to integer rings (see Examples 1.1.1 and 1.1.2). Before we explain how ν describes a secret sharing scheme we introduce some notation.

Let without loss of generality $\mathcal{P} = \{1, \ldots, n\}$. We index the entries of tuples of length $|\mathcal{P}| + 1$ as follows. We index the first entry by s, the second entry by the first participant 1, the third entry by the second participant 2, and so on. Let $\chi = (\chi_s, \chi_1, \ldots, \chi_n) \in \mathcal{A}$ be a tuple of length $n + 1$. Let $A \subseteq \{s\} \cup \mathcal{P}$. Then *the restriction of* χ *to* A is denoted by χ_A, so

$$\chi_A = (\chi_x)_{x \in A}.$$

The restriction of $\mathcal{A}$ to A is denoted by $\mathcal{A}_A$, so $\mathcal{A}_A = \times_{i \in A} \mathcal{A}_i$. Thus $\chi_A \in \mathcal{A}_A$.

The measure ν induces a probability mass function ν_A on $\alpha \in \mathcal{A}_A$ by the rule

$$\nu_A(\alpha) = \sum_{\{\chi : \chi_A = \alpha\}} \nu(\chi).$$

The set of tuples α of length $|A|$ for which ν_A evaluated in α is strictly positive is denoted by

$$[A]_\nu = \{\alpha : \nu_A(\alpha) > 0\}.$$

For example *the set of possible secrets* is $[s]_\nu$. So far we considered tuples of which the entries are indexed by $\{s\} \cup \mathcal{P}$. Of course we can define restrictions of any tuple in a similar manner. Thus for $B \subseteq A$ and $\chi \in [A]_\nu$ we have that $\chi_B = (\chi_x)_{x \in B}$.

To simplify the notation we will write in the remainder of this thesis AB for $A \cup B$ and a for $\{a\}$. For example we write $s\mathcal{P}$ for $\{s\} \cup \mathcal{P}$. For $A, B \subseteq s\mathcal{P}$ and $\alpha \in [A]_\nu$ and $\beta \in [B]_\nu$ with $\alpha_{A \cap B} = \beta_{A \cap B}$ we write $\nu_{AB}(\alpha\beta)$ to mean $\nu_{AB}(\gamma)$, where $\gamma \in [AB]_\nu$ with $\gamma_A = \alpha$ and $\gamma_B = \beta$. For $A, B \subseteq s\mathcal{P}$ and $\alpha \in [A]_\nu$ and $\beta \in [B]_\nu$ we define the *conditional* probability $\nu_{A|B}(\alpha|\beta)$ by

$$\nu_{A|B}(\alpha|\beta) = \begin{cases} 0, & \text{if } \alpha_{A \cap B} \neq \beta_{A \cap B} \\ \nu_{AB}(\alpha\beta)/\nu_B(\beta), & \text{if } \alpha_{A \cap B} = \beta_{A \cap B}. \end{cases}$$

Suppose that $\chi \in [s\mathcal{P}]_\nu$ has been selected according to the probability mass function ν. Then $\nu_{A|B}(\alpha|\beta)$ is the probability that $\chi_A = \alpha$ given the knowledge (condition) that $\chi_B = \beta$.

Figure 1.5 depicts how ν describes a secret sharing scheme with set of participants $\mathcal{P}$. The MTA selects $\chi \in [s\mathcal{P}]_\nu$ with probability $\nu(\chi)$. The secret will be χ_s and the share of participant i will be χ_i.

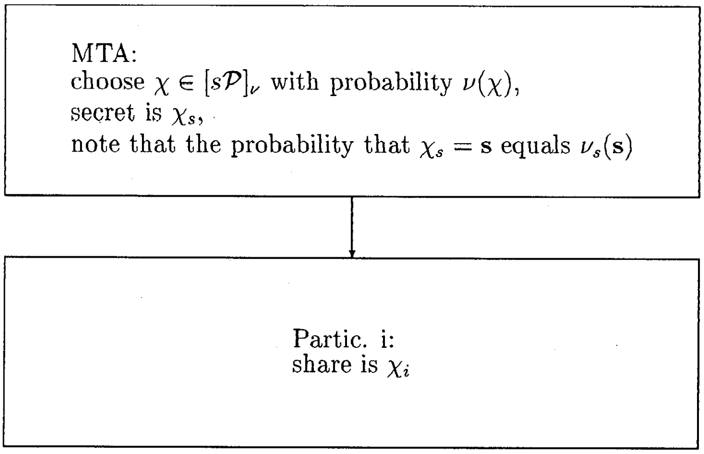
1.2.3 An Information Theoretic Definition of Secret Sharing Schemes

The most precise definition of a secret sharing scheme is in terms of information theory and was first introduced by Capocelli et al. in [30]. We provide the basic definitions in information theory here and refer the reader to, for example, Gallager [54] or Cover [34].

Let X and Y be (dependent) random variables with probability measures p_X and p_Y respectively. We define $p \log_2 p$ evaluated in $p = 0$ to be equal to 0. Then the *entropy* $H(X)$ is defined to be

$$H(X) = -\sum_x p_X(x) \log_2 p_X(x)$$

$(= -E(\log_2 p_X(X))$, where E denotes the expectation). $H(X)$ is also called *the uncertainty about* X. Its interpretation is as follows. $H(X)$ measures the



MTA:
choose $\chi \in [s\mathcal{P}]_\nu$ with probability $\nu(\chi)$,
secret is χ_s,
note that the probability that $\chi_s = \mathbf{s}$ equals $\nu_s(\mathbf{s})$

Partic. i:
share is χ_i

Figure 1.5: A secret sharing scheme described by a probability measure ν.

average amount of bits needed to describe a realization of random variable X. In other words $H(X)$ measures the amount of information contained in X.

The *conditional entropy* $H(X|Y = y)$ is defined by

$$H(X|Y = y) = -\sum_x p_{X|Y}(x|y) \log_2 p_{X|Y}(x|y)$$

$(= -E(\log_2 p_{X|Y}(X|y)))$. The *conditional entropy* $H(X|Y)$ is now defined by

$$H(X|Y) = \sum_y p_Y(y) H(X|Y = y)$$

$(= -E(\log_2 p_{X|Y}(X|Y)))$. It measures the average amount of bits needed to describe X given the knowledge of Y.

Equations and inequalities with natural interpretations can be derived now. For example

$$H(XY) = H(X) + H(Y|X),$$

i.e, the information needed to describe both X and Y equals the information needed to describe X together with the information needed to describe Y given the knowledge (information) of X. Another example is the following inequality:

$$0 \leq H(X|Y) \leq H(X) \leq \log_2 |\{x : p_X(x) > 0\}|,$$

where $|\{x : p_X(x) > 0\}|$ is the cardinality of $\{x : p_X(x) > 0\}$.

Example 1.2.2 Let us consider a particular case of the secret sharing scheme in Example 1.1.1 (see Figure 1.2). Let

$$\mathcal{X} = \{(0,0,0,0),(0,1,1,1),(1,0,1,0),(1,1,0,1)\}$$

and let $p_X(x) = 1/4$ for $x \in \mathcal{X}$ (see (1.2): $\nu = p_X$ and $[sP]_\nu = \mathcal{X}$). Then $H(X) = 2$. Only 2 bits are needed to describe X. For example the first two entries represent uniquely each tuple from $\mathcal{X}$. Let $i, j \in \{0,1\}$. The probability that the first entry (the secret) equals i given that the third entry (the share of the second participant) equals j is $1/2$ and is the same as the probability that the first entry (the secret) equals i. Hence, the uncertainty about the first entry equals the uncertainty (conditional entropy) about the first entry given the third entry. The interpretation is that the third entry (the share of the second participant) gives no information about the first entry (the secret).

The *mutual information* between X and Y is defined as $I(X;Y) = H(X) - H(X|Y)$. Let Z be another random variable. The *conditional mutual information* between X and Y given Z is defined as $I(X;Y|Z) = H(X|Z) - H(X|YZ)$. These notions will be used in the next chapter. The mutual information between X and Y measures the amount of information X and Y have in common (it is easy to see that $I(X;Y) = I(Y;X)$).

We will now give a formal definition of secret sharing schemes by means of the entropy function. Firstly, to be able to use the entropy function we define for $A \subseteq s\mathcal{P}$

$$A_\nu$$

as a random variable with probability measure ν_A. Hence, the amount of information needed to describe the share of participant i is equal to $H(i_\nu)$. The amount of information needed to describe the secret is $H(s_\nu)$. Let $A \subseteq \mathcal{P}$. Then the amount of information needed to describe the secret given the knowledge of all the shares of members of A equals $H(s_\nu|A_\nu)$.

A *secret sharing scheme* (or *scheme* for short) *for* (Γ, Δ) *on participant set* $\mathcal{P}$ is a probability measure ν, which describes a secret sharing scheme with set of participants $\mathcal{P}$, such that, for $A \subseteq \mathcal{P}$,

[SS1] if $A \in \Gamma$ then $H(s_\nu|A_\nu) = 0$;

[SS2] if $A \in \Delta$ then $H(s_\nu|A_\nu) = H(s_\nu)$.

In general, where there is no ambiguity we will omit the subscript ν. Note that the security offered by this model is *unconditional*. This means that it is independent of the amount of computing time and resources that are available when attempting to obtain information about the secret by some unauthorized means. (In Example 1.1.3 Micali's fair public key crypto system is not unconditionally secure since Diffie Hellman's public key crypto system is not unconditionally secure.) Sometimes one needs schemes ν in which the distribution of the secret ν_s equals a certain fixed probability distribution p, as in Examples 1.1.1 and 1.1.2. Usually one requires ν_s to be uniformly distributed over some finite set.

Example 1.2.3 Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, 2, 3, 4\}$ defined by $[\Gamma]^- = \{123, 124, 134, 234\}$ and $[\Delta]^+ = \{1, 2, 3, 4\}$. Then the uniform distribution over the collection of the following tuples:

$$\begin{array}{ccccc}
s & 1 & 2 & 3 & 4 \\
(0 & 0 & 0 & 0 & 0) \\
(1 & 0 & 0 & 1 & 1) \\
(0 & 1 & 1 & 1 & 1) \\
(1 & 1 & 1 & 0 & 0) \\
(2 & 1 & 0 & 1 & 0) \\
(3 & 1 & 0 & 0 & 1) \\
(2 & 0 & 1 & 0 & 1) \\
(3 & 0 & 1 & 1 & 0)
\end{array}$$

is a secret sharing scheme ν for (Γ, Δ) on $\mathcal{P}$. It is easy to see that each triple of participants can recover the secret and that each single participant does not have any information about the secret. These observations should correspond to the definition of secret sharing schemes. For example let us show that $H(s_\nu|(123)_\nu) = 0$. By definition $\nu_{s|123}(\alpha|\beta) = \nu_{s123}(\alpha\beta)/\nu_{123}(\beta)$. From the list of tuples we obtain that $\nu_{s123}(\alpha\beta)$ equals $\nu_{123}(\beta)$ for $\alpha \in [s]_\nu$. Hence, $\nu_{s|123}(\alpha|\beta)$ is either 0 or 1. Thus $H(s_\nu|(123)_\nu = \beta) = 0$, and therefore $H(s_\nu|(123)_\nu) = 0$.

Note that in a secret sharing scheme for (Γ, Δ), if a set $A \notin \Gamma \cup \Delta$ then [SS1] and [SS2] do not specify a relationship between $H(s|A)$ and $H(s)$. All we can say is that $0 \leq H(s|A) \leq H(s)$. We say that a scheme *has* access structure (Γ', Δ') if $\Gamma' = \{A \,|\, A \subseteq \mathcal{P}, H(s|A) = 0\}$ and $\Delta' = \{A \,|\, A \subseteq \mathcal{P}, H(s|A) = H(s)\}$. Thus a scheme for (Γ, Δ) has access structure (Γ', Δ') for some Γ' containing Γ and Δ' containing Δ. Notice that $\emptyset \in \Delta'$. So, w.l.o.g. $\emptyset \in \Delta$ (see the definition of non-trivial access structures). Further if a scheme has access structure (Γ', Δ') then for any $A \notin \Gamma' \cup \Delta'$ it follows that $0 < H(s|A) < H(s)$.

We use the so-called entropy model for secret sharing schemes. Other frequently used models are the Brickell-Davenport model [26] and Brickell-Stinson model [27]. In [58] a detailed comparison of several existing models for secret sharing schemes is given. The following lemma is easily established (for a proof, see for example [58]) and describes a more combinatorial approach.

Lemma 1.2.4 *Let* (Γ, Δ) *be an access structure on* $\mathcal{P}$ *and suppose that* ν *describes a secret sharing scheme. Then* ν *is a scheme for* (Γ, Δ) *if and only if the following two conditions hold.*

[SS1] For all $A \in \Gamma$ *and* $\alpha \in [A]_\nu$ *there is exactly one* $\sigma \in [s]_\nu$ *such that* $\nu_{sA}(\sigma\alpha) \neq 0$, *and*

[SS2] For all $B \in \Delta$, $\alpha \in [B]_\nu$ *and* $\sigma \in [s]_\nu$, *we have* $\nu_{sB}(\sigma\alpha) = \nu_s(\sigma)\nu_B(\alpha)$.

1.2.4 Information Rates

In a practical implementation of a secret sharing scheme, it is important to keep the size of the shares as small as possible. This is for reasons of efficiency and security. Thus we are interested in measures for the amount of information that must be given to the participants. We can use the *worst-case information rate*, which is the ratio between the size of the secret and the maximum size of the shares [27] or we can use the *average information rate*, which is the ratio between the size of the secret and the arithmetic mean of the size of all shares [15, 76, 77]. The next definitions concern these measures.

Let ν be a scheme for (Γ, Δ). We define the *size* of the secret by $H(s_\nu)$, which is the expected number of bits needed to store the secret. Similarly, the size of i's share is defined by $H(i_\nu)$. A different definition of the size of the secret is $\log_2 |[s]_\nu|$, which is the maximal number of bits needed to store the secret. Similarly, the size of i's share can be defined as $\log_2 |[i]_\nu|$. In the literature usually only schemes ν for which the secret is uniformly distributed are considered. For such schemes the shares are usually uniformly distributed as well. Hence, $H(s_\nu) = \log_2 |[s]_\nu|$ and $H(i_\nu) = \log_2 |[i]_\nu|$. Then both approaches to define the size are equivalent. In the literature the cardinality definition of size is often used (simply because the entropy model for secret sharing was not discovered yet). We prefer the entropy definition of size.

We define the *individual information rate* or the *contribution* of participant i in scheme ν as

$$c_i(\nu) = H(i_\nu)/H(s_\nu).$$

It is the ratio between the size of i's share and the size of the secret. As explained before we like c_i as small as possible. The vector with all contributions as entries is called the *contribution vector* (or *convec*) $c(\nu)$ of scheme ν [60], that is

$$c(\nu) = (c_i(\nu))_{i \in \mathcal{P}}.$$

Let

$$w = \max_{i \in \mathcal{P}} c_i(\nu)$$

be the maximal (worst) contribution and let

$$a = \frac{1}{|\mathcal{P}|} \sum_{i \in \mathcal{P}} c_i(\nu)$$

be the average contribution. We define the *worst-case information rate* $\dot{\rho}(\nu)$ and *average information rate* $\tilde{\rho}(\nu)$ for ν by $\dot{\rho}(\nu) = 1/w$ and $\tilde{\rho}(\nu) = 1/a$. So we like $\tilde{\rho}$ and $\dot{\rho}$ to be as high as possible.

Example 1.2.5 Let p be the uniform distribution in the scheme of Example 1.1.2. Then its convec is

$$c(\nu) = (3/2, 1, 1, 1/2).$$

Hence, $\dot{\rho}(\nu) = 2/3$ and $\tilde{\rho}(\nu) = 1$.

Example 1.2.6 A well known class of schemes are *ramp schemes.* They are defined as follows. Let $\mathcal{P} = \{1, \dots, n\}$ and let $0 \leq \omega < \lambda \leq n$. Let Γ consist of all the subsets of $\mathcal{P}$ of size at least λ and let Δ consist of all the subsets of $\mathcal{P}$ of size at most ω. A scheme for (Γ, Δ) is called a (ω, λ, n)-*ramp scheme* (see Example 1.2.3, where a (1,3,4)-ramp scheme is presented). The special case of $(\lambda - 1, \lambda, n)$-ramp schemes are called (λ, n)-*threshold schemes.* Threshold schemes were the first to be investigated in the literature.

We now give an example of a (ω, λ, n)-ramp scheme. Let $q \geq n + 1$ be a prime power. Suppose a MTA wants to share $\mathbf{s} = (s_1, \dots, s_{\lambda-\omega}) \in GF(q)^{\lambda-\omega}$ with uniform distribution among all participants. Then he first selects nonzero distinct elements $\alpha_1, \dots, \alpha_n \in GF(q)$. He stores these elements such that they are publicly available and are therefore known to all participants. Secondly, he selects securely random variables $a_1, \dots, a_\omega \in GF(q)$, and he securely transmits to i share

$$p_i = \sum_{1 \leq j \leq \omega} a_j \alpha_i^{j-1} + \sum_{1 \leq j \leq \lambda-\omega} s_j \alpha_i^{\omega+j-1}.$$

A group of λ members $i_1, \dots, i_\lambda$ can construct

$$G = \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_{i_1} & \cdots & \alpha_{i_\lambda} \\ \vdots & \ddots & \vdots \\ \alpha_{i_1}^{\lambda-1} & \cdots & \alpha_{i_\lambda}^{\lambda-1} \end{pmatrix}$$

and its inverse. Hence, they can compute

$$(p_1, \dots, p_\lambda) G^{-1} = (a_1, \dots, a_\omega, s_1, \dots, s_{\lambda-\omega}),$$

which reveals $\mathbf{s}$. Thus [SS1] is satisfied.

The shares of a group of ω members $i_1, \dots, i_\omega$ is given by the entries of the vector

$$(a_1, \dots, a_\omega) \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_{i_1} & \cdots & \alpha_{i_\omega} \\ \vdots & \ddots & \vdots \\ \alpha_{i_1}^{\omega-1} & \cdots & \alpha_{i_\omega}^{\omega-1} \end{pmatrix} + \mathbf{s} \begin{pmatrix} \alpha_{i_1}^{\omega} & \cdots & \alpha_{i_\omega}^{\omega} \\ \alpha_{i_1}^{\omega+1} & \cdots & \alpha_{i_\omega}^{\omega+1} \\ \vdots & \ddots & \vdots \\ \alpha_{i_1}^{\lambda-1} & \cdots & \alpha_{i_\omega}^{\lambda-1} \end{pmatrix}.$$

The knowledge about s contained in this vector equals the knowledge about s contained in the vector

$$(a_1,\ldots,a_\omega)+\mathrm{s}\begin{pmatrix}\alpha_{i_1}^{\omega} & \cdots & \alpha_{i_\omega}^{\omega}\\ \alpha_{i_1}^{\omega+1} & \cdots & \alpha_{i_\omega}^{\omega+1}\\ \vdots & \ddots & \vdots\\ \alpha_{i_1}^{\lambda-1} & \cdots & \alpha_{i_\omega}^{\lambda-1}\end{pmatrix}\begin{pmatrix}1 & \cdots & 1\\ \alpha_{i_1} & \cdots & \alpha_{i_\omega}\\ \vdots & \ddots & \vdots\\ \alpha_{i_1}^{\omega-1} & \cdots & \alpha_{i_\omega}^{\omega-1}\end{pmatrix}^{-1}.$$

Since $a_1,\ldots,a_\omega,\mathrm{s}$ are statistically independent, and $a_1,\ldots,a_\omega$ are uniformly chosen random variables a group of ω members can not obtain any information about s. So, [SS2] is satisfied. We conclude that we have described a (ω,λ,n)-ramp scheme.

The contribution of i is

$$1/(\lambda-\omega).$$

The worst-case information rate and average information rate are both equal to

$$\lambda-\omega.$$

We will show that our scheme is the best in terms of its worst case information rate. Let ν be any (ω,λ,n)-ramp scheme. Let $i_1,\ldots,i_{\lambda-\omega},j_1,\ldots,j_\omega$ be distinct participants. Then

$$\begin{aligned}\sum_{1\leq k\leq\lambda-\omega} H(i_j) &\geq H(i_1\ldots i_{\lambda-\omega})\\ &\geq H(i_1\ldots i_{\lambda-\omega}|j_1\ldots j_\omega)\\ &\geq H(i_1\ldots i_{\lambda-\omega}|j_1\ldots j_\omega)-H(i_1\ldots i_{\lambda-\omega}|j_1\ldots j_\omega s)\\ &= I(i_1\ldots i_{\lambda-\omega};s|j_1\ldots j_\omega)\\ &= H(s|j_1\ldots j_\omega)-H(s|i_1\ldots i_{\lambda-\omega}j_1\ldots j_\omega)\\ &= H(s)-0,\end{aligned}$$

since $j_1\ldots j_\omega\in\Delta$ and $i_1\ldots i_{\lambda-\omega}j_1\ldots j_\omega\in\Gamma$. Hence, there is a contribution which is at least $1/(\lambda-\omega)$. Thus for any (ω,λ,n)-ramp scheme ν

$$\dot{\rho}(\nu)\leq\lambda-\omega.$$

We conclude that our scheme has an optimal worst-case information rate! (The derivation can be used to prove that our scheme has also optimal average information rate. We leave it to the reader to check this.)

The *optimal worst-case information rate* of (Γ,Δ) is defined as

$$\dot{\rho}(\Gamma,\Delta)=\sup\left\{\dot{\rho}(\nu):\nu\text{ is a scheme for }(\Gamma,\Delta)\right\}.$$

The *optimal average information rate* of (Γ,Δ) is defined as

$$\tilde{\rho}(\Gamma,\Delta)=\sup\left\{\tilde{\rho}(\nu):\nu\text{ is a scheme for }(\Gamma,\Delta)\right\}.$$

These optimal rates equal the best rates a scheme for (Γ, Δ) can possibly achieve. For complete access structures Γ we write $\dot{\rho}(\Gamma)$ and $\tilde{\rho}(\Gamma)$ respectively. An interesting research problem is to construct *optimal* schemes, these are schemes attaining the optimal (worst-case or average) information rate.

In [22] the *randomness coefficient* $\mu(\nu) = H(\mathcal{P}_\nu|s_\nu)/H(s_\nu)$ for schemes ν is defined. The average amount of bits needed to describe the combination of all shares given the knowledge of the secret is $H(\mathcal{P}_\nu|s_\nu)$. Thus $H(\mathcal{P}_\nu|s_\nu)$ represents the number of random bits needed by the MTA to share a secret. Hence, the randomness coefficient measures the amount of randomness required by the MTA. For a further discussion see [22].

We make an observation about a unusual type of participants; participants that do not belong to the core of an access structure. We will show that the participants not in the core never have to use their share. So, their individual information rates are w.l.o.g. equal to 0.

Lemma 1.2.7 *Let ν be a scheme for an access structure* (Γ, Δ) *on $\mathcal{P}$. Then there exists a scheme τ for* (Γ, Δ) *on $\mathcal{P}$ such that $H(s_\tau) = H(s_\nu)$, $H(i_\tau) = H(i_\nu)$ for i in* core Γ, *and $H(i_\tau) = 0$ for i not in* core Γ. *(Thus $c_i(\tau) = c_i(\nu)$ if $i \in$* core Γ, *and $c_i(\tau) = 0$ for i not in* core Γ.

Proof: Suppose ν is a scheme for (Γ, Δ) and $i \in \mathcal{P}$ is not in core Γ. Then no minimal authorized set contains i. Scheme τ defined by $\tau_{\mathcal{P}\backslash i} = \nu_{\mathcal{P}\backslash i}$ and $|[i]_\tau| = 1$ is also a scheme for (Γ, Δ) by the following argument. By the definition of τ we have that $H(i_\tau) = 0$ and $\tau_{sA}(\pi) = \tau_{sA\backslash i}(\pi_{sA\backslash i}) = \nu_{sA\backslash i}(\pi_{sA\backslash i})$ for $\pi \in [sA]_\tau$. Hence, $H(s_\tau|A_\tau) = H(s_\tau|(A\backslash i)_\tau) = H(s_\nu|(A\backslash i)_\nu)$, in particular $H(s_\tau) = H(s_\nu)$.

To check [SS1] consider $A \in \Gamma$. Then $A \setminus i \in \Gamma$, since i not in core Γ, and hence $H(s_\tau|A_\tau) = H(s_\nu|(A \setminus i)_\nu) = 0$. To check [SS2] consider $A \in \Delta$. Then $A \setminus i \in \Delta$ and hence $H(s_\tau|A_\tau) = H(s_\nu|(A \setminus i)_\nu) = H(s_\nu) = H(s_\tau)$.

We conclude that τ is a scheme for (Γ, Δ) such that $H(s_\tau) = H(s_\nu)$, $H(i_\tau) = 0$, and $H(j_\tau) = H(j_\nu)$ for participants $j \neq i$.

□

1.2.5 Perfect Schemes

The most studied class of secret sharing schemes are *perfect* schemes. These are schemes for complete access structures; a group is either qualified or forbidden. In applications of secret sharing usually perfect schemes are needed (see the examples considered so far). Perfect secret sharing schemes have been well studied since the inaugural papers by Shamir [93] and Blakley [12]. For a good introduction to this area see the survey paper [97]. For an extended introduction see Simmons [95, Chapter 9]. In this thesis we will concentrate on perfect secret sharing schemes.

It can be easily shown (for example see Corollary 2.1.3) that for any scheme for a complete access structure Γ and any i in core Γ we have $H(i) \geq$

$H(s)$. Thus for any perfect scheme ν for a complete connected access structure Γ we have $0 \leq \dot{\rho}(\nu) \leq \tilde{\rho}(\nu) \leq 1$. Hence, for complete connected access structures Γ we have that $0 \leq \dot{\rho}(\Gamma) \leq \tilde{\rho}(\Gamma) \leq 1$. These bounds lead in a natural way to the definition of *ideal schemes* and *ideal access structures.* Ideal schemes are defined as perfect schemes ν for which $\dot{\rho}(\nu) = 1$. Ideal access structures are defined as complete, connected access structures for which the optimal worst-case information rate is $\dot{\rho}(\Gamma) = 1$. An open problem is to characterize ideal access structures. The difference when considering incomplete access structures (Γ, Δ) is that it is possible to have $H(i) < H(s)$ and hence $\dot{\rho}(\nu)$ and $\tilde{\rho}(\nu)$ are no longer bounded above by 1.

We notice that it is beneficial to consider incomplete access structures for the following reasons. Firstly, incomplete access structures have a less restrictive definition than complete access structures and so it may be easier to find secret sharing schemes for an incomplete access structure. Secondly, the information rates are no longer bounded above by 1. Thirdly, in Chapter 5 we will present a construction of perfect secret sharing schemes by using schemes for incomplete access structures. This is an indirect application of schemes for incomplete access structures. A well known class of incomplete schemes are ramp schemes (see Example 1.2.6). Ramp schemes were the first class of incomplete access structures to be investigated. For more information see [14, 29, 59]. In [63] an algorithm for constructing schemes with incomplete access structures is proposed. More general incomplete access structures were considered in [72, 87, 86]. In particular they considered schemes for special classes of incomplete access structures where groups outside Γ and Δ may only have a limited amount of information about the secret (for instance $H(s|A) \leq H(s)/2$ for $A \notin \Gamma \cup \Delta$) An example of schemes with this type of restriction on their access structures are *linear* ramp schemes, see [29, 59].

In the following sections we discuss particular types of access structures and schemes.

1.3 Access Structures and their Duals

Let (Γ, Δ) be an access structure on $\mathcal{P}$. For $X \subseteq \mathcal{P}$ we define its *complement* as $X^c = \mathcal{P} \setminus X$. The *dual* $(\Gamma^\perp, \Delta^\perp)$ of (Γ, Δ) is defined by

$$\{X : X^c \in \Delta\} = \Gamma^\perp,$$
$$\{X : X^c \in \Gamma\} = \Delta^\perp$$

(see [96]). For example the access structure (Γ, Δ) given by Figure 1.3 is *self-dual,* that is $\Gamma^\perp = \Gamma$ and $\Delta^\perp = \Delta$. The dual of a complete access structure Γ is $\Gamma^\perp = \{X : X^c \in \Gamma^c\}$.

Example 1.3.1 Let $\mathcal{P} = \{1, \ldots, n\}$, and let λ be some integer less than n. Let $\Gamma_\lambda = \{X \subseteq \mathcal{P} : |X| \geq \lambda + 1\}$. Then $(\Gamma_\lambda)^c = \{X : |X| < \lambda + 1\} = \{X :$

$|X^c| \geq n - \lambda\} = \{X^c : |X| \geq n - \lambda\}$. Hence the dual of the complete access structure Γ_λ is $(\Gamma_\lambda)^\perp = \{X : X^c \in \Gamma_\lambda^c\} = \Gamma_{n-\lambda-1}$. Note that Γ_λ is self-dual in the case that $n = 2\lambda + 1$.

Let $x \in \mathcal{P}$. Let $\Gamma = \{X \subseteq \mathcal{P} : x \in X\}$. Then $\Gamma^c = \{X : x \notin X\} = \{X : x \in X^c\} = \{X^c : x \in X\}$. Hence Γ is self-dual.

The following properties concern the structure of $(\Gamma^\perp, \Delta^\perp)$ (see [96, Lemma 3] as well). These properties will give a better understanding about the relation between access structures and their duals. The first property states that the dual of an access structure is an access structure as well. The other properties will be used in Chapter 3 to prove a relation between certain schemes for access structures and schemes for their duals.

Lemma 1.3.2 [1] *Let* (Γ, Δ) *be an access structure. Then*

(i) $(\Gamma^\perp, \Delta^\perp)$ *is an access structure.*

(ii) $[\Gamma^\perp]^- = \{X : X^c \in [\Delta]^+\}$,
$[\Delta^\perp]^+ = \{X : X^c \in [\Gamma]^-\}$.

(iii) $\Gamma^{\perp\perp} = \Gamma$,
$\Delta^{\perp\perp} = \Delta$.

(iv) $\Gamma^\perp = \{X : \forall_{Y \in [\Delta^c]^-}\ X \cap Y \neq \emptyset\}$,
$\Delta^\perp = \{X : \forall_{Y \in [\Gamma^c]^+}\ X \cap Y \neq \emptyset\}$.

(v) $[\Gamma^\perp]^- = \{X : \forall_{x \in X}\ \exists_{Y \in [\Delta^c]^-}\ X \cap Y = \{x\}$ *and* $\forall_{Y \in [\Delta^c]^-}\ X \cap Y \neq \emptyset\}$,
$[\Delta^\perp]^+ = \{X : \forall_{x \in X}\ \exists_{Y \in [\Gamma^c]^+}\ X \cap Y = \{x\}$ *and* $\forall_{Y \in [\Gamma^c]^+}\ X \cap Y \neq \emptyset\}$.

Proof: (i) Trivially $\Gamma^\perp \cap \Delta^\perp = \emptyset$. So it remains to check the monotonicity of $\Gamma^\perp$ and $\Delta^\perp$. If $X \in \Gamma^\perp$ and $X \subseteq Y$ then $Y^c \subseteq X^c \in \Delta$. Hence, $Y^c \in \Delta$ by the monotonicity of Δ, i.e. $Y \in \Gamma^\perp$. Similarly if $X \in \Delta^\perp$ and $Y \subseteq X$ then $Y \in \Delta^\perp$.

(ii) To prove the first statement we first show that any $Y \in \Gamma^\perp$ contains a set from $\{X : X^c \in [\Delta]^+\}$ and next that $\{X : X^c \in [\Delta]^+\} \subseteq [\Gamma^\perp]^-$. Let $Y \in \Gamma^\perp$. By definition $Y^c \in \Delta$ and hence there exists a set $X^c \in [\Delta]^+$ such that $Y^c \subseteq X^c$, or equivalently $X \subseteq Y$. Hence, Y contains an element from $\{X : X^c \in [\Delta]^+\}$.

Let $X^c \in [\Delta]^+$. Then $X \in \Gamma^\perp$ since $X^c \in \Delta$. Let $Y \subseteq X$ with $Y \in [\Gamma^\perp]^-$. By the first part of the proof there exists a X' with $X' \subseteq Y$ and $X'^c \in [\Delta]^+$. Notice that $X' \subseteq Y \subseteq X$ and that both X and X' are maximal elements of Δ. Therefore X, X', and Y are equal. So, $X \in [\Gamma^\perp]^-$.

In a similar way $[\Delta^\perp]^+ = \{X : X^c \in [\Gamma]^-\}$ can be proved.

[1] In [77] the definitions of addition (+), multiplication (·), and substitution (←) for complete access structures can be found. Let Γ and Γ' be access structures. Without proof we mention the following relations $(\Gamma + \Gamma')^\perp = \Gamma^\perp \cdot \Gamma'^\perp$, and $(\Gamma(z \leftarrow \Gamma'))^\perp = \Gamma^\perp(z \leftarrow \Gamma'^\perp)$.

(iii) The third property follows immediately.

(iv) We observe the equivalence of the following statements $X \in \Gamma^\perp$, $X^c \in \Delta$, $X^c \notin \Delta^c$, $\forall_{Y\in[\Delta^c]^-}\ Y \not\subseteq X^c$ (use the monotonicity of Δ^c), and $\forall_{Y\in[\Delta^c]^-}\ X \cap Y \neq \emptyset$. In a similar way the second part of the fourth property can be proved.

(v) We will prove the first statement. The second statement can be dealt with in a similar way and is left to the reader. Let $X \in \Gamma^\perp$ such that

$$X \notin \Phi := \{X : \forall_{x\in X}\ \exists_{Y\in[\Delta^c]^-}\ X \cap Y = \{x\} \text{ and } \forall_{Y\in[\Delta^c]^-}\ X \cap Y \neq \emptyset\}.$$

These requirements together with (iv) imply that there exists an $x \in X$ such that $X \cap Y \neq \{x\}$ and $X \cap Y \neq \emptyset$ for all $Y \in [\Delta^c]^-$. Thus $(X \setminus \{x\}) \cap Y \neq \emptyset$ for all $Y \in [\Delta^c]^-$. So, $X \setminus \{x\} \in \Gamma^\perp$ by (iv). Hence, $X \notin [\Gamma^\perp]^-$ and we conclude that $[\Gamma^\perp]^- \subseteq \Phi$.

Let $X \in \Phi$. Then, by (iv), $X \in \Gamma^\perp$ such that for all $x \in X$ the intersection $X \cap Y$ equals $\{x\}$ for some $Y \in [\Gamma]^-$. Thus $X \setminus \{x\} \notin \Gamma^\perp$ for all $x \in X$. This proves that $X \in [\Gamma^\perp]^-$. We have shown $\Phi \subseteq [\Gamma^\perp]^-$, and hence $\Phi = [\Gamma^\perp]^-$.

□

Example 1.3.3 Let $\mathcal{P} = \{1,2,3,4,5\}$. Let the access structure Γ be defined by $[\Gamma]^- = \{\{1,2\},\{2,3\},\{3,4\},\{2,5\},\{3,5\}\}$. Then $[\Gamma^c]^+ = \{\{1,3\}, \{2,4\}, \{1,4,5\}\}$. Hence, by applying Lemma 1.3.2(ii), $[\Gamma^\perp]^- = \{\{2,4,5\}, \{1,3,5\}, \{2,3\}\}$.

1.4 Access Structures Based on Graphs

In this section we consider perfect schemes for access structures defined by the edges of a graph. Given a graph G with the participants as its vertices, the access structure $\Gamma(G)$ based on G consists of all subsets containing an edge of G. The optimal worst-case resp. average information rate of an access structure based on graph G is denoted by $\hat{\rho}(G)$ resp. $\tilde{\rho}(G)$. For a graph G we denote its vertex set by $V(G)$ and its edge set by $E(G)$. We notice that $[\Gamma(G)]^- = E(G)$. In Chapter 4 we will study the optimal worst-case information rate of all connected graphs on six vertices.

In this section we will recall some results from the literature. G' is called a *subgraph* of G if $V(G') \subseteq V(G)$ and $E(G') \subseteq E(G)$. G' is called an *induced subgraph* of G if in addition for all $\{i,j\} \subseteq V(G')$ one has $\{i,j\} \in E(G')$ if and only if $\{i,j\} \in E(G)$.

Lemma 1.4.1 *[21] Suppose G is a graph and G' is an induced subgraph of G. Then $\hat{\rho}(G) \leq \hat{\rho}(G')$.*

The following theorem, by Brickell and Davenport [26], characterizes ideal schemes on connected graphs. Let G be a connected graph with vertex set

V. Suppose that V can be partitioned into subsets $V_1, \ldots, V_k$ such that the edges in G are defined by all pairs of vertices from different subsets. Then G is called a *complete multipartite graph.*

Theorem 1.4.2 *Suppose that G is a connected graph. Then $\dot{\rho}(G) = 1$ iff G is a complete multipartite graph.*

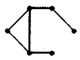
Example 1.4.3 Let G be a complete multipartite graph and let the subsets $V_1, \ldots, V_k$ be a partitioning of its vertex set such that the edges in G are defined by all pairs of vertices from different subsets. Let $q \geq k$ be a prime power. To share a uniformly distributed secret $s \in GF(q)$ a MTA chooses a random element $r \in GF(q)$. The value of r is kept secret by the MTA. Then the MTA gives to the participants in V_j, $1 \leq j \leq k$, share share $r + js$. It is easy to see that if the participants in V_j combine their shares they do not gain any knowledge about the secret. If $\{a, b\}$ is an edge then $a \in V_i$ and $b \in V_j$ with $i \neq j$. Hence, a and b have shares $r + is$ and $r + js$ respectively. Since $i \neq j$ they can compute the secret by pooling their shares. So, both [SS1] and [SS2] are satisfied.

Theorem 1.4.4 *[21] If G is not a multipartite graph then $\dot{\rho}(G) \leq 2/3$.*

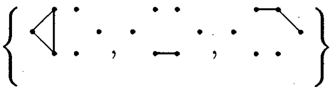
Let G be a graph and let $G_1, \ldots, G_n$ be subgraphs of G such that each edge of G occurs in at least one of the G_i's. Then the collection $\Pi = \{G_1, \ldots, G_n\}$ is called a covering of G. If each G_i is a complete multipartite graph we say that Π is a *complete multipartite covering* (CMC) of G. By giving an explicit construction Blundo et al. [21] proved the following theorem.

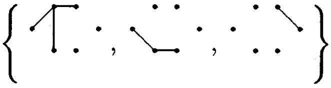
Theorem 1.4.5 *(Multiple Construction Technique) Suppose G is a graph with vertex set V for which l complete multipartite coverings exist, say $\Pi_j = \{G_{j,1}, \ldots, G_{j,n_j}\}$, $1 \leq j \leq l$. For every vertex v and for $1 \leq j \leq l$ define $R_{j,v} = |\{i : v \in V_{j,i}\}|$, where $V_{j,i}$ denotes the vertex set of $G_{j,i}$. So $R_{j,v}$ is the number of graphs with vertex v in the j-th multipartite covering. Define $R_v = \sum_{1 \leq j \leq l} R_{j,v}$, let $R = \max\{R_v : v \in V\}$, and let $\tilde{R} = \frac{1}{|V|} \sum_{v \in V} R_v$. Then $\dot{\rho}(G) \geq l/R$ and $\tilde{\rho}(G) \geq l/\tilde{R}$.*

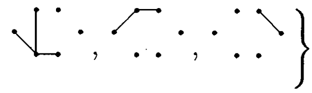
Example 1.4.6 Let

$G =$ 

Let us number the vertices clockwise with leftmost vertex 1. Let

$\Pi_1 =$ ,

$\Pi_2 =$ ,

$\Pi_3 = \Big\{$  $\Big\}.$

All Π_i are complete multipartite coverings of G. Let $q \geq 3$ be a prime power. For the three graphs in Π_1 there exist schemes $\nu^{1,i}, i \in \{1,2,3\}$, such that $\nu_s^{1,i}$ is the uniform distribution over $GF(q)$ for $i \in \{1,2,3\}$, and such that the convecs are

$$\begin{aligned} c(\nu^{1,1}) &= (1,1,0,0,0,1), \\ c(\nu^{1,2}) &= (0,0,0,0,1,1), \text{ and} \\ c(\nu^{1,3}) &= (0,1,1,1,0,0) \end{aligned}$$

(see Theorem 1.4.2 and Example 1.4.3). Suppose that a MTA selects a secret $s_1 \in GF(q)$ with uniform distribution. Further suppose that the MTA uses schemes $\nu^{1,1}$, $\nu^{1,2}$, and $\nu^{1,3}$ to share s_1. Then this results in a scheme ν^1 for G for which ν_s^1 is the uniform distribution over $GF(q)$ and for which the convec equals

$$c(\nu^1) = \sum_i c(\nu^{1,i}) = (1,2,1,1,1,2).$$

In a similar way we can construct a scheme ν^2 for G to share a second secret $s_2 \in GF(q)$ by using Π_2. Its convec will be equal to

$$\begin{aligned} c(\nu^2) &= \sum_i c(\nu^{2,i}) \\ &= (1,1,1,0,0,1) + (1,0,0,0,1,1) + (0,0,1,1,0,0) \\ &= (2,1,2,1,1,2). \end{aligned}$$

Similarly for Π_3 we can construct a scheme ν^3 for G to share a third secret $s_3 \in GF(q)$. Its convec will be equal to

$$\begin{aligned} c(\nu^3) &= \sum_i c(\nu^{3,i}) \\ &= (1,1,0,0,1,1) + (1,1,1,0,0,0) + (0,0,1,1,0,0) \\ &= (2,2,2,1,1,1). \end{aligned}$$

Suppose that a MTA selects a secret $\mathbf{s} = (s_1, s_2, s_3) \in GF(q)^3$ with uniform distribution. Further suppose that the MTA uses scheme ν^i to share s_i for $i \in \{1,2,3\}$. Then this leads to a scheme ν with convec

$$c(\nu) = \sum_i c(\nu^i)/3 = (5,5,5,3,3,5)/3,$$

and, hence, $\dot{\rho} = 3/5$ and $\tilde{\rho} = 9/13$. This corresponds to Theorem 1.4.5; $l = 3$, $R_{j,v} = c_v(\nu^j)$, and $R_v = l \cdot c_v(\nu)$.

Stinson [99] generalized this technique.

Theorem 1.4.7 *(Decomposition Construction) Suppose G is a graph with vertex set V and edge set E for which a complete multipartite covering exists, say $\Pi = \{G_1, \ldots, G_n\}$. For every vertex $v \in V$ define $R_v = |\{i : v \in V_i\}|$, where V_i denotes the vertex set of G_i. For every edge $e \in E$ define $T_e = |\{i : e \in E_i\}|$, where E_i denotes the edge set of G_i. Let $R = \max\{R_v : v \in V\}$, $\tilde{R} = \frac{1}{|V|} \sum_{v \in V} R_v$, and $T = \min\{T_e : e \in E\}$. Then $\dot{\rho}(G) \geq T/R$ and $\tilde{\rho}(G) \geq T/\tilde{R}$.*

Example 1.4.8 Let us proceed with Example 1.4.6. Let $q \geq 10$ be a prime power. Let Π denote the collection of all graphs in Π_1, Π_2, and Π_3 (notice that Π can contain a graph several times). For each graph we have a scheme by using Example 1.4.3 in which the secret is uniformly distributed over $GF(q)$. From Example 1.2.6 we obtain a $(0, 3, 9)$-ramp scheme ($\omega = 0$, $\lambda = 3$, and $n = 9$) in which the secret is uniformly distributed over $GF(q)^3$. All the shares p_i, $1 \leq i \leq 9$, in the ramp scheme are uniformly distributed over $GF(q)$. Suppose we use the scheme for the i-th graph in Π to share p_i. Then we have constructed a scheme ν in which the secret is uniformly distributed over $GF(q)^3$ and of which the convec equals the sum of all convecs of schemes for the graphs in Π divided by 3, that is it equals $(5, 5, 5, 3, 3, 5)/3$ as in Example 1.4.6.

Scheme ν is a scheme for G. Here, we only check [SS1]. To check [SS2] is more difficult and will be postponed to Chapter 5 where we prove a more general theorem (Theorem 5.2.2). Let $\{i, j\}$ be an edge in G. Then it is an edge of at least 3 graphs in Π. Hence, when i and j combine their shares they obtain at least three shares in the ramp scheme. So, they can compute the secret. We leave it to the reader to show that Theorem 1.4.7 gives the same results: $n = 9$, $R_v = \lambda \cdot c_v(\nu)$, and $T = \lambda$.

For a graph G we denote its maximum degree by $d(G)$. Using the decomposition construction Stinson proved the following theorem.

Theorem 1.4.9 *For any graph G there exists a perfect secret sharing scheme for $\Gamma(G)$ with worst-case information rate at least $2/(d(G)+1)$.*

In Chapter 2 we will show that this bound is tight, that is for all $\varepsilon > 0$ and $d \geq 3$ there exists a graph G with maximum degree d such that $\dot{\rho}(G) \leq \tilde{\rho}(G) \leq 2/(d + 1 + \varepsilon)$.

1.5 Secret Sharing with Extended Capabilities

It is assumed that a secret sharing scheme is being set up by a mutually trusted authority, this is a person or device unconditionally trusted by all participants. This trusted party first chooses the secret and then constructs and distributes in secret to each of the participants the private shares. Generally no one is trusted by all of the participants. Meadows [84] discusses the problem of setting up secret sharing schemes in the absence of a MTA, the related problem of how new participants can be enrolled in an already existing sharing of the secret, and the problem of how previously enrolled participants can be cut out (see also Blundo et al. [16]).

Ingemarsson and Simmons [56] developed MTA-free schemes. They introduced *democratic* schemes. These are schemes in which each participant has an equal influence on the determination of the secret. Ingemarsson and Simmons proposed a solution consisting of two phases. In the first phase each participant i selects a private contribution of the secret, a random element s_i. During the initialization of the mechanism that implements the shared control (for example a bank vault or safety deposit box), each participant i secretly enters s_i. The sum of all s_i becomes the jointly defined secret s. In the second phase each participant i shares his private contribution among the other participants such that groups of participants whom i trusts are qualified to reconstruct s_i but the groups of participants whom i does not trust are forbidden to obtain extra knowledge about s_i by pooling their shares. Thus participant i shares s_i using a scheme for his private access structure corresponding to the trust relations of i. We conclude that each participant knows that only groups are able to recover the secret s that either include him or include a subset of participants whom he trusts. This is also the risk of accepting a MTA (with its corresponding access structure) if there had been one. See for a further discussion Jackson et al. [62] and Simmons [95].

A MTA computes and securely distributes all shares. In general there is no secure channel. Such a channel needs to be created. Therefore securely transmitting shares is costly in terms of required resources, e.g. time. What to do if there is no time (a question posed by Simmons [95]), that is if immediate secret sharing is required? For example [95] in an advanced state of alert the higher command of an army wants to share secret keys such that actions (like launching missiles) can be initiated by lower levels of command. However, in an advanced state of alert there is no time to set up a secret sharing scheme with secure channels. At any time the central command can be destroyed in a surprise attack. Thus in an advanced state of alert the central command has to be able to activate a secret sharing scheme at once. Then the army can initiate actions at all times if necessary. We can not share all keys in peace time, simply because the law does not permit a concurrence of (non-responsible) people to be able to initiate military actions. It should be possible to precompute all private shares needed for the secret sharing scheme such that even if all of the participants pool their shares together, they would have no better chance of recovering the secret than an outsider (of the army) has of guessing it. Also as we have argued it should be possible to activate the secret sharing scheme at once by public broadcasting a single piece of information. These features can be achieved as follows. A MTA sets up a secret sharing scheme in which it shares a random element r. Then the public broadcast message can be $r+s$, where s is the secret. See for a further discussion Simmons [95] and Blundo et al. [16].

In the literature one can also find secret secret sharing schemes with other extended capabilities: secret sharing schemes with disenrollment (which is related to MTA-free schemes), secret sharing secure against a coalition of dishonest players [33], verifiable secret sharing [3] (for example the trustees in Micali's proposal can verify the correctness of their shares), multi-secret sharing schemes [61, 18], etc.

1.6 Outline of the First Part of the Thesis

The fundamental problem in secret sharing is to construct optimal schemes. This problem consists of two parts. Firstly, we search for methods to construct schemes. Secondly, we want to bound information rates in a smart manner.

In Chapter 2 [44, 46] we develop a method to lower bound individual information rates. The lower bound $2/(d(G)+1)$ on the optimal worst-case and average information rate of access structures based on graphs is proved to be tight. This shows that shares may need to be impractically large.

Construction results can be split into two types; decomposition constructions and basic constructions. Decomposition constructions are methods to construct secret sharing schemes using existing ones. Theorems 1.4.5 and 1.4.7 are examples. To find a scheme for some access structure (Γ, Δ) we combine schemes for other access structures $(\Gamma_i, \Delta_i), i \in I$. We call the collection $\{(\Gamma_i, \Delta_i) : i \in I\}$ a decomposition of (Γ, Δ). In Chapter 5 [50] (joint work with Wen-Ai Jackson and Keith Martin) a decomposition construction for secret sharing schemes will be discussed. It generalizes all known decomposition constructions.

Basic constructions are methods to construct secret sharing schemes without using existing ones. Theorem 1.4.2 is an example (its proof uses a construction for each complete multipartite graph, see Example 1.4.6). Almost all examples for basic constructions are linear, that is they use subspaces. Jackson and Martin [57] describe linear basic constructions by using a geometrical approach. In Chapter 3 [41, 51, 48] we describe the generalized vector space construction. This construction leads to a description of linear basic constructions by means of a matrix approach by using codes. In geometry subspaces are called lines, planes, and so on. In coding theory they are called linear codes, and they are characterized by generator matrices. By using the matrix approach for secret sharing schemes for incomplete access structures a duality theorem will be proved (a joint result with Jackson and Martin

[51]) and in [48] an upper bound on the optimal worst-case information rate for linear secret sharing schemes can be derived. The matrix approach leads to an algorithm for finding perfect secret sharing schemes. Optimal perfect secret sharing schemes for access structures based on connected graphs on six vertices constructed by this algorithm are presented in Chapter 4 [44] (Perry Moerland implemented the algorithm). There are 112 access structures of this type. For 94 of them the optimal worst-case information rate is determined.

In Chapter 6 [49] we discuss an application of secret sharing in authentication theory. In the conventional authentication problem [94] a sender wants to transmit messages to a receiver in the presence of a malicious adversary. The sender and receiver trust each other, however, they communicate over an insecure channel. The adversary can insert a message into the channel (impersonation attack), or observe a transmitted message and then replace it with another message (substitution attack). The receiver wants to detect false messages sent by the adversary. Towards this end the sender and receiver use a so-called authentication code.

The conventional authentication problem can be extended to the case where the capability to authenticate a message is given to groups instead of a single person. This problem has still not attained much attention. In Chapter 6 (joint work with Christian Gehrmann and Ben Smeets) we deal with a scenario where among a group of participants only certain subsets of the group are able to authenticate a message in order to send it to a trustable receiver. For example, the group could consist of bank clerks authorizing a large transaction for a bank (the receiver). We only consider unconditionally secure schemes, that is the security does not rely on any computational complexity. As pointed out in [38] the problem is not solved by simply combining a secret sharing and authentication scheme because such a solution would give the users of a qualified group not only the capability to authenticate after they combined their shares, but also full knowledge of the underlying secret. We will use an approach where we extend existing secret sharing schemes to unconditionally secure group authentication schemes. The idea of combining secret sharing and authentication is not new; threshold signatures have been introduced by Desmedt and Frankel [39]. Their paper deals almost only with conditionally secure schemes. The problem is further developed and discussed by Desmedt in [38].

Chapter 2

Upper Bounds on the Information Rate

In this chapter (based on [44, 46]) we use the entropy approach of Capocelli et al. [30] to derive upper bounds on the optimal worst-case and optimal average information rate of perfect secret sharing schemes. We consider non-trivial complete connected access structures Γ on $\mathcal{P}$. In Section 2.1 we investigate equivalent definitions of perfect secret sharing schemes. In Section 2.2 these will lead to a method with which upper bounds on the information rates can be derived. The remaining sections contain examples of upper bounds.

2.1 Characterizations of Perfect Schemes

Let ν be a scheme for Γ. Consider two groups of participants X and Y such that Y is a forbidden subset ($Y \notin \Gamma$) but $X \cup Y$ is a qualified subset ($X \cup Y \in \Gamma$). Then the combination of the shares of the participants in Y contains absolutely no information about the secret, but if groups X and Y pool their shares then they will be able to reconstruct the secret. Thus, firstly the uncertainty about s_ν given Y_ν equals the uncertainty about s_ν (so $H(s_\nu|Y_\nu) = H(s_\nu)$). Secondly, group X is able to reconstruct the secret if they are aware of the additional information contained in the combination of the shares of the participants in Y. Hence, the mutual information between X_ν and s_ν given Y_ν equals the information contained in s_ν (so $I(s_\nu; X_\nu|Y_\nu) = H(s_\nu)$). The following theorem is about this property, and gives a new characterization of perfect schemes.

Theorem 2.1.1 *Let ν be a probability measure describing a scheme for Γ on $\mathcal{P}$. Then ν is a perfect scheme for Γ on $\mathcal{P}$ iff for all $X, Y \subseteq \mathcal{P}$*

$$I(X_\nu; s_\nu|Y_\nu) = \begin{cases} H(s_\nu), & \textit{if } Y \notin \Gamma \textit{ and } X \cup Y \in \Gamma, \\ 0, & \textit{otherwise.} \end{cases} \tag{2.1}$$

Proof: Let ν be a perfect scheme for Γ on $\mathcal{P}$. We consider several cases in order to prove the left to right implication of the theorem. If $Y \notin \Gamma$ and $X \cup Y \in \Gamma$ then $I(X; s|Y) = H(s|Y) - H(s|XY) = H(s) - 0$ by [SS1] and [SS2]. If $Y \in \Gamma$ then $X \cup Y \in \Gamma$ because Γ is monotone increasing. Hence $I(X; s|Y) = H(s|Y) - H(s|XY) = 0 - 0$ by [SS1]. Similarly if $X \cup Y \notin \Gamma$ (which implies $Y \notin \Gamma$) then $I(X; s|Y) = H(s|Y) - H(s|XY) = H(s) - H(s) = 0$ by [SS2]. We have proved the theorem in one direction.

Let us prove the right to left implication. So, assume that ν describe a scheme on $\mathcal{P}$ for which (2.1) holds. By taking $Y = \emptyset$ in (2.1) we obtain $H(s) - H(s|X) = I(X; s) = H(s)$ for $X \in \Gamma$ and $H(s) - H(s|X) = I(X; s) = 0$ for $X \notin \Gamma$. So, $H(s|X) = 0$ for $X \in \Gamma$ and $H(s|X) = H(s)$ for $X \notin \Gamma$. Hence, ν is a scheme for Γ on $\mathcal{P}$ by [SS1] and [SS2]. We have proved the theorem.

□

We notice that two of the three left to right cases, namely $X \cup Y \notin \Gamma$ ($\Rightarrow I(X; s|Y) = 0$) and $Y \notin \Gamma, X \cup Y \in \Gamma$ ($\Rightarrow I(X; s|Y) = H(s)$) in Theorem 2.1.1, have first been proven in [30].

Suppose that Y is a forbidden subset. Let $X \subseteq \mathcal{P}$ such that $X \cup Y$ is a qualified subset. If the participants in Y obtain additional information such that they are able to reconstruct the shares of the participants in X then they are able to reconstruct the secret as well (since $X \cup Y \in \Gamma$). In other words the uncertainty about X_ν given Y_ν is at least the uncertainty about s_ν, which is generalized in the next corollary.

Corollary 2.1.2 *For any scheme for Γ on $\mathcal{P}$ and for all $X, Y, Z \subseteq \mathcal{P}$ if $Y \cup Z \notin \Gamma$, but $X \cup Y \cup Z \in \Gamma$, then $H(s) \leq H(X|Y)$.*

Proof: Theorem 2.1.1 implies $H(s) = I(X; s|YZ) = H(X|YZ) - H(X|YZs)$ $\leq H(X|YZ) \leq H(X|Y)$.

□

The case $Z = \emptyset$ in Corollary 2.1.2, as well as the following corollary have already been proven in [30]. The following corollary shows that $\hat{\rho}(\Gamma) \leq 1$.

Corollary 2.1.3 *For all schemes for non-trivial complete connected access structures*
$H(s) \leq H(a)$ holds for any participant $a \in \mathcal{P}$.

Proof: Since $\emptyset \notin \Gamma$ and Γ is nonempty (Γ is not trivial) there exists a set $Z \subseteq \mathcal{P}$ such that $aZ \in \Gamma$ and $Z \notin \Gamma$. This follows from the monotonicity and connectivity of Γ. Thus Corollary 2.1.2 with $X = a$ and $Y = \emptyset$ proves the desired result.

□

In the following theorem we characterize, as in Theorem 2.1.1, perfect secret sharing schemes. The corollary corresponding to the next theorem will be needed for the derivation of upper bounds on the information rate of perfect secret sharing schemes. First we quote some basic properties in information theory [54].

Lemma 2.1.4 *For all random variables X, Y, Z, Q*

(i) $I(XQ;Y|Z) = I(X;Y|Z) + I(Q;Y|XZ)$,

(ii) $H(XY|Z) = H(X|Z) + H(Y|XZ)$, *and*

(iii) $H(X|Z) + H(Y|Z) = H(XY|Z) + I(X;Y|Z)$.

Theorem 2.1.5 *Let ν be a probability measure describing a scheme for Γ on $\mathcal{P}$. Then ν is a perfect scheme for Γ on $\mathcal{P}$ iff for all $X, Y, Z \subseteq \mathcal{P}$*

$$I(X_\nu;Y_\nu|(sZ)_\nu) = \begin{cases} I(X_\nu;Y_\nu|Z_\nu) & \textit{if } (X \cup Z \in \Gamma) \\ -H(s_\nu), & \quad \wedge(Y \cup Z \in \Gamma) \\ & \quad \wedge(Z \notin \Gamma), \\ I(X_\nu;Y_\nu|Z_\nu) & \textit{if } (X \cup Z \notin \Gamma) \\ +H(s_\nu), & \quad \wedge(Y \cup Z \notin \Gamma) \\ & \quad \wedge(X \cup Y \cup Z \in \Gamma), \\ I(X_\nu;Y_\nu|Z_\nu), & \textit{otherwise.} \end{cases} \tag{2.2}$$

Proof: Let us prove the left to right implication. Let ν be a scheme for Γ on $\mathcal{P}$. Lemma 2.1.4(i) implies $I(X;Y|sZ) + I(X;s|Z) = I(X;Ys|Z) = I(X;Y|Z) + I(X;s|YZ)$. Suppose that $(X \cup Z \in \Gamma) \wedge (Y \cup Z \in \Gamma) \wedge (Z \notin \Gamma)$ (the first case). Then $I(X;s|Z) = H(s)$ and $I(X;s|YZ) = 0$, by Theorem 2.1.1. Hence, $I(X;Y|sZ) = I(X;Y|Z) - H(s)$. The other cases can be proved similarly.

Let us now prove the right to left implication. Suppose that ν describes a scheme for which (2.2) holds. Let $X = Y$ in (2.2). Then $H(X|YZ) = H(X|sZY) = 0$. So $I(X;Y|Z) - I(X;Y|sZ) = H(X|Z) - H(X|sZ) = I(X;s|Z)$. Let us show the first case of (2.1). If $(X \cup Z \in \Gamma) \wedge (Z \notin \Gamma)$ then $(X \cup Z \in \Gamma) \wedge (X \cup Y \in \Gamma) \wedge (Z \notin \Gamma)$ and, hence, $I(X;Y|sZ) = I(X;Y|Z) - H(s)$. Thus $I(X;s|Z) = H(s)$.

Let us now show that the second case of (2.1) holds. If $(X \cup Z \notin \Gamma) \vee (Z \in \Gamma)$ then $(X \cup Y \cup Z \notin \Gamma) \vee (Z \in \Gamma)$ and, hence, $I(X;Y|sZ) = I(X;Y|Z)$. Thus $I(X;s|Z) = 0$. So, formula (2.1) holds, and we infer from Theorem 2.1.1 that ν is a perfect scheme.

□

We immediately obtain

Corollary 2.1.6 *For any scheme for Γ on $\mathcal{P}$ and for all $X, Y, Z \subseteq \mathcal{P}$*

(i) $X \cup Z \in \Gamma$, $Y \cup Z \in \Gamma$, *and* $Z \notin \Gamma$ *implies* $H(s) \leq I(X;Y|Z)$, *and*

(ii) $X \cup Z \notin \Gamma$, $Y \cup Z \notin \Gamma$, *and* $X \cup Y \cup Z \in \Gamma$ *implies* $H(s) \leq I(X;Y|sZ)$.

Suppose that $Y \cup Z \notin \Gamma$, but $X \cup Y \cup Z \in \Gamma$. Then the first part of Corollary 2.1.6 implies that $H(s) \leq I(X;\mathcal{P}|YZ) \leq H(X|YZ) \leq H(X|Y)$ (note that $\mathcal{P} \in \Gamma$). Thus Corollary 2.1.2 is implied by the first part of Corollary 2.1.6. By noticing that $I(X;Y|sZ) \leq H(X|sZ)$ we obtain from Corollary 2.1.6(ii):

Corollary 2.1.7 *For any scheme for Γ on $\mathcal{P}$ and for all $X, Y, Z \subseteq \mathcal{P}$ if $X \cup Z \notin \Gamma$, $Y \cup Z \notin \Gamma$, and $X \cup Y \cup Z \in \Gamma$ then $H(s) \leq H(X|sZ)$.*

Lemma 2.1.4, and Corollaries 2.1.2, 2.1.6, and 2.1.7 will be used in a method to derive upper bounds on information rates in the next section.

2.2 A Method to Upper Bound Information Rates

We will prove new upper bounds on the optimal worst-case and average information rate of certain access structures by using a method described in general terms below and depicted in Figure 2.1.

The procedure is as follows. First we choose a group of participants $p_1, \ldots, p_k \in \mathcal{P}$. By repeatedly using Lemma 2.1.4(iii) we obtain an equality like

$$\sum_{1 \leq i \leq k} H(p_i) = H(p_1, \ldots, p_k) + \sum I(.., ..). \tag{2.3}$$

Again, we choose a group of participants $p'_1, \ldots, p'_l \in \mathcal{P}$. By the definition of mutual information

$$\begin{aligned} H(p_1, \ldots, p_k) &= I(p_1, \ldots, p_k; p'_1, \ldots, p'_l) + \\ &\quad H(p_1, \ldots, p_k | p'_1, \ldots, p'_l). \end{aligned} \tag{2.4}$$

Now all mutual informations in (2.3) and (2.4) can be decomposed into more mutual informations by means of Lemma 2.1.4(i). By applying Corollary 2.1.6(i) we show that some of these mutual informations will be at least $H(s)$. The conditional entropy in (2.4) can be decomposed into more conditional entropies by applying Lemma 2.1.4(ii). Finally, by applying Corollary 2.1.2 we show that some of these conditional entropies will be at least $H(s)$. Combining all the above one arrives at an inequality of the type

$$\sum_{1 \leq i \leq k} H(p_i) \geq aH(s).$$

Thus for some participant p_i

$$H(p_i) \geq \frac{a}{k} H(s).$$

$$\begin{tikzcd}
 & \sum\limits_{1\le i\le k} H(p_i) \arrow[d, "\text{Lem. 2.1.4(iii)}"] & & \\
\sum I(..,..) \arrow[ddr] & + & H(p_1,\dots,p_k) \arrow[d] & \\
 & I(p_1,\dots,p_k; p'_1,\dots,p'_l) \arrow[d, "\text{Lem. 2.1.4(i)}"'] & + & H(p_1,\dots,p_k| p'_1,\dots,p'_l) \arrow[d, "\text{Lem. 2.1.4(ii)}"] \\
 & \sum I(..;..|..) \arrow[d, "\text{Cor. 2.1.6(i)}"'] & + & \sum H(..|..) \arrow[d, "\text{Cor. 2.1.2}"] \\
\geq & a_0 H(s) & + & a_1 H(s)
\end{tikzcd}$$

Figure 2.1: A method to upper bound information rates.

Hence, $\dot{\rho}(\Gamma) \leq k/a$, and we have obtained an upper bound on the optimal worst-case information rate. If $\mathcal{P} = \{p_1, \ldots, p_k\}$ we obtain $\tilde{\rho}(\Gamma) \leq k/a$ as upper bound on the optimal average information rate.

We notice that instead of (2.3) we can also obtain an equality like

$$H(s) + \sum_{1 \leq i \leq k} H(p_i) = H(s, p_1, \ldots, p_k) + \sum I(.., ..).$$

Then Corollary 2.1.7 and Corollary 2.1.6(ii) have to be used in the derivations as well.

The following theorem and corollary, both from [30], can systematically be proved by this method. In what follows a, b, etc. denote participants in $\mathcal{P}$ (capitals X, Y, and Z denote groups of participants).

Theorem 2.2.1 *Let Γ be an access structure such that $ad, ac, b \notin \Gamma$, and $bc, ab, acd \in \Gamma$ (see Figure 1.3, where $1 = b$, $2 = d$, $3 = c$, and $4 = a$). Then $H(b) + H(c) \geq 3H(s)$ for any scheme for Γ.*

Proof: See Figure 2.1. We derive $H(b) + H(c) = I(b; c) + H(bc)$, $H(bc) = I(bc; a) + H(bc|a)$, $I(bc; a) = I(b; a) + I(c; a|b)$, and $H(bc|a) = H(c|a) + H(b|ac)$. Thus $H(b) + H(c) \geq I(c; a|b) + H(c|a) + H(b|ac)$. From Corollary 2.1.6(i), $b \notin \Gamma$, and $bc, ab \in \Gamma$ we infer that $I(c; a|b) \geq H(s)$. Further by taking $Z = d$ in Corollary 2.1.2 and noticing that $ad \notin \Gamma$ and $acd \in \Gamma$ we obtain $H(c|a) \geq H(s)$. Similarly, $H(b|ac) \geq H(s)$ (by taking $Z = \emptyset$ in Corollary 2.1.2 and noticing that $ac \notin \Gamma$ and $abc \in \Gamma$ because $ab \in \Gamma$ and Γ is monotone increasing). This proves $H(b) + H(c) \geq 3H(s)$.

□

This immediately leads to the following corollary.

Corollary 2.2.2 *For all graphs G with four vertices a, b, c, and d such that bc, cd, and ab are in the edge set of G and ad and ac are not contained in the edge set of G*

$$\dot{\rho}(G) \leq \frac{2}{3}.$$

In [21] Corollary 2.2.2 is used together with Lemma 1.4.1 to prove Theorem 1.4.4.

We notice that the method explained above forces one to decide in advance in which direction to rewrite the formula's. The next section will show that this way of thinking leads to new interesting upper bounds. However, there are also other ways to derive interesting bounds on the information rate. The next lemma and example will demonstrate this. In the example we improve an upper bound in [60] on the optimal average information rate of a certain access structure by applying Lemma 2.2.3. We conjecture that this lemma can be used to improve more upper bounds on the optimal average information rate in [60].

Lemma 2.2.3 *For any scheme for Γ on $\mathcal{P}$ and for all $X, Y, Z \subseteq \mathcal{P}$*

(i) if $X \cup Y, X \cup Z \in \Gamma$ and $X, Z \cup Y \notin \Gamma$ then

$$H(Z|X) + H(X|Y) \geq 2H(s) + H(Z|Y),$$

(ii) if $X \cup Y, X \cup Z \in \Gamma$ and $X \notin \Gamma$ then

$$H(Z|X) + H(Y|X) \geq H(s) + H(YZ|X).$$

Proof: To prove (i) we use

$$\begin{aligned} H(X) + H(Z|X) &= H(XZ) = I(XZ;Y) + H(XZ|Y) \\ &= I(X;Y) + I(Z;Y|X) + H(Z|Y) + H(X|YZ) \\ &= H(X) - H(X|Y) + I(Z;Y|X) + H(Z|Y) + \\ &\quad H(X|YZ). \end{aligned}$$

From Corollary 2.1.6(i) we infer that $I(Z;Y|X) \geq H(s)$ and from Corollary 2.1.2 we infer that $H(X|YZ) \geq H(s)$. Now (i) follows.

To prove (ii) we note that

$$H(Z|X) + H(Y|X) = I(Z;Y|X) + H(YZ|X).$$

From Corollary 2.1.6(i) we infer that $I(Z;Y|X) \geq H(s)$. This implies (ii).

□

Example 1 Let $\mathcal{P} = \{a, b, c, d, e\}$ and let $[\Gamma]^- = \{ab, ac, bd, ce, ade\}$, which is access structure number 73 in [60]. In [60] it is shown that $5/8 \leq \tilde{\rho}(\Gamma) < 5/7$. In this example we improve the upper bound. We derive

$H(e|c) + H(c|a) \geq 2H(s) + H(e|a)$

by Lemma 2.2.3(i) with $Z = e, X = c, Y = a$,

$H(a|b) + H(d|b) \geq H(s) + H(ad|b)$

by Lemma 2.2.3(ii) with $Z = a, X = b, Y = d$,

$H(e|ad) + H(ad|b) \geq 2H(s) + H(e|b)$

by Lemma 2.2.3(i) with $Z = e, X = ad, Y = b$,

$H(e|b) \geq H(s)$

by Corollary 2.1.2 with $Z = c, X = e, Y = b$.

By noticing that $H(X) \geq H(X|Y)$ for any two random variables X and Y we obtain

$$H(a) + H(c) + H(d) + H(e) \geq 6H(s).$$

This inequality can not be proved by solely using Theorem 2.2.1. From Theorem 2.2.1 we do obtain

$$\begin{aligned} &H(a) + H(b) \geq 3H(s), \\ &H(c) + H(e) \geq 3H(s), \\ &H(b) + H(d) \geq 3H(s). \end{aligned}$$

Hence, $2\sum_{p\in\mathcal{P}} H(p) \geq 15H(s)$. We conclude that $\tilde{\rho}(\Gamma) \leq 2/3$.

2.3 Examples of Upper Bounds

The next theorems with corresponding corollary result in the description of a class of graphs for which the worst-case information rate is at most 3/5. Each of these theorems has been found by applying the method of Section 2.2. They will be used in Chapter 4 to study perfect secret sharing schemes based on connected graphs on six vertices.

Theorem 2.3.1 *Let Γ be an access structure such that $d, ce, aef, bef \notin \Gamma$, and de, $abef$, cef, df, $bd \in \Gamma$. Then $H(f) + H(d) + H(b) \geq 5H(s)$ for any scheme for Γ.*

Proof: By Lemma 2.1.4(iii) $H(f)+H(d)+H(b) = H(fd)+I(f;d)+H(b) = H(fdb)+I(fd;b)+I(f;d)$ which equals by Lemma 2.1.4(i) $H(fdb)+I(f;b|d)+I(d;b) + I(f;d)$ and is at least $H(fdb)+$ $I(f;b|d)$. Hence

$$H(f) + H(d) + H(b) \geq H(fdb) + I(f;b|d).$$

By Corollary 2.1.6(i)

$$I(f;b|d) \geq H(s),$$

and by the definition of mutual information $H(fdb) = I(fdb;e) + H(fdb|e)$ which is, by Lemma 2.1.4(i) and twice Lemma 2.1.4(ii), equal to $I(d;e) + I(fb;e|d) + H(f|e)+$ $H(b|ef) + H(d|ebf)$. Hence

$$H(fdb) \geq I(fb;e|d) + H(f|e) + H(b|ef) + H(d|ebf).$$

Finally $I(fb;e|d) \geq H(s)$ by Corollary 2.1.6(i) and $H(f|e), H(b|ef)$, and $H(d|ebf)$ are at least $H(s)$ by Corollary 2.1.2 with $Z = c$, $Z = a$, and $Z = \emptyset$ respectively. Hence $H(f) + H(d) + H(b) \geq H(fdb) + I(f;b|d) \geq 4H(s) + H(s) = 5H(s)$.

□

Theorem 2.3.2 *Let Γ be an access structure such that $d, ce, aef, bef \notin \Gamma$, $de, abef, cef \in \Gamma$, and at least one of the following conditions holds*

- *$bc, cd \in \Gamma$,*

- *$bc, bd \in \Gamma$, or*

- *$cd, bd \in \Gamma$.*

Then $H(b) + H(c) + H(d) \geq 5H(s)$ for any scheme for Γ.

Proof: We first show that any of the three conditions $bc, cd \in \Gamma$, $bc, bd \in \Gamma$, and $cd, bd \in \Gamma$ implies that

$$H(b) + H(c) + H(d) \geq H(bcd) + H(s). \tag{2.5}$$

Suppose that $bc, cd \in \Gamma$. By the same arguments as in Theorem 2.3.1 we can prove $H(b) + H(c) + H(d) \geq H(bcd) + I(b; d|c)$. We notice that $c \notin \Gamma$ since Γ is monotone and $ce \notin \Gamma$. By Corollary 2.1.6(i) $I(b; d|c) \geq H(s)$. Similarly if $bc, bd \in \Gamma$ or $cd, bd \in \Gamma$ inequality (2.5) holds.

It remains to show that $H(bcd) \geq 4H(s)$. By the definition of mutual information

$$H(bcd) = I(bcd; ef) + H(bcd|ef).$$

By Lemma 2.1.4(i) $I(bcd; ef) = I(bcd; e) + I(bcd; f|e)$,

$$\begin{aligned} I(bcd; e) &= I(d; e) + I(bc; e|d), \text{ and} \\ I(bcd; f|e) &= I(c; f|e) + I(bd; f|ec). \end{aligned}$$

We notice that $bcd \in \Gamma$ since Γ is monotone and at least one of the subsets bc, cd, and bd is an element of Γ. By Corollary 2.1.6(i) $I(bc; e|d)$, and $I(bd; f|ec)$ are at least $H(s)$. Hence

$$I(bcd; ef) \geq 2H(s).$$

By Lemma 2.1.4(ii)

$$\begin{aligned} H(bcd|ef) &= H(b|ef) + H(c|efb) + H(d|efbc) \\ &\geq H(b|ef) + H(c|efb), \end{aligned}$$

where $H(b|ef)$ and $H(c|efb)$ are at least $H(s)$ by Corollary 2.1.2 with $Z = a$ and $Z = \emptyset$ respectively. Hence $H(b) + H(c) + H(d) \geq 5H(s)$.

□

The following corollary describes graphs for which the information rate is at most 3/5. This corollary will be used in Chapter 4 to study perfect secret sharing schemes based on connected graphs on six vertices.

Corollary 2.3.3 *Let Γ be an access structure based on a graph G with six vertices a, b, c, d, e, and f satisfying*

- *$ab, cf, de \in \Gamma$,*

- *$ae, af, be, bf, ce, ef \notin \Gamma$,* *and at least one of the following conditions:*

- $df, bd \in \Gamma$,
- $bc, cd \in \Gamma$,
- $bc, bd \in \Gamma$, *or*
- $cd, bd \in \Gamma$.

Then $\dot{\rho}(G) \leq 3/5$.

Proof: We infer from Theorems 2.3.1 and 2.3.2 that $H(b) + H(c) + H(d) \geq 5H(s)$ or $H(f) + H(d) + H(b) \geq 5H(s)$. Hence for one of the participants p the ratio between $H(s)$ and $H(p)$ is at most 3/5.

□

The graphs mentioned in Corollary 2.3.3 are depicted in Figure 2.2. The lines are edges, and at least two of the dotted lines have to be chosen as edges such that the conditions of Corollary 2.3.3 are satisfied.

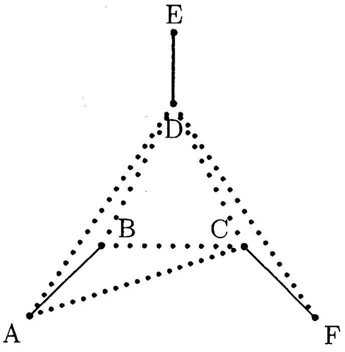
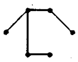
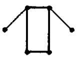
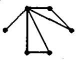
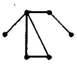
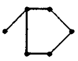


Figure 2.2: Graphs with information rate at most 3/5

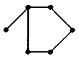
For graphs G containing one of the induced subgraphs

, , , , 

(thus the conditions in Corollary 2.3.3 are satisfied) the upper bound $\dot{\rho}(G) \leq 3/5$ has been proved in [19].

The results we have discussed so far can not only be used to derive upper bounds on the optimal worst-case information rate but they can also be used to obtain upper bounds on the optimal average information rate.

Example 2 Consider the graph



Let us number the vertices clockwise with the leftmost vertex 1. Then $H(1) \geq H(s)$ by Corollary 2.1.3, $H(4)+H(5) \geq 3H(s)$ by Theorem 2.2.1 with $a=3$, $b=4$, $c=5$, $d=6$, and $H(2)+H(3)+H(6) \geq 5H(s)$ by Theorem 2.3.1 with $a=5$, $b=6$, $c=4$, $d=2$, $e=1$, $f=3$. Hence, this graph has optimal average information rate at most 2/3, which solves an open problem in [19].

We finish this section by mentioning three more results from [60]. In [60] the method in Figure 2.1 is used to prove them.

Theorem 2.3.4 *Suppose that* $cde \notin \Gamma$, $ab, ac \in \Gamma$, *and one of the following conditions holds:*

(i) $a, bcd, bde \notin \Gamma$, $ad, bcde \in \Gamma$,

(ii) $bc, be, ade \notin \Gamma$, $bce, bde \in \Gamma$, *or*

(iii) $ad, bc, bde \notin \Gamma$, $bcd, ade \in \Gamma$.

Then $H(a)+H(b)+H(c) \geq 5H(s)$ *for any scheme for* Γ.

We notice that Theorems 2.2.1, 2.3.1, 2.3.2, and 2.3.4 can be generalized to incomplete access structures (Γ, Δ) by replacing $\notin \Gamma$ for $\in \Delta$. Their proofs follow from similar generalizations of the other results in this chapter.

2.4 The Lower Bound 2/(d+1)

Stinson [99] proved the general result that, for any graph G having maximum degree d, there exists a perfect secret sharing scheme realizing G in which the worst-case information rate is at least $2/(d+1)$. In this section we show that these lower bounds are tight in the following sense. We construct a family of graphs U_k^p having $6p^k$ vertices, maximum degree

$$d(U_k^p) = k+2,$$

and optimal worst-case information rate and optimal average information rate satisfying

$$\frac{2}{d(U_k^p)+1} \leq \rho(U_k^p) \leq \tilde{\rho}(U_k^p) \leq \frac{2}{d(U_k^p)+1-\frac{d(U_k^p)-3}{p}}$$

for $k \geq 1$ and $p \geq 3$. So, for any integer d there exists a graph (U_k^∞) with an infinite number of vertices and maximum degree d such that its optimal worst-case information rate and optimal average information rate both equal $2/(d+1)$. It also shows the existence of access structures (U_∞^p) for which the optimal worst-case information rate and optimal average information rate go to zero as the number of participants tends to infinity. Thus shares may need to be impractically large. Csirmaz [35] obtained independently a similar result for the optimal worst-case information rate. Recently, Blundo et al. [17] improved the proofs presented in this section and they showed that in fact $\rho(U_k^p) = \tilde{\rho}(U_k^p) = 2/(d(U_k^p)+1)$ for our family of graphs U_k^p. So, for any integer d there exists a graph with a finite number of vertices and maximum degree d such that its optimal worst-case information rate and optimal average information rate both equal $2/(d+1)$.

We are now going to construct the family of graphs U_k^p. A set of vertices in a graph with the property that there does not exist an edge connecting two of its vertices is called independent. Let graph U_0^p, $p \geq 1$, represent the cycle on six vertices. Then the vertices of U_0^p can be split into two disjoint independent sets of equal size (size three). We proceed to construct graphs U_k^p by induction on k. Suppose that U_k^p has vertices $v_1, \ldots, v_{6p^k}$ such that $\{v_1, \ldots, v_{3p^k}\}$ and $\{v_{3p^k+1}, \ldots, v_{6p^k}\}$ are independent sets of U_k^p. We label the vertices of U_{k+1}^p by

$$N_{i,a}, \text{ for } 1 \leq i \leq 6p^k, a \in \mathbb{Z}_p.$$

In what follows we write $N_{i,a}$ instead of $N_{i,a\text{mod}p}$. We define the edge set of U_{k+1}^p by

- the edges $N_{i,a}N_{j,a}$ such that v_iv_j is an edge in U_k^p for $a \in \mathbb{Z}_p$, and by
- the edges $N_{i,a}N_{3p^k+i,a+1}$ for all $1 \leq i \leq 3p^k$ and $a \in \mathbb{Z}_p$.

In other words, U_{k+1}^p consists of p numbered copies of U_k^p with matchings between the points of one of the independent sets in one copy and the points of the other independent set in the next copy (see Figure 2.3).

The construction of graphs U_k^p is well-defined since it is possible to split the vertices $N_{i,a}$, $1 \leq i \leq 6p^k, 0 \leq a \leq p-1$ into two disjoint independent sets

$$\bigcup_{0 \leq a \leq p-1} \left\{N_{i,a} : 1 \leq i \leq 3p^k\right\} \text{ and}$$

$$\bigcup_{0 \leq a \leq p-1} \left\{N_{i,a} : 3p^k+1 \leq i \leq 6p^k\right\}.$$

We introduce some helpful notation. By $L(a)$ and $R(a)$ we denote the vertices of the two independent sets of the a-th copy of U_k^p in graph U_{k+1}^p;

$$\begin{aligned} L(a) &= \left\{N_{1,a}, \ldots, N_{3p^k,a}\right\}, \text{ and} \\ R(a) &= \left\{N_{3p^k+1,a}, \ldots, N_{6p^k,a}\right\}. \end{aligned}$$

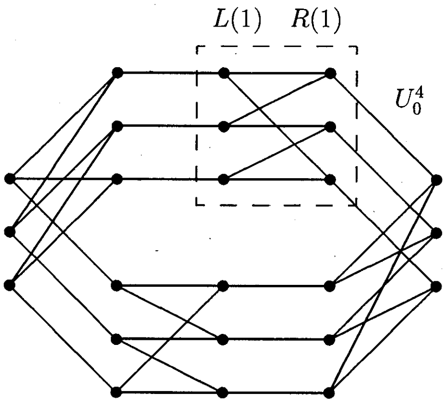


Figure 2.3: U_1^4

By $T(a)$ we denote all vertices of the a-th copy of U_k^p in graph U_{k+1}^p;

$$T(a) = L(a) \cup R(a).$$

We define $L(a)^i, L(a)_i, R(a)^i$, and $R(a)_i$ by

$$\begin{aligned} L(a)^i &= \{N_{1,a}, \ldots, N_{i-1,a}\}, \\ L(a)_i &= \{N_{i+1,a}, \ldots, N_{3p^k,a}\}, \\ R(a)^i &= \{N_{3p^k+1,a}, \ldots, N_{3p^k+i-1,a}\}, \text{ and} \\ R(a)_i &= \{N_{3p^k+i+1,a}, \ldots, N_{6p^k,a}\}. \end{aligned}$$

Thus $L(a) = L(a)^i N_{i,a} L(a)_i$, $R(a) = R(a)^i N_{3p^k+i,a} R(a)_i$, and $T(a) = L(a)R(a)$. The next lemma is about these sets and will be needed in our discussion on the information rates of the graphs U_k^p.

Lemma 2.4.1 *Let $a, b \in \mathbb{Z}_p$ with b not equal to $a-1$ or $a-2$. Let ν be a perfect scheme for the access structure based on U_{k+1}^p. Then*

(i) $I(T(a-1)_\nu; T(a)_\nu) \geq (3p^k+1)H(s_\nu)$,

(ii) $I(T(a)_\nu \ldots T(b)_\nu; T(a-1)_\nu T(b+1)_\nu) \geq (6p^k+1)H(s_\nu)$.

Proof: Let us prove (i). We derive by repeatedly applying Lemma 2.1.4(i)

$$\begin{aligned} I(L(a-1); T(a)) &= I(N_{1,a-1}; T(a)) + I(L(a-1)_1; T(a)|L(a-1)^1) \\ &= I(N_{1,a-1}; T(a)) + I(N_{2,a-1}; T(a)|L(a-1)^1) + \\ &\quad I(L(a-1)_2; T(a)|L(a-1)^2) \\ &\vdots \\ &= \sum_{1 \leq i \leq 3p^k} I(N_{i,a-1}; T(a)|L(a-1)^i). \end{aligned}$$

To lower bound the summation above we note that for $1 \leq i \leq 3p^k$

$$\begin{aligned} & I(N_{i,a-1}; T(a)|L(a-1)^i) \\ = \; & I(N_{i,a-1}; L(a)R(a)^i R(a)_i|L(a-1)^i N_{3p^k+i,a}) + \\ & I(N_{i,a-1}; N_{3p^k+i,a}|L(a-1)^i) \\ \geq \; & H(s) + 0 = H(s), \end{aligned}$$

by Lemma 2.1.4(i) and Corollary 2.1.6(i) respectively. We conclude that

$$I(L(a-1); T(a)) \geq 3p^k H(s). \tag{2.6}$$

Now, note that $I(T(a-1); T(a)) = I(L(a-1); T(a)) + I(R(a-1); T(a)|L(a-1))$ and that the last mutual information in this equality is at least $H(s)$ by Corollary 2.1.6(i). We conclude that (i) holds.

Let us now prove (ii). First notice that

$$\begin{aligned} & I(T(a)\ldots T(b); T(a-1)T(b+1)) \\ = \; & I(T(a)\ldots T(b); L(a-1)) + \\ & I(T(a)\ldots T(b); R(a-1)T(b+1)|L(a-1)) \\ \geq \; & I(T(a); L(a-1)) + I(T(b); R(a-1)T(b+1)|L(a-1)). \end{aligned}$$

From formula (2.6) we infer for the first term in this last expression that $I(T(a); L(a-1)) \geq 3p^k H(s)$. By repeatedly using Lemma 2.1.4(i) we obtain for the second term

$$\begin{aligned} & I(T(b); R(a-1)T(b+1)|L(a-1)) \\ = \; & \sum_{1 \leq i \leq 3p^k} I(T(b); N_{3p^k+i,b+1}|L(a-1)R(b+1)_i) + \\ & I(T(b); R(a-1)L(b+1)|L(a-1)R(b+1)). \end{aligned}$$

The last mutual information in the equality is at least $H(s)$ by Corollary 2.1.6(i). For the i-th term in the summation above it holds that

$$\begin{aligned} & I(T(b); N_{3p^k+i,b+1}|L(a-1)R(b+1)_i) \\ = \; & I(L(b)^i L(b)_i R(b); N_{3p^k+i,b+1}|L(a-1)N_{i,b}R(b+1)_i) + \\ & I(N_{i,b}; N_{3p^k+i,b+1}|L(a-1)R(b+1)_i) \\ \geq \; & H(s) + 0 = H(s) \end{aligned}$$

by Lemma 2.1.4(i) and Corollary 2.1.6(i) (notice that $a-1$ is not congruent to b or $b+1$ modulo p). This proves (ii).

□

The following properties of the graphs U_k^p are important in the context of this section.

Lemma 2.4.2

(i) U_k^p is a connected graph and the degree of each vertex of U_k^p equals $k+2$.

(ii) If ν is a perfect scheme for the access structure based on U_k^p, with vertices $v_1, \ldots, v_{6p^k}$, then

$$\sum_{1\le i\le 6p^k} H((v_i)_\nu) \ge H((v_1 \ldots v_{6p^k})_\nu) + \left(3\left(\frac{p-1}{p}k+2\right)p^k - 1\right) H(s_\nu).$$

(iii) If $k \ge 1$ and $p \ge 3$ then

$$\sum_{1\le i\le 6p^k} H((v_i)_\nu) \ge 3\left(\frac{p-1}{p}(k-1)+4\right)p^k H(s_\nu).$$

Proof: Lemma 2.4.2(i) is obvious. Lemma 2.4.2(ii) will be proved by induction. Let $a, b, c, d, e,$ and f be the vertices of U_0^p and let $ab, bc, cd, de, ef,$ and fa be the edges of U_0^p. Then, by repeatedly applying Lemma 2.1.4(iii) and 2.1.4(i) we obtain

$$\begin{aligned}
& H(a)+H(b)+H(c)+H(d)+H(e)+H(f) \\
= \;& H(ab)+I(a;b)+H(c)+H(de)+I(d;e)+H(e) \\
\ge \;& H(ab)+H(c)+H(de)+H(f) \\
= \;& H(abc)+I(ab;c)+H(def)+I(de;f) \\
= \;& H(abcdef)+I(ab;c)+I(de;f)+I(abc;def) \\
= \;& H(abcdef)+I(b;c)+I(a;c|b)+I(e;f)+ \\
& I(d;f|e)+I(a;def)+I(c;def|a)+I(b;def|ac) \\
= \;& H(abcdef)+I(b;c)+I(a;c|b)+I(e;f)+ \\
& I(d;f|e)+I(a;f)+I(a;de|f)+I(c;d|a)+ \\
& I(c;ef|ad)+I(b;def|ac) \\
\ge \;& H(abcdef)+I(a;c|b)+I(d;f|e)+I(a;de|f)+ \\
& I(c;ef|ad)+I(b;def|ac).
\end{aligned}$$

By Corollary 2.1.6(i) the right side of the last inequality is at least

$$H(abcdef)+5H(s).$$

Thus Lemma 2.4.2(ii) holds for $k=0$.

Let us prove the induction step. Suppose Lemma 2.4.2(ii) holds for U_k^p. The subgraph of U_{k+1}^p induced by the vertices in $T(a)$ is the a-th copy of U_k^p. Hence

$$\sum_{1\le i\le 6p^k} H(N_{i,a}) \ge \left(3\left(\frac{p-1}{p}k+2\right)p^k - 1\right) H(s) + H(T(a)).$$

Thus for the access structure based on U^p_{k+1}

$$\sum_{0\le a\le p-1, 1\le i\le 6p^k} H(N_{i,a}) \ge \left(3\left(\frac{p-1}{p}k+2\right)p^{k+1}-p\right)H(s)+ \sum_{0\le a\le p-1} H(T(a)). \tag{2.7}$$

From Lemmas 2.1.4(i), 2.1.4(iii), and 2.4.1(i) we infer

$$\begin{aligned} &\sum_{0\le a\le p-1} H(T(a)) && (2.8)\\ =\ & H(T(0)\dots T(p-1)) + \sum_{1\le a\le p-1} I(T(0)\dots T(a-1);T(a)) \\ \ge\ & H(T(0)\dots T(p-1)) + \sum_{1\le a\le p-1} I(T(a-1);T(a)) \\ \ge\ & H(T(0)\dots T(p-1)) + (p-1)(3p^k+1)H(s). && (2.9)\end{aligned}$$

Hence, by (2.7) and (2.9),

$$\sum_{1\le i\le 6p^k, 0\le a\le p-1} H(N_{i,a}) \ge H(T(0)\dots T(p-1)) + \left(3\left(\frac{p-1}{p}(k+1)+2\right)p^{k+1}-1\right)H(s),$$

which is Lemma 2.4.2(ii) for U^p_{k+1}. Now Lemma 2.4.2(ii) follows by induction.

To prove Lemma 2.4.2(iii) let $p \ge 3$. By Lemmas 2.4.2(ii), 2.1.4(i), and 2.4.1(ii) (with $a = b$, notice that a is not congruent $a-1$ or $a-2$ modulo p since $p \ge 3$) the following inequality for graph U^p_{k+1} and $a \in \mathbb{Z}_p$ holds

$$\begin{aligned}\sum_{1\le i\le 6p^k} H(N_{i,a}) &\ge H(T(a)) + \left(3\left(\frac{p-1}{p}k+2\right)p^k-1\right)H(s)\\ &= I(T(a);T(a-1)T(a+1)) + \\ &\quad H(T(a)|T(a-1)T(a+1)) + \\ &\quad \left(3\left(\frac{p-1}{p}k+2\right)p^k-1\right)H(s)\\ &\ge (6p^k+1)H(s) + 0 + \\ &\quad \left(3\left(\frac{p-1}{p}k+2\right)p^k-1\right)H(s)\\ &= 3\left(\frac{p-1}{p}k+4\right)p^kH(s).\end{aligned}$$

This proves Lemma 2.4.2(iii).

□

From these properties the main result of this section can be derived.

Theorem 2.4.3 *Let $d \geq 3$ and $\varepsilon > 0$. Then there exists a graph G with maximum degree d and optimal worst-case and optimal average information rate satisfying*

$$\frac{2}{d+1} \leq \dot{\rho}(G) \leq \tilde{\rho}(G) \leq \frac{2}{d+1-\varepsilon}.$$

Proof: Stinson [99] proved that the optimal worst-case information rate for access structures based on graphs with maximum degree d is at least $2/(d+1)$. Let $d \geq 3$ and $\varepsilon > 0$. Select k such that $k = d-2$ and p such that $p \geq 3$ and $p \geq (d-3)/\varepsilon$. Let $v_1, \ldots, v_{6p^k}$ be the vertices of U_k^p. Then the maximum degree of U_k^p equals $k+2 = d$ (cf. Lemma 2.4.2(i)), and

$$\sum_{1 \leq i \leq 6p^k} H(v_i) \geq 3\left(\frac{p-1}{p}(k-1)+4\right) p^k H(s)$$

(Lemma 2.4.2(iii)). Hence the average information rate of U_k^p equals by definition

$$\frac{6p^k H(s)}{\sum\limits_{1 \leq i \leq 6p^k} H(v_i)} \leq \frac{2}{\frac{p-1}{p}(k-1)+4} = \frac{2}{d+1-\frac{d-3}{p}} \leq \frac{2}{d+1-\varepsilon}.$$

□

We finish this section with a recent improvement of inequality (2.9) by Blundo et al. [17]. They noticed that

$$\begin{aligned}
&\sum_{p-2 \leq a \leq p-1} I(T(0)\ldots T(a-1); T(a)) \\
= \;& I(T(0)\ldots T(p-3); T(p-2)) + \\
& I(T(0)\ldots T(p-3); T(p-1)|T(p-2)) + I(T(p-2); T(p-1)) \\
= \;& I(T(0)\ldots T(p-3); T(p-1)T(p-2)) + I(T(p-2); T(p-1)) \\
\geq \;& (6p^k+1)H(s) + (3p^k+1)H(s),
\end{aligned}$$

by Lemmas 2.4.1(i) and 2.4.1(ii) (with $a = 0$ and $b = p-3$). This improvement leads to

$$\sum_{0 \leq a \leq p-1} H(T(a)) \geq H(T(0)\ldots T(p-1)) + (p(3p^k+1)-1)H(s)$$

with which Lemma 2.4.2(ii) and 2.4.2(iii) can be improved to:

$$\begin{aligned}
\sum_{1 \leq i \leq 6p^k} H(v_i) \;&\geq\; H(v_1 \ldots v_{6p^k}) + \left(3\,(k+2)\,p^k - 1\right) H(s), \text{ and} \\
\sum_{1 \leq i \leq 6p^k} H(v_i) \;&\geq\; 3\,(k+3)\,p^k H(s).
\end{aligned}$$

Using the last inequality in the proof of Theorem 2.4.3 gives $\tilde{\rho}(U_k^p) \leq 2/(d+1)$, where $d = k+2$ is the maximum degree of U_k^p.

Chapter 3

Linear Construction of Schemes

Let Γ be a complete access structure on $\mathcal{P}$ and let q be a prime power. A secret sharing scheme is linear if each qualified group can reconstruct the secret by linearly combining the parts of the shares of the participants in the qualified group. One of the first linear constructions is the *vector space construction* due to Brickell [25]. Brickell proved the following result. Let l be an integer, and let $\mathbf{e}^i$ be the i-th unit vector in $GF(q)^l$. Suppose we have vectors $\mathbf{v}^i \in GF(q)^l$, $i \in \mathcal{P}$, such that the linear span of vectors $\mathbf{v}^i$, $i \in X$, contains $\mathbf{e}^1$ iff $X \in \Gamma$. Then we can construct an ideal scheme for Γ with set of possible secrets $GF(q)$. The method to construct such an ideal scheme is called the vector space construction.

In this chapter, we generalize the vector space construction. This type of generalization, started by Bertilsson [9], leads to secret sharing schemes with rational information rates in which the secret can be computed efficiently by each qualified group. A one-to-one correspondence between the generalized construction and linear block codes is stated. It turns out that the approach of minimal codewords by Massey [80], and the construction of Bertilsson and Ingemarsson [10] are special cases of this construction.

Let $n = |\mathcal{P}|$, q be a prime power, and the numbers k, p_i, $1 \leq i \leq n$, be integers. We prove that there exists a generalized vector space construction for access structure (Γ, Δ) and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$ iff there exists a generalized vector space construction for $(\Gamma^\perp, \Delta^\perp)$ and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$. First Jackson and Martin [57] and later Van Dijk [41] proved this result for complete access structures. The generalization towards incomplete access structures is joint work with Wen-Ai Jackson and Keith Martin. We have produced a different proof using geometry and matroid theory [51].

A sufficient and necessary condition for the existence of a generalized vector space construction for access structure (Γ, Δ) in terms of matrices is given. Based on this result a sharp combinatorial upper bound of the worst-case information rate of linear schemes for a given complete access structure is presented in [48]. As a side-result the duality result for incomplete access structures follows immediately.

We present an outline of an algorithm for determining whether a secret sharing scheme for (Γ, Δ) and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$ can be realized by means of the generalized vector space construction. If so, the algorithm produces a secret sharing scheme with this convec. This algorithm will be applied in Chapter 4.

3.1 The Generalized Vector Space Construction

We denote the vector space of all k-tuples over $GF(q)$, where q is a prime power, by $GF(q)^k$. Let the set of possible secrets be

$$\mathcal{S} = GF(q)^k.$$

In the remainder of this chapter $\mathcal{P} = \{1, \ldots, n\}$ and (Γ, Δ) is an access structure on $\mathcal{P}$.

Let each participant $i \in \mathcal{P}$ have an $l \times p_i$ matrix G_i over $GF(q)$ with full column rank, where l is some integer satisfying $l \geq k$. These matrices are not secret, they are public knowledge. Suppose an MTA wants to share a secret $\mathbf{s} \in \mathcal{S}$ according to a uniform probability distribution. Then the MTA uniformly chooses a vector $\mathbf{a} \in GF(q)^{l-k}$ and distributes securely to participant $i \in \mathcal{P}$ the share

$$(\mathbf{s}, \mathbf{a})G_i,$$

where $(\mathbf{s}, \mathbf{a})$ is the vector $\mathbf{s}$ concatenated with the vector $\mathbf{a}$. Vector $\mathbf{a}$ is kept secret from each participant by the MTA. It is not public knowledge. We call this construction of a secret sharing scheme *the generalized vector space construction* based on matrices G_i, $i \in \mathcal{P}$. We notice that for all $i \in \mathcal{P}$ the matrix G_i is publicly accessible and is not part of the share of participant i. One can share a sequence of secrets, $\mathbf{s}^1, \mathbf{s}^2, \ldots \in \mathcal{S}$, by repeatedly using the same scheme. That is, the MTA uses matrices G_i and arbitrary chosen vectors $\mathbf{a}^1, \mathbf{a}^2, \ldots \in GF(q)^{l-k}$ to distribute to participant i its share consisting of vectors $(\mathbf{s}^j, \mathbf{a}^j)G_i$, $j = 1, 2, \ldots$.

Example 3.1.1 Let us consider the access structure based on the graph depicted in Figure 3.1. Suppose we want to share a secret $\mathbf{s} = (s_1, s_2)$, $k = 2$. To that end we select $l = 8$, take all p_i's equal to 3 and use

$$G[\mathcal{P}] = \left(\; G_1 \; \middle| \; \ldots \; \middle| \; G_6 \; \right) =$$

$$\left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
\hline
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right).$$

So, after choosing a vector $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5, a_6)$ at random, we distribute to

- participant 1 the share $(\mathbf{s}, \mathbf{a})G_1 = (s_1 + a_1, s_2 + a_3, a_6)$ $(p_1 = 3)$,
- participant 2 the share $(\mathbf{s}, \mathbf{a})G_2 = (a_1, s_1 + s_2 + a_2 + a_4, s_2 + a_6)$ $(p_2 = 3)$,
- participant 3 the share $(\mathbf{s}, \mathbf{a})G_3 = (a_2, a_4, s_1 + a_1)$ $(p_3 = 3)$,
- participant 4 the share $(\mathbf{s}, \mathbf{a})G_4 = (s_2 + a_4, s_1 + a_2, a_5)$ $(p_4 = 3)$,
- participant 5 the share $(\mathbf{s}, \mathbf{a})G_5 = (s_1 + s_2 + a_1 + a_3, a_4, s_1 + a_5)$ $(p_5 = 3)$,
- participant 6 the share $(\mathbf{s}, \mathbf{a})G_6 = (a_1, s_2 + a_4, a_3)$ $(p_6 = 3)$.

Let us consider edge $\{1, 6\}$. The combination of participants 1 and 6 can obtain s_1 by subtracting a_1 from $s_1 + a_1$, and s_2 by subtracting a_3 from $s_2 + a_3$. In a similar way the reader can prove that all qualified groups of the access structure based on the graph in Figure 3.1 can reconstruct the secret.

The maximal forbidden subsets are $\{1, 3, 5\}, \{2, 4, 6\}, \{1, 4\}$, and $\{2, 5\}$. Let us consider the forbidden group $\{1, 4\}$. The combination of participants 1 and 4 can not obtain any linear combination of s_1 and s_2, since the components of their shares contain different a_i. Since all a_i are uniformly distributed the shares of participants 1 and 4 together give no information about $\mathbf{s}$. Therefore the forbidden group $\{1, 4\}$ can do no better than guessing $\mathbf{s}$ according to its uniform probability distribution. In a similar way the reader can prove that each forbidden group can do no better than guessing $\mathbf{s}$ according to its uniform probability distribution. Notice the resemblance of the arguments used here and used in Example 1.1.1.

Each share consists of 3 q-ary symbols while the secret consists of 2 q-ary symbols. Hence the worst-case information rate, as well as the average information rate, is 2/3.

The previous example shows that it is very difficult to check whether the generalized vector space construction based on matrices G_i, $i \in \mathcal{P}$, leads to a scheme for (Γ, Δ). Furthermore we do not have a method to construct matrices G_i. Given an arbitrary access structure (Γ, Δ) the best we can do is to search for matrices G_i for which the generalized vector space construction

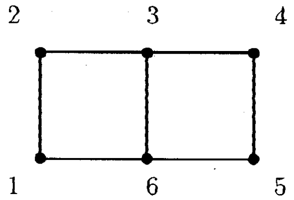


Figure 3.1: Graph

gives rise to a scheme for (Γ, Δ) with optimal information rates. These are pessimistic thoughts. In the remainder of this chapter we will carefully analyse the generalized vector space construction. This will lead to an exhaustive search algorithm with backtracking (which will be applied in Chapter 4) and a duality result.

In the following theorem sufficient and necessary conditions are given in order to be able to define a secret sharing scheme for (Γ, Δ) by means of the generalized vector space construction. For perfect secret sharing schemes the theorem has already been mentioned in [44] and independently been proved by Van Dijk in [41] and by Blakley and Kabatianskii in [13].

Theorem 3.1.2 *For $1 \leq i \leq n$ let G_i be an $l \times p_i$ matrix over $GF(q)$ with full column rank. For $X = \{i_1, \ldots, i_m\} \subseteq \mathcal{P}$, with $i_1 < \ldots < i_m$, we define the $l \times p[X]$ matrix $G[X]$ over $GF(q)$, with $p[X] = \sum\limits_{i \in X} p_i$, by*

$$G[X] = \left(\; G_{i_1} \; \middle| \cdots \middle| \; G_{i_m} \; \right).$$

The generalized vector space construction based on the matrices $G_i, i \in \mathcal{P}$, defines a secret sharing scheme for access structure (Γ, Δ) on $\mathcal{P}$ and set of possible secrets $\mathcal{S} = GF(q)^k$ iff

[V1] for all $X \in \Gamma$ the unit vectors $\mathbf{e}^i \in GF(q)^l$ for $1 \leq i \leq k$ can be expressed as a linear combination of the columns of matrix $G[X]$, and

[V2] for all $X \in \Delta$ none of the non-zero linear combinations of $\{\mathbf{e}^1, \ldots, \mathbf{e}^k\}$ can be expressed as a linear combination of the columns of matrix $G[X]$.

The corresponding secret sharing scheme has convec $(p_1/k, \ldots, p_n/k)$, worst-case information rate $k/\max\{p_i : i \in \mathcal{P}\}$, and average information rate $k/\frac{1}{|\mathcal{P}|}\sum_{i \in \mathcal{P}} p_i$.

Let $p_i = 1$ for $i \in \mathcal{P}$ and let $k = 1$. Then conditions [V1] and [V2] for complete access structures are equivalent to the condition that $\mathbf{e}^1$ is a linear combination of the columns of $G[X]$, iff $X \in \Gamma$. This is the *vector space* *construction* due to Brickell [25]. Further we notice that the construction of Bertilsson and Ingemarsson [10] (see also [9]) is the generalized vector space construction for complete access structures in which $k = 1$.

Example 3.1.1 and the following example illustrate the generalized vector space construction. In Example 3.1.1 it suffices to check [V1] for all edges and to check [V2] for all maximal forbidden subsets. The reader is invited to do this and to conclude that the sharing of secrets in this example is a perfect secret sharing scheme according to Theorem 3.1.2.

Example 3.1.3 Let us consider the access structure based on the graph depicted in Figure 3.2. Suppose we want to share a secret $\mathbf{s} = (s_1, s_2)$, $k = 2$. To that end we select $l = 7$ and use

$$G[\mathcal{P}] = (\ G_1 \,|\, \ldots \,|\, G_6\ ) =$$

$$\left(\begin{array}{ccc|ccc|ccc|ccc|ccc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right).$$

So, after choosing a vector $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5)$ at random, we distribute to

- participant 1 the share $(\mathbf{s}, \mathbf{a})G_2 = (s_1 + a_3, s_2 + a_2, a_4)$ $(p_2 = 3)$,
- participant 2 the share $(\mathbf{s}, \mathbf{a})G_1 = (a_1, a_2, a_3)$ $(p_1 = 3)$,
- participant 3 the share $(\mathbf{s}, \mathbf{a})G_3 = (s_1 + a_1, s_2 + a_2, a_5)$ $(p_3 = 3)$,
- participant 4 the share $(\mathbf{s}, \mathbf{a})G_4 = (s_1 + a_5, a_2, a_3 + a_4)$ $(p_4 = 3)$,
- participant 5 the share $(\mathbf{s}, \mathbf{a})G_5 = (s_2 + a_4, a_3, a_5)$ $(p_5 = 3)$,
- participant 6 the share $(\mathbf{s}, \mathbf{a})G_6 = (s_1 + a_3 + a_5, a_4)$ $(p_6 = 2)$.

The reader is invited to verify [V1] and [V2]. The worst-case information rate of this scheme is 2/3 and the average information rate is 12/17. The worst-case information rate is optimal (see Corollary 2.2.2).

We notice that $s_1, s_2, a_1, \ldots$ are in $GF(q)$ in the schemes of the previous examples. Only additions and subtractions are needed by qualified groups to reconstruct the secret. So, w.l.o.g. we can take $s_1, s_2, a_1, \ldots$ from the integer ring $\mathbb{Z}_m$ in Examples 3.1.1 and 3.1.3.

A set of matrices $G_i, i \in \mathcal{P}$, is said to be *suitable* (to define a secret sharing scheme) for access structure (Γ, Δ) on $\mathcal{P}$ if conditions [V1] and [V2] are satisfied. Below we will prove that the generalized vector space construction based

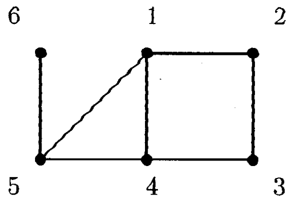


Figure 3.2: Graph

on a suitable set of matrices G_i for (Γ, Δ) leads to a secret sharing scheme for (Γ, Δ). Secondly, we prove that conditions [V1] and [V2] are necessary as well, i.e., we prove the right to left implication of Theorem 3.1.2. In the next section we present a description of suitable sets of matrices in terms of codes. This will lead to a backtracking algorithm that searches for suitable sets of matrices. We will derive this algorithm in Section 3.4. A duality result will be presented in Section 3.5.

Proof of Theorem 3.1.2 $\Leftarrow$: Let the set of matrices G_i, $1 \leq i \leq n$, be suitable for (Γ, Δ). We will prove that the generalized vector space construction based on the matrices G_i, $1 \leq i \leq n$, leads to a secret sharing scheme ν for (Γ, Δ).

Let X be a qualified subset. We will show that the participants in X together can compute the secret $\mathbf{s}$. The participants in X can construct $(\mathbf{s}, \mathbf{a})G[X]$, because they know $(\mathbf{s}, \mathbf{a})G_i$, for all $i \in X$. All unit vectors $\mathbf{e}^i$ for $1 \leq i \leq k$ can be written as linear combinations of columns in $G[X]$ (cf. [V1]). Hence, the participants in X can compute a matrix B such that

$$\begin{pmatrix} I_k \\ O \end{pmatrix} = G[X]B,$$

where I_k denotes the $k \times k$ identity matrix, and O denotes the all zero matrix of size $(l - k) \times k$. Hence

$$\mathbf{s} = (\mathbf{s}, \mathbf{a})G[X]B.$$

Thus the participants in X can efficiently compute $\mathbf{s}$ by combining their shares and their knowledge of the public matrices G_i for $i \in X$, so $H(s_\nu|X_\nu) = 0$, i.e., [SS1] is satisfied.

Let us check [SS2]. Let X be a forbidden subset. Let $\mathbf{s}$ be the secret shared among the participants by selecting a random vector $\mathbf{a}$. Then the shares distributed among the participants in X are given by the vector $(\mathbf{s}, \mathbf{a})G[X] = \mathbf{c}$. We will show that for each $\mathbf{s}' \in \mathcal{S}$ there are equally many vectors $\mathbf{a}'$ such that $(\mathbf{s}', \mathbf{a}')G[X] = \mathbf{c}$. This implies that $\nu_{sX}(\mathbf{s}'\mathbf{c})$ equals $\nu_s(\mathbf{s}')$

times a factor independent of $\mathbf{s}'$, and hence $\nu_{s|X}(\mathbf{s}'|\mathbf{c}) = \nu_s(\mathbf{s}')$. As a consequence $H(s_\nu|X_\nu) = H(s_\nu)$, i.e., the combination of the shares given to the participants in X will contain no information about $\mathbf{s}$, hence, [SS2] is satisfied.

We denote by e the dimension of the linear span of the columns of $G[X]$. By $G[X]^1$ we denote the matrix consisting of the first k rows of $G[X]$. By $G[X]^2$ we denote the matrix consisting of the last $l-k$ rows of $G[X]$. Hence

$$G[X] = \begin{pmatrix} G[X]^1 \\ G[X]^2 \end{pmatrix}.$$

From [V2] we infer that for all $\mathbf{b} \in GF(q)^{p[X]}$ if $G[X]^2\mathbf{b}^T = \mathbf{0}$ then $G[X]\mathbf{b}^T = \mathbf{0}$. Thus the rank of matrix $G[X]$, say e, equals the rank of matrix $G[X]^2$. Hence, the rows of matrix $G[X]^1$ are linear combinations of the rows of matrix $G[X]^2$.

Choose any $\mathbf{s}' \in S$, and consider the system of equations

$$(\mathbf{s}', \mathbf{a}')G[X] = \mathbf{c},$$

which is equivalent to

$$\mathbf{a}'G[X]^2 = \mathbf{c} - \mathbf{s}'G[X]^1.$$

This is a system of linear equations in the $l-k$ unknowns given by the coordinates of $\mathbf{a}'$. The coefficient matrix $G[X]^2$ has rank e. This system of linear equations is not conflicting, since there exists a vector $\mathbf{a}''$ such that $\mathbf{a}''G[X]^2 = (\mathbf{s} - \mathbf{s}')G[X]^1$, and hence $(\mathbf{a} + \mathbf{a}'')G[X]^2 = \mathbf{c} - \mathbf{s}'G[X]^1$. So, the solution space has dimension $l-k-e$. Thus there are q^{l-k-e} solutions $\mathbf{a}'$. This number is independent of the value of $\mathbf{s}'$ (notice that $\nu_{sX}(\mathbf{s}'\mathbf{c}) = \nu_s(\mathbf{s}')q^{-e}$). Hence X does not obtain any additional knowledge about the secret, so $H(s_\nu|X_\nu) = H(s_\nu)$.

We conclude that the generalized vector space construction describes a secret sharing scheme. Since $|[s]_\nu| = q^k$, $|[i]_\nu| = q^{p_i}$, $i \in \mathcal{P}$, (matrix G_i has full column rank) and the secret and each of the shares is uniformly distributed the convec equals $(p_1/k, \ldots, p_n/k)$, the worst-case information rate equals $k/\max\{p_i : i \in \mathcal{P}\}$, and the average information rate equals $k/\frac{1}{|\mathcal{P}|}\sum_{i\in\mathcal{P}} p_i$.

□

Proof of Theorem 3.1.2 ⇒: Let G_i, $1 \le i \le n$, form a set of matrices such that either [V1] or [V2] is not valid. In both cases we will prove that the generalized vector space construction based on the matrices G_i, $1 \le i \le n$, does not lead to a secret sharing scheme for (Γ, Δ).

Suppose that condition [V1] is not valid. I.e., there exists an $X \in \Gamma$ and a unit vector $\mathbf{e}^j \in GF(q)^l$, for some $1 \le j \le k$, such that $\mathbf{e}^j$ is not a linear combination of the columns of matrix $G[X]$. We will prove that the generalized vector space construction based on the matrices G_i, $1 \le i \le n$, does not lead to a secret sharing scheme by showing that $H(s_\nu|X_\nu) > 0$.

Suppose that there exist vectors $\mathbf{s}'' \in GF(q)^k \setminus \{\mathbf{0}\}$ and $\mathbf{a}'' \in GF(q)^{l-k}$ such that

$$\mathbf{s}''G[X]^1 = \mathbf{a}''G[X]^2. \tag{3.1}$$

Then there exist vectors $\mathbf{s} \neq \mathbf{s}' \in GF(q)^k$ and $\mathbf{a}, \mathbf{a}' \in GF(q)^{l-k}$ such that

$$(\mathbf{s}, \mathbf{a})G[X] = (\mathbf{s}', \mathbf{a}')G[X].$$

Thus there remains some uncertainty about the secret given the shares of the participants in X ($\mathbf{s}$ can not always uniquely be determined), i.e. $H(s_\nu|X_\nu) > 0$. So, it is enough to prove that (3.1) holds given the non-validity of [V1], or equivalently the non-validity of (3.1) implies [V1].

W.l.o.g. let

$$G[X]^2 = \begin{pmatrix} G[X]^{2.1} \\ G[X]^{2.2} \end{pmatrix}$$

where the rows of $G[X]^{2.1}$ are independent of each other and where the rows of $G[X]^{2.2}$ are linear combinations of the rows of $G[X]^{2.1}$. In other words $G[X]^{2.1}$ has full rank and $G[X]^{2.2} = EG[X]^{2.1}$ for some matrix E. Suppose that (3.1) is not valid. Then

$$\mathbf{s}''G[X]^1 = \mathbf{a}''G[X]^2 \Rightarrow \mathbf{s}'' = \mathbf{0}$$

for all $\mathbf{s}'' \in GF(q)^k$ and $\mathbf{a}'' \in GF(q)^{l-k}$. From this (by taking $\mathbf{a}'' = \mathbf{0}$) we infer that $G[X]^1$ has full row rank. Further this implies that no non-zero linear combination of rows of $G[X]^1$ can be written as linear combination of rows of $G[X]^2$. Thus matrix

$$G[X]^3 = \begin{pmatrix} G[X]^1 \\ G[X]^{2.1} \end{pmatrix}$$

has full row rank. We observe the equality of the following quantities: the length of the columns of $G[X]^3$, the number of rows of $G[X]^3$, the row rank of $G[X]^3$, the column rank of $G[X]^3$, and the dimension of the column space of $G[X]^3$. This implies that for $1 \leq j \leq k$ the j-th unit vector is a linear combination of the columns of $G[X]^3$. Thus $G[X]^1\mathbf{b}^T = \mathbf{e}^j$, where e^j is the j-th unit vector in $GF(q)^k$, and $G[X]^{2.1}\mathbf{b}^T = \mathbf{0}$ for some vector $\mathbf{b}$. Hence,

$$G[X]\mathbf{b}^T = \begin{pmatrix} G[X]^1 \\ G[X]^{2.1} \\ G[X]^{2.2} \end{pmatrix} \mathbf{b}^T = \begin{pmatrix} G[X]^1\mathbf{b}^T \\ G[X]^{2.1}\mathbf{b}^T \\ EG[X]^{2.1}\mathbf{b} \end{pmatrix} = (\mathbf{e}^j|\mathbf{0}|\mathbf{0})^T,$$

the transpose of the j-th unit vector in $GF(q)^l$. We conclude that [V1] holds. Thus the non-validity of (3.1) implies [V1]. We conclude that the generalized vector space construction based on the matrices G_i, $1 \leq i \leq n$, does not lead to a secret sharing scheme for (Γ, Δ) if [V1] does not hold.

Suppose that condition [V2] is not valid. I.e., there exists an $X \in \Delta$ and vectors $\mathbf{s}' \in GF(q)^k \setminus \{\mathbf{0}\}$ and $\mathbf{b} \in GF(q)^{p[\mathcal{P}]}$ such that $(\mathbf{s}', \mathbf{0})^T = G[X]\mathbf{b}^T$. Suppose that the secret $\mathbf{s}$ has been shared. Then the participants of X know $(\mathbf{s}, \mathbf{a})G[X]$ for some $\mathbf{a} \in GF(q)^{l-k}$. Since matrix $G[X]$ is public knowledge the participants of X can compute vectors $\mathbf{s}'$ and $\mathbf{b}$. Thus they are able to reconstruct

$$(\mathbf{s}, \mathbf{a})G[X]\mathbf{b}^T = (\mathbf{s}, \mathbf{a})(\mathbf{s}', \mathbf{0})^T = \mathbf{s}\mathbf{s}'^T.$$

I.e., the participants of X obtain some information about the secret $\mathbf{s}$. In other words $H(s_\nu|X_\nu) < H(s_\nu)$. Hence, the generalized vector space construction based on the matrices G_i, $1 \leq i \leq n$, does not lead to a secret sharing scheme for (Γ, Δ).

□

3.2 Code Description

For a suitable set of matrices G_i, $i \in \mathcal{P}$, for (Γ, Δ) we define the corresponding linear block code $\mathcal{C}$ of length $k + p[\mathcal{P}]$ over $GF(q)$ by its parity check matrix

$$H = \left(\begin{array}{c|c} I_k & \\ O & G[\mathcal{P}] \end{array} \right). \tag{3.2}$$

In this section we characterize these codes. We start with some definitions.

Definition 3.2.1 *Let $\mathbf{c}^i$ be in $GF(q)^{p_i}$, $1 \leq i \leq n$, and $\mathbf{c} = (\mathbf{c}^1, \ldots, \mathbf{c}^n) \in GF(q)^{p[\mathcal{P}]}$. The p-support of vector $\mathbf{c}$, $supp_p(\mathbf{c})$, is defined as the set of coordinates $i, 1 \leq i \leq n$, for which $\mathbf{c}^i \neq \mathbf{0}$, i.e.*

$$supp_p(\mathbf{c}) = \{i : \mathbf{c}^i \neq \mathbf{0}\}.$$

Let $X = \{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$, with $i_1 < \ldots < i_m$. Then the projection of vector $\mathbf{c}$ on X, $\mathbf{c}_X$ for short, is defined as

$$\mathbf{c}_X = (\mathbf{c}^{i_1}, \ldots, \mathbf{c}^{i_m}).$$

We notice that $\mathbf{c} = \mathbf{c}_{\mathcal{P}}$.

Definition 3.2.2 *Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, \ldots, n\}$ and let $\mathcal{S} = GF(q)^k$ be a set of possible secrets. Let $[\Gamma]^- = \{X_1, \ldots, X_r\}$. Let p_i, $1 \leq i \leq n$, be integers. We define $\mathcal{E}$ as $\mathcal{E} = \{(i,j) : 1 \leq i \leq r, 1 \leq j \leq k\}$. Then a set of vectors $C = \{\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]} : (i,j) \in \mathcal{E}\}$ is said to be suitable (to define a secret sharing scheme) for access structure (Γ, Δ) and set of possible secrets $GF(q)^k$ if C satisfies*

[C1] the $g(\Gamma)$-property: $supp_p(\mathbf{c}^{i,j}) \subseteq X_i$ for all $(i,j) \in \mathcal{E}$, and

[C2] the $d^-(\Delta)$-property: for each $r \times k$ q-ary matrix B with the property that the elements of at least one column in B do not add up to 0 (so, that column is not orthogonal to the all-one vector) there exists a minimal set X of Δ^c ($X \in [\Delta^c]^-$, for its definition see Section 1.1.1) such that

$$X \subseteq sup_p\left(\sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j}\right).$$

In [C1] and [C2] we defined the $g(\Gamma)$-property and $d^-(\Delta)$-property. Both properties should be regarded as boolean functions of Γ and Δ. For instance in Section 3.5 we will talk about the $g(\Gamma^\perp)$-property and $d^-(\Delta^\perp)$-property: the $g(.)$-property and $d^-(.)$-property for the dual access structure. In Section 3.3 we will define the $d^+(.)$-property, which is the reason to write $d^-(.)$-property in Definition 3.2.2.

Example 3.2.3 Let Γ be a complete access structure on $\mathcal{P} = \{1,2,3,4\}$ defined by its minimal elements $X_1 = 12$, $X_2 = 34$, and $X_3 = 23$, so $r = 3$. Then $[\Delta^c]^- = \{12, 34, 23\}$ since $\Gamma = \Delta^c$. Let $q = 2$, $k = 2$, $p_1 = p_4 = 2$, and $p_2 = p_3 = 3$. We define

$$\begin{aligned}
\mathbf{c}^{1,1} &= (10|100|000|00)\\
\mathbf{c}^{2,1} &= (00|000|100|10)\\
\mathbf{c}^{3,1} &= (00|100|001|00)\\
\mathbf{c}^{1,2} &= (01|010|000|00)\\
\mathbf{c}^{2,2} &= (00|000|010|01)\\
\mathbf{c}^{3,2} &= (00|001|010|00).
\end{aligned}$$

Let $C = \{\mathbf{c}^{i,j} : (i,j) \in \mathcal{E}\}$. Clearly, C has the $g(\Gamma)$-property. For instance, $\mathbf{c}^{2,1}$ has p-support $\{3,4\}$ which is indeed contained in X_2. Let us check the $d^-(\Gamma^c)$-property. Let B be a q-ary $r \times k$, i.e. 3×2, matrix. Then

$$\begin{aligned}
\mathbf{c} &:= \sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j}\\
&= (B_{1,1}, B_{1,2}|B_{1,1} + B_{3,1}, B_{1,2}, B_{3,2}|B_{2,1}, B_{2,2} + B_{3,2}, B_{3,1}|B_{2,1}, B_{2,2}).
\end{aligned}$$

The maximal elements of Γ^c are 13, 14, and 24. Suppose that $sup_p(\mathbf{c}) \subseteq 13$. Then $B_{1,1} + B_{3,1} = B_{1,2} = B_{3,2} = B_{2,1} = B_{2,2} = 0$. Hence, $B_{1,1} + B_{2,1} + B_{3,1} = B_{1,2} + B_{2,2} + B_{3,2} = 0$. Thus both columns of B add up to 0. In general we can prove that if there exists an $X \in [\Gamma^c]^+$ such that $sup_p(\mathbf{c}) \subseteq X$ then both columns of B add up to 0. Therefore, if at least one of the columns of B do not add up to 0 then there exists an $X \in [\Gamma]^-$ such that $X \subseteq sup_p(\mathbf{c})$. We conclude that the $d^-(\Gamma^c)$-property is satisfied as well, and that C is a suitable set of vectors for Γ.

Example 3.2.4 Let $k = 1$, and $p_i = 1$ for $i \in \mathcal{P} = \{1, \dots n\}$. Notice that these parameters correspond to the vector space construction. Let $\mathcal{C}$ be a linear code of length $n+1$ over $GF(q)$. We define the *support* of a codeword $\mathbf{c} = (c_0, \dots, c_n)$ as $sup(\mathbf{c}) = \{0 \le i \le n : c_i \ne 0\}$. Massey [80] defines a non zero codeword $\mathbf{c}$ to be *minimal* if

(i) no other codeword has a support properly contained in $sup(\mathbf{c})$ and

(ii) its leftmost non-zero component is a 1.

We leave it to the reader to check that for any $\mathbf{c} \in \mathcal{C}$ there exists a minimal code word $\mathbf{c}'$ with $sup(\mathbf{c}') \subseteq sup(\mathbf{c})$.

Let $C = \{\mathbf{c}^{1,1}, \dots, \mathbf{c}^{r,1}\}$ be the set of words $(c_1, \dots, c_n)$ for which $(1, c_1, \dots, c_n) \in \mathcal{C}$ is minimal. Let Γ be a complete access structure such that $[\Gamma]^-$ consists of all elements $X_i = sup((1, \mathbf{c}^{i,1})) \setminus \{0\}$, $1 \le i \le r$. Then C satisfies the $g(\Gamma)$-property since $sup_p(\mathbf{c}^{i,1}) = X_i$, $1 \le i \le r$.

We will now show that besides [C1] also [C2] is satisfied. Let B be an $r \times k$ q-ary matrix such that the elements of at least one column in B do not add up to 0. Because $k = 1$ matrix B has only 1 column. Hence, $\sum_{(i,j)\in\mathcal{E}} B_{i,j} \ne 0$, where $\mathcal{E} = \{(i, 1) : 1 \le i \le r\}$. Thus there exists an m such that $sup((1, \mathbf{c}^{m,1})) \subseteq sup(\sum_{(i,j)\in\mathcal{E}} B_{i,j}(1, \mathbf{c}^{i,j}))$ for some minimal code word $(1, \mathbf{c}^m)$. Hence, $X_m \subseteq sup_p(\sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j})$. In other words C satisfies the $d^-(\Gamma^c)$-property. We conclude that C is a suitable set of vectors for Γ and set of possible secrets $GF(q)$.

We will not give more examples of suitable sets of vectors since only computers recognize the suitability of such sets. The purpose of the code description is to derive the search algorithm in Section 3.4. The following two theorems show how a suitable set of matrices defines a suitable set of vectors and vice versa. The proofs of both theorems are postponed to the end of this section.

Theorem 3.2.5 *Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, \dots, n\}$ and let $\mathcal{S} = GF(q)^k$ be a set of possible secrets. Let $[\Gamma]^- = \{X_1, \dots, X_r\}$ and let $\mathcal{E} = \{(i, j) : 1 \le i \le r, 1 \le j \le k\}$. Let G_i, $1 \le i \le n$, be $l \times p_i$ matrices over $GF(q)$ such that the set of matrices G_i is suitable for access structure (Γ, Δ) and set of possible secrets $GF(q)^k$. Then there exists a suitable set of vectors $\{\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]} : (i,j) \in \mathcal{E}\}$ for (Γ, Δ) and set of possible secrets $GF(q)^k$ such that $G'H^T = O$, where*

$$H = \left(\begin{array}{c|c} I_k & \\ O & G[\mathcal{P}] \end{array} \right),$$

and G' is a generator matrix of the code defined by the linear span of the vectors $(\mathbf{e}^j, \mathbf{c}^{i,j})$, $(i, j) \in \mathcal{E}$.

Theorem 3.2.6 *Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, \ldots, n\}$. Let $[\Gamma]^- = \{X_1, \ldots, X_r\}$ and let $\mathcal{E} = \{(i,j) : 1 \leq i \leq r, 1 \leq j \leq k\}$. Let the vectors $\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]}$, $(i,j) \in \mathcal{E}$, define a suitable set of vectors for (Γ, Δ) and set of possible secrets $GF(q)^k$. Let H be a parity check matrix of the code defined by the linear span of the vectors $(\mathbf{e}^j, \mathbf{c}^{i,j})$, $(i,j) \in \mathcal{E}$. W.l.o.g. H is of the form*

$$H = \left(\begin{array}{c|c} \begin{matrix} I_k \\ O \end{matrix} & H' \end{array} \right).$$

Then the set of matrices G_i, $1 \leq i \leq n$, defined by $G[\mathcal{P}] = H'$ is suitable for (Γ, Δ) and set of possible secrets $GF(q)^k$.

Example 3.2.7 We continue with Example 3.2.3. Let $\mathcal{C}$ be the code defined by the linear span of the vectors $(\mathbf{e}^j, \mathbf{c}^{i,j})$, $(i,j) \in \mathcal{E}$. Then $\mathcal{C}$ has generator matrix

$$\left(\begin{array}{c|c} 10 & \mathbf{c}^{1,1} \\ 10 & \mathbf{c}^{2,1} \\ 10 & \mathbf{c}^{3,1} \\ 01 & \mathbf{c}^{1,2} \\ 01 & \mathbf{c}^{2,2} \\ 01 & \mathbf{c}^{3,2} \end{array} \right).$$

Its parity check matrix can be written as

$$H = \left(\begin{array}{c|c} \begin{matrix} I_k \\ O \end{matrix} & H' \end{array} \right)$$

with

$$H' = \left(\begin{array}{cc|ccc|ccc|cc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{array} \right).$$

By Theorem 3.2.6 the set of matrices G_i, $1 \leq i \leq n$, defined by $G[\mathcal{P}] = H'$ is suitable for Γ and set of possible secrets $GF(q)^k$. The reader is invited to verify [V1] and [V2].

Example 3.2.8 Theorem 3.2.6 can be applied in Example 3.2.4. Let H be the parity check matrix of the subcode of $\mathcal{C}$ defined as the linear span of the minimal code words of $\mathcal{C}$ with leftmost coordinate equal to 1. Then the set of columns of H, except for the first column, is a suitable set of matrices for Γ and set of possible secrets $GF(q)$. The generalized vector space construction can be used to obtain a perfect secret sharing scheme for Γ and set of possible secrets $GF(q)$, see Theorem 3.1.2. This shows that the approach of minimal code words by Massey [80] is a particular case of the vector space construction.

Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, \ldots, n\}$. Let numbers k, q, and p_i, $1 \leq i \leq n$, be fixed. Then the combination of Theorems 3.2.5, 3.2.6, and Theorem 3.1.2 tells us that there exists a generalized vector space construction, with parameters k, q, and p_i, $1 \leq i \leq n$, leading to a secret sharing scheme for (Γ, Δ) and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$ iff there exists a suitable set of vectors for (Γ, Δ) and set of possible secrets $GF(q)^k$ with parameters p_i, $1 \leq i \leq n$. Given such a suitable set of vectors one can obtain efficiently a corresponding secret sharing scheme (see Theorem 3.2.6). In the coming sections we will concentrate on the search for suitable sets of vectors for (Γ, Δ) and set of possible secrets $GF(q)^k$ with parameters p_i, $1 \leq i \leq n$. The $g(\Gamma)$-property is in general easy to satisfy. The $d^-(\Delta)$-property is difficult to satisfy and will be discussed further in the next section.

We finish this section with the proofs of Theorems 3.2.5 and 3.2.6.

Proof of Theorem 3.2.5: We are going to investigate the structure of $\mathcal{C}$ defined by (3.2). We infer from [V1] that for $(i, j) \in \mathcal{E}$ there exists a vector $\mathbf{b}^{i,j} \in GF(q)^{p[X_i]}$ such that $(\mathbf{e}^j, \mathbf{0})^T = G[X_i]\mathbf{b}^{i,j^T}$, where $\mathbf{e}^j$ is the j-th unit vector in $GF(q)^k$. Let $\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]}$ be the vector defined by $\mathbf{c}^{i,j}_{X_i} = -\mathbf{b}^{i,j}$ and $sup_p(\mathbf{c}^{i,j}) \subseteq X_i$ (i.e. $\mathbf{c}^{i,j}_{X_i^c} = \mathbf{0}$). Then $H(\mathbf{e}^i, \mathbf{c}^{i,j})^T = \mathbf{0}^T$, and hence $G'H^T = O$, where G' is a generator matrix of the code defined by the linear span of the vectors $(\mathbf{e}^j, \mathbf{c}^{i,j})$, $(i, j) \in \mathcal{E}$. We will prove that $C = \{\mathbf{c}^{i,j} : (i, j) \in \mathcal{E}\}$ is a suitable set of vectors. Note that we have constructed C such that the $g(\Gamma)$-property is satisfied.

Let $B_{i,j} \in GF(q)$ for $(i, j) \in \mathcal{E}$. Then the linear combination

$$(\mathbf{s}, \mathbf{c}) = \sum_{(i,j)\in\mathcal{E}} B_{i,j}(\mathbf{e}^j, \mathbf{c}^{i,j}) = (\sum_{1\leq i\leq r} B_{i,1}, \ldots, \sum_{1\leq i\leq r} B_{i,k}, \sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j})$$

is in $\mathcal{C}$. Thus $H(\mathbf{s}, \mathbf{c})^T = \mathbf{0}^T$, and hence $(\mathbf{s}, \mathbf{0})^T = -G[\mathcal{P}]\mathbf{c}^T$ by (3.2). Hence

$$(\mathbf{s}, \mathbf{0})^T = G[sup_p(\mathbf{c})](-\mathbf{c}_{sup_p(\mathbf{c})})^T.$$

From [V2] we infer that if $sup_p(\mathbf{c}) \in \Delta$ then $\mathbf{s} = \mathbf{0}$. So either $\mathbf{s} = \mathbf{0}$ or $sup_p(\mathbf{c}) \in \Delta^c$. Hence, either $\sum_{1\leq i\leq r} B_{i,j} = 0$ for all $1 \leq j \leq k$ or there exists a set $X \in [\Delta^c]^-$ such that $X \subseteq sup_p(\mathbf{c})$. Hence, C satisfies the $d^-(\Delta)$-property. Now we have proved that $\mathcal{C} = \{\mathbf{c}^{i,j} : (i, j) \in \mathcal{E}\}$ is a suitable set of vectors.

□

Proof of Theorem 3.2.6: Let $\{\mathbf{c}^{i,j} : (i, j) \in \mathcal{E}\}$ be a suitable set of vectors. Define code $\mathcal{C}$ of length $k + p[\mathcal{P}]$ over $GF(q)$ by the linear span of the vectors $(\mathbf{e}^j, \mathbf{c}^{i,j})$. Let H be a parity check matrix of $\mathcal{C}$. We will prove

$$H(\mathbf{s}, \mathbf{c})^T = \mathbf{0}^T \Rightarrow (\mathbf{s} = \mathbf{0} \vee sup_p(\mathbf{c}) \in \Delta^c). \quad (3.3)$$

If $H(\mathbf{s},\mathbf{c})^T = \mathbf{0}^T$ then $(\mathbf{s},\mathbf{c}) \in \mathcal{C}$. Hence, for $(i,j) \in \mathcal{E}$ there exist $B_{i,j} \in GF(q)$ such that

$$(\mathbf{s},\mathbf{c}) = \sum_{(i,j)\in\mathcal{E}} B_{i,j}(\mathbf{e}^j, \mathbf{c}^{i,j}),$$

i.e., $\mathbf{s}_j = \sum_{1\leq i\leq r} B_{i,j}$ for $1 \leq j \leq k$ and $\mathbf{c} = \sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j}$. If $sup_p(\mathbf{c}) \notin \Delta^c$ then $\neg(\exists_{X\in[\Delta^c]^-}\ X \subseteq sup_p(\mathbf{c}))$ and hence, by [C2], $\sum_{1\leq i\leq r} B_{i,j} = 0$ for all $1 \leq j \leq k$, i.e. $\mathbf{s} = \mathbf{0}$. This proves (3.3). Since $sup_p(\mathbf{0}) = \emptyset \in \Delta$

$$H(\mathbf{s},\mathbf{0})^T = \mathbf{0}^T \Rightarrow \mathbf{s} = \mathbf{0}.$$

In other words the first k columns of H are independent. Hence, by elementary row operations H can be put into the form

$$H = \left(\begin{array}{c|c} I_k & \\ O & H' \end{array} \right).$$

Now, define the matrices $G_i, 1 \leq i \leq n$, by

$$G[\mathcal{P}] = H'.$$

Let $X \in \Delta$ and let $(\mathbf{s},\mathbf{0})^T = G[X]\mathbf{b}^T$. Let vector $\mathbf{c}$ be defined by $\mathbf{c}_X = -\mathbf{b}$ and $sup_p(\mathbf{c}) \subseteq X$ (i.e. $\mathbf{c}_{X^c} = \mathbf{0}$), so $H(\mathbf{s},\mathbf{c})^T = \mathbf{0}^T$. From (3.3) and $sup_p(\mathbf{c}) \in \Delta$ we infer that $\mathbf{s} = \mathbf{0}$. Hence [V2] is satisfied.

Let $X \in \Gamma$. Then there exists a set $X_i \in [\Gamma]^-$ with $X_i \subseteq X$. Let $1 \leq j \leq k$. By [C1] and the definition of code $\mathcal{C}$ equality $H(\mathbf{e}^j, \mathbf{c}^{i,j})^T = \mathbf{0}^T$,with $sup(\mathbf{c}^{i,j}) \subseteq X_i$, holds. Hence, $(\mathbf{e}^j,\mathbf{0})^T = G[P](-\mathbf{c}^{i,j})^T$. So the j-th unit vector in $GF(q)^l$, $1 \leq j \leq k$, can be expressed as a linear combination of columns of matrix $G[X]$. Hence [V1] is satisfied.

□

3.3 The $d^-(\Delta)$-Property

Here we investigate the $d^-(\Delta)$-property. Figure 3.3 may be helpful to the reader to understand the next definition in which the $d^+(\Delta)$-property is defined. This new notion will be the main tool in the algorithm described in Section 3.4.

Definition 3.3.1 *Let (Γ, Δ) be an access structure and let $\mathcal{S} = GF(q)^k$ be a set of possible secrets. Let $X \subseteq \{1,\ldots,n\}$ and $Y \subseteq \mathcal{E} = \{(i,j) : 1 \leq i \leq r, 1 \leq j \leq k\}$, where r is the number of minimal elements of Γ. Let $\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]}, (i,j) \in \mathcal{E}$, define a set of vectors C. Then $C[Y,X]$ is defined as a matrix consisting of the $|Y|$ rows $\mathbf{c}^{i,j}_{X^c} \in GF(q)^{p[X^c]}$ with $(i,j) \in Y$. Similarly, the corresponding matrix $I[Y,X]$ has rows $I[Y,X]_l \in GF(q)^k$, $1 \leq l \leq |Y|$, defined by $I[Y,X]_l = \mathbf{e}^j$ iff there exists an i such that $C[Y,X]_l = \mathbf{c}^{i,j}_{X^c}$. Set*

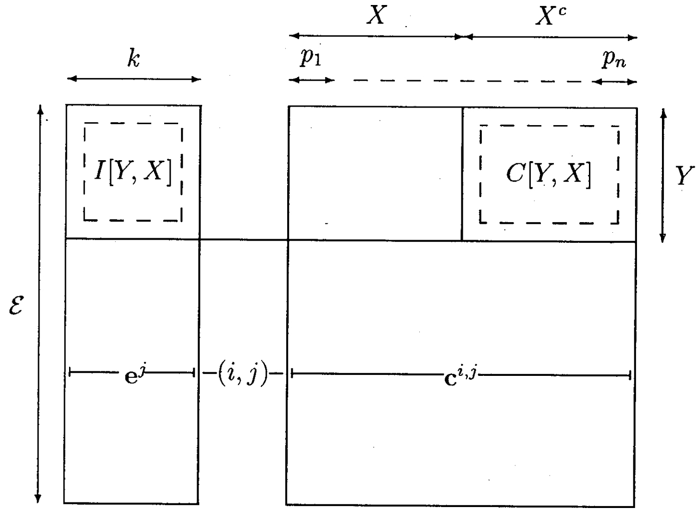


Figure 3.3: The $d^+(\Delta)$-property for Y and $X \in [\Delta]^+$: $\exists_{A \in GF(q)^{p[X^c]\times k}}\ I[Y,X] = C[Y,X]A$

C is said to have the $d^+(\Delta)$-property for Y and $X \in [\Delta]^+$ if the columns of $I[Y,X]$ can be written as linear combinations of the columns of $C[Y,X]$, i.e., if

$$\exists_{A \in GF(q)^{p[X^c]\times k}}\ I[Y,X] = C[Y,X]A.$$

Set C is said to have the $d^+(\Delta)$-property for Y if it has the $d^+(\Delta)$-property for Y and all $X \in [\Delta]^+$.

Notice that the $d^+(\Delta)$-property for $Y = \emptyset$ always holds (matrices $I[Y,X]$ and $C[Y,X]$ contain no rows). The following theorem is about the relation between the $d^-(.)$-property and the $d^+(.)$-property.

Theorem 3.3.2 *Let (Γ, Δ) be an access structure and let Γ have exactly r minimal elements. Let $\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]}, (i,j) \in \mathcal{E} = \{(i,j) : 1 \le i \le r, 1 \le j \le k\}$, define a set of vectors C. Then set C has the $d^-(\Delta)$-property iff C has the $d^+(\Delta)$-property for $\mathcal{E}$.*

Proof: We notice that the set of rows of $C[\mathcal{E}, \emptyset]$ is equal to C because $X^c = \{1, \ldots, n\}$ for $X = \emptyset$. The rows of $I[\mathcal{E}, \emptyset]$ are the corresponding unit vectors. Let B be a $r \times k$ q-ary matrix. Let vector $\mathbf{b} \in GF(q)^{|\mathcal{E}|}$ be defined as the concatenation of the columns of B. Thus $\mathbf{b}$ consists of all entries in B. Then w.l.o.g. $(\mathbf{b}I[\mathcal{E}, \emptyset])_j$ equals the addition of the elements of column j in B, and $\sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j} = \mathbf{b}C[\mathcal{E}, \emptyset]$. So the $d^-(\Delta)$-property is equivalent to each of the following equivalent statements

$$\begin{array}{l}
\forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ \left[\mathbf{b}I[\mathcal{E},\emptyset] \neq \mathbf{0} \ \Rightarrow \ \exists_{X\in[\Delta^c]^-} \ X \subseteq sup_p(\mathbf{b}C[\mathcal{E},\emptyset])\right], \\
\forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ \left[(\forall_{X\in[\Delta^c]^-} \ X \not\subseteq sup_p(\mathbf{b}C[\mathcal{E},\emptyset])) \ \Rightarrow \ \mathbf{b}I[\mathcal{E},\emptyset] = \mathbf{0}\right], \\
\forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ \left[(\exists_{X\in[\Delta]^+} \ sup_p(\mathbf{b}C[\mathcal{E},\emptyset]) \subseteq X) \ \Rightarrow \ \mathbf{b}I[\mathcal{E},\emptyset] = \mathbf{0}\right], \\
\forall_{X\in[\Delta]^+} \ \forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ \left[sup_p(\mathbf{b}C[\mathcal{E},\emptyset]) \subseteq X \ \Rightarrow \ \mathbf{b}I[\mathcal{E},\emptyset] = \mathbf{0}\right], \\
\forall_{X\in[\Delta]^+} \ \forall_{\mathbf{b}\in GF(q)^{|\mathcal{E}|}} \ \left[\mathbf{b}C[\mathcal{E},X] = \mathbf{0} \ \Rightarrow \ \mathbf{b}I[\mathcal{E},X] = \mathbf{0}\right].
\end{array}$$

In other words for all $X \in [\Delta]^+$ the zero space of $C[\mathcal{E},X]^T$ is contained in the zero space of $I[\mathcal{E},X]^T$ which is by elementary matrix theory [73] equivalent to the $d^+(\Delta)$-property for $\mathcal{E}$,

$$\forall_{X\in[\Delta]^+} \ \exists_A \ I[\mathcal{E},X] = C[\mathcal{E},X]A.$$

□

The last theorem of this section is about an inductive relation with which the algorithm in Section 3.4 systematically (by using backtracking) searches for a set satisfying the $d^+(\Delta)$-property for $\mathcal{E}$. By Theorem 3.3.2 this set will have the $d^-(\Delta)$-property. The algorithm will only search among sets having the $g(\Gamma)$-property. Thus the algorithm will determine whether there exists a suitable set of vectors for (Γ,Δ) or not. If the answer is positive a particular suitable set will also have been found.

Theorem 3.3.3 *Let (Γ,Δ) be an access structure and let $\mathcal{S} = GF(q)^k$ be a set of possible secrets. Let Γ have exactly r minimal elements. Let $\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]}, (i,j) \in \mathcal{E} = \{(i,j) : 1 \leq i \leq r, 1 \leq j \leq k\}$, define a set of vectors C. Suppose that C has the $d^+(\Delta)$-property for $Y \neq \emptyset$ and $X \in [\Delta]^+$. Let A be a matrix such that $I[Y,X] = C[Y,X]A$. Let $C_Z[Y,X]$ be defined as a matrix consisting of columns which form a basis of the right zero space of $C[Y,X]$ (i.e., a basis of $\{\mathbf{c} \in GF(q)^{p[X^c]} : C[Y,X]\mathbf{c}^T = \mathbf{0}\}$). Let $(i,j) \notin Y$. Then C has the $d^+(\Delta)$-property for $Y \cup \{(i,j)\}$ and $X \in [\Delta]^+$ iff*

- $\mathbf{c}^{i,j}_{X^c}A = \mathbf{e}^j$

or

- *there exists a column $\mathbf{b}$ of $C_Z[Y,X]$ such that $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$.*

Proof: W.l.o.g.

$$C[Y \cup \{(i,j)\},X] = \begin{pmatrix} C[Y,X] \\ \mathbf{c}^{i,j}_{X^c} \end{pmatrix}.$$

If $\mathbf{c}^{i,j}_{X^c}A = \mathbf{e}^j$ then $I[Y \cup \{(i,j)\},X] = C[Y \cup \{(i,j)\},X]A$, i.e., C has the $d^+(\Delta)$-property for $Y \cup \{(i,j)\}$ and X.

To finish the proof we first show that if $\mathbf{c}^{i,j}_{X^c}A \neq \mathbf{e}^j$ and C has the $d^+(\Delta)$-property for $Y \cup \{(i,j)\}$ and X then there exists a column $\mathbf{b}$ of $C_Z[Y,X]$ such that $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$. Secondly, we show that if there exists a column $\mathbf{b}$ of $C_Z[Y,X]$ such that $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$ then C has the $d^+(\Delta)$-property for $Y \cup \{(i,j)\}$ and X, which finishes the proof.

Let $\mathbf{c}^{i,j}_{X^c}A \neq \mathbf{e}^j$. Suppose that C has the $d^+(\Delta)$-property for $Y \cup \{(i,j)\}$ and X, i.e.,

$$I[Y \cup \{(i,j)\}, X] = C[Y \cup \{(i,j)\}, X]A'$$

for some matrix A'. Then $\mathbf{e}^j = \mathbf{c}^{i,j}_{X^c}A'$ and $C[Y,X](A'-A) = O$, the all zero matrix. Hence, the columns of $A'-A$ are in the zero space of $C[Y,X]$. Thus $A' = A + C_Z[Y,X]D$ for some matrix D. Now $\mathbf{0} \neq \mathbf{e}^j - \mathbf{c}^{i,j}_{X^c}A = \mathbf{c}^{i,j}_{X^c}(A'-A) = \mathbf{c}^{i,j}_{X^c}C_Z[Y,X]D$. Hence, $\mathbf{c}^{i,j}_{X^c}C_Z[Y,X] \neq \mathbf{0}$, in other words there exists a column $\mathbf{b}$ in $C_Z[Y,X]$ such that $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$.

Let $\mathbf{b}$ be a column in $C_Z[Y,X]$ (thus $C[Y,X]\mathbf{b}$ is the all-zero column) such that $\mathbf{c}^{i,j}_{X^c}\mathbf{b} \neq 0$. Then $C[Y,X](A+\mathbf{b}(\mathbf{c}^{i,j}_{X^c}\mathbf{b})^{-1}(\mathbf{e}^j - \mathbf{c}^{i,j}_{X^c}A)) = I[Y,X]$ and $\mathbf{c}^{i,j}_{X^c}(A + \mathbf{b}(\mathbf{c}^{i,j}_{X^c}\mathbf{b})^{-1}(\mathbf{e}^j - \mathbf{c}^{i,j}_{X^c}A)) = \mathbf{e}^j$ (notice that $\mathbf{b}$ is a column vector and $\mathbf{e}^j$ and $\mathbf{c}^{i,j}_{X^c}$ are row vectors). From these two equations we infer that

$$I[Y \cup \{(i,j)\}, X] = C[Y \cup \{(i,j)\}, X](A + \mathbf{b}(\mathbf{c}^{i,j}_{X^c}\mathbf{b})^{-1}(\mathbf{e}^j - \mathbf{c}^{i,j}_{X^c}A)).$$

Hence, C has the $d^+(\Delta)$-property for $Y \cup \{(i,j)\}$ and X.

□

3.4 Search Algorithm

Let $n = |\mathcal{P}|$, q be a prime power, and the numbers k, p_i, $1 \leq i \leq n$, be integers. We present an outline of an algorithm for determining whether a secret sharing scheme for a given non-trivial access structure (Γ, Δ) and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$ can be realized by means of the generalized vector space construction. If so, the algorithm produces a secret sharing scheme with this convec.

Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, \ldots, n\}$. Then the combination of Theorems 3.2.5, 3.2.6, and Theorem 3.1.2 tells us that there exists a generalized vector space construction, with parameters k, q, and p_i, $1 \leq i \leq n$, leading to a secret sharing scheme for (Γ, Δ) and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$ iff there exists a suitable set of vectors for (Γ, Δ) and set of possible secrets $GF(q)^k$ with parameters p_i, $1 \leq i \leq n$. Given such a suitable set of vectors one can obtain efficiently a corresponding secret sharing scheme (see Theorem 3.2.6). We will explain how to search for a suitable set of vectors for (Γ, Δ) and set of possible secrets $GF(q)^k$ when the parameters p_i, $1 \leq i \leq n$, are given. It will be an exhaustive search among sets of vectors $C = \{\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]} : (i,j) \in \mathcal{E}\}$ satisfying the $g(\Gamma)$-property. In Subsection 3.4.1 we define a search tree and we discuss its properties. Subsection 3.4.2 presents a design of our search algorithm using this tree, and Subsection 3.4.3 presents its complexity analysis.

3.4.1 The Search Tree and its Properties

Let $[\Gamma]^- = \{X_1, \ldots, X_r\}$. As in the previous sections we define

$$\mathcal{E} = \{(i,j) : 1 \leq i \leq r, 1 \leq j \leq k\} = \{(i_1, j_1), \ldots, (i_{rk}, j_{rk})\}.$$

Further let $[\Delta]^+ = \{D_1, \ldots, D_t\}$.

The best way to understand the exhaustive search algorithm is by means of a directed labeled tree, see Figure 3.4. The tree consists of *nodes* on *levels* s, $0 \leq s \leq rk$. The unique node on level 0 is called the *root* and is denoted by $\mathbf{r}$. The nodes on level rk are called *leafs*. Leafs have no outgoing edges. We consider a directed tree, so each node besides the root has exactly one incoming edge. Each edge is labeled by some set of vectors $S \subseteq GF(q)^{p[\mathcal{P}]}$. Labels have the property that if they label an edge from level $s-1$ to level s then they are subsets of $\{\mathbf{c} \in GF(q)^{p[\mathcal{P}]} : sup_p(\mathbf{c}) \in X_{i_s}\}$. Edges need not necessarily have different labels.

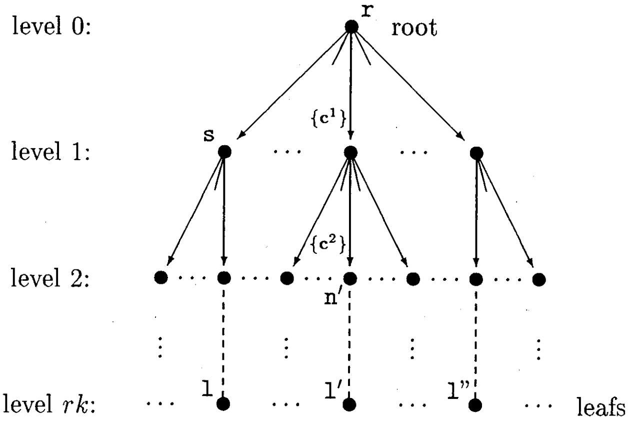


Figure 3.4: Tree

We construct the labeled tree level by level. We start at level $s = 0$. As soon as we have designed the tree up to and including the nodes on level s we will continue designing the outgoing labeled edges from the nodes on level s and we obtain the tree up to and including the nodes on level $s+1$. In this way we continue until we have reached level $s = rk$.

Initially, $s = 0$ and the tree up to and including the nodes on level $s = 0$ only consists of the root, the unique node on level 0. Suppose we have designed the tree up to and including the nodes on level s. So, for $0 \leq m < s$ the labels of the edges from nodes on level m to nodes on level $m+1$ are sets of vectors $S \subseteq GF(q)^{p[\mathcal{P}]}$ having the property that for all $\mathbf{c} \in S$

$$sup_p(\mathbf{c}) \subseteq X_{i_{m+1}}.$$

Let $\mathbf{n}$ be a node on level s. There exists a unique path from the root to $\mathbf{n}$. Let $S^m \subseteq GF(q)^{p[\mathcal{P}]}$, $1 \leq m \leq s$, be the label of the incoming edge of the node on level m visited by the path. We define code $\mathcal{C}(\mathbf{n})$ as the linear span of the vectors in

$$\bigcup_{1 \leq m \leq s} S^m.$$

For example, if $s = 0$ then $\mathbf{n} = \mathbf{r}$, hence, $\mathcal{C}(\mathbf{r}) = \{\mathbf{0}\}$, which is the linear span of the empty set of vectors. We can now design the outgoing edges from node $\mathbf{n}$ to level $s + 1$ in the following manner. One outgoing edge gets the label

$$S_{\mathbf{n}} = \{\mathbf{c} \in \mathcal{C}(\mathbf{n}) : sup_p(\mathbf{c}) \subseteq X_{i_{s+1}}\}.$$

Notice that $\mathbf{0} \in S_{\mathbf{n}}$. The singleton sets $\{\mathbf{c}\}$ having the property that $sup_p(\mathbf{c}) \subseteq X_{i_{s+1}}$ and $\mathbf{c} \notin \mathcal{C}(\mathbf{n})$ are the labels of the remaining outgoing edges. In this way we design the outgoing edges from nodes $\mathbf{n}$ on level s. One of these outgoing edges has label $S_{\mathbf{n}}$, the other outgoing edges have labels $\{\mathbf{c}\}$, for $\mathbf{c} \notin \mathcal{C}(\mathbf{n})$ with $sup_p(\mathbf{c}) \subseteq X_{i_{s+1}}$. By designing all outgoing edges from nodes on level s we indirectly design all nodes on level $s + 1$. The labels of outgoing edges from nodes on level s to nodes on level $s + 1$ are subsets of $\{\mathbf{c} \in GF(q)^{p[\mathcal{P}]} : sup_p(\mathbf{c}) \subseteq X_{i_{s+1}}\}$. We notice that the number of outgoing edges from one node on level s is at most $q^{p[X_{i_{s+1}}]}$ and we notice that different outgoing edges from different nodes on level s may have the same label. By using induction on s we obtain the final structure of the tree.

Let $S^1, \ldots, S^{rk}$ be the labels of a path from root $\mathbf{r}$ to some leaf. A set of vectors $C = \{\mathbf{c}^{i_s, j_s} : 1 \leq s \leq rk\}$ is said to *correspond* to the path with labels $S^1, \ldots, S^{rk}$ if and only if $\mathbf{c}^{i_s, j_s} \in S^s$ for $1 \leq s \leq rk$. Thus there are $\prod_{1 \leq s \leq rk} |S^s|$ sets of vectors corresponding to the path with labels $S^1, \ldots, S^{rk}$. Since S^s is the label of an edge on level $s - 1$ to a node on level s we have that for all $\mathbf{c} \in S^s$

$$sup_p(\mathbf{c}) \subseteq X_{i_s}.$$

So, if C corresponds to the path with labels $S^1, \ldots, S^{rk}$ then C has the $g(\Gamma)$-property. We notice that the tree is constructed such that each set of vectors having the $g(\Gamma)$-property corresponds to some path from the root to a leaf. Our algorithm will perform a walk through the directed tree in order to find a suitable set of vectors among the sets of vectors having the $g(\Gamma)$-property.

We need the following notions. A set of vectors C *corresponds to node* $\mathbf{n}$ if C corresponds to a path from root $\mathbf{r}$ to node $\mathbf{n}$ to some leaf. For example C corresponds to $\mathbf{n}'$ in Figure 3.4 iff $\mathbf{c}^{i_1, j_1} = \mathbf{c}^1$ and $\mathbf{c}^{i_2, j_2} = \mathbf{c}^2$. Notice that the sets corresponding to the leafs are exactly all sets of vectors having the $g(\Gamma)$-property. The next notion is valuable as well. A leaf $\mathbf{l}$ is *on the left side of node* $\mathbf{n}$ if the path from root $\mathbf{r}$ to leaf $\mathbf{l}$ is such that the node on the level of $\mathbf{n}$ visited by the path is on the left side of $\mathbf{n}$ in the tree. For example, in Figure 3.4, $\mathbf{l}$ is on the left side of $\mathbf{n}'$, where $\mathbf{l}'$ and $\mathbf{l}$" are not on the left side of $\mathbf{n}'$.

Let n be a node on level s. Let $S^1, \dots, S^s$ be the labels of the unique path from the root to n. Let $1 \leq m \leq s$. If S^m is not a singleton set unequal to $\{\mathbf{0}\}$ then the design of the tree tells us that S^m is the label of a special outgoing edge in the construction procedure of the tree. Hence, the vectors $\mathbf{c} \in S^m$ are linear combinations of the vectors $\mathbf{c} \in S^w$, $1 \leq w \leq m-1$. This is the reason to introduce and define $\mathcal{S}(\mathrm{n})$ and $\mathcal{S}_L(\mathrm{n})$ by

$$\mathcal{S}(\mathrm{n}) = \{1 \leq m \leq s : |S^m| = 1, S^m \neq \{\mathbf{0}\}\},$$

and

$$\mathcal{S}_L(\mathrm{n}) = \{1 \leq m \leq s : m \notin \mathcal{S}(\mathrm{n})\}.$$

So, we conclude that the vectors $\mathbf{c} \in S^m$, $m \in \mathcal{S}_L(\mathrm{n})$, are linear combinations of the vectors $\mathbf{c} \in S^m$, $m \in \mathcal{S}(\mathrm{n})$ $(S^m = \{\mathbf{c}\})$. Further the design of the tree tells us that the vectors $\mathbf{c} \in S^m$, $m \in \mathcal{S}(\mathrm{n})$, are linearly independent. So:

Lemma 3.4.1 *There are linearly independent vectors* $\mathbf{c}^m$, $m \in \mathcal{S}(\mathrm{n})$, *such that for each set of vectors* $C = \{\mathbf{c}^{i_m,j_m} : 1 \leq m \leq rk\}$ *corresponding to* n, $\mathbf{c}^{i_m,j_m} = \mathbf{c}^m$ *for* $m \in \mathcal{S}(\mathrm{n})$ *and each vector* $\mathbf{c}^{i_m,j_m}$, $m \in \mathcal{S}_L(\mathrm{n})$, *is a linear combination of the vectors* $\mathbf{c}^{i_m,j_m}$, $m \in \mathcal{S}(\mathrm{n})$. *A consequence is that for each set of vectors* $C = \{\mathbf{c}^{i_m,j_m} : 1 \leq m \leq rk\}$ *corresponding to* n *set* $\{\mathbf{c}^{i_m,j_m} : m \in \mathcal{S}(\mathrm{n})\}$ *is a basis of the vector space* $\mathcal{C}(\mathrm{n})$.

Since there are at most $p[\mathcal{P}]$ linearly independent vectors in $GF(q)^{p[\mathcal{P}]}$

$$|\mathcal{S}(\mathrm{n})| \leq p[\mathcal{P}]. \tag{3.4}$$

Using $\mathcal{S}(\mathrm{n})$ we define subset $\mathcal{E}(\mathrm{n})$ of $\mathcal{E}$ by

$$\mathcal{E}(\mathrm{n}) = \{(i_m, j_m) : m \in \mathcal{S}(\mathrm{n})\}.$$

We need a further important notion. Let n be a node on level s. Let $S^1, \dots, S^s$ be the labels of the unique path from the root to n. We define code $\mathcal{C}_L(\mathrm{n})$ as the linear span of the vectors in

$$\bigcup_{m \in \mathcal{S}(\mathrm{n})} \{(\mathbf{e}^{j_m}, \mathbf{c}) : S^m = \{\mathbf{c}\}\}.$$

Notice that by Lemma 3.4.1 $\mathcal{C}(\mathrm{n})$ is the linear span of the vectors in

$$\bigcup_{m \in \mathcal{S}(\mathrm{n})} \{\mathbf{c} : S^m = \{\mathbf{c}\}\}.$$

We call n a *candidate node* if either

- n is the root, or
- n is not the root but the (unique) incoming edge to n comes from a candidate node and there exists a vector $\mathbf{c} \in S^s$ with $(\mathbf{e}^{j_s}, \mathbf{c}) \in \mathcal{C}_L(\mathrm{n})$.

If n is a candidate node and there exists a path from node n′ to n then n′ is a candidate node as well. If n is not a candidate node and there exists a path from n to node n′ then n′ is not a candidate node as well. As a consequence, the following lemma holds.

Lemma 3.4.2 *For each leaf* l *there exists a node* n *visited by the path from the root to* l *such that all nodes, including* n*, visited by the path from the root to* n *are candidate nodes and such that all nodes, excluding* n*, visited by the path from* n *to* l *are not candidate nodes.*

Let n be a candidate node and let a be a node such that there exist an edge from n to a labeled by a singleton set $\{\mathbf{c}\} \neq \{\mathbf{0}\}$. Let s be the level of a. Then $(\mathbf{e}^{j_s}, \mathbf{c}) \in \mathcal{C}_L(\mathrm{a})$ by the definition of $\mathcal{C}_L(\mathrm{a})$. Thus a is a candidate node as well. This proves the next lemma.

Lemma 3.4.3 *Let* n *be a candidate node and let* a *be a node such that there exist an edge from* n *to* a *labeled by a singleton set unequal to* $\{\mathbf{0}\}$*. Then* a *is a candidate node as well.*

We notice that if n is a candidate node then for all $m \in \mathcal{S}_L(\mathrm{n})$ there exists a vector $\mathbf{c} \in S^m$ with $(\mathbf{e}^{j_m}, \mathbf{c}) \in \mathcal{C}_L(\mathrm{n})$. This proves the following lemma. In this lemma we define the notion *a set of candidate vectors of a candidate node* n.

Lemma 3.4.4 *If* n *is a candidate node then there exists a set* $C = \{\mathbf{c}^{i_m,j_m} : 1 \leq m \leq rk\}$ *corresponding to* n *such that each vector* $(\mathbf{e}^{j_m}, \mathbf{c}^{i_m,j_m})$, $m \in \mathcal{S}_L(\mathrm{n})$*, is a linear combination of the vectors* $(\mathbf{e}^{j_m}, \mathbf{c}^{i_m,j_m})$, $m \in \mathcal{S}(\mathrm{n})$ *(which span* $\mathcal{C}_L(\mathrm{n})$*). We call set* $\{\mathbf{c}^{i_m,j_m} : 1 \leq m \leq s\}$ *a set of candidate vectors of node* n*. If* l *is a candidate leaf then each set of candidate vectors of* l *corresponds to* l.

We notice that $\mathcal{S}_L(\mathrm{r}) = \emptyset$, hence, $\emptyset$ is a set of candidate vectors of the root r.

Now we are ready to define two important boolean statements $D^+(\mathrm{n})$ and $D^-(\mathrm{n})$ for nodes n:

[D^+] The value of $D^+(\mathrm{n})$ is true iff n is a candidate node and the $d^+(\Delta)$-property for $\mathcal{E}(\mathrm{n})$ holds for any set of vectors corresponding to node n.

[D^-] The value of $D^-(\mathrm{n})$ is true iff none of the sets corresponding to candidate leafs on the left side of n has the $d^-(\Delta)$-property.

Thus $D^+(\mathrm{n})$ and $D^-(\mathrm{n})$ tell us something about the suitability of sets corresponding to node n and sets corresponding to leafs on the left side of node n as the following lemma's will show.

Lemma 3.4.5 *Suppose that* (Γ, Δ) *is a non-trivial access structure and suppose that none of the sets corresponding to candidate leafs has the* $d^-(\Delta)$*-property. Then there does not exist a suitable set of vectors for* (Γ, Δ).

Proof: We will first prove that none of the sets corresponding to leafs which are not candidate nodes has the $d^-(\Delta)$-property. Let $\mathtt{l}$ be a leaf and suppose that $\mathtt{l}$ is not a candidate node. Let $\mathtt{n}$ be the unique node as described by Lemma 3.4.2. Let $\mathtt{a}$ be the node visited by the outgoing edge from $\mathtt{n}$ on the path from the root to $\mathtt{n}$ to $\mathtt{l}$. We notice that $\mathtt{n}$ is a candidate node but $\mathtt{a}$ is not. Hence, by Lemma 3.4.3 the edge from $\mathtt{n}$ to $\mathtt{a}$ is not labeled by a singleton set unequal to $\{\mathbf{0}\}$. Suppose that the level of $\mathtt{a}$ is s then $s \notin \mathcal{S}(\mathtt{a})$. Let C be a set of vectors corresponding to $\mathtt{l}$.

By Lemma 3.4.1 the vectors $\mathbf{c}^{i_m,j_m}$, $m \in \mathcal{S}(\mathtt{a})$, span $\mathcal{C}(\mathtt{a})$ which contains vector $\mathbf{c}^{i_s,j_s}$. We have already seen that $s \notin \mathcal{S}(\mathtt{a})$. Thus there exists a q-ary $r \times k$ matrix B such that $B_{i_s,j_s} = 1$, $B_{i_m,j_m} = 0$ for $s < m \leq rk$, and

$$\mathbf{0} = \sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j}. \tag{3.5}$$

We notice that $\mathtt{a}$ is not a candidate node, $\mathtt{n}$ is a candidate node, and $\mathbf{c}^{i_s,j_s}$ is an element of the label of the edge from $\mathtt{n}$ to $\mathtt{a}$ (because C corresponds to $\mathtt{l}$). By the definition of being a candidate node we have that $(\mathbf{e}^{j_s}, \mathbf{c}^{i_s,j_s}) \notin \mathcal{C}_L(\mathtt{a})$, that is it is not a linear combination of the vectors $(\mathbf{e}^{j_m}, \mathbf{c}^{i_m,j_m})$, $m \in \mathcal{S}(\mathtt{a})$. Hence,

$$\mathbf{0} \neq \sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{e}^{j}.$$

In other words the elements of at least one column in B do not add up to 0.

Suppose that C has the $d^-(\Delta)$-property. Then there exists a minimal set X of Δ^c such that

$$X \subseteq sup_p\left(\sum_{(i,j)\in\mathcal{E}} B_{i,j}\mathbf{c}^{i,j}\right).$$

From this and (3.5) we infer that $X = \emptyset$, hence, $\Delta^c = 2^{\mathcal{P}}$. That is $\Delta = \emptyset$, a contradiction since (Γ, Δ) is supposed to be non-trivial. Thus C can not have the $d^-(\Delta)$-property. Hence, none of the sets corresponding to leafs which are not candidate nodes has the $d^-(\Delta)$-property. By assumption, none of the sets corresponding to candidate leafs has the $d^-(\Delta)$-property. So, in general the sets corresponding to the leafs do not have the $d^-(\Delta)$-property. The design of the tree is such that the sets corresponding to the leafs are exactly all sets of vectors having the $g(\Gamma)$-property. Thus, by Definition 3.2.2 there does not exist a suitable set of vectors for (Γ, Δ).

□

We notice that at the beginning of this section we stated that we would only consider non-trivial access structures. The next two lemma's will be important as well.

Lemma 3.4.6 *Let* l *be a leaf for which* $D^+(\mathtt{l})$ *holds. Then each set of candidate vectors of* l *is also a suitable set of vectors for* (Γ, Δ).

Proof: Let $C = \{\mathbf{c}^{i_m,j_m} \in GF(q)^{p[\mathcal{P}]} : 1 \leq m \leq rk\}$ be a set of candidate vectors of l. From the assumption that $D^+(\mathtt{b})$ holds we obtain that C has the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{b})$. Thus for $1 \leq w \leq t$ there exist q-ary matrices A_w such that

$$I[\mathcal{E}(\mathtt{b}), D_w] = C[\mathcal{E}(\mathtt{b}), D_w]A_w. \tag{3.6}$$

Let $1 \leq m \leq rk$. Then $m \in \mathcal{S}_L(\mathtt{b}) \cup \mathcal{S}(\mathtt{b})$. By Lemma 3.4.4 vectors $(\mathbf{e}^{j_m}, \mathbf{c}^{i_m,j_m})$, $m \in \mathcal{S}_L(\mathtt{l})$, are linear combinations of the vectors $(\mathbf{e}^{j_m}, \mathbf{c}^{i_m,j_m})$, $m \in \mathcal{S}(\mathtt{l})$. So, there exists a row vector $\mathbf{b}$ such that

$$(\mathbf{e}^{j_m}, \mathbf{c}^{i_m,j_m}_{D^c_w}) = \mathbf{b}(I[\mathcal{E}(\mathtt{b}), D_w] \| C[\mathcal{E}(\mathtt{b}), D_w]). \tag{3.7}$$

From (3.6) and (3.7) we infer that

$$\mathbf{c}^{i_m,j_m}_{D^c_w} A_w = \mathbf{b}C[\mathcal{E}(\mathtt{b}), D_w]A_w = \mathbf{b}I[\mathcal{E}(\mathtt{b}), D_w] = \mathbf{e}^{j_m}.$$

Since m has been chosen arbitrarily

$$I[\mathcal{E}, D_w] = C[\mathcal{E}, D_w]A_w$$

for $1 \leq w \leq t$. By Definition 3.3.1 C has the $d^+(\Delta)$-property for $\mathcal{E}$. So, Theorem 3.3.2 implies that C has the $d^-(\Delta)$-property. Further, by Lemma 3.4.4 set C corresponds to b. Thus, set C has the $g(\Gamma)$-property as well and we conclude that C is a suitable set of vectors for (Γ, Δ).

□

Lemma 3.4.7 *Let* n *be a node for which* $D^+(\mathtt{n})$ *does not hold. Let* l *be a candidate leaf for which there exists a path from the root to* n *to* l. *Then none of the sets corresponding to* l *has the* $d^-(\Delta)$*-property.*

Proof: Since l is a candidate node, node n is a candidate node as well by Lemma 3.4.2. Notice that the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{n})$ of a set of vectors $C = \{\mathbf{c}^{i_1,j_1}, \ldots, \mathbf{c}^{i_{rk},j_{rk}}\}$ corresponding to n only depends on the vectors $\mathbf{c}^{i_m,j_m}$, $m \in \mathcal{S}(\mathtt{n})$ (see Definition 3.3.1). From Lemma 3.4.1 we infer that these vectors are the same for any set of vectors corresponding to n. Since $D^+(\mathtt{n})$ is false and n is a candidate node none of the sets corresponding to node n has the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{n})$. Hence, none of the sets corresponding to leaf l has the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{n})$. If the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{n})$ does not hold then the $d^+(\Delta)$-property for $\mathcal{E}$ does not hold and, by Theorem 3.3.2, the $d^-(\Delta)$-property does not hold.

□

As in the proof of the previous lemma, notice that the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{n})$ of a set of vectors $C = \{\mathbf{c}^{i_1,j_1}, \ldots, \mathbf{c}^{i_{rk},j_{rk}}\}$ corresponding to n only depends on the vectors $\mathbf{c}^{i_m,j_m}$, $m \in \mathcal{S}(\mathtt{n})$ (see Definition 3.3.1). From Lemma 3.4.1 we infer that these vectors are the same for any set of vectors corresponding to n. Thus (see Definition 3.3.1):

Lemma 3.4.8

[A] If $D^+(\mathrm{n})$ is true then there exist q-ary matrices $A_i(\mathrm{n})$, $1 \leq i \leq t$, such that for each set of vectors C corresponding to node n

$$I[\mathcal{E}(\mathrm{n}), D_i] = C[\mathcal{E}(\mathrm{n}), D_i]A_i(\mathrm{n}).$$

[B] There exist q-ary matrices $B_i(\mathrm{n})$, $1 \leq i \leq t$, such that for each set of vectors C corresponding to n *the set of columns of $B_i(\mathrm{n})$ span linearly the right zero space of $C[\mathcal{E}(\mathrm{n}), D_i]$.*

By Lemma 3.4.4:

[C] If $D^+(\mathrm{n})$ is true then there exists a set of candidate vectors $C(\mathrm{n})$ of n.

In the remainder of this chapter matrices $B_i(\mathrm{n})$ denote matrices having the property as described in [B] and if $D^+(\mathrm{n})$ is true then matrices $A_i(\mathrm{n})$ denote matrices having the property as described in [A] and sets $C(\mathrm{n})$ denote sets having the property as described in [C]. The matrices will be used in the algorithm in relation to Theorem 3.3.3.

We notice that $\mathcal{S}(\mathrm{n}') \subseteq \mathcal{S}(\mathrm{n})$, hence, $\mathcal{E}(\mathrm{n}') \subseteq \mathcal{E}(\mathrm{n})$, for any node n′ visited by the path from the root to n. Further by Lemma 3.4.2 if node n′ is visited by the path from the root to a candidate node n then also n′ is a candidate node. So:

Lemma 3.4.9 *Let* n *be such that $D^+(\mathrm{n})$ is true. Then $D^+(\mathrm{n}')$ holds for any node* n′ *visited by the path from the root to* n, *and $A_i(\mathrm{n})$ is an example of a solution for $A_i(\mathrm{n}')$ in statement [A]. Let s be the level of* n, *let s' be the level of* n′, *and suppose that $C(\mathrm{n}) = \{\mathbf{c}^{i_m,j_m} : 1 \leq m \leq s\}$. Then $\{\mathbf{c}^{i_m,j_m} : 1 \leq m \leq s'\}$ is a solution for $C(\mathrm{n}')$ in statement [C].*

Finally:

Lemma 3.4.10 *Suppose that $\mathcal{S}(\mathrm{n}') = \mathcal{S}(\mathrm{n})$, hence, $\mathcal{E}(\mathrm{n}') = \mathcal{E}(\mathrm{n})$. Then w.l.o.g. $B_i(\mathrm{n}') = B_i(\mathrm{n})$, $1 \leq i \leq t$, and if in addition both $D^+(\mathrm{n}')$ and $D^+(\mathrm{n})$ are true then w.l.o.g. $A_i(\mathrm{n}') = A_i(\mathrm{n})$, $1 \leq i \leq t$.*

3.4.2 The Search Algorithm

We will now describe how our algorithm walks through the tree and how it checks the $d^-(\Delta)$-property for sets corresponding to the leafs. For root r we have that $D^+(\mathrm{r})$ is true since the $d^+(\Delta)$-property for $\mathcal{E}(\mathrm{r}) = \emptyset$ always hold. For the leftmost node s on the first level we have that $D^-(\mathrm{s})$ is true since there exist no leafs on the left side of s. We notice that matrices $A_i(\mathrm{r})$ can be anything (for instance the all zero matrix) since matrices $I[\mathcal{E}(\mathrm{r}), D_i]$ and $C[\mathcal{E}(\mathrm{r}), D_i]$ contain no rows. Matrix $B_i(\mathrm{r})$ is equal to the q-ary $p[D_i^c] \times p[D_i^c]$ identity matrix. Further $C(\mathrm{r}) = \emptyset$ is a set of candidate vectors of root r.

The walk starts in the root and continues to node s. We make use of a procedure Dplus with input and output conditions given in Table 3.1. In Section 3.4.1 we will describe such a procedure. We apply Dplus for input $(\mathtt{r},\mathtt{s}), A_i(\mathtt{r}), B_i(\mathtt{r}), 1 \leq i \leq t, C(\mathtt{r})$. By means of this procedure we find out whether $D^+(\mathtt{s})$ is true or not. The choice of the new node to which the algorithm will walk depends on the value of $D^+(\mathtt{s})$.

Let us consider the general case. Suppose the algorithm has walked to node b such that its (unique) incoming edge, say from a, has the property that both $D^+(\mathtt{a})$ and $D^-(\mathtt{b})$ hold. Further suppose that at that moment each matrix $A_i(\mathtt{a})$, $1 \leq i \leq t$, and each matrix $B_i(\mathtt{n}')$, $1 \leq i \leq t$, for nodes $\mathtt{n}'$ visited by the path from the root to a, are known. Moreover, we assume that a set $C(\mathtt{a})$ is known. Notice that at the start of the algorithm this situation holds since the values of both $D^+(\mathtt{r})$ and $D^-(\mathtt{s})$ are true, matrices $A_i(\mathtt{r}), B_i(\mathtt{r}), 1 \leq i \leq t$, are known, and set $C(\mathtt{r})$ is known. We make use of Dplus to find out whether $D^+(\mathtt{b})$ is true or not. In addition, if $D^+(\mathtt{b})$ turns out to be true then Dplus outputs matrices $A_i(\mathtt{b})$, $1 \leq i \leq t$, matrices $B_i(\mathtt{n}')$, $1 \leq i \leq t$, for nodes $\mathtt{n}'$ visited by the path from the root to b, and a set $C(\mathtt{b})$. If $D^+(\mathtt{b})$ does not hold then the algorithm leaves matrices $A_i(\mathtt{a})$, $1 \leq i \leq t$, matrices $B_i(\mathtt{n}')$, $1 \leq i \leq t$, for nodes $\mathtt{n}'$ visited by the path from the root to a, and set $C(\mathtt{a})$ unchanged.

To determine the next node to which the algorithm walks we distinguish a few cases accordingly to the value of $D^+(\mathtt{b})$ and the position in the tree.

Input:

A tuple of nodes $(\mathtt{a},\mathtt{b})$ such that $D^+(\mathtt{a})$ holds.
Matrices $A_i(\mathtt{a})$, $1 \leq i \leq t$, matrices $B_i(\mathtt{n}')$, $1 \leq i \leq t$, for nodes $\mathtt{n}'$ visited by the path from the root to a, and set $C(\mathtt{a})$.

Output:

The value of $D^+(\mathtt{b})$.
If $D^+(\mathtt{b})$ holds then the algorithm also produces matrices $A_i(\mathtt{b})$, $1 \leq i \leq t$, matrices $B_i(\mathtt{n}')$, $1 \leq i \leq t$, for nodes $\mathtt{n}'$ visited by the path from the root to b, and set $C(\mathtt{b})$.
If $D^+(\mathtt{b})$ does not hold then the algorithm leaves matrices $A_i(\mathtt{a})$, $1 \leq i \leq t$, matrices $B_i(\mathtt{n}')$, $1 \leq i \leq t$, for nodes $\mathtt{n}'$ visited by the path from the root to a, and set $C(\mathtt{a})$ unchanged.

Table 3.1: Procedure Dplus

If $D^+(\mathtt{b})$ is false we distinguish three types of positions, see Figures 3.5, 3.6, and 3.7. In Figures 3.6 and 3.7 there does not exist an edge from a to a node d on the right side of b. For node a with incoming edge from a" to a a similar situation can occur. That is there does not exist an edge from a" to a node d on the right side of a. We can continue to lower levels until we encounter a node a′ as depicted in Figure 3.6 or until we encounter the root as depicted in Figure 3.7.

CASE(i) $D^+(\mathtt{b})$ is false and the situation is as in Figure 3.5:

Let n be the right neighbour of b on the same level. By Lemma 3.4.7, each candidate leaf l for which the path from the root to l visits b has the property that none of the sets corresponding to l has the $d^-(\Delta)$-property. From this and the fact that $D^-(\mathtt{b})$ is true we infer that $D^-(\mathtt{n})$ is true.

The algorithm continues to node n. Its incoming edge from a to n has the property that both $D^+(\mathtt{a})$ and $D^-(\mathtt{n})$ hold. So, we are in a situation similar to the one we started with and we can go back to the beginning of the description of the general case.

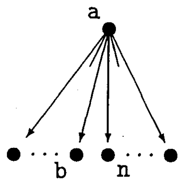


Figure 3.5: Case (i)

CASE(ii) $D^+(\mathtt{b})$ is false and the situation is as in Figure 3.6:

Let n be the node reached by the leftmost outgoing edge from a′ on the right side of the path from a′ to b. By Lemma 3.4.7, each candidate leaf l for which the path from the root to l visits b has the property that none of the sets corresponding to l has the $d^-(\Delta)$-property. From this and the fact that $D^-(\mathtt{b})$ is true we infer that $D^-(\mathtt{n})$ is true.

The value of $D^+(\mathtt{a})$ is true. So, by Lemma 3.4.9 $D^+(\mathtt{a}')$ holds. The algorithm continues to node n. Its incoming edge from a′ to n has the property that both $D^+(\mathtt{a}')$ and $D^-(\mathtt{n})$ hold. By Lemma 3.4.9 matrices $A_i(\mathtt{a}')$, $1 \leq i \leq t$, and a set $C(\mathtt{a}')$ can be computed easily by means of $A_i(\mathtt{a})$, $1 \leq i \leq t$, and $C(\mathtt{a})$. We notice that $B_i(\mathtt{n}')$, $1 \leq i \leq t$, for nodes n′ visited by the path from the root to a′ are already known since a′ is visited by the path from the root to b. So, we are in a situation similar to the one we started with and we can go back to the beginning of the description of the general case.

CASE(iii) $D^+(\mathtt{b})$ is false and the situation is as in Figure 3.7:

By Lemma 3.4.7, each candidate leaf l for which the path from the root to l visits b has the property that none of the sets corresponding to l has the $d^-(\Delta)$-property. From this and the fact that $D^-(\mathtt{b})$ is true we infer that for

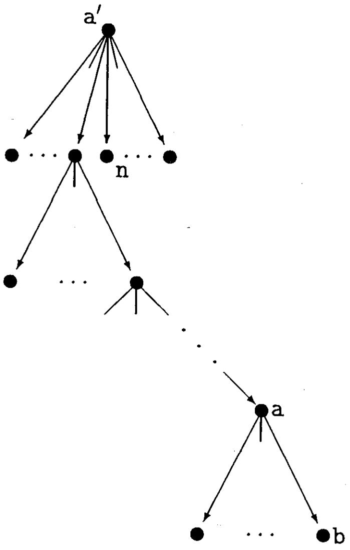


Figure 3.6: Case (ii)

all sets corresponding to a candidate leaf the $d^{-}(\Delta)$-property does not hold. By Lemma 3.4.5 there does not exist a suitable set of vectors for (Γ, Δ) and set of possible secrets $GF(q)^k$ with parameters p_i, $1 \leq i \leq n$.

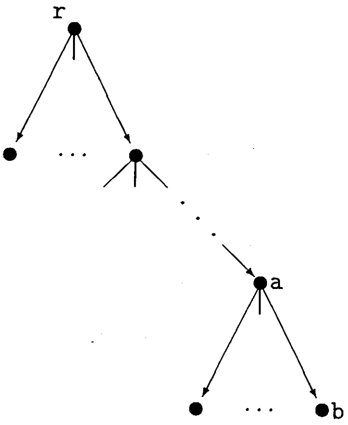


Figure 3.7: Case (iii)

If $D^{+}(\mathtt{b})$ is true we distinguish two cases.

Case(iv) $D^+(\mathtt{b})$ is true and $\mathtt{b}$ is not a leaf:

We are in the situation of Figure 3.8. Let $\mathtt{n}$ be the node reached by the leftmost outgoing edge from $\mathtt{b}$. The leafs on the left side of $\mathtt{n}$ are also leafs on the left side of $\mathtt{b}$. Thus $D^-(\mathtt{n})$ holds since $D^-(\mathtt{b})$ holds. The algorithm continues to node $\mathtt{n}$. Its incoming edge from $\mathtt{b}$ to $\mathtt{n}$ has the property that both $D^+(\mathtt{b})$ and $D^-(\mathtt{n})$ hold. So, we have extended the path with one edge and we can go back to the beginning of the description of the general case.

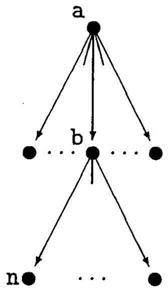


Figure 3.8: Case (iv)

Case(v) $D^+(\mathtt{b})$ is true and $\mathtt{b}$ is a leaf:

In this case we make use of Lemma 3.4.6 and we conclude that $C(\mathtt{b})$ is a suitable set of vectors for (Γ, Δ) and set of possible secrets $GF(q)^k$ with parameters p_i, $1 \leq i \leq n$!

We have described an exhaustive search with backtracking. In Subsection 3.4.5 we summarize some small improvements of our algorithm. In Subsection 3.4.4 we describe procedure `Dplus`. In the next subsection we analyse the complexity of the search algorithm.

3.4.3 Complexity Analysis

In the worst-case the algorithm applies `Dplus` for each edge. As we shall see in the next subsection the evaluation of `Dplus` costs at most

$$c_{\mathtt{Dplus}} tp[\mathcal{P}]^2$$

q-ary multiplications and additions, where $c_{\mathtt{Dplus}}$ is a problem independent constant. The number of edges is upper bounded by $|\mathcal{E}| = rk$ times the number of leafs. We notice that a node on level s has at most $q^{p[X_{i_s+1}]} - 1$ outgoing edges labeled by singleton sets unequal to $\{\mathbf{0}\}$. Let $\mathcal{S} \subseteq \{1, \ldots, rk\}$. Then there are no leafs with $\mathcal{S}(\mathtt{l}) = \mathcal{S}$ if $|\mathcal{S}| > p[\mathcal{P}]$ (cf. (3.4)). If $|\mathcal{S}| \leq p[\mathcal{P}]$ then the number of leafs $\mathtt{l}$ with $\mathcal{S}(\mathtt{l}) = \mathcal{S}$ is at most

$$\prod_{s \in \mathcal{S}} (q^{p[X_{i_s}]} - 1).$$

We conclude that the number of leafs is at most

$$\sum_{\mathcal{S}\subseteq\{1,\ldots,rk\},|\mathcal{S}|\leq p[\mathcal{P}]} \prod_{s\in\mathcal{S}} (q^{p[X_{i_s}]} - 1). \tag{3.8}$$

Thus the worst-case complexity is at most $c_{\texttt{Algorithm}} rktp[\mathcal{P}]^2$ times this number, where $c_{\texttt{Algorithm}}$ is a problem independent constant. If $p[\mathcal{P}] \geq rk$ then (3.8) equals

$$\prod_{1\leq s\leq rk} q^{p[X_{i_s}]} = \prod_{(i,j)\in\mathcal{E}} q^{p[X_i]} = \left(\prod_{X\in[\Gamma]^-} q^{p[X]}\right)^k = q^{k\sum_{X\in[\Gamma]^-} p[X]}.$$

If $rk \geq p[\mathcal{P}]$ then

$$\begin{aligned} & \sum_{\mathcal{S}\subseteq\{1,\ldots,rk\},|\mathcal{S}|\leq p[\mathcal{P}]} \prod_{s\in\mathcal{S}} (q^{p[X_{i_s}]} - 1) \\ \leq & \sum_{0\leq i\leq p[\mathcal{P}]} \binom{rk}{i} \left(q^{\max\{p[X]:X\in[\Gamma]^-\}} - 1\right)^i \\ \leq & \binom{rk}{p[\mathcal{P}]} q^{p[\mathcal{P}]\max\{p[X]:X\in[\Gamma]^-\}}. \end{aligned}$$

So, in practise we can only apply our algorithm if parameters q, k, r, $p[\mathcal{P}]$, and $\sum_{X\in[\Gamma]^-} p[X]$ are not too large. In that case our algorithm is much faster than an exhaustive search for a matrix $G[\mathcal{P}]$ defining a suitable set of matrices, for which

$$\left(\begin{array}{c|c} \begin{matrix} I_k \\ O \end{matrix} & G[\mathcal{P}] \end{array}\right)$$

has full row rank (w.l.o.g. this matrix has full row rank if it defines a suitable set of matrices, see Theorem 3.1.2, such an algorithm has a worst-case complexity of order $q^{p[\mathcal{P}](k+p[\mathcal{P}])}$). If parameters q, k, r, $p[\mathcal{P}]$, and $\sum_{X\in[\Gamma]^-} p[X]$ are large then any exhaustive search algorithm is impractical.

The complexity of our algorithm is asymmetric in $[\Gamma]^-$ and $[\Gamma^\perp]^-$. In Section 3.5 we mention as a side-result that there exists a generalized vector space construction for access structure (Γ, Δ) and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$ iff there exists a generalized vector space construction for $(\Gamma^\perp, \Delta^\perp)$ and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$ [57, 51]. Thus the problem of finding suitable sets of vectors is symmetric in $[\Gamma]^-$ and $[\Gamma^\perp]^-$. For this reason it may sometimes be advantageous to apply our algorithm to the dual scheme $(\Gamma^\perp, \Delta^\perp)$.

3.4.4 Procedure `Dplus`

We will describe `Dplus` by using the following lemma's, of which the first will be proved by means of Theorem 3.3.3 and its proof.

Lemma 3.4.11 *Let* a *and* b *be nodes such that* $D^+(\mathtt{a})$ *holds and such that there is an edge from* a *to* b *labeled by a singleton set* $\{\mathbf{c}\} \neq \{\mathbf{0}\}$. *Let matrices* $A_i(\mathtt{a})$, $1 \leq i \leq t$, *matrices* $B_i(\mathtt{a})$, $1 \leq i \leq t$, *and set* $C(\mathtt{a})$ *have the properties as described in Lemma 3.4.8 [A], [B], and [C]. Let* s *be the level of node* b *and let* $\mathbf{e} = \mathbf{e}^{j_s}$. *Then the following results hold.*

(i) Node b *is a candidate node.*

(ii) $D^+(\mathtt{b})$ *is true iff for each* $1 \leq i \leq t$ *condition* $\mathbf{c}_{D_i^c} A_i(\mathtt{a}) = \mathbf{e}$ *or condition* $\mathbf{c}_{D_i^c} B_i(\mathtt{a}) \neq \mathbf{0}$ *holds.*

Suppose that $D^+(\mathtt{b})$ *holds and let* $1 \leq i \leq t$.

(iii) If $\mathbf{c}_{D_i^c} A_i(\mathtt{a}) = \mathbf{e}$ *then* $A_i(\mathtt{a})$ *is an example of a solution for* $A_i(\mathtt{b})$ *in Lemma 3.4.8 [A].*

(iv) If $\mathbf{c}_{D_i^c} B_i(\mathtt{a}) \neq \mathbf{0}$ *and* $\mathbf{b}$ *is a column of* $B_i(\mathtt{a})$ *such that* $\mathbf{c}_{D_i^c}\mathbf{b} \neq 0$ *then*

$$A_i(\mathtt{a}) + \mathbf{b}(\mathbf{c}_{D_i^c}\mathbf{b})^{-1}(\mathbf{e} - \mathbf{c}_{D_i^c} A_i(\mathtt{a}))$$

is an example of a solution for $A_i(\mathtt{b})$ *in Lemma 3.4.8 [A].*

(v) If $\mathbf{c}_{D_i^c} B_i(\mathtt{a}) = \mathbf{0}$ *then* $B_i(\mathtt{a})$ *is an example of a solution for* $B_i(\mathtt{b})$ *in Lemma 3.4.8 [B].*

(vi) If $\mathbf{c}_{D_i^c} B_i(\mathtt{a}) \neq \mathbf{0}$ *and* $\mathbf{b}$ *is a column of* $B_i(\mathtt{a})$ *such that* $\mathbf{c}_{D_i^c}\mathbf{b} \neq 0$ *then*

$$B_i(\mathtt{a}) - \mathbf{b}(\mathbf{c}_{D_i^c}\mathbf{b})^{-1}\mathbf{c}_{D_i^c} B_i(\mathtt{a})$$

is an example of a solution for $B_i(\mathtt{b})$ *in Lemma 3.4.8 [B].*

(vii) $C(\mathtt{a}) \cup \{\mathbf{c}^{i_s,j_s} = \mathbf{c}\}$ *is an example of a solution for* $C(\mathtt{b})$ *in Lemma 3.4.8 [C].*

Proof: (i) This has already been shown in Lemma 3.4.3.

(ii) We want to compute $D^+(\mathtt{b})$. Let $C = \{\mathbf{c}^{i_m,j_m} : 1 \leq m \leq rk\}$ be any set of vectors corresponding to node b. We notice that $\mathcal{S}(\mathtt{b}) = \mathcal{S}(\mathtt{a}) \cup \{s\}$, hence, $\mathcal{E}(\mathtt{b}) = \mathcal{E}(\mathtt{a}) \cup \{(i_s, j_s)\}$, and that $\mathbf{c}^{i_s,j_s} = \mathbf{c}$. Let $1 \leq i \leq t$. Since $D^+(\mathtt{a})$ holds we have that C has the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{a})$ and $D_i \in [\Delta]^+$ (see Definition 3.3.1). Theorem 3.3.3 tells us that C has the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{b})$ and $D_i \in [\Delta]^+$ iff $\mathbf{c}_{D_i^c} A_i(\mathtt{a}) = \mathbf{e}$ or $\mathbf{c}_{D_i^c} B_i(\mathtt{a}) \neq \mathbf{0}$. This proves that all sets of vectors corresponding to node b have the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{b})$ iff for each $1 \leq i \leq t$ condition $\mathbf{c}_{D_i^c} A_i(\mathtt{a}) = \mathbf{e}$ or condition $\mathbf{c}_{D_i^c} B_i(\mathtt{a}) \neq \mathbf{0}$ holds. Together with (i) this proves (ii).

(iii), (iv) We infer both statements from the proof of Theorem 3.3.3.

(v) follows trivially from the definition of the matrices $B_i(\mathtt{b})$ in Lemma 3.4.8 [B].

(vi) Suppose that $\mathbf{c}_{D_i^c}B_i(\mathsf{a}) \neq \mathbf{0}$ and that $\mathbf{b}$ is a column of $B_i(\mathsf{a})$ such that $\mathbf{c}_{D_i^c}\mathbf{b} \neq 0$. Let $B = B_i(\mathsf{a}) - \mathbf{b}(\mathbf{c}_{D_i^c}\mathbf{b})^{-1}\mathbf{c}_{D_i^c}B_i(\mathsf{a})$. Then $\mathbf{c}_{D_i^c}B = \mathbf{0}$. Let $\mathbf{v}$ be some row of $C[\mathcal{E}(\mathsf{a}), D_i]$. Then $\mathbf{v}B_i(\mathsf{a}) = \mathbf{0}$ (see Lemma 3.4.8 [B]) and in particular $\mathbf{vb} = 0$. Hence, $\mathbf{v}B = \mathbf{0}$. Thus the columns of B span a subspace of the right zero space of $C[\mathcal{E}(\mathsf{b}), D_i]$.

Let $C[\mathcal{E}(\mathsf{b}), D_i]\mathbf{v}^T = \mathbf{0}^T$. Then $C[\mathcal{E}(\mathsf{a}), D_i]\mathbf{v}^T = \mathbf{0}^T$ and $\mathbf{c}_{D_i^c}\mathbf{v}^T = 0$. Thus, $\mathbf{v}^T = B_i(\mathsf{a})\mathbf{d}^T$ is a linear combination of the columns of $B_i(\mathsf{a})$. Hence,

$$\begin{aligned} B\mathbf{d}^T &= B_i(\mathsf{a})\mathbf{d}^T - \mathbf{b}(\mathbf{c}_{D_i^c}\mathbf{b})^{-1}\mathbf{c}_{D_i^c}B_i(\mathsf{a})\mathbf{d}^T \\ &= \mathbf{v}^T - \mathbf{b}(\mathbf{c}_{D_i^c}\mathbf{b})^{-1}\mathbf{c}_{D_i^c}\mathbf{v}^T \\ &= \mathbf{v}^T. \end{aligned}$$

Thus $\mathbf{v}$ is a linear combination of the columns of B. We conclude that the columns of B span the right zero space of $C[\mathcal{E}(\mathsf{b}), D_i]$. Thus B is an example of a solution for $B_i(\mathsf{b})$ in Lemma 3.4.8 [B].

(vii) follows trivially from the definition of candidate nodes and sets of candidate vectors.

□

Lemma 3.4.12 *Let* a *and* b *be nodes such that* $D^+(\mathsf{a})$ *holds and such that there is an edge from* a *to* b *not labeled by a singleton set* $\{\mathbf{c}\} \neq \{\mathbf{0}\}$. *Let matrices* $A_i(\mathsf{a})$, $1 \leq i \leq t$, *matrices* $B_i(\mathsf{a})$, $1 \leq i \leq t$, *and set* $C(\mathsf{a})$ *have the properties as described in Lemma 3.4.8 [A], [B], and [C]. Let* s *be the level of node* b *and let* $C(\mathsf{a}) = \{\mathbf{c}^{i_m, j_m} = \mathbf{c}^m : 1 \leq m \leq s-1\}$. *Then the following results hold.*

(i) The $d^+(\Delta)$*-property for* $\mathcal{E}(\mathsf{b})$ *holds for any set of vectors corresponding to node* b.

(ii) $D^+(\mathsf{b})$ *is true iff there exist q-ary elements* $b_m, m \in \mathcal{S}(\mathsf{a})$, *such that*

$$(\mathbf{e}^{j_s}, \mathbf{0}) = \sum_{m \in \mathcal{S}(\mathsf{a})} b_m(e^{j_m}, \mathbf{c}^m_{X^c_{i_s}}),$$

where $\mathbf{0}$ *is the all-zero vector of length* $p[X^c_{i_s}]$.

Suppose that $D^+(\mathsf{b})$ *holds and let* $1 \leq i \leq t$. *Further, let elements* $b_m, m \in \mathcal{S}(\mathsf{a})$, *have the property as described in (ii). Then the next results hold.*

(iii) $A_i(\mathsf{a})$ *is an example of a solution for* $A_i(\mathsf{b})$ *in Lemma 3.4.8 [A].*

(iv) $B_i(\mathsf{a})$ *is an example of a solution for* $B_i(\mathsf{b})$ *in Lemma 3.4.8 [B].*

(v) $C(\mathsf{a}) \cup \{\mathbf{c}^{i_s, j_s} = \sum_{m \in \mathcal{S}(\mathsf{a})} b_m \mathbf{c}^m\}$ *is an example of a solution for* $C(\mathsf{b})$ *in Lemma 3.4.8 [C].*

Proof: (i) Sets $\mathcal{S}(\mathtt{a})$ and $\mathcal{S}(\mathtt{b})$ are the same because $s \notin \mathcal{S}(\mathtt{b})$. Hence, $\mathcal{E}(\mathtt{a}) = \mathcal{E}(\mathtt{b})$. We notice that $D^+(\mathtt{a})$ is true. Thus the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{a}) = \mathcal{E}(\mathtt{b})$ holds for any set of vectors corresponding to a. We notice that if a set corresponds to b then it also corresponds to a. Hence, the $d^+(\Delta)$-property for $\mathcal{E}(\mathtt{b})$ holds for any set of vectors corresponding to node b.

(ii) From (i) we infer that $D^+(\mathtt{b})$ holds iff b is a candidate node. Since $D^+(\mathtt{a})$ is true a is a candidate node. Hence, b is a candidate node iff the edge from a to b has a label S^s such that there exists a vector $\mathbf{c} \in S^s$ with $(\mathbf{e}^{j_s}, \mathbf{c}) \in \mathcal{C}_L(\mathtt{b})$. We notice that $\mathcal{C}_L(\mathtt{b}) = \mathcal{C}_L(\mathtt{a})$ since $\mathcal{S}(\mathtt{a}) = \mathcal{S}(\mathtt{b})$. Further, by Lemma 3.4.4 $\mathcal{C}_L(\mathtt{a})$ is spanned by the vectors $(\mathbf{e}^{j_m}, \mathbf{c}^m), m \in \mathcal{S}(\mathtt{a})$. A vector $\mathbf{c} \in S^s$ iff $sup_p(\mathbf{c}) \subseteq X_{i_s}$ and $\mathbf{c} \in \mathcal{C}(\mathtt{a})$. We notice that $\mathcal{C}(\mathtt{a})$ is spanned by the vectors $\mathbf{c}^m, m \in \mathcal{S}(\mathtt{a})$. We conclude that b is a candidate node iff there exists a vector $\mathbf{c}$ with $sup_p(\mathbf{c}) \subseteq X_{i_s}$ such that $(\mathbf{e}^{j_s}, \mathbf{c})$ is a linear combination of the vectors $(\mathbf{e}^{j_m}, \mathbf{c}^m), m \in \mathcal{S}(\mathtt{a})$. Thus, b is a candidate node iff $(\mathbf{e}^{j_s}, \mathbf{0})$ is a linear combination of the vectors $(\mathbf{e}^{j_m}, \mathbf{c}^m_{X^c_{i_s}}), m \in \mathcal{S}(\mathtt{a})$. This proves the second statement. Furthermore if $(\mathbf{e}^{j_s}, \mathbf{0}) = \sum_{m \in \mathcal{S}(\mathtt{a})} b_m(e^{j_m}, \mathbf{c}^m_{X^c_{i_s}})$ then $\mathbf{c} = \sum_{m \in \mathcal{S}(\mathtt{a})} b_m \mathbf{c}^m \in S^s$ and $(\mathbf{e}^{j_s}, \mathbf{c}) \in \mathcal{C}_L(\mathtt{b})$. This proves (v).

(iii), (iv) Both statements follow from Lemma 3.4.10 and $\mathcal{E}(\mathtt{a}) = \mathcal{E}(\mathtt{b})$.

(v) See the proof of (ii).

□

The description of `Dplus` follows immediately from Lemma's 3.4.11 and 3.4.12 and is depicted in Table 3.2. The loop in `Dplus` will be processed at most t times. In `Dplus` we add $p[\mathcal{P}] \times p[\mathcal{P}]$ matrices or we multiply vectors with these matrices. So, the evaluation of `Dplus` costs at most

$$c_{\mathtt{Dplus}} t p[\mathcal{P}]^2$$

q-ary multiplications and additions, where $c_{\mathtt{Dplus}}$ is a problem independent constant.

3.4.5 Refinements

We first mention some necessary conditions for a set of vectors to be suitable. Using this we will show that w.l.o.g. we can fix some vectors of a to be found suitable set of vectors, which leads to a refinement of our search algorithm.

Lemma 3.4.13 *Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, \ldots, n\}$ and let C be a suitable set of vectors for (Γ, Δ). Let f_i, $1 \leq i \leq n$, be automorphisms of $(GF(q)^{p_i}, +)$. Define for $\mathbf{c}^i \in GF(q)^{p_i}$, $1 \leq i \leq n$, function f by*

$$f(\mathbf{c}^1, \ldots, \mathbf{c}^n) = (f_1(\mathbf{c}^1), \ldots, f_n(\mathbf{c}^n)).$$

Then $\{f(\mathbf{c}) : \mathbf{c} \in C\}$ is a suitable set of vectors for (Γ, Δ).

```
Algorithm:

• Let $s$ be the level of node $\mathtt{b}$.
• If the label of the edge from $\mathtt{a}$ to $\mathtt{b}$ is a singleton set $\{\mathbf{c}\}$, with $\mathbf{c} \neq \mathbf{0}$ then:
    – Compute $C(\mathtt{b}) := C(\mathtt{a}) \cup \{\mathbf{c}^{i_s,j_s} = \mathbf{c}\}$.
    – Compute $\mathbf{e} := \mathbf{e}^{j_s}$ and give the boolean variable stop the value false. (If stop is true then $\mathbf{c}_{D_i^c} A_i(\mathtt{a}) = \mathbf{e}$ or $\mathbf{c}_{D_i^c} B_i(\mathtt{a}) \neq \mathbf{0}$ for some $1 \leq i \leq t$, hence, $D^+(\mathtt{b})$ does not hold.)
    – For $1 \leq i \leq t$, until stop is true:
        ∗ Compute $\mathbf{f} := \mathbf{e} - \mathbf{c}_{D_i^c} A_i(\mathtt{a})$.
        ∗ If there exists a column $\mathbf{b}$ of $B_i(\mathtt{a})$ such that $\mathbf{c}_{D_i^c}\mathbf{b} \neq 0$ then:
            · If $\mathbf{f} \neq \mathbf{0}$ compute $A_i(\mathtt{b}) := A_i(\mathtt{a}) + \mathbf{b}(\mathbf{c}_{D_i^c}\mathbf{b})^{-1}\mathbf{f}$.
            · If $\mathbf{f} = \mathbf{0}$ compute $A_i(\mathtt{b}) := A_i(\mathtt{a})$.
            · Compute $B_i(\mathtt{b}) := B_i(\mathtt{b}) - \mathbf{b}(\mathbf{c}_{D_i^c}\mathbf{b})^{-1}\mathbf{c}_{D_i^c} B_i(\mathtt{a})$.
        ∗ Otherwise ($\mathbf{c}_{D_i^c} B_i(\mathtt{a}) = \mathbf{0}$):
            · Compute $A_i(\mathtt{b}) := A_i(\mathtt{a})$ and $B_i(\mathtt{b}) := B_i(\mathtt{a})$.
            · Compute the boolean variable stop $:= \neg(\mathbf{f} = \mathbf{0})$.
    – The value of $D^+(\mathbf{b})$ will be $\neg$stop.
• Otherwise (the label of the edge from $\mathtt{a}$ to $\mathtt{b}$ is not a singleton set unequal to $\{\mathbf{0}\}$):
    – Compute $A_i(\mathtt{b}) := A_i(\mathtt{a})$ and $B_i(\mathtt{b}) := B_i(\mathtt{a})$ for $1 \leq i \leq t$.
    – Search for $b_m, m \in \mathcal{S}(\mathtt{a})$, such that $(\mathbf{e}^{j_s}, \mathbf{0}) = \sum_{m \in \mathcal{S}(\mathtt{a})} b_m(e^{j_m}, \mathbf{c}^m_{X_{i_s}^c})$.
    – The value of $D^+(\mathbf{b})$ is true iff $b_m$ exists for all $m \in \mathcal{S}(\mathtt{a})$.
    – If $D^+(\mathbf{b})$ is true compute $C(\mathtt{b}) := C(\mathtt{a}) \cup \{\mathbf{c}^{i_s,j_s} = \sum_{m \in \mathcal{S}(\mathtt{a})} b_m \mathbf{c}^m\}$.
```

Table 3.2: Procedure Dplus

Proof: For linear combinations of $\mathbf{c}^{i,j}$ we have that

$$sup_p(\sum B_{i,j}f(\mathbf{c}^{i,j})) = sup_p(f(\sum B_{i,j}\mathbf{c}^{i,j})) = sup_p(\sum B_{i,j}\mathbf{c}^{i,j}).$$

Hence, the p-support, and therefore the $g(\Gamma)$- and $d^-(\Delta)$-property remain invariant under application of function f.

□

Lemma 3.4.14 *Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, \ldots, n\}$. Let $\{X_1, \ldots, X_r\}$ be the minimal elements of Γ. Let $C = \{\mathbf{c}^{i,j} : (i,j) \in \mathcal{E}\}$, where $\mathcal{E} = \{(i,j) : 1 \leq i \leq r, 1 \leq j \leq k\}$, be a suitable set of vectors for (Γ, Δ). Suppose $X \subseteq X_i$ such that $X_i \setminus X \in \Delta$. Then the vectors in $\{\mathbf{c}_X^{i,j} : 1 \leq j \leq k\} \subseteq GF(q)^{p[X]}$ are linearly independent. Hence, $k \leq p[X]$.*

Proof: If $\sum_{1 \leq j \leq k} b_j \mathbf{c}_X^{i,j} = \mathbf{0}$ then $sup_p(\sum_{1 \leq j \leq k} b_j \mathbf{c}^{i,j}) \subseteq X_i \setminus X \in \Delta$, and hence $b_j = 0$ for $1 \leq j \leq k$ by the $d^-(\Delta)$-property for C.

□

For connected complete access structures Γ each participant m is member of some group $X_i \in [\Gamma]^-$. Since $X_i \setminus \{m\} \in \Delta$ inequality $k \leq p_m$ holds by Lemma 3.4.14. Thus, if $k > p_m$ for some participant m then the generalized vector space construction can only lead to schemes having access structures (Γ, Δ) where $\Delta \neq \Gamma^c$. This particular class of access structures has been studied by Bertilsson [9].

The previous lemma's immediately lead to the following result.

Corollary 3.4.15 *Let Γ be a complete access structure on $\mathcal{P} = \{1, \ldots, n\}$ defined by $[\Gamma]^- = \{X_1, \ldots, X_r\}$. Let $\{\mathbf{c}^{i,j} : (i,j) \in \mathcal{E}\}$, where $\mathcal{E} = \{(i,j) : 1 \leq i \leq r, 1 \leq j \leq k\}$, be a suitable set for Γ. Then without loss of generality $\mathbf{c}_{\{m\}}^{i,j} = \mathbf{e}^j \in GF(q)^{p_m}$ if $m \in X_i$ and $m \notin X_h$ for $h < i$.*

Proof: Let $m \in X_i$ and $m \notin X_h$ for $h < i$. From Lemma 3.4.14 we infer that $\mathbf{c}_{\{m\}}^{i,j}$, $1 \leq j \leq k$, are linearly independent. Hence, there exist automorphisms f_i, $1 \leq i \leq n$, such that $f_m(\mathbf{c}_{\{m\}}^{i,j}) = \mathbf{e}^j$, $1 \leq j \leq k$. Now Lemma 3.4.13 proves the corollary.

□

Lemma 3.4.14 and Corollary 3.4.15 can be used to fix w.l.o.g. some vectors of a to be found suitable set of vectors. The next lemma shows that sometimes searching for a solution in one part of the tree is equivalent to searching for a solution in other parts of the tree. This can be used to refine the search algorithm in some cases.

Lemma 3.4.16 *Let (Γ, Δ) be an access structure defined by $[\Gamma]^- = \{X_1, \ldots, X_r\}$ and $[\Delta]^+ = \{D_1, \ldots, D_t\}$. Let C be a suitable set of vectors for (Γ, Δ). Let f be a permutation of the elements in $\mathcal{P}$. Suppose that $[\Gamma]^- = \{\{f(x) : x \in X_i\} : 1 \leq i \leq r\}$ and $[\Delta]^- = \{\{f(x) : x \in D_i\} : 1 \leq i \leq t\}$. Then*

$$\{(\mathbf{c}_{\{f(1)\}}, \ldots, \mathbf{c}_{\{f(n)\}}) : \mathbf{c} \in C\}$$

is a suitable set of vectors for (Γ, Δ) *as well.*

Proof: Follows immediately from Definition 3.2.2.

□

3.5 Duality Result

Let $n = |\mathcal{P}|$, q be a prime power, and numbers k, p_i, $1 \leq i \leq n$, be integers. We will prove that there exists a generalized vector space construction for access structure (Γ, Δ) and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$ iff there exists a generalized vector space construction for $(\Gamma^\perp, \Delta^\perp)$ and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$. The following lemma and theorem characterize suitable sets of vectors for an access structure by using its dual access structure.

Lemma 3.5.1 *Let* (Γ, Δ) *be an access structure on* $\mathcal{P} = \{1, \ldots, n\}$ *and let* $\mathcal{S} = GF(q)^k$ *be a set of possible secrets. Let* $[\Gamma]^- = \{X_1, \ldots, X_r\}$ *and* $[\Gamma^\perp]^- = \{Z_1, \ldots, Z_t\}$. *We define* $\mathcal{E}$ *by* $\{(i,j) : 1 \leq i \leq r, 1 \leq j \leq k\}$ *and* $\mathcal{E}^\perp$ *by* $\mathcal{E}^\perp = \{(m,j) : 1 \leq m \leq t, 1 \leq j \leq k\}$. *Let* $C = \{\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]} : (i,j) \in \mathcal{E}\}$ *and* $H = \{\mathbf{h}^{m,j} \in GF(q)^{p[\mathcal{P}]} : (m,j) \in \mathcal{E}^\perp\}$ *be sets of vectors.*

Corresponding to C *let the q-ary* $k \times p[\mathcal{P}]$ *matrix* $C[X]$, $X = X_i \in [\Gamma]^-$, *be defined by the* k *rows* $C[X]_j = \mathbf{c}^{i,j}$, $1 \leq j \leq k$. *In a similar way we define corresponding to* H *the q-ary* $k \times p[\mathcal{P}]$ *matrix* $H[Z]$, $Z = Z_i \in [\Gamma^\perp]^-$, *by the* k *rows* $H[Z]_j = \mathbf{h}^{i,j}$, $1 \leq j \leq k$.

Then C *has the* $d^-(\Delta)$*-property iff there exists a set* H *having the* $g(\Gamma^\perp)$*-property such that* $C[X]H[Z]^T = -I_k$ *for all* $Z \in [\Gamma^\perp]^-$ *and all* $X \in [\Gamma]^-$.

Proof: We will start proving the left to right implication. Suppose that C has the $d^-(\Delta)$-property. We define $\mathcal{E}(i)$, $1 \leq i \leq r$, by $\mathcal{E}(i) = \{(i,j) : 1 \leq j \leq k\}$ and we define $\mathcal{E}^\perp(m)$, $1 \leq m \leq t$, by $\mathcal{E}^\perp(m) = \{(m,j) : 1 \leq j \leq k\}$. We notice that $[\Delta]^+ = \{(Z_m)^c : 1 \leq m \leq t\}$ by Lemma 1.3.2(ii). Further we note that w.l.o.g. $C[X_i] = C[\mathcal{E}(i), \emptyset]$ and $I[\mathcal{E}(i), (Z_m)^c] = I_k$ for $1 \leq i \leq r$ and $1 \leq m \leq t$ (see Definition 3.3.1).

By Theorem 3.3.2 there exist matrices A_m, $1 \leq m \leq t$, such that $I[\mathcal{E}, (Z_m)^c] = C[\mathcal{E}, (Z_m)^c]A_m$. Hence,

$$I_k = I[\mathcal{E}(i), (Z_m)^c] = C[\mathcal{E}(i), (Z_m)^c]A_m, \; 1 \leq i \leq r, 1 \leq m \leq t. \tag{3.9}$$

Let $(m,j) \in \mathcal{E}^\perp$. Then we define the vector $\mathbf{h}^{m,j} \in GF(q)^{p[\mathcal{P}]}$ by $\mathbf{h}^{m,j}_{Z_m} = -(\mathbf{a}^{m,j})^T$ and $supp_p(\mathbf{h}^{m,j}) \subseteq Z_m$ (i.e. $\mathbf{h}^{m,j}_{(Z_m)^c} = \mathbf{0}$), where $\mathbf{a}^{m,j}$ is the j-th column of A_m. In this way we design a set of vectors $H = \{\mathbf{h}^{m,j} : (m,j) \in \mathcal{E}^\perp\}$ having the $g(\Gamma^\perp)$-property such that

$$-A_m = \left((\mathbf{h}^{m,1}_{Z_m})^T \,\middle|\, \cdots \,\middle|\, (\mathbf{h}^{m,k}_{Z_m})^T \right). \tag{3.10}$$

By equations (3.9), (3.10), and the $g(\Gamma^\perp)$-property of H

$$\begin{aligned} -I_k &= C[\mathcal{E}(i),(Z_m)^c]\,\big(\,(\mathbf{h}^{m,1}_{Z_m})^T \,\big|\, \cdots \,\big|\, (\mathbf{h}^{m,k}_{Z_m})^T\,\big) \\ &= C[\mathcal{E}(i),\emptyset]\,\big(\,(\mathbf{h}^{m,1})^T \,\big|\, \cdots \,\big|\, (\mathbf{h}^{m,k})^T\,\big) \\ &= C[X_i]H[Z_m]^T. \end{aligned} \tag{3.11}$$

This finishes the proof of the left to right implication.

We will now prove the right to left implication. Suppose that H has the $g(\Gamma^\perp)$-property such that (3.11) holds for $1 \leq i \leq r$ and $1 \leq m \leq t$. Let $(i,j) \in \mathcal{E}$ and $(m,j') \in \mathcal{E}^\perp$. Set H has the $g(\Gamma^\perp)$-property, hence, $supp_p(\mathbf{h}^{m,j'}) \subseteq Z_m$ and we infer that

$$\begin{aligned} &\mathbf{c}^{i,j}_{Z_m}(-\mathbf{h}^{m,j'}_{Z_m})^T = -\mathbf{c}^{i,j}(\mathbf{h}^{m,j'})^T = -C[X_i]_j(H[Z_m]_{j'})^T \\ &= (-C[X_i]H[Z_m]^T)_{j,j'} = (I_k)_{j,j'} = (\mathbf{e}^j)_{j'}. \end{aligned}$$

Let A_m be defined by equation (3.10). Then we obtain equation (3.9), that is $I[\mathcal{E}(i),(Z_m)^c] = C[\mathcal{E}(i),(Z_m)^c]A_m$. Hence, $I[\mathcal{E},(Z_m)^c] = C[\mathcal{E},(Z_m)^c]A_m$. Thus C has the $d^-(\Delta)$-property.

□

This lemma leads to the following theorem. Its significance is presented in [48] in which an easier to compute upper bound of the worst-case information rate of linear schemes is proved. This upper bound is discussed in the next section.

Theorem 3.5.2 *Let (Γ,Δ) be an access structure on $\mathcal{P} = \{1,\ldots,n\}$ and let $\mathcal{S} = GF(q)^k$ be a set of possible secrets. Let p_i, $1 \leq i \leq n$, be integers. Then there exists a generalized vector space construction for (Γ,Δ) and set of possible secrets $GF(q)^k$ with convec $(p_1/k,\ldots,p_n/k)$ iff there exist q-ary $k \times p_u$ matrices $M^{X,u}$, for $X \in [\Gamma]^-$ and $u \in X$, and q-ary $k \times p_u$ matrices $N^{Z,u}$, for $Z \in [\Gamma^\perp]^-$ and $u \in Z$, such that for all $X \in [\Gamma]^-$ and $Z \in [\Gamma^\perp]^-$*

$$\sum_{u \in X \cap Z} M^{X,u}(N^{Z,u})^T = I_k.$$

Proof: Let $[\Gamma]^- = \{X_1,\ldots,X_r\}$ and $[\Gamma^\perp]^- = \{Z_1,\ldots,Z_t\}$. We infer from Theorems 3.1.2, 3.2.5, and 3.2.6 that there exists a generalized vector space construction for (Γ,Δ) and set of possible secrets $GF(q)^k$ iff there exists a suitable set of vectors C for (Γ,Δ) and set of possible secrets $GF(q)^k$ with parameters convec $(p_1/k,\ldots,p_n/k)$. Or equivalently, by Lemma 3.5.1, C has the $g(\Gamma)$-property and there exists a set H having the $g(\Gamma^\perp)$-property such that $C[X]H[Z]^T = -I_k$ for $X \in [\Gamma]^-$ and $Z \in [\Gamma^\perp]^-$.

Let $M^{X,u}$, for $X = X_i \in [\Gamma]^-$ and $u \in X$, be a q-ary $k \times p_u$ matrix defined by the rows

$$(M^{X,u})_j = \mathbf{c}^{i,j}_{\{u\}}. \tag{3.12}$$

Let $N^{Z,u}$, for $Z = Z_i \in [\Gamma^\perp]^-$ and $u \in Z$, be a q-ary $k \times p_u$ matrix defined by the rows

$$(N^{Z,u})_j = -\mathbf{h}^{i,j}_{\{u\}}. \tag{3.13}$$

Since C has the $g(\Gamma)$-property and H has the $g(\Gamma^\perp)$-property

$$\sum_{u \in X \cap Z} M^{X,u}(N^{Z,u})^T = C[X](-H[Z])^T = I_k \tag{3.14}$$

for $X \in [\Gamma]^-$ and $Z \in [\Gamma^\perp]^-$.

We have proved the left to right implication of the theorem. Now suppose that the right side holds. Then we can construct by means of (3.12) and (3.13) sets of vectors C and H having the $g(\Gamma)$-property and $g(\Gamma^\perp)$-property respectively. Then (3.14) holds again, and by Lemma 3.5.1 set C is suitable for (Γ, Δ). This finishes the proof.

□

The main result of this section is the next corollary, and is called the duality result in secret sharing. It follows immediately from the previous theorem. First Jackson and Martin [57] and later Van Dijk [41] proved the duality result for complete access structures. The generalization towards incomplete access structures described below is joint work with Wen-Ai Jackson and Keith Martin. A different (easy to understand) proof using geometry and matroid theory can be found in [51].

Corollary 3.5.3 *Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, \ldots, n\}$ and let $\mathcal{S} = GF(q)^k$ be a set of possible secrets. Let p_i, $1 \leq i \leq n$, be integers. Then there exists a generalized vector space construction for access structure (Γ, Δ) and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$ iff there exists a generalized vector space construction for $(\Gamma^\perp, \Delta^\perp)$ and set of possible secrets $GF(q)^k$ with convec $(p_1/k, \ldots, p_n/k)$.*

The last result of this section shows the relationship between duality in coding theory and duality in secret sharing.

Theorem 3.5.4 *Let (Γ, Δ) be an access structure on $\mathcal{P} = \{1, \ldots, n\}$ and let $\mathcal{S} = GF(q)^k$ be a set of possible secrets. Let $[\Gamma]^- = \{X_1, \ldots, X_r\}$ and $[\Gamma^\perp]^- = \{Z_1, \ldots, Z_t\}$. Let $\mathcal{E} := \{(i,j) : 1 \leq i \leq r, 1 \leq j \leq k\}$ and $\mathcal{E}^\perp := \{(m,j) : 1 \leq m \leq t, 1 \leq j \leq k\}$.*

Then there exists a suitable set $C = \{\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]} : (i,j) \in \mathcal{E}\}$ for (Γ, Δ) iff there exists a suitable set $H = \{\mathbf{h}^{m,j} \in GF(q)^{p[\mathcal{P}]} : (m,j) \in \mathcal{E}^\perp\}$ for $(\Gamma^\perp, \Delta^\perp)$.

Suppose there exist a suitable set C for (Γ, Δ) and a suitable set H for $(\Gamma^\perp, \Delta^\perp)$. Let $\mathcal{C}$ be the code defined by the linear span of vectors $(\mathbf{e}^j, \mathbf{c}^{i,j})$, $(i,j) \in \mathcal{E}$, and let $\mathcal{H}$ be the code defined by the linear span of vectors $(\mathbf{e}^j, \mathbf{h}^{i,j})$, $(i,j) \in \mathcal{E}^\perp$. Then w.l.o.g. codes $\mathcal{C}$ and $\mathcal{H}$ are orthogonal to one another.

Proof: Firstly, from Lemma 3.5.1 and Definition 3.2.2 we infer that $C = \{\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]} : (i,j) \in \mathcal{E}\}$ is suitable for (Γ, Δ) iff both C has the $g(\Gamma)$-property and there exists a set $H = \{\mathbf{h}^{m,j} \in GF(q)^{p[\mathcal{P}]} : (m,j) \in \mathcal{E}^{\perp}\}$ having the $g(\Gamma^{\perp})$-property such that $C[X]H[Z]^T = -I_k$ for all $Z \in [\Gamma^{\perp}]^-$ and all $X \in [\Gamma]^-$. Secondly, interchanging the role of Γ and $\Gamma^{\perp}$, and C and H we obtain by using $\Gamma = (\Gamma^{\perp})^{\perp}$ (Lemma 1.3.2(iii)) the following result. Set $H = \{\mathbf{h}^{m,j} \in GF(q)^{p[\mathcal{P}]} : (m,j) \in \mathcal{E}^{\perp}\}$ is suitable for $\Gamma^{\perp}$ iff H has the $g(\Gamma^{\perp})$-property and if there exists a set $C = \{\mathbf{c}^{i,j} \in GF(q)^{p[\mathcal{P}]} : (i,j) \in \mathcal{E}\}$ having the $g(\Gamma)$-property such that $H[Z]C[X]^T = -I_k$ (thus $C[X]H[Z]^T = -I_k$) for all $Z \in [\Gamma^{\perp}]^-$ and all $X \in [(\Gamma^{\perp})^{\perp}]^- = [\Gamma]^-$. Combination of the two statements proves the first part of the theorem. Now, notice that $\mathcal{C}$ and $\mathcal{H}$ are orthogonal to one another iff $C[X]H[Z]^T = -I_k$ for all $Z \in [\Gamma^{\perp}]^-$ and all $X \in [\Gamma]^-$. From this we infer the second part of the theorem.

□

3.6 The Optimal Linear Worst-Case Information Rate

The *optimal linear worst-case information rate* $\dot{\rho}_l(\Gamma)$ of a complete access structure Γ is defined as the supremum of all worst-case information rates of linear secret sharing schemes for Γ. Thus

$$\dot{\rho}_l(\Gamma) = \sup\left\{1/\max\{c_i : i \in \mathcal{P}\} : \begin{array}{l}\text{there exists a linear scheme for } \Gamma \\ \text{with contribution vector } (c_1, \ldots, c_n)\end{array}\right\}.$$

We notice that

$$\dot{\rho}_l(\Gamma) \leq \dot{\rho}(\Gamma).$$

The following theorem describes how to find upper bounds on the optimal linear worst-case information rate. The result is stated symmetrically in terms of the access structure of the secret sharing scheme and its dual access structure. Its proof is combinatorial and uses Theorem 3.5.2 as basis. A generalization towards incomplete access structures can be found in [48] but is difficult to use in an efficient way and difficult to explain. This section contains no proofs, all missing proofs can be found in [48]. At the end of this section we define access structures on $n = v + 2^v$ participants for which the optimal worst-case linear information rate equals $v/(2^v - 1)$ which is of order $(\log n)/n$.

Theorem 3.6.1 *Let Γ be a complete access structure on $\mathcal{P} = \{1, \ldots, n\}$.*

Let $T = \{X_0, \ldots, X_t\} \subseteq [\Gamma]^-$ such that $X_i \backslash \tilde{X}_i \neq \emptyset$ where $\tilde{X}_i = \bigcup_{0 \leq m < i} X_m$, for $0 \leq i \leq t$. Similarly, let $T^{\perp} = \{Z_0, \ldots, Z_{t^{\perp}}\} \subseteq [\Gamma^{\perp}]^-$ such that $Z_i \backslash \tilde{Z}_i \neq \emptyset$ where $\tilde{Z}_i = \bigcup_{0 \leq m < i} Z_m$, for $0 \leq i \leq t^{\perp}$. Further, let $x_i \in X_i \setminus \tilde{X}_i$, $0 \leq i \leq t$, and $z_i \in Z_i \setminus \tilde{Z}_i$, $0 \leq i \leq t^{\perp}$.

Define $\mathcal{X}$ by

$$\mathcal{X} = \{0 \leq i \leq t : X_i \cap \tilde{X}_i \cap Z \neq \emptyset \textit{ for all } Z \in T^{\perp}\}$$

and define $\mathcal{Z}$ by

$$\mathcal{Z} = \{0 \leq i \leq t^{\perp} : Z_i \cap \tilde{Z}_i \cap X \neq \emptyset \textit{ for all } X \in T\}.$$

Define $f(u)$, $u \in \mathcal{P}$, as the minimal value of

$$|\{i \in \mathcal{X} : x_i = u\}| + |\{Z \in T^{\perp} : u \in Z\}|$$

and

$$|\{i \in \mathcal{Z} : z_i = u\}| + |\{X \in T : u \in X\}|,$$

and define for $i \geq 0$

$$v_i = |\{u \in \mathcal{P} : f(u) = i\}|.$$

Suppose that $\sum_{0 \leq i \leq m} i \cdot v_i \leq t + t^{\perp}$. Then

$$\dot{\rho}_l(\Gamma) \leq \frac{\sum\limits_{m+1 \leq i} v_i}{t + t^{\perp} + 1 - \sum\limits_{0 \leq i \leq m} i \cdot v_i}.$$

We will give two examples.

Example 3.6.2 Let us consider the complete access structure Γ on $\mathcal{P} = \{1,2,3,4,5,6\}$ defined by

$$[\Gamma]^{-} = \{X_0 = 34, X_1 = 36, X_2 = 35, X_3 = 23, X_4 = 12, X_5 = 26, X_6 = 56\}.$$

Then

$$[\Gamma^c]^{+} = \{245, 145, 146, 13\}.$$

Using $[\Gamma^{\perp}]^{-} = \{X : X^c \in [\Gamma^c]^{+}\}$ we obtain

$$[\Gamma^{\perp}]^{-} = \{Z_0 = 136, Z_1 = 236, Z_2 = 235, Z_3 = 2456\}.$$

Let $t = 4$, $x_0 = 3$, $x_1 = 6$, $x_2 = 5$, $x_3 = 2$, and $x_4 = 1$, and let $t^{\perp} = 2$, $z_0 = 3$, $z_1 = 2$, and $z_2 = 5$. Notice that $\tilde{X}_0 = \emptyset$, $\tilde{X}_1 = \{34\}$, $\tilde{X}_2 = \{346\}$, $\tilde{X}_3 = \{3456\}$, and $\tilde{X}_4 = \{23456\}$. Thus elements $x_i \in X_i \setminus \tilde{X}_i$, $0 \leq i \leq t$. Further, $\mathcal{X} = \{1,2,3\}$. In a similar way we can show that elements $z_i \in Z_i \setminus \tilde{Z}_i$, $0 \leq i \leq t^{\perp}$, and $\mathcal{Z} = \{2\}$. Now, we can compute $f(1) = \min\{0+1, 0+1\} = 1$, $f(2) = \min\{1+2, 0+2\} = 2$, $f(3) = \min\{0+3, 0+4\} = 3$, $f(4) = \min\{0+0, 0+1\} = 0$, $f(5) = \min\{1+1, 1+1\} = 2$, and $f(6) = \min\{1+2, 0+1\} = 1$. Hence,

$$v_0 = 1, v_1 = 2, v_2 = 2, v_3 = 1,$$

and $v_i = 0$ for $i \geq 4$. Application of Theorem 3.6.1 with $m = 1$ leads to

$$\dot{\rho}_l(\Gamma) \leq \frac{2+1}{4+2+1-0-2} = \frac{3}{5}.$$

To our knowledge this is the best bound one can obtain by using the general information theoretical method described in Chapter 2 (see also Chapter 4, graph number 22).

Example 3.6.3 Let us consider the complete access structure Γ on $\mathcal{P} = \{1,2,3,4,5,6\}$ defined by

$$[\Gamma]^- = \{X_0 = 23, X_1 = 34, X_2 = 35, X_3 = 56, X_4 = 12, X_5 = 45, X_6 = 16\}.$$

Then

$$[\Gamma^c]^+ = \{25, 246, 136, 146, 15\},$$

and, hence,

$$[\Gamma^\perp]^- = \{Z_0 = 1346, Z_1 = 135, Z_2 = 245, Z_3 = 235, Z_4 = 2346\}.$$

Let $t = 4$, $x_0 = 3$, $x_1 = 4$, $x_2 = 5$, $x_3 = 6$, and $x_4 = 1$, and let $t^\perp = 1$, $z_0 = 3$, and $z_1 = 5$. Notice that $\tilde{X}_0 = \emptyset$, $\tilde{X}_1 = \{23\}$, $\tilde{X}_2 = \{234\}$, $\tilde{X}_3 = \{2345\}$, and $\tilde{X}_4 = \{23456\}$. Thus elements x_i are well chosen. Further, $\mathcal{X} = \{1,2\}$. In a similar way we can show that elements z_i are well chosen and $\mathcal{Z} = \emptyset$. Now, we can compute $f(1) = \min\{0+2, 0+1\} = 1$, $f(2) = \min\{0+0, 0+2\} = 0$, $f(3) = \min\{0+2, 0+3\} = 2$, $f(4) = \min\{1+1, 0+1\} = 1$, $f(5) = \min\{1+1, 0+2\} = 2$, and $f(6) = \min\{0+1, 0+1\} = 1$. Hence,

$$v_0 = 1, v_1 = 3, v_2 = 2,$$

and $v_i = 0$ for $i \geq 3$. Application of Theorem 3.6.1 with $m = 1$ leads to

$$\dot{\rho}_l(\Gamma) \leq \frac{2}{4+1+1-0-3} = \frac{2}{3}.$$

To our knowledge this is the best bound one can obtain by using the general information theoretical method described in Chapter 2 (see also Chapter 4, graph number 37).

We have applied Theorem 3.6.1 to the list of access structures presented in Chapter 4 for which the determination of the optimal worst-case information rate is still an open problem. We found exactly the same upper bounds as those presented in Chapter 4, which had been proved by using the general information theoretical method described in Chapter 2. Our combinatorial method, however, is easier to implement as an algorithm. Such an algorithm needs to search among all possible sets T, T', and corresponding elements

x_i, $i \in \mathcal{X}$, and z_i, $i \in \mathcal{Z}$. An algorithm based on the information theoretical method would need to check many more possibilities, since it uses decompositions of mutual informations and uncertainties, and each possible decomposition may lead to the best upper bound the algorithm can find. But, the information theoretical method is more general in the sense that it finds upper bounds on the optimal worst-case information rate and not only upper bounds on the optimal linear worst-case information rate. However, we notice that the most studied secret sharing schemes are linear, and for a good reason. Because the sharing and reconstruction functions used in linear schemes are linear they are efficient to compute. Since both methods seem to lead to the same bounds, Theorem 3.6.1 can be used as indication of what one can prove by using the information theoretical method.

We notice that Theorem 3.6.1 only uses subsets $T \subseteq [\Gamma]^-$ and $T^\perp \subseteq [\Gamma^\perp]^-$. Thus the bound stated in Theorem 2.2 holds for any access structure Γ for which $T \subseteq [\Gamma]^-$ and $T^\perp \subseteq [\Gamma^\perp]^-$.

In Theorem 3.6.1 elements x_i are selected such that they are different from one another, and elements z_i are selected such that they are different from one another. So, $f(u)$ is 1 or 0 plus the minimal value of $|\{Z \in T^\perp : u \in Z\}|$ and $|\{X \in T : u \in X\}|$. Suppose we modify values $f(u)$ slightly into the minimal value of

$$|\{0 \leq i \leq t : x_i = u\}| + |\{Z \in T^\perp : u \in Z\}|$$

and

$$|\{0 \leq i \leq t^\perp : z_i = u\}| + |\{X \in T : u \in X\}|.$$

Then $f(x_i) \geq 1$, $f(z_i) \geq 1$, and if $x_i = z_j$ then $f(x_i) = f(z_j) \geq 2$. Thus

$$\begin{aligned} 2 \sum_{m+1 \leq v_i} + \sum_{0 \leq i \leq m} i v_i &\geq v_1 + 2 \sum_{2 \leq i} v_i \\ &= |\{u : f(u) = 1\}| + 2|\{u : f(u) \geq 2\}| \\ &\geq t + 1 + t^\perp + 1. \end{aligned}$$

Hence, the upper bound stated in Theorem 3.6.1 will be $> 1/2$. The next theorem states that there are access structures on $n = v + 2^v$ participants for which the optimal linear worst-case information rate equals $v/(2^v - 1)$ which is of order $(\log n)/n$. Its proof uses Theorem 3.6.1. Thus $\mathcal{X}$ and $\mathcal{Z}$ play a crucial role in Theorem 3.6.1.

Theorem 3.6.4 *Let $V = \{0, \ldots, v-1\}$ be a set and let $\mathcal{P}$ be a group of participants defined by $\mathcal{P} = V \cup \{A : A \subseteq V\}$. Let Γ be an access structure on $\mathcal{P}$ with minimal elements*

$$[\Gamma]^- = \{A \cup \{B : A \subseteq B \subseteq V\} : A \subseteq V\}.$$

Then

$$[\Gamma^\perp]^- = \{A \cup \{V \setminus A\} : A \subseteq V\}$$

and

$$\rho_l(\Gamma) = \rho_l(\Gamma^\perp) = \frac{v}{2^v - 1}.$$

3.7 Ideal Schemes

We present a result which characterizes complete access structures for which ideal linear schemes exist.

Corollary 3.7.1 *For integer k and prime power q we define $GL(k,q)$ as the set of all invertible $k \times k$ matrices over $GF(q)$. Let Γ be a complete connected access structure on $\mathcal{P} = \{1, \dots, n\}$. Then there exists a generalized vector space construction for Γ leading to an ideal secret sharing scheme iff for some integer k and prime power q there exist matrices $M^{X,u} \in GL(k,q)$, for $X \in [\Gamma]^-$ and $u \in X$, and matrices $N^{Z,u} \in GL(k,q)$, for $Z \in [\Gamma^\perp]^-$ and $u \in Z$, such that for all $X \in [\Gamma]^-$ and $Z \in [\Gamma^\perp]^-$*

$$\sum_{u \in X \cap Z} M^{X,u} N^{Z,u} = I_k.$$

Proof: For ideal linear schemes $p_i = k$, $1 \leq i \leq n$. Thus, the corollary follows from Theorem 3.5.2 if we can prove in addition that the matrices $M^{X,u}$ and $N^{Z,u}$ are invertible, i.e., are in $GL(k,q)$. Let $u \in X \in [\Gamma]^-$. By Lemma 1.3.2(v) there exists an $Z \in [\Gamma^\perp]^-$ such that $X \cap Z = \{u\}$. Hence, $M^{X,u} N^{Z,u} = I_k$ and $M^{X,u}$ must be invertible. In a similar way, all matrices $N^{Z,u}$ are invertible as well.

□

To illustrate this result we consider Γ defined by

$$[\Gamma]^- = \{12, 23, 34, 14, 15, 25, 35, 45\}$$

and we wonder wether there exists a linear ideal scheme for Γ. We notice that

$$[\Gamma^c]^+ = \{13, 24, 5\}.$$

Thus by Lemma 1.3.2(ii)

$$[\Gamma^\perp]^- = \{245, 135, 1234\}.$$

In order to use Corollary 3.7.1 we want to characterize rings $\mathcal{R}$ with elements $f^{X,u}$, $X \in [\Gamma]^-$, $u \in X$, and elements $h^{Z,u}$, $Z \in [\Gamma^\perp]^-$, $u \in Z$, such that for all $X \in [\Gamma]^-$ and $Z \in [\Gamma^\perp]^-$

$$e = \sum_{u \in X \cap Z} f^{X,u} h^{Z,u}$$

where e is the identity element in $\mathcal{R}$. In other words we want to characterize rings $\mathcal{R}$ with elements g_i, $1 \leq i \leq 26$, such that

$$\begin{pmatrix} e & e & e \\ e & e & e \\ e & e & e \\ e & e & e \\ e & e & e \\ e & e & e \\ e & e & e \\ e & e & e \end{pmatrix} = \begin{pmatrix} g_1 & g_2 & 0 & 0 & 0 \\ 0 & g_3 & g_4 & 0 & 0 \\ 0 & 0 & g_5 & g_6 & 0 \\ g_7 & 0 & 0 & g_8 & 0 \\ g_9 & 0 & 0 & 0 & g_{10} \\ 0 & g_{11} & 0 & 0 & g_{12} \\ 0 & 0 & g_{13} & 0 & g_{14} \\ 0 & 0 & 0 & g_{15} & g_{16} \end{pmatrix} \begin{pmatrix} 0 & g_{17} & 0 & g_{18} & g_{19} \\ g_{20} & 0 & g_{21} & 0 & g_{22} \\ g_{23} & g_{24} & g_{25} & g_{26} & 0 \end{pmatrix}^T,$$

which equals

$$\begin{pmatrix} g_2g_{17} & g_1g_{20} & g_1g_{23}+g_2g_{24} \\ g_3g_{17} & g_4g_{21} & g_3g_{24}+g_4g_{25} \\ g_6g_{18} & g_5g_{21} & g_5g_{25}+g_6g_{26} \\ g_8g_{18} & g_7g_{20} & g_7g_{23}+g_8g_{26} \\ g_{10}g_{19} & g_9g_{20}+g_{10}g_{22} & g_9g_{23} \\ g_{11}g_{17}+g_{12}g_{19} & g_{12}g_{22} & g_{11}g_{24} \\ g_{14}g_{19} & g_{13}g_{21}+g_{14}g_{22} & g_{13}g_{25} \\ g_{15}g_{18}+g_{16}g_{19} & g_{16}g_{22} & g_{15}g_{26} \end{pmatrix}. \tag{3.15}$$

After having characterized all possible rings $\mathcal{R}$ satisfying (3.15) we wonder whether there is one isomorphic to $GL(k,q)$ for some prime power q and integer k. Then Corollary 3.7.1 tells us that only if such a ring exists then there exists a linear ideal scheme for Γ.

From (3.15) we immediately obtain that

$$\begin{array}{lll} g_1 = g_{20}^{-1}, & g_7 = g_{20}^{-1}, & g_{13} = g_{25}^{-1}, \\ g_2 = g_{17}^{-1}, & g_8 = g_{18}^{-1}, & g_{14} = g_{19}^{-1}, \\ g_3 = g_{17}^{-1}, & g_9 = g_{23}^{-1}, & g_{15} = g_{26}^{-1}, \\ g_4 = g_{21}^{-1}, & g_{10} = g_{19}^{-1}, & g_{16} = g_{22}^{-1}, \\ g_5 = g_{21}^{-1}, & g_{11} = g_{24}^{-1}, & \\ g_6 = g_{18}^{-1}, & g_{12} = g_{22}^{-1}. & \end{array} \tag{3.16}$$

Substituting these in (3.15) we get

$$\begin{array}{ll} e = g_{20}^{-1}g_{23} + g_{17}^{-1}g_{24}, & e = g_{23}^{-1}g_{20} + g_{19}^{-1}g_{22}, \\ e = g_{17}^{-1}g_{24} + g_{21}^{-1}g_{25}, & e = g_{24}^{-1}g_{17} + g_{22}^{-1}g_{19}, \\ e = g_{21}^{-1}g_{25} + g_{18}^{-1}g_{26}, & e = g_{25}^{-1}g_{21} + g_{19}^{-1}g_{22}, \\ e = g_{20}^{-1}g_{23} + g_{18}^{-1}g_{26}, & e = g_{26}^{-1}g_{18} + g_{22}^{-1}g_{19}. \end{array} \tag{3.17}$$

Thus a ring has elements satisfying (3.15) iff it has elements satisfying both (3.16) and (3.17). From the four equations on the left side of (3.17) we obtain

$$g_{20}^{-1}g_{23} = g_{21}^{-1}g_{25}, g_{17}^{-1}g_{24} = g_{18}^{-1}g_{26}. \tag{3.18}$$

We leave it to the reader to check that a ring has elements satisfying (3.17) iff it has elements satisfying both (3.18) and

$$e = g_{20}^{-1}g_{23} + g_{17}^{-1}g_{24}, e = g_{23}^{-1}g_{20} + g_{19}^{-1}g_{22}, e = g_{24}^{-1}g_{17} + g_{22}^{-1}g_{19}. \qquad (3.19)$$

Equations (3.16), (3.18), and (3.19) can be solved iff there exists an invertible element a ($a = g_{20}^{-1}g_{23}$) such that $e - a$ ($e - a = g_{17}^{-1}g_{24}$) and $e - a^{-1}$ ($e - a^{-1} = g_{19}^{-1}g_{22}$) are invertible as well and $(e - a)^{-1} + (e - a^{-1})^{-1} = e$. As the reader can check the latter equality always hold if $e - a$ and $e - a^{-1}$ are invertible. Thus a ring has a solution of the set of equations given by (3.15) iff there exists an invertible element a such that $e - a$ and $e - a^{-1}$ are invertible. For example $a = 2$ with $\mathcal{R} = GF(3)$. Since $GL(1,3) \cong GF(3)$ we conclude that there exists a linear ideal scheme for Γ.

The next corollary of this section follows immediately from the previous one and is about the vector space construction.

Corollary 3.7.2 *Let Γ be a complete connected access structure on $\mathcal{P} = \{1, \ldots, n\}$. Then there exists a vector space construction for Γ and set of possible secrets $GF(2)$ iff $|X \cap Y|$ is odd for all $X \in [\Gamma]^-$ and all $Y \in [\Gamma^\perp]^-$. Let q be a prime power. Then there exists a vector space construction for Γ and set of possible secrets $GF(q)$ if $|X \cap Y|$ equals 1 modulo q for all $X \in [\Gamma]^-$ and all $Y \in [\Gamma^\perp]^-$.*

Proof: The second statement follows immediately from Corollary 3.7.1 with $k = 1$. By taking $q = 2$ and by noticing that $GL(1,2) = \{1\}$ the first statement follows.

□

Example 3.7.3 Let $[\Gamma]^- = \{\{1,2,3\},\{1,4,5\},\{2,4,6\},\{3,5,6\}\}$. Then $[\Gamma]^- = [\Gamma^\perp]^-$, so, Γ is self-dual. By Corollary 3.7.2 there exists an ideal secret sharing scheme for Γ (which is a counter example for Theorem 27 in [9]). As in the proof of Corollary 3.7.2 we take $k = 1$, $q = 2$, and all $M^{X,u} = 1$, $X \in [\Gamma]^-$, $u \in X$. Using (3.14) we obtain (see Lemma 3.5.1 for the definition of matrices $C[X]$, $X \in [\Gamma]^-$)

$$\begin{aligned} C[123] &= (111000), \\ C[145] &= (100110), \\ C[246] &= (010101), \\ C[356] &= (001011). \end{aligned}$$

These matrices define a set of suitable vectors $C = \{\mathbf{c}^{1,1}, \ldots, \mathbf{c}^{4,1}\}$ ($k = 1$, $|\Gamma^-| = 4$) for Γ and set of possible secrets $GF(2)$. The code spanned by $(1, \mathbf{c}^{i,1})$, $1 \leq i \leq 4$, ($(1, \mathbf{c}^{4,1}) = \sum_{1 \leq i \leq 3}(1, \mathbf{c}^{i,1})$) has generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

and parity check matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

We notice that the parity check matrix is the generator matrix of the $[7,4,3]$ Hamming code. Applying Theorem 3.2.6 gives a suitable set of matrices defined by

$$G[\mathcal{P}] = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

The reader is invited to verify [V1] and [V2].

Application of Theorem 3.6.1 for checking whether there exists an ideal scheme for a given access structure leads to the last result of this section (see [48] for its proof).

Corollary 3.7.4 *Let Γ be a complete access structure. Let $T = \{X_0, \dots, X_t\} \subseteq [\Gamma]^-$ such that $X_i \setminus \tilde{X}_i \neq \emptyset$ where $\tilde{X}_i = \bigcup_{0 \le m < i} X_m$, for $0 \le i \le t+1$. Similarly, let $T^\perp = \{Z_0, \dots, Z_{t^\perp}\} \subseteq [\Gamma^\perp]^-$ such that $Z_i \setminus \tilde{Z}_i \neq \emptyset$ where $\tilde{Z}_i = \bigcup_{0 \le m < i} Z_m$, for $0 \le i \le t^\perp + 1$. Define $\mathcal{X}$ by $\mathcal{X} = \{0 \le i \le t : X_i \cap \tilde{X}_i \cap Z \neq \emptyset$ for all $Z \in T^\perp\}$ and define $\mathcal{Z}$ by $\mathcal{Z} = \{0 \le i \le t^\perp : Z_i \cap \tilde{Z}_i \cap X \neq \emptyset$ for all $X \in T\}$. Let $\tilde{X} = \bigcup_{X \in T} X$ and let $\tilde{Z} = \bigcup_{Z \in T^\perp} Z$. Then there does not exist a linear ideal scheme for Γ if*

$$|\{i \in \mathcal{X} : X_i \cap \tilde{Z} \subseteq \tilde{X}_i\}| + |\{i \in \mathcal{Z} : Z_i \cap \tilde{X} \subseteq \tilde{Z}_i\}| + |\tilde{X} \cap \tilde{Z}| \le t + t^\perp.$$

Example 3.7.5 Let us consider the complete access structure Γ on $\mathcal{P} = \{1,2,3,4\}$ defined by

$$[\Gamma]^- = \{X_0 = 12, X_1 = 23, X_2 = 34, X_3 = 24\}.$$

Then

$$[\Gamma^c]^+ = \{13, 14, 2\},$$

and, hence,

$$[\Gamma^\perp]^- = \{Z_0 = 24, Z_1 = 23, Z_2 = 134\}.$$

Let $t = 2$ and $t^\perp = 1$. Notice that $\tilde{X}_0 = \emptyset$, $\tilde{X}_1 = \{12\}$, $\tilde{X}_2 = \{123\}$, $\tilde{X} = \{1234\}$, and $\mathcal{X} = \{1\}$. Further $\tilde{Z}_0 = \emptyset$, $\tilde{Z}_1 = \{24\}$, $\tilde{Z} = \{234\}$, and $\mathcal{Z} = \emptyset$. Notice that $X_1 \cap \tilde{Z} = \{23\}$ is not a subset of $\tilde{X}_1$, and notice that $|\tilde{X} \cap \tilde{Z}| = 3$. Application of Corollary 3.7.4 tells us that there does not exist a linear ideal scheme for Γ.

Let us consider the complete access structure Γ on $\mathcal{P} = \{1, 2, 3, 4\}$ defined by

$$[\Gamma]^- = \{X_0 = 12, X_1 = 23, X_2 = 34\}.$$

Then

$$[\Gamma^c]^+ = \{13, 14, 24\},$$

and, hence,

$$[\Gamma^\perp]^- = \{Z_0 = 24, Z_1 = 23, Z_2 = 13\}.$$

By using exactly the same arguments we conclude that there does not exist a linear ideal scheme for Γ.

Chapter 4

Connected Graphs on Six Vertices

Stinson [97] determined the optimal worst-case and optimal average information rate of all possible access structures on at most four participants. There exist 30 connected graphs on at most five vertices. In [21] the optimal worst-case information rate in 26 of these and the optimal average information rate in 28 of them are determined. Stinson [99, 98] determined the exact values for the optimal worst-case information rate and optimal average information rate in the remaining connected graphs on five vertices. In this chapter we study the optimal worst-case information rate of all connected graphs on six vertices. They are listed in Section 4.2. There are in total 112 connected graphs on six vertices. The results presented in this chapter appeared in [44] and is joint work with Perry Moerland. We notice that after the time that [44] was submitted independent results on the optimal worst-case information rate and optimal average information rate were obtained in [2] and [90].

4.1 The Optimal Worst-Case Information Rate

Before analysing the optimal worst-case information rate of all connected graphs on six vertices we prove a useful lemma.

Lemma 4.1.1 *(Splitting Technique) Let Γ be an access structure with $a, b \in \mathcal{P}$, such that for all $X \subseteq \mathcal{P}$*

$$aX \in \Gamma \textit{ if and only if } b(X \setminus a) \in \Gamma.$$

Define Γ' by

$$\Gamma' = \{X \in \Gamma : a \notin X\}.$$

Then $\dot{\rho}(\Gamma) = \dot{\rho}(\Gamma')$.

Proof: Simply observe that for all intents and purposes a and b can be treated as the same participant. Hence, they can be given exactly the same share. In [27] Γ is said to be obtained from Γ' by splitting participant b. It is shown there that $\dot{\rho}(\Gamma) = \dot{\rho}(\Gamma')$.

□

We immediately obtain the following corollary, first proved by Brickell and Stinson [27].

Corollary 4.1.2 *Let G be a graph with vertices a and b such that ad is an edge iff bd is an edge for all vertices d. Define G' by deleting edges ad, for all vertices d, and by deleting vertex a. Then $\dot{\rho}(G) = \dot{\rho}(G')$.*

If Corollary 4.1.2 can be applied to connected graphs G on six vertices we can determine the optimal worst-case information rate (since the optimal worst-case information rate is known for graphs on five vertices). If G is a complete multipartite graph then the optimal information rate equals 1 (see Theorem 1.4.2).

If G is not a complete multipartite graph then $\dot{\rho}(G) \leq 2/3$ by Theorem 1.4.4. If G is one of the graphs of Figure 2.2 then $\dot{\rho}(G) \leq 3/5$ (see Corollary 2.3.3). By using Theorem 1.4.5, Theorem 1.4.7, or Theorem 3.1.2 we can prove lower bounds on $\dot{\rho}(G)$.

In Table 4.1 upper and lower bounds on the optimal worst-case information rate are listed for the connected graphs on six vertices. In 94 of the 112 connected graphs on six vertices we determine the exact value of the optimal worst-case information rate. In Table 4.1 we explain which results we use by using the following abbreviations:

M Complete Multipartite Graph (Theorem 1.4.2),

ST Splitting Technique (Corollary 4.1.2),

MCT Multiple Construction Technique (Theorem 1.4.5),

DC Decomposition Construction (Theorem 1.4.7),

GVSC Generalized Vector Space Construction (Theorem 3.1.2),

U 3/5 Upper Bound (Corollary 2.3.3).

In Table 4.1 we also give references to papers in which perfect schemes attaining the optimal worst-case information rate are constructed.

In Section 4.3 we list for the graphs with abbreviations MCT or DC, if necessary (there is no reference to a paper), the decompositions needed in Theorem 1.4.5 or Theorem 1.4.7. See Section 1.3 for an explanation how to use the decomposition listed in Section 4.3. In Section 1.3 graph 13 is discussed as an example.

Nr.	$\dot{\rho}$	Res.	Nr.	$\dot{\rho}$	Res.	Nr.	$\dot{\rho}$	Res.
1	1	M	41	2/3	ST	81	2/3	ST
2	2/3	ST	42	4/7–3/5	U,DC	82	2/3	MCT
3	2/3	ST	43	4/7–3/5	U,DC	83	2/3	ST
4	3/5	U,MCT,[19]	44	2/3	ST	84	3/5–2/3	DC
5	2/3	ST	45	2/3	MTC	85	2/3	DC
6	2/3	MCT,[21]	46	3/5–2/3	DC	86	2/3	ST
7	2/3	ST	47	2/3	ST	87	2/3	GVSC
8	2/3	ST	48	3/5	U,MCT	88	2/3	DC
9	1/2–3/5	U,MCT	49	2/3	ST	89	2/3	ST
10	3/5	U,MCT,[19]	50	2/3	ST	90	2/3	DC
11	2/3	ST	51	2/3	ST	91	5/8–2/3	DC
12	2/3	ST	52	1	M	92	2/3	ST
13	3/5	U,MCT	53	2/3	GVSC	93	4/7–2/3	DC
14	3/5	U,MCT,[19]	54	2/3	ST	94	2/3	ST
15	2/3	ST	55	3/5–2/3	DC	95	2/3	MCT
16	2/3	MCT	56	2/3	MCT	96	2/3	ST
17	2/3	ST	57	2/3	GVSC	97	2/3	DC
18	3/5	U,MCT,[19]	58	2/3	ST	98	2/3	ST
19	2/3	MCT,[21]	59	3/5–2/3	DC	99	2/3	MCT
20	2/3	ST	60	2/3	GVSC	100	1	M
21	2/3	ST	61	1/2–3/5	U,DC	101	2/3	DC
22	5/9–3/5	U,DC	62	3/5–2/3	DC	102	2/3	DC
23	2/3	ST	63	2/3	ST	103	2/3	ST
24	3/5	U,MCT	64	2/3	ST	104	2/3	MCT
25	3/5	U,MCT,[19]	65	2/3	MCT	105	1	M
26	3/5	U,MCT	66	1	M	106	2/3	DC
27	2/3	ST	67	2/3	ST	107	2/3	ST
28	2/3	ST	68	2/3	GVSC	108	1	M
29	3/5	U,DC	69	2/3	MCT	109	2/3	MCT
30	2/3	MCT	70	3/5–2/3	DC	110	1	M
31	3/5	U,DC	71	3/5–2/3	DC	111	1	M
32	2/3	ST	72	2/3	ST	112	1	M
33	2/3	GVSC	73	2/3	ST			
34	2/3	ST	74	2/3	GVSC			
35	2/3	MCT	75	3/5–2/3	DC			
36	2/3	GVSC	76	2/3	DC			
37	3/5–2/3	DC	77	3/5–2/3	DC			
38	2/3	ST	78	2/3	ST			
39	2/3	ST	79	2/3	DC			
40	5/9–3/5	U,DC	80	1	M			

Table 4.1: Optimal worst-case information rates for connected graphs on six vertices

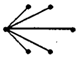
For the graphs with abbreviation GVSC the corresponding optimal schemes can be found in Section 4.4, in Example 3.1.3 (graph 33), and in Example 3.1.1 (graph 36). These have been obtained by using the algorithm of Section 3.4 (without using the notions of candidate nodes and sets of candidate vectors). Once the algorithm found optimal schemes we modified them such that in those schemes the coordinates of the secret, s_1 and s_2, and the coordinates of the random variable chosen by the MTA, a_1, a_2, ..., can be taken from any integer ring $\mathbb{Z}_m$. The algorithm also showed the following result.

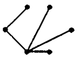
Property 4.1.3 *There does not exist a generalized vector space construction with parameters $q = 2$, $k = 2$, and $p_i \leq 3$, $1 \leq i \leq 6$, for access structures based on the graphs 37, 46, 55, and 70. Further, there does not exist a generalized vector space construction with parameters $q \in \{2, 3\}$, $k = 2$, and $p_i \leq 3$, $1 \leq i \leq 6$, for the access structure based on graph 62.*

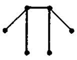
In order to obtain constructions attaining the optimal worst-case information rate we proceeded as follows. Firstly, we tried result M, if this result is not applicable we tried result ST, and so on, following the order M, ST, MCT, DC, and GVSC. For example a perfect scheme for graph 16 can be found by applying the multiple construction technique, however, the graph is not multipartite and the splitting technique is not applicable.

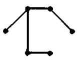
4.2 The Connected Graphs on 6 Vertices

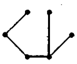
5 edges:

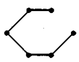

1


2

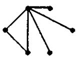

3

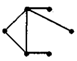

4

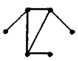

5

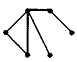

6

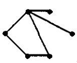
6 edges:

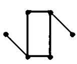

7

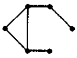

8

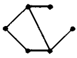

9

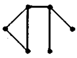

10

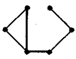

11

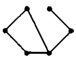

12

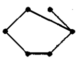

13

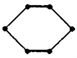

14


15

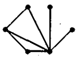

16

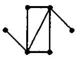

17

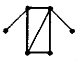

18

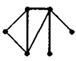

19

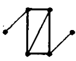
7 edges:

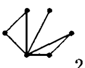

20

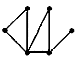

21

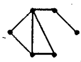

22

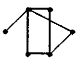

23

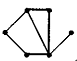

24

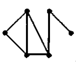

25

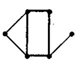

26

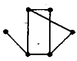

27

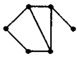

28

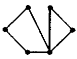

29

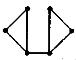

30

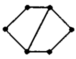

31

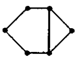

32

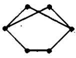

33


34

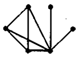

35

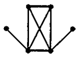

36

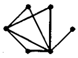

37

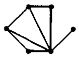

38

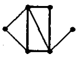
8 edges:

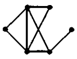

39

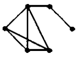

40

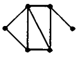

41

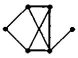

42

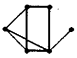

43

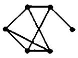

44

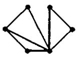

45

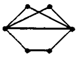

46

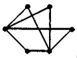

47

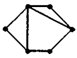

48

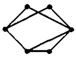

49

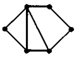

50

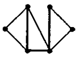

51

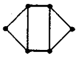

52

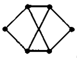

53

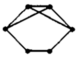

54

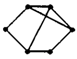

55


56

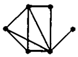

57

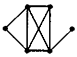

58

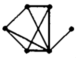

59

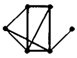

60

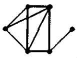
9 edges:

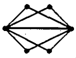

61

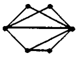

62

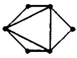

63

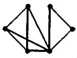

64

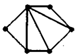

65

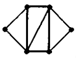

66

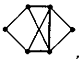

67

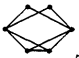

68

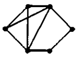

69

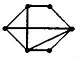

70

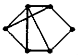

71

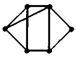

72

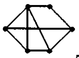

73

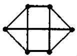

74

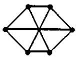

75


76

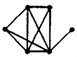

77

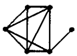

78

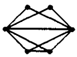

79

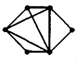

80

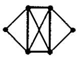
10 edges:

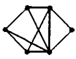

81

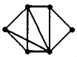

82

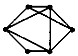

83

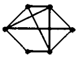

84

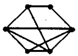

85

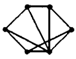

86

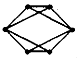

87

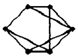
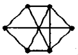

88


89

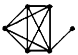
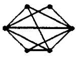
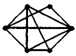
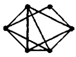
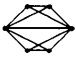
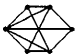
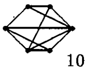
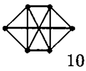
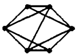

90


91

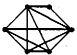
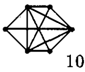
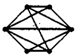
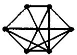
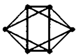

92


93

94

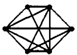
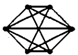
11 edges:


95

96

97

98

99

100

101

102

103

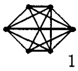
12 edges:


104

105

106

107

108

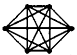
13 edges:


109

110

14 edges:

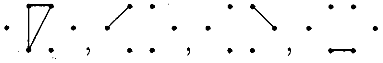

111

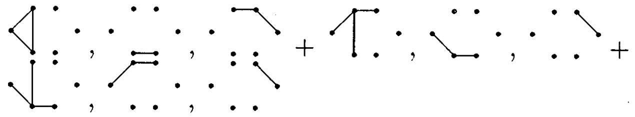
15 edges:

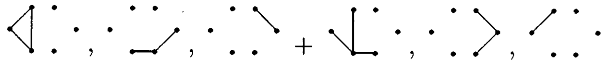

112

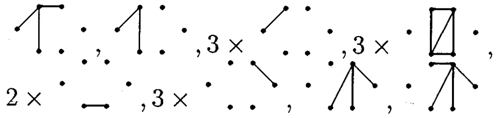
4.3 Decompositions

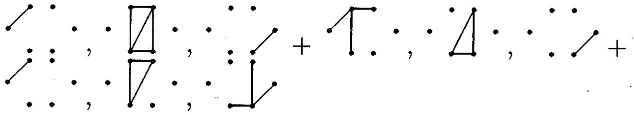
Nr. Decomposition

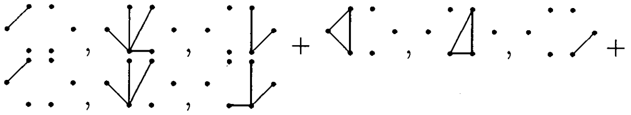
9 

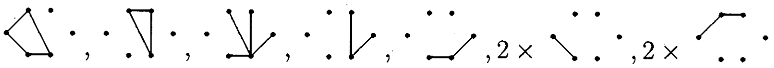
13 

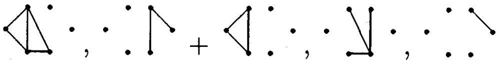
16 

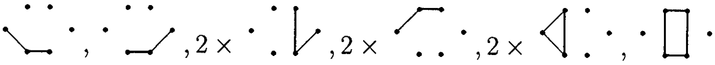
22 

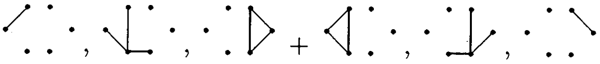
24 

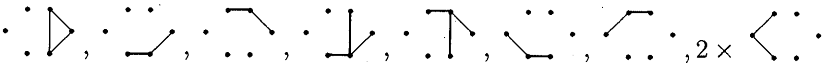
26 

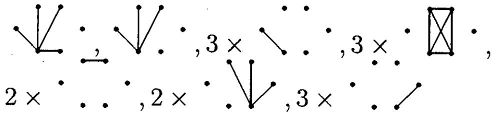
29 

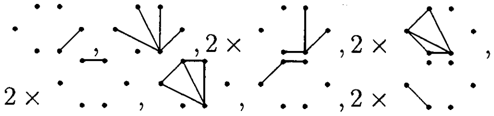
30 

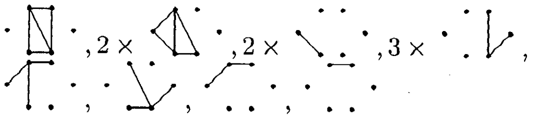
31 

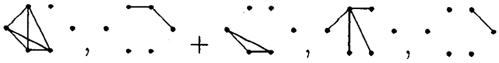
35 

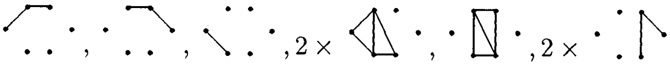
37 

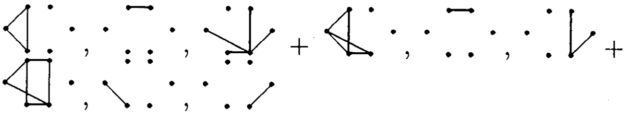
40 

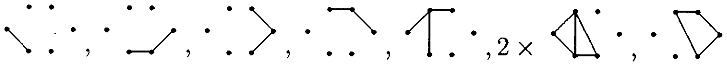
42 

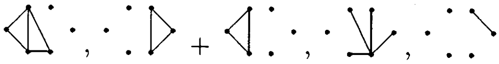
43


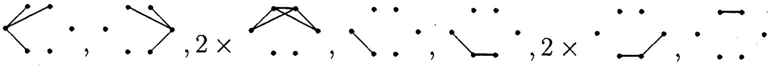
45


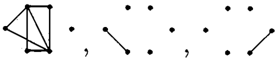
46


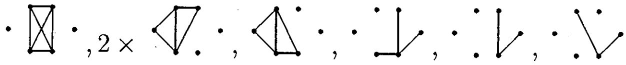
48


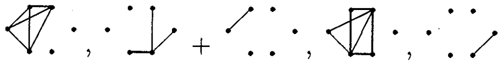
55


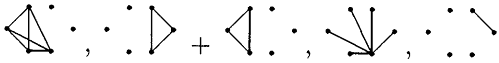
56


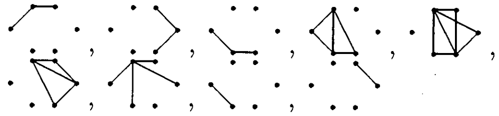
59


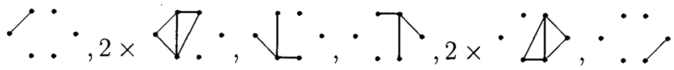
61


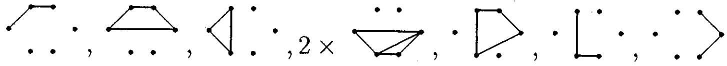
62


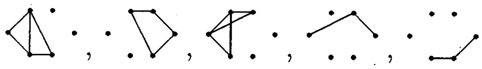
65


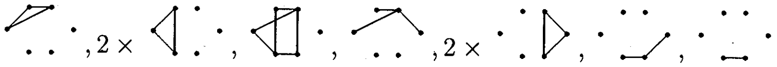
69


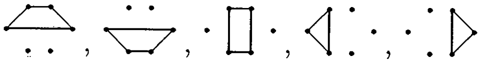
70


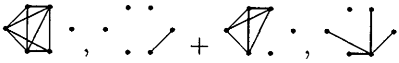
71


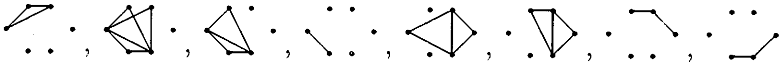
75


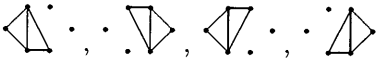
76 

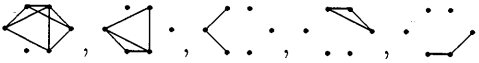
77 

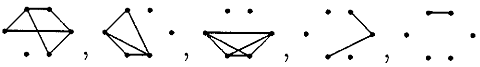
79 

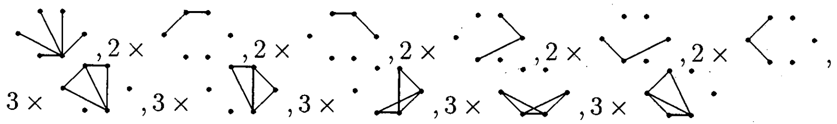
82 

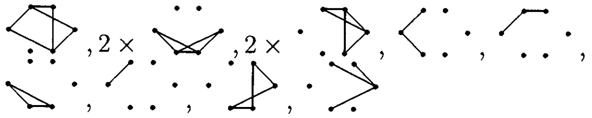
84 

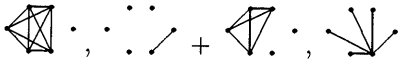
85 

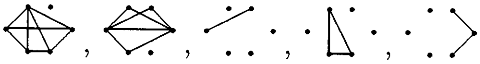
88 

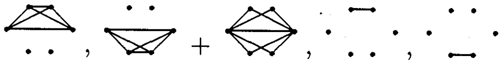
90 

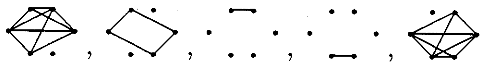
91 

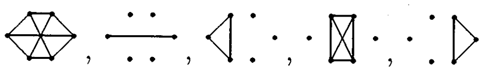
93 

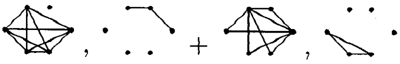
95 

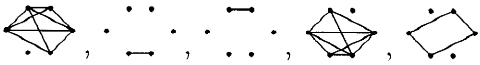
97 

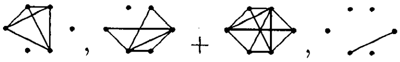
99 

101 

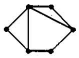
102 

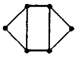
104 

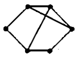
106 

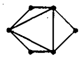
109 

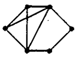
4.4 GVSConstructions

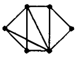
$\{1,2\}$, $\{1,3\}$, $\{2,3\}$, $\{2,5\}$, $\{2,6\}$, $\{3,4\}$, $\{4,5\}$, $\{5,6\}$ 53 : 	$(\mathbf{s},\mathbf{a})G_1 = (a_1, a_2, a_3)$, $(\mathbf{s},\mathbf{a})G_2 = (s_1 + a_3, s_2 + a_2, a_4)$, $(\mathbf{s},\mathbf{a})G_3 = (s_1 + a_4, s_1 + a_2 + a_3, s_2 + a_1)$, $(\mathbf{s},\mathbf{a})G_4 = (a_1, a_4, a_5)$, $(\mathbf{s},\mathbf{a})G_5 = (s_1 + a_4, s_2 + a_5, a_2)$, $(\mathbf{s},\mathbf{a})G_6 = (a_3, a_5, a_2 - a_4)$

$\{1,2\}$, $\{1,6\}$, $\{2,3\}$, $\{2,6\}$, $\{3,4\}$, $\{3,5\}$, $\{4,5\}$, $\{5,6\}$ 57 : 	$(\mathbf{s},\mathbf{a})G_1 = (a_1, a_2, a_3)$, $(\mathbf{s},\mathbf{a})G_2 = (s_1 + a_3, s_2 + a_2, a_4)$, $(\mathbf{s},\mathbf{a})G_3 = (s_1 + s_2 + a_4, a_3, a_5)$, $(\mathbf{s},\mathbf{a})G_4 = (s_1 + a_5, s_1 + a_3 + a_4, a_1 + a_4 - a_5)$, $(\mathbf{s},\mathbf{a})G_5 = (s_2 + a_3 + a_5, a_1, a_4)$, $(\mathbf{s},\mathbf{a})G_6 = (s_1 + a_1 + a_4, s_1 + a_2 + a_3, s_2 - a_1)$

$\{1,2\}$, $\{1,6\}$, $\{2,3\}$, $\{2,4\}$, $\{3,4\}$, $\{3,6\}$, $\{4,5\}$, $\{5,6\}$ 60 : 	$(\mathbf{s},\mathbf{a})G_1 = (a_1, a_2, a_3)$, $(\mathbf{s},\mathbf{a})G_2 = (s_1 + a_3, s_2 + a_2, a_4)$, $(\mathbf{s},\mathbf{a})G_3 = (s_2 + a_4, a_3, a_5)$, $(\mathbf{s},\mathbf{a})G_4 = (s_1 + s_2 + a_4, s_2 + a_5, a_2)$, $(\mathbf{s},\mathbf{a})G_5 = (s_2 + a_2 + a_4, a_5, a_1 + a_3)$, $(\mathbf{s},\mathbf{a})G_6 = (s_1 + a_3, s_2 + a_5, a_1 + a_5)$

$\{1,2\}$, $\{1,6\}$, $\{2,3\}$, $\{2,4\}$, $\{2,6\}$, $\{3,4\}$, $\{4,5\}$, $\{4,6\}$, $\{5,6\}$ 68 : 	$(\mathbf{s},\mathbf{a})G_1 = (a_1, a_2, a_3)$, $(\mathbf{s},\mathbf{a})G_2 = (s_1 + a_3, s_2 + a_2, a_4)$, $(\mathbf{s},\mathbf{a})G_3 = (s_2 + a_4, a_3, a_5)$, $(\mathbf{s},\mathbf{a})G_4 = (s_1 + s_2 + a_4, s_2 + a_5, a_2)$, $(\mathbf{s},\mathbf{a})G_5 = (s_2 + a_2 + a_4, a_1, a_5)$, $(\mathbf{s},\mathbf{a})G_6 = (s_1 + a_1, s_2 + a_4, a_1 + a_2 + a_4)$

$\{1,2\}$, $\{1,5\}$, $\{1,6\}$, $\{2,3\}$, $\{2,5\}$, $\{2,6\}$, $\{3,4\}$, $\{4,5\}$, $\{5,6\}$ 74 : 	$(\mathbf{s},\mathbf{a})G_1 = (a_1, a_2, a_3)$, $(\mathbf{s},\mathbf{a})G_2 = (s_1 + a_3, s_2 + a_2, a_4)$, $(\mathbf{s},\mathbf{a})G_3 = (s_2 + a_4, a_3, a_5)$, $(\mathbf{s},\mathbf{a})G_4 = (s_1 + a_5, a_1 + a_3, a_4)$, $(\mathbf{s},\mathbf{a})G_5 = (s_1 + a_1 + a_2, s_2 + a_4, a_2 - a_3 + a_4)$, $(\mathbf{s},\mathbf{a})G_6 = (s_1 - a_2 + a_3, s_2 + a_1, a_1 + a_3 - a_4)$

$\{1,2\}$, $\{1,5\}$, $\{1,6\}$, $\{2,3\}$, $\{2,5\}$, $\{2,6\}$, $\{3,4\}$, $\{3,5\}$, $\{4,5\}$, $\{5,6\}$ 87 : 	$(\mathbf{s},\mathbf{a})G_1 = (a_1, a_2, a_3)$, $(\mathbf{s},\mathbf{a})G_2 = (s_1 + a_3, s_2 + a_2, a_4)$, $(\mathbf{s},\mathbf{a})G_3 = (s_2 + a_4, a_3, a_5)$, $(\mathbf{s},\mathbf{a})G_4 = (s_1 + a_3 + a_4, s_2 + a_5, a_1 + a_2 + a_3)$, $(\mathbf{s},\mathbf{a})G_5 = (s_1 + a_4, s_2 + a_3, a_1 + a_2 - a_4)$, $(\mathbf{s},\mathbf{a})G_6 = (s_1 - a_2, s_2 + a_1, a_1 - a_4)$

Chapter 5

Decomposition Construction

Decomposition constructions are methods to construct secret sharing schemes using existing ones. Powerful decomposition constructions have been developed in [21, 27, 77, 97, 98, 99]. Theorem 1.4.5 from [21] and Theorem 1.4.7 from [99] are examples. These constructions enable efficient schemes to be constructed using other schemes. In this chapter we generalize known decomposition results to produce a new decomposition theorem. This chapter is joint work with Wen–Ai Jackson and Keith M. Martin and is submitted to Designs, Codes and Cryptography [50].

In Section 5.1 we define and discuss decompositions of secret sharing schemes. Our main decomposition construction is given in Section 5.2, its proof in Section 5.4. Examples of the application of the decomposition theorem, including how to obtain previous decomposition results, are given in Section 5.3.

5.1 Decompositions

Let $\mathcal{P}$ be a finite set of participants with $|\mathcal{P}| = n$, and let $\mathcal{X}$ be some non-empty set disjunct from $\mathcal{P}$. Let $(\tilde{\Gamma}, \tilde{\Delta})$ be an access structure on $\mathcal{X}$, and for each $Y \subseteq \mathcal{X}$ let (Γ^Y, Δ^Y) be an access structure on $\mathcal{P}$. We refer to the tuple

$$\mathcal{D} = \left(\mathcal{X}, (\tilde{\Gamma}, \tilde{\Delta}), \{(\Gamma^Y, \Delta^Y)\}_{Y \in 2^{\mathcal{X}}}\right)$$

as a *decomposition* on set $\mathcal{P}$. We call $(\tilde{\Gamma}, \tilde{\Delta})$ the *domain structure* of $\mathcal{D}$ and refer to the sets (Γ^Y, Δ^Y) as the *indicator structures* of $\mathcal{D}$.

We are interested in decompositions on $\mathcal{P}$ for which we have a secret sharing scheme for the domain structure and secret sharing schemes for each of the indicator structures. The idea is to share a secret s by means of the scheme for the domain structure. This produces shares s^x, for $x \in \mathcal{X}$. For $Y \subseteq \mathcal{X}$ the secret sharing scheme for indicator structure (Γ^Y, Δ^Y) is used to share among the participants in $\mathcal{P}$ the secret $(s^x)_{x \in Y}$. This secret is the showing that it is sufficient to find *any* appropriate secret sharing scheme, regardless of the probability measure defined on its secret set.

In this section and in the remainder of this chapter we heavily use the notation introduced in Section 1.2.2; probability measures ν and their restrictions ν_A with sets $[A]_\nu$, Section 1.2.3; random variable A_ν with probability measure ν_A, and Section 1.3.4; individual information rates $c_i(\nu)$ and convec $c(\nu)$. We suggest the reader to refresh his/her memory.

Lemma 5.2.1 *Let ν be a scheme for an access structure (Γ, Δ) on $\mathcal{P}$. Let μ be a probability measure defined on $[s]_\nu$. For each $\sigma \in [s]_\nu$ and $\pi \in [\mathcal{P}]_\nu$, define $\tau(\sigma\pi) = \nu_{\mathcal{P}|s}(\pi|\sigma)\mu(\sigma)$. Then τ is also a scheme for (Γ, Δ). Further, $\tau_s = \mu$, and for $i \in \mathcal{P}$, if $\{i\} \in \Delta$, we have $\tau_i = \nu_i$, hence, $H(i_\tau) = H(i_\nu)$.*

In all proofs in this section we use Lemma 1.2.4 which says that if ν describes a secret sharing scheme then ν is a scheme for (Γ, Δ) if and only if the following two conditions hold.

[SS1] For all $A \in \Gamma$ and $\alpha \in [A]_\nu$ there is exactly one $\sigma \in [s]_\nu$ such that $\nu_{sA}(\sigma\alpha) \neq 0$, and

[SS2] For all $B \in \Delta$, $\alpha \in [B]_\nu$ and $\sigma \in [s]_\nu$, we have $\nu_{sB}(\sigma\alpha) = \nu_s(\sigma)\nu_B(\alpha)$.

Proof of Lemma 5.2.1: We notice that τ is a probability measure with $\tau_s = \mu$ and clearly describes a secret sharing scheme with set of participants $\mathcal{P}$. We use Lemma 1.2.4 to show that τ is a scheme for (Γ, Δ). We first analyse $[A]_\tau$ for $A \subseteq \mathcal{P}$. Let $\alpha \in [A]_\tau$. Since $\alpha \in [A]_\tau$ there exists a $\sigma \in [s]_\tau$ such that $\tau_{sA}(\sigma\alpha) \neq 0$. We notice that $\mu = \tau_s$ and μ is a probability measure on $[s]_\nu$. Thus $[s]_\tau \subseteq [s]_\nu$, and therefore $\sigma \in [s]_\nu$, that is $\nu_s(\sigma) \neq 0$. This implies that

$$\tau_{sA}(\sigma\alpha) = \nu_{A|s}(\alpha|\sigma)\mu(\sigma) = \nu_{sA}(\sigma\alpha)\mu(\sigma)/\nu_s(\sigma).$$

Hence, from $\tau_{sA}(\sigma\alpha) \neq 0$ we obtain that $\nu_{sA}(\sigma\alpha) \neq 0$, and, hence, $\alpha \in [A]_\nu$. Thus if $\alpha \in [A]_\tau$ then $\alpha \in [A]_\nu$ and there exists a $\sigma \in [s]_\tau \subseteq [s]_\nu$ such that $\tau_{sA}(\sigma\alpha) \neq 0$. For such α and σ also $\nu_{sA}(\sigma\alpha) \neq 0$ holds.

We first prove that [SS1] of Lemma 1.2.4 holds, that is we prove that for all $A \in \Gamma$ and $\alpha \in [A]_\tau$ there is exactly one $\sigma \in [s]_\tau$ such that $\tau_{sA}(\sigma\alpha) \neq 0$. Let $A \in \Gamma$ and $\alpha \in [A]_\tau$. We have showed that $\alpha \in [A]_\nu$ and that there exists a $\sigma \in [s]_\tau \subseteq [s]_\nu$ such that $\tau_{sA}(\sigma\alpha) \neq 0$. We have also showed that $\nu_{sA}(\sigma\alpha) \neq 0$ for such an element σ. Since ν is a scheme for (Γ, Δ) we have that σ is uniquely defined by [SS1] of Lemma 1.2.4. Thus there is only one such σ, which proves [SS1] for τ.

We now prove that [SS2] of Lemma 1.2.4 holds, that is we prove that for all $B \in \Delta$, $\alpha \in [B]_\tau$ and $\sigma \in [s]_\tau$, we have $\tau_{sB}(\sigma\alpha) = \tau_s(\sigma)\tau_B(\alpha)$. Let $B \in \Delta$, $\alpha \in [B]_\tau$ and $\sigma \in [s]_\tau \subseteq [s]_\nu$. In the first paragraph we have showed that $\alpha \in [B]_\nu$. Since ν is a scheme for (Γ, Δ) we have that $\nu_{sB}(\sigma\alpha) = \nu_s(\sigma)\nu_B(\alpha)$

by [SS2] of Lemma 1.2.4. Thus $\tau_{sB}(\sigma\alpha) = \nu_{sB}(\sigma\alpha)\mu(\sigma)/\nu_s(\sigma) = \nu_B(\alpha)\tau_s(\sigma)$, hence, $\tau_{sB}(\sigma\tau)/\tau_s(\sigma)$ is independent of σ. Therefore $\tau_{sB}(\sigma\alpha) = \tau_B(\alpha)\tau_s(\sigma)$. This proves [SS2] for τ. From this derivation we also infer that $\nu_B = \tau_B$. So, we conclude firstly that τ is a scheme for (Γ, Δ) by Lemma 1.2.4, and secondly that if $B = \{i\} \in \Delta$ then $\nu_i = \tau_i$, hence, $H(i_\tau) = H(i_\nu)$.

□

Lemma 5.2.1 shows that by suitably redefining the probability measure of a secret sharing scheme we can change the probability measure on the secret set while not altering the size of the shares in the scheme (with the exception of the shares which already give additional information about the secret). The following theorem states the general decomposition result. Its proof is presented in Section 5.4.

Theorem 5.2.2 *Let* $\mathcal{D} = \left(\mathcal{X}, (\tilde\Gamma, \tilde\Delta), \{(\Gamma^Y, \Delta^Y)\}_{Y\subseteq\mathcal{X}}\right)$ *be a suitable decomposition for* (Γ, Δ) *on* $\mathcal{P}$. *Suppose that* $\tilde\nu$ *is a scheme for* $(\tilde\Gamma, \tilde\Delta)$ *on* $\mathcal{X}$, *and suppose that for each* $Y \subseteq \mathcal{X}$, ν^Y *is a scheme for* (Γ^Y, Δ^Y) *such that* $\nu_s^Y = \tilde\nu_Y$. *Then there exists a scheme* ν *for* (Γ, Δ) *with its convec* $c(\nu)$ *having the property that for* $i \in \mathcal{P}$

$$c_i(\nu) \le \frac{1}{H(s_{\tilde\nu})}\left(H(\mathcal{X}(i)_{\tilde\nu}) + \sum_{\{Y: i \notin \Gamma^Y\}} H(i_{\nu^Y})\right) \le \frac{1}{H(s_{\tilde\nu})}\sum_{Y\subseteq\mathcal{X}} H(i_{\nu^Y}).$$

We notice that if access structure (Γ^Y, Δ^Y) is empty then there exists a scheme ν^Y for (Γ^Y, Δ^Y) such that $\nu_s^Y = \tilde\nu_Y$ and $H(i_{\nu^Y}) = 0$ for $i \in \mathcal{P}$. Suppose that for non-singleton sets $Y \subseteq \mathcal{X}$ access structure (Γ^Y, Δ^Y) is empty. Thus only for singleton sets $Y = j$, $j \in \mathcal{X}$, access structure (Γ^Y, Δ^Y) is not empty. From $\nu_s^Y = \tilde\nu_Y$ we infer that $[s]_{\nu^Y} = [Y]_{\tilde\nu}$ and $s_{\nu^Y} = Y_{\tilde\nu}$. So, for scheme ν in Theorem 5.2.2 we have that for $i \in \mathcal{P}$

$$\begin{aligned} c_i(\nu) &\le \frac{1}{H(s_{\tilde\nu})}\sum_{j\in\mathcal{X}} H(i_{\nu^j}) \\ &= \sum_{j\in\mathcal{X}} \frac{H(i_{\nu^j})}{H(s_{\nu^j})}\frac{H(j_{\tilde\nu})}{H(s_{\tilde\nu})} \\ &= \sum_{j\in\mathcal{X}} c_i(\nu^j)c_j(\tilde\nu). \end{aligned}$$

This proves the following corollary.

Corollary 5.2.3 *Let* $\mathcal{D} = \left(\mathcal{X}, (\tilde\Gamma, \tilde\Delta), \{(\Gamma^Y, \Delta^Y)\}_{Y\subseteq\mathcal{X}}\right)$ *be a suitable decomposition for* (Γ, Δ) *on* $\mathcal{P}$ *such that only for singleton sets* $Y = j$, $j \in \mathcal{X}$, *access structure* (Γ^Y, Δ^Y) *is not empty. Suppose that* $\tilde\nu$ *is a scheme for* $(\tilde\Gamma, \tilde\Delta)$ *on*

$\mathcal{X}$, and suppose that for each $j \in \mathcal{X}$, ν^j is a scheme for (Γ^j, Δ^j) such that $\nu^j_s = \tilde{\nu}_j$. Then there exists a scheme ν for (Γ, Δ) with convec

$$c(\nu) \leq \sum_{j \in \mathcal{X}} c_j(\tilde{\nu}) c(\nu^j).$$

Example 5.2.4 We continue with Example 5.1.1. Let $q \geq 8$ be a prime power. We mention that there exists a scheme $\tilde{\nu}$ for $\tilde{\Gamma}$ and set of possible secrets $GF(q)$ with convec $(1, 2, 1, 1, 1)$, $\tilde{\nu}_j$, $j \in \mathcal{X}$, $\tilde{\nu}_s$ are uniform, and $|[s]_{\tilde{\nu}}| = q$. For $j \in \mathcal{X}$, Γ^j is ideal. For any positive integer k there exists a scheme ν^j for Γ^j and set of possible secrets $GF(q)^k$ with ν^j uniform and $|[s]_{\nu^j}| = q^k$. Choosing $k = 1$ for $j \neq 2$ and choosing $k = 2$ for $j = 2$, we have that $\nu^j_s = \tilde{\nu}_j$ for $j \in \mathcal{X}$. Schemes ν^j, for $j \in \mathcal{X} = \{1, 2, 3, 4, 5\}$, have convecs $(1, 1, 1, 0, 0)$, $(0, 1, 1, 0, 0)$, $(0, 0, 0, 1, 0)$, $(0, 0, 0, 0, 1)$ and $(1, 0, 0, 0, 0)$ respectively. Thus applying Corollary 5.2.3 gives a scheme ν for Γ with convec

$$\begin{aligned} c(\nu) &\leq (1,1,1,0,0) + 2(0,1,1,0,0) + (0,0,0,1,0) + \\ &\quad\ (0,0,0,0,1) + (1,0,0,0,0) \\ &= (2,3,3,1,1). \end{aligned}$$

Although this scheme does not have a particularly good information rate, in [60] this scheme was combined with another one to construct a more efficient scheme for access structure Γ. It was shown in [60] that this particular decomposition is a special case of an infinite family of decompositions that can be used to construct efficient secret sharing schemes for a family of access structures.

We have presented a generalized decomposition technique which can be used to construct schemes that have incomplete access structures. The technique shows that schemes for incomplete access structures can be used as part of the decomposition procedure to construct perfect secret sharing schemes, these are schemes for complete access structures. Decompositions using incomplete secret sharing schemes have also been used in [62] to construct secret sharing schemes that do not need a MTA to be initialized.

A further possible generalization of the decomposition techniques discussed here is to consider multi-secret sharing schemes (secret sharing schemes with more than one secret) with incomplete access structures. Such structures have already found use in modelling various key distribution problems (for example, [20, 62]).

Examples of the application of the decomposition theorem, including how to obtain previous decomposition results, are given in the next section.

5.3 Simple Decompositions

To see that Theorem 5.2.2 is indeed a generalization of previous decomposition results we review previous constructions based on decomposition techniques. They are listed in Table 5.1. Note that all these previous constructions are 1) for complete Γ, 2) all probability measures are uniform, and 3) all indicator structures are empty except those corresponding to singleton sets Y. Our decomposition result does not require these restrictions.

Type	Reference	Domain Structure	Indicator Structures
1	[27]	$(1, r)$ – threshold	graph-based
2	[77]	$(1, 2)$ – threshold	general
3	[77]	$(2, 2)$ – threshold	general
4	[21]	$(1, r)$ – threshold	multipartite graph-based
5	[21]	$(0, r, r)$ – ramp	type 4
6	[97]	$(1, r)$ – threshold	ideal
7	[97]	$(0, r, r)$ – ramp	type 5
8	[98]	$(1, r)$ – threshold	general
9	[99]	$(0, \lambda, r)$ – ramp	general

Table 5.1: Decomposition Constructions

An indicator structure is said to be of *type-n*, where n corresponds to the numbering in Table 5.1, if there exists a decomposition of type-n that is suitable for that indicator structure. Types 1, 4 and 5 only construct secret sharing schemes for access structures based on graphs. Type 4 is a special case of type 1 where the indicator structures are based on multipartite graphs (see Example 1.4.6). In [21, 97] a decomposition of type 4 was referred to as a *complete multipartite covering* (CMC), type 5 as a *multiple CMC* (see Theorem 1.4.5) and type 6 as an *ideal decomposition.* In [99] a decomposition of type 9 is referred to as a λ-*decomposition* (see Theorem 1.4.7 with Example 1.4.8 for λ-decompositions with multipartite graph-based indicator structures).

Table 5.1 is not complete. In [77] a decomposition was described for a complete access structure with a general complete domain structure and one general complete indicator structure (this was referred to as an *insertion*). In [4] schemes were constructed for access structures (Γ, Δ) with $\Delta = \emptyset$. A decomposition was used with a $(0, \lambda, r)$-ramp domain structure and indicator structures consisting of single participants.

We conclude that Theorem 5.2.2 is a generalization on the decompositions listed in Table 5.1 because it constructs schemes for (incomplete) access structures with non-uniform probability distributions and uses general (incomplete) domain and indicator structures that can correspond to sets Y with $|Y| > 1$. As type 9 is the most general of the decompositions in Table 1 we show that it is a special case of Corollary 5.2.3. To do this we describe a new construction arising from Corollary 5.2.3 of which type 9 is clearly a special case.

Let (Γ, Δ) be an access structure on $\mathcal{P}$. Let λ, ω, with $\lambda > \omega$, be integers. A (λ, ω)-*decomposition* of (Γ, Δ) consists of a collection $\{(\Gamma^1, \Delta^1), \ldots, (\Gamma^h, \Delta^h)\}$ of access structures on $\mathcal{P}$ such that the following holds. Firstly, if $A \in \Gamma$ then $A \in \Gamma^i$ for at least λ distinct values of i, $1 \le i \le h$, and secondly, if $A \in \Delta$ then $A \notin \Delta^i$ for at most ω distinct values of i, $1 \le i \le h$. In [99] the following was proved for $\omega = 0$, $\Delta = \Gamma^c$, and $\Delta^i = (\Gamma^j)^c$, $1 \le j \le h$ (rewritten to be consistent with our notation).

Corollary 5.3.1 *Let (Γ, Δ) be an access structure on $\mathcal{P}$ and suppose that there exists a (λ, ω)-decomposition $\{(\Gamma^1, \Delta^1), \ldots, (\Gamma^h, \Delta^h)\}$ of (Γ, Δ). Suppose there exists a prime power $q > h$ and secret sharing schemes ν^j for Γ^j, $1 \le j \le h$, with convec $c(\nu^j)$, $|[s]_{\nu^j}| = q$, and ν^j_s is uniform. Then there exists a secret sharing scheme ν for Γ with convec*

$$c(\nu) \le \frac{c(\nu^1) + \cdots + c(\nu^h)}{\lambda - \omega}.$$

Proof: Let $\mathcal{X} = \{1, \ldots, h\}$, $\tilde{\Gamma} = \{Y \subseteq \mathcal{X} : |Y| \ge \lambda\}$, and $\tilde{\Delta} = \{Y \subseteq \mathcal{X} : |Y| \le \omega\}$. Let $\tilde{\nu}$ be a (ω, λ, h)-ramp scheme with $\mathcal{X}$ as set of participants, $H(s_{\tilde{\nu}}) = (\lambda - \omega) \log q$, $|[j]_{\tilde{\nu}}| = q$, and $\tilde{\nu}_j$ is uniform for $j \in \mathcal{X}$. So $\tilde{\nu}_j = \nu^j_s$, and $c_j(\tilde{\nu}) = 1/(\lambda - \omega)$ for $j \in \mathcal{X}$. Such a scheme has access structure $(\tilde{\Gamma}, \tilde{\Delta})$ and exists, see Example 1.2.6. If $A \in \Gamma$ then $|\mathcal{X}(A)| \ge \lambda$ and so $\mathcal{X}(A) \in \tilde{\Gamma}$. If $A \in \Delta$ then $|\mathcal{X}(A)| \le \omega$ and so $\mathcal{X}(A) \in \tilde{\Delta}$. Thus [D1] and [D2] hold. Now we can apply Corollary 5.2.3 to obtain the required scheme ν.

□

Example 5.3.2 Let $\mathcal{P} = \{a, b, c, d, e, f\}$ and let Γ be a complete access structure on $\mathcal{P}$ defined by its minimal elements

$$[\Gamma]^- = \{ab, bc, ac, ad, be, cf, def\}.$$

Then

$$[\Gamma^c]^+ = \{aef, bdf, cde\}.$$

We will use Corollary 5.3.1 to exhibit a scheme ν for Γ with $\dot{\rho}(\nu) = 2/3$. Let complete access structures $\Gamma^1, \Gamma^2, \Gamma^3$ be defined by their minimal elements

$$\begin{aligned} [\Gamma^1]^- &= \{a, bc, be, cf, ef\}, \\ [\Gamma^2]^- &= \{b, ac, ad, cf, df\}, \text{ and} \\ [\Gamma^3]^- &= \{c, ab, ad, be, de\}. \end{aligned}$$

It is easy to check that $\{\Gamma^1, \Gamma^2, \Gamma^3\}$ is a $(1,3)$-decomposition of Γ. For example, $ab \in [\Gamma]^-$ and $ab \in \Gamma^1, \Gamma^2, \Gamma^3$, $aef \in [\Gamma^c]^+$ and $aef \in \Gamma^1$, $aef \notin \Gamma^2, \Gamma^3$. Let q be a prime power, $q > 3$. Now Γ^1, Γ^2 and Γ^3 can all be seen to be ideal access structures. There exist schemes ν^1, ν^2, ν^3 for $\Gamma^1, \Gamma^2, \Gamma^3$ with convecs

$c(\nu^1) = (1,1,1,0,1,1)$, $c(\nu^2) = (1,1,1,1,0,1)$, $c(\nu^3) = (1,1,1,1,1,0)$ and for each $1 \le j \le 3$, $|[s]_{\nu^j}| = q$, and ν^j_s is uniform.

We can apply Corollary 5.3.1. It follows that there exists a secret sharing scheme ν for Γ with convec $c(\nu) \le (3,3,3,2,2,2)/2$. Thus $\dot\rho(\nu) \ge 2/3$. It can be shown that any scheme for Γ has $\dot\rho(\nu) \le 2/3$ (see Theorem 2.2.1) and so the above scheme has optimal information rate $\dot\rho(\Gamma) = 2/3$.

We finish this section with another example. Let (Γ, Δ) be an access structure on $\mathcal{P}$. Let λ, ω, with $\lambda > \omega$, be integers. A (λ,ω)-*decomposition function* of (Γ,Δ) is a function $\Psi \in \mathcal{P} \to \mathbb{N}$ such that the following holds. Firstly, if $A \in \Gamma$ then $\sum_{a\in A} \Psi(a) \ge \lambda$, and secondly, if $B \in \Delta$ then $\sum_{b \in B} \Psi(b) \le \omega$.

Example 5.3.3 Let (Γ,Δ) be an access structure on $\mathcal{P}$ and let Ψ be a (λ,ω)-decomposition function of (Γ,Δ). Let $h = \sum_{i\in\mathcal{P}} \Psi(i)$ and define h complete access structures by $[\Gamma^{i,j}]^- = \{i\}$, $i \in \mathcal{P}$, $1 \le j \le \Psi(i)$. Hence, $A \in \Gamma^{i,j}$ iff $i \in A$. Thus if $A \in \Gamma$ then there are $\sum_{a\in A} \Psi(a) \ge \lambda$ access structures $\Gamma^{i,j}$ with $A \in \Gamma^{i,j}$. If $B \in \Delta$ then $B \in \Gamma^{i,j}$ iff $i \in B$. Thus if $B \in \Delta$ then there are $\sum_{b\in B} \Psi(b) \le \omega$ access structures $\Gamma^{i,j}$ with $B \in \Gamma^{i,j}$. Hence, $\{\Gamma^{i,j} : i \in \mathcal{P}, 1 \le j \le \Psi(i)\}$ is a (λ,ω)-decomposition of (Γ,Δ). Let $q > h$ be a prime power. For access structure $\Gamma^{i,j}$ there exists an ideal scheme $\nu^{i,j}$ such that $c_i(\nu^{i,j}) = 1$, $c_m(\nu^{i,j}) = 0$ for $i \ne m \in \mathcal{P}$, $|[s]_{\nu^{i,j}}| = q$, and $\nu^{i,j}_s$ is uniform. Hence, we can use Corollary 5.3.1 to conclude that there exists a secret sharing scheme ν for (Γ,Δ) with convec $c(\nu)$ having the property that for $m \in \mathcal{P}$

$$c_m(\nu) \le \frac{1}{\lambda-\omega} \sum_{i\in\mathcal{P}} \sum_{1\le j\le\Psi(i)} c_m(\nu^{i,j}) = \frac{\Psi(m)}{\lambda-\omega}.$$

Let $\mathcal{P} = \{a,b,c,d,e,f,g\}$, and let access structure (Γ,Δ) on $\mathcal{P}$ be defined by

$$[\Gamma]^- = \{abc, acd, aefg\}$$

and

$$[\Delta]^+ = \{a,b,c,d,e,f,g\}.$$

Let function $\Psi \in \mathcal{P} \to \mathbb{N}$ be defined by

$$\Psi(a) = 3, \Psi(b) = 3, \Psi(c) = 3, \Psi(d) = 3, \Psi(e) = 2, \Psi(f) = 2, \Psi(g) = 2.$$

Then Ψ is a $(9,3)$-decomposition function of (Γ,Δ). Thus a scheme ν for Γ exists with convec

$$c(\nu) \le (1/2, 1/2, 1/2, 1/2, 1/3, 1/3, 1/3).$$

Thus $\dot\rho(\nu) \ge 2$ and $\tilde\rho(\nu) \ge 7/3$.

We see that for any scheme for (Γ,Δ), we have

$$\begin{aligned} H(ab) &\ge H(ab|c) \ge I(ab : s|c) = H(s|c) - H(s|abc) = H(s), \\ H(cd) &\ge H(cd|a) \ge I(cd : s|a) = H(s|a) - H(s|acd) = H(s), \\ H(efg) &\ge H(efg|a) \ge I(efg : s|a) = H(s|a) - H(s|aefg) = H(s). \end{aligned}$$

So, $\sum_{i \in \mathcal{P}} H(i) \geq 3H(s)$, and $H(a)+H(b) \geq H(ab) \geq H(s)$. Thus the optimal average information rate $\tilde{\rho}(\Gamma, \Delta)$ is bounded above by 7/3, and the optimal worst-case information rate $\dot{\rho}(\Gamma, \Delta)$ is bounded above by 2. We conclude that scheme ν achieves both the optimal average information rate and the optimal worst-case information rate.

5.4 Proof of the Main Theorem

We finish this section by giving the proof of the general decomposition theorem which needs the next lemma.

Lemma 5.4.1 *Let ν be a scheme for an access structure (Γ, Δ) on $\mathcal{P}$ and let $i \in \mathcal{P}$. Let access structure $(\bar{\Gamma}, \bar{\Delta})$ on $\mathcal{P}$ be defined by $\bar{\Gamma} = \Gamma \cup \{A \subseteq \mathcal{P} : i \in A\}$ and $\bar{\Delta} = \Delta \cap \{A \subseteq \mathcal{P} : i \notin A\}$. Then there exists a scheme $\bar{\nu}$ for $(\bar{\Gamma}, \bar{\Delta})$ such that $\bar{\nu}_i = \bar{\nu}_s = \nu_s$ $(H(i_{\bar{\nu}}) = H(s_{\bar{\nu}}) = H(s_\nu))$ and $\bar{\nu}_j = \nu_j$ $(H(j_{\bar{\nu}}) = H(j_\nu))$ for $j \neq i$.*

Proof: For (n+1)-tuples π with $\pi_{s\mathcal{P}\setminus i} \in [s\mathcal{P}\setminus i]_\nu$ we define $\bar{\nu}(\pi) = \nu_{s\mathcal{P}\setminus i}(\pi_{s\mathcal{P}\setminus i})$ if $\pi_i = \pi_s$ and $\bar{\nu}(\pi) = 0$ if $\pi_i \neq \pi_s$. Note that $\bar{\nu}_{s\mathcal{P}\setminus i} = \nu_{s\mathcal{P}\setminus i}$ and $\bar{\nu}_{is}(\pi_i\pi_s) = \nu_s(\pi_s)$ if $\pi_i = \pi_s$ and $\bar{\nu}(\pi) = 0$ if $\pi_i \neq \pi_s$. Thus $\bar{\nu}_j = \nu_j$ for $j \neq i$, $\bar{\nu}_i = \bar{\nu}_s = \nu_s$, and $\bar{\nu}_{i|s}(\pi_i|\pi_s) = 1$ iff $\pi_i = \pi_s$.

Clearly, $\bar{\nu}$ is a probability measure and, hence, describes a secret sharing scheme. By using Lemma 1.2.4 with $\bar{\nu}_{i|s}(\pi_i|\pi_s) = 1$ iff $\pi_i = \pi_s$ we check that $\bar{\nu}$ is a scheme for $(\bar{\Gamma}, \bar{\Delta})$. We first prove that [SS1] of Lemma 1.2.4 holds, that is we prove that for all $A \in \bar{\Gamma}$ and $\alpha \in [A]_{\bar{\nu}}$ there is exactly one $\sigma \in [s]_{\bar{\nu}} = [s]_\nu$ such that $\bar{\nu}_{sA}(\sigma\alpha) \neq 0$. Let $A \in \bar{\Gamma}$ such that $i \notin A$ and let $\alpha \in [A]_{\bar{\nu}}$. Then $\bar{\nu}_{sA} = \nu_{sA}$, hence $\alpha \in [A]_\nu$, and $A \in \Gamma$. Thus, by [SS1] of Lemma 1.2.4 for ν we obtain that there is exactly one $\sigma \in [s]_\nu = [s]_{\bar{\nu}}$ such that $\bar{\nu}_{sA}(\sigma\alpha) = \nu_{sA}(\sigma\alpha) \neq 0$. Now suppose that $A \in \bar{\Gamma}$ such that $i \in A$ and let $\alpha \in [A]_{\bar{\nu}}$. Since $\alpha \in [A]_{\bar{\nu}}$ there exists a $\sigma \in [s]_{\bar{\nu}}$ such that $\bar{\nu}_{sA}(\sigma\alpha) \neq 0$. By the definition of $\bar{\nu}$ we have $\sigma = \alpha_i$, and, hence, σ is uniquely defined. This proves [SS1] for $\bar{\nu}$.

We now prove that [SS2] of Lemma 1.2.4 holds, that is we prove that for all $B \in \bar{\Delta}$, $\alpha \in [B]_{\bar{\nu}}$ and $\sigma \in [s]_{\bar{\nu}} = [s]_\nu$, we have $\bar{\nu}_{sB}(\sigma\alpha) = \bar{\nu}_s(\sigma)\bar{\nu}_B(\alpha)$. Let $B \in \bar{\Delta}$, $\alpha \in [B]_{\bar{\nu}}$, and $\sigma \in [s]_{\bar{\nu}}$. Then $i \notin B$ and $B \in \Delta$. Thus $B \in \Delta$, $\bar{\nu}_{sB} = \nu_{sB}$, and, hence, $\alpha \in [B]_\nu$. Thus, by [SS2] of Lemma 1.2.4 for ν, we have that [SS2] for $\bar{\nu}$ holds. We conclude that $\bar{\nu}$ is a scheme for $(\bar{\Gamma}, \bar{\Delta})$ by Lemma 1.2.4.

□

An immediate consequence is that if ν is a scheme for an access structure (Γ, Δ) on $\mathcal{P}$ with $\{i\} \in \Gamma$ then $(\Gamma, \Delta) = (\bar{\Gamma}, \bar{\Delta})$, and hence w.l.o.g. $\nu_i = \nu_s$. This is what we will use in the proof of the general decomposition theorem.

The general decomposition Theorem 5.2.2 states the following.

Let $\mathcal{D} = \left(\mathcal{X}, (\tilde{\Gamma}, \tilde{\Delta}), \{(\Gamma^Y, \Delta^Y)\}_{Y \subseteq \mathcal{X}}\right)$ be a suitable decomposition for (Γ, Δ) on $\mathcal{P}$. Suppose that $\tilde{\nu}$ is a scheme for $(\tilde{\Gamma}, \tilde{\Delta})$ on $\mathcal{X}$, and suppose that for each $Y \subseteq \mathcal{X}$, ν^Y is a scheme for (Γ^Y, Δ^Y) such that $\nu^Y_s = \tilde{\nu}_Y$. Then there exists a scheme ν for (Γ, Δ) with its convec $c(\nu)$ having the property that for $i \in \mathcal{P}$

$$c_i(\nu) \leq \frac{1}{H(s_{\tilde{\nu}})} \left(H(\mathcal{X}(i)_{\tilde{\nu}}) + \sum_{\{Y : i \notin \Gamma^Y\}} H(i_{\nu^Y}) \right) \leq \frac{1}{H(s_{\tilde{\nu}})} \sum_{Y \subseteq \mathcal{X}} H(i_{\nu^Y}).$$

Its proof is split into a few steps.

1. We define a probability measure ν.
2. We prove that [SS1] holds.
3. We prove that [SS2] holds as well, and we conclude that ν is a scheme for (Γ, Δ).
4. We give another interpretation of ν_i, which will lead to a different expression for the individual information rate $c_i(\nu)$.
5. We prove the bounds on the individual information rates as stated in the theorem by using two equations, which proofs are postponed.
6. We prove the first equation.
7. Finally, we prove the second equation.

1. Probability Measure: Let Π be the set of tuples $\pi = (\pi_x)_{x \in s\mathcal{P}}$ where $\pi_s \in [s]_{\tilde{\nu}}$ and π_i, $i \in \mathcal{P}$, is a tuple indexed by the elements of $2^{\mathcal{X}}$ such that $\pi_i = ((\pi_i)_Y)_{Y \in 2^{\mathcal{X}}}$ with $(\pi_i)_Y \in [i]_{\nu^Y}$, $Y \subseteq \mathcal{X}$. For $A \subseteq \mathcal{P}$ and $Y \subseteq \mathcal{X}$ we write $\pi^Y_A = ((\pi_i)_Y)_{i \in A}$. Further, we notice that $\nu^Y_s = \tilde{\nu}_Y$, hence, $[s]_{\nu^Y} = [Y]_{\tilde{\nu}}$.

Define a function ν on Π by

$$\nu(\pi) = \sum_{\tilde{\pi} \in [\mathcal{X}]_{\tilde{\nu}}} \tilde{\nu}(\pi_s \tilde{\pi}) \prod_{Y \subseteq \mathcal{X}} \nu^Y_{\mathcal{P}|s}(\pi^Y_{\mathcal{P}} | \tilde{\pi}_Y),$$

where $\pi \in \Pi$. We first show that ν is a probability measure on Π. Firstly, notice that for $\pi \in \Pi$ and $A \subseteq \mathcal{P}$,

$$\nu_{sA}(\pi_{sA}) = \sum_{\{\hat{\pi} \in \Pi \,|\, \hat{\pi}_{sA} = \pi_{sA}\}} \nu(\hat{\pi}) = \sum_{\tilde{\pi} \in [\mathcal{X}]_{\tilde{\nu}}} \tilde{\nu}(\pi_s \tilde{\pi}) \prod_{Y \subseteq \mathcal{X}} \nu^Y_{A|s}(\pi^Y_A | \tilde{\pi}_Y). \quad (5.1)$$

By putting $A = \emptyset$ in (5.1) we see that

$$\nu_s(\pi_s) = \tilde{\nu}_s(\pi_s). \quad (5.2)$$

Then using (5.2),

$$\sum_{\pi \in \Pi} \nu(\pi) = \sum_{\pi_s \in [s]_{\tilde{\nu}}} \nu_s(\pi_s) = \sum_{\pi_s \in [s]_{\tilde{\nu}}} \tilde{\nu}_s(\pi_s) = 1,$$

since $\tilde{\nu}_s$ is a probability measure on $[s]_{\tilde{\nu}}$. Thus ν describes a secret sharing scheme.

2. [SS1]: We now use Lemma 1.2.4 to show that ν is a scheme for (Γ, Δ). We first prove that [SS1] holds, that is for all $A \in \Gamma$ and $\pi \in [\mathcal{P}]_\nu$ there is exactly one $\sigma \in [s]_\nu$ such that $\nu_{sA}(\sigma\pi_A) \neq 0$. Let $A \in \Gamma$ and let $\pi \in [\mathcal{P}]_\nu$. Since $\pi \in [\mathcal{P}]_\nu$ there exists a $\sigma \in [s]_\nu$ such that $\nu_{sA}(\sigma\pi_A) \neq 0$. Then by (5.1) there exists a $\tilde{\pi} \in [\mathcal{X}]_{\tilde{\nu}}$ with $\tilde{\nu}_{s\mathcal{X}}(\sigma\tilde{\pi}) \neq 0$ and $\prod_{Y \in 2^{\mathcal{X}}} \nu^Y_{A|s}(\pi^Y_A|\tilde{\pi}_Y) \neq 0$. Since $\tilde{\pi} \in [\mathcal{X}]_{\tilde{\nu}}$ we have that $\tilde{\pi}_Y \in [Y]_{\tilde{\nu}} = [s]_{\nu^Y}$, thus $\nu^Y_s(\tilde{\pi}_Y) \neq 0$. Together with $\nu^Y_{A|s}(\nu^Y_A|\tilde{\nu}_Y) \neq 0$ this implies that $\nu^Y_A(\pi^Y_A) \neq 0$, that is $\pi^Y_A \in [A]_{\nu^Y}$, for $Y \subseteq \mathcal{X}$. So, if $A \in \Gamma^Y$ then by the combination of $\pi^Y_A \in [A]_{\nu^Y}$ and [SS1] of Lemma 1.2.4 for ν^Y there exists a unique $\psi^Y \in [s]_{\nu^Y} = [Y]_{\tilde{\nu}}$ such that $\nu^Y_{sA}(\psi^Y\pi^Y_A) \neq 0$. Notice that $\nu^Y_{sA}(\psi^Y\pi^Y_A) = \nu^Y_{A|s}(\pi^Y_A|\psi^Y)\nu^Y_s(\psi^Y)$ and $\nu^Y_s(\psi) \neq 0$. Hence, if $A \in \Gamma^Y$ then ψ^Y is the unique element in $[Y]_{\tilde{\nu}}$ such that $\nu^Y_{A|s}(\pi^Y_A|\psi^Y) \neq 0$. Notice that $\nu^Y_{A|s}(\pi^Y_A|\tilde{\pi}_Y) \neq 0$. We conclude that if $A \in \Gamma^Y$ then $\psi^Y = \tilde{\pi}_Y$. This implies that $\omega = \tilde{\pi}_{\mathcal{X}(A)}$ is uniquely defined by $\psi^Y = \tilde{\pi}_Y$ for $Y \subseteq \mathcal{X}$ with $A \in \Gamma^Y$. Since $A \in \Gamma$, we have that $\mathcal{X}(A) \in \tilde{\Gamma}$ by [D1]. Thus by [SS1] of Lemma 1.2.4 for $\tilde{\nu}$ there exists a unique $\tau \in [s]_{\tilde{\nu}}$ with $\tilde{\nu}_{s\mathcal{X}(A)}(\tau\omega) \neq 0$. Now notice that $\tilde{\pi}_{\mathcal{X}(A)} = \omega$ and $\tilde{\nu}_{s\mathcal{X}(A)}(\sigma\tilde{\pi}_{\mathcal{X}(A)}) \neq 0$ since $\tilde{\nu}_{s\mathcal{X}}(\sigma\tilde{\pi}) \neq 0$. Hence, σ equals the uniquely defined element τ. This proves [SS1] for ν.

3. [SS2]: We now prove that [SS2] holds, that is for all $B \in \Delta$, $\pi \in [\mathcal{P}]_\nu$ and $\sigma \in [s]_\nu$, we have $\nu_{sB}(\sigma\pi_B) = \nu_s(\sigma)\nu_B(\alpha)$. Suppose that $B \in \Delta$ and hence that $\bar{\mathcal{X}}(B) \in \tilde{\Delta}$ by [D2]. Let $\pi \in [\mathcal{P}]_\nu$ and $\sigma \in [s]_\nu$. We notice that if $Y \subseteq \mathcal{X}$ with $B \in \Delta^Y$ then $\nu^Y_{sB}(\tau\pi^Y_B) = \nu^Y_s(\tau)\nu^Y_B(\pi^Y_B)$, that is $\nu^Y_{B|s}(\pi^Y_B|\tau) = \nu^Y_B(\pi^Y_B)$, for all $\tau \in [s]_{\nu^Y} = [Y]_{\tilde{\nu}}$, by [SS2] of Lemma 1.2.4 for ν^Y. This proves the second equality in the following derivation. The fourth equality in the following derivation follows from $\bar{\mathcal{X}}(B) \in \tilde{\Delta}$, hence, $\tilde{\nu}_{s\bar{\mathcal{X}}(B)}(\sigma\omega) = \tilde{\nu}_s(\sigma)\tilde{\nu}_{\bar{\mathcal{X}}(B)}(\omega)$ for all $\omega \in [\bar{\mathcal{X}}(B)]_{\tilde{\nu}}$, by [SS2] of Lemma 1.2.4 for $\tilde{\nu}$. Starting with (5.1) we obtain

$$\begin{aligned}
&\nu_{sB}(\sigma\pi_B)\\
=\ & \sum_{\tilde{\pi} \in [\mathcal{X}]_{\tilde{\nu}}} \tilde{\nu}(\sigma\tilde{\pi}) \prod_{Y \subseteq \mathcal{X}} \nu^Y_{B|s}(\pi^Y_B|\tilde{\pi}_Y)\\
=\ & \sum_{\tilde{\pi} \in [\mathcal{X}]_{\tilde{\nu}}} \tilde{\nu}(\sigma\tilde{\pi}) \prod_{\{Y \subseteq \mathcal{X} : B \notin \Delta^Y\}} \nu^Y_{B|s}(\pi^Y_B|\tilde{\pi}_Y) \prod_{\{Y \subseteq \mathcal{X} : B \in \Delta^Y\}} \nu^Y_B(\pi^Y_B)\\
=\ & \sum_{\omega \in [\bar{\mathcal{X}}(B)]_{\tilde{\nu}}} \tilde{\nu}_{s\bar{\mathcal{X}}(B)}(\sigma\omega) \prod_{\{Y \subseteq \mathcal{X} : B \notin \Delta^Y\}} \nu^Y_{B|s}(\pi^Y_B|\omega_Y) \prod_{\{Y \subseteq \mathcal{X} : B \in \Delta^Y\}} \nu^Y_B(\pi^Y_B)
\end{aligned}$$

$$= \tilde{\nu}_s(\sigma) \sum_{\omega \in [\bar{\mathcal{X}}(B)]_{\tilde{\nu}}} \tilde{\nu}_{\bar{\mathcal{X}}(B)}(\omega) \prod_{\{Y \subseteq \mathcal{X} : B \notin \Delta^Y\}} \nu^Y_{B|s}(\pi^Y_B|\omega_Y) \prod_{\{Y \subseteq \mathcal{X} : B \in \Delta^Y\}} \nu^Y_B(\pi^Y_B).$$

From (5.2) we see that $\tilde{\nu}_s(\sigma) = \nu_s(\sigma)$ and hence that $\nu_{sB}(\sigma\pi_B)/\nu_s(\sigma)$ is independent of σ. Therefore $\nu_{sB}(\sigma\pi_B) = \nu_s(\sigma)\nu_B(\pi_B)$. This proves [SS2] for ν. By Lemma 1.2.4 ν is a scheme for (Γ, Δ).

4. Another interpretation of ν_i: Let $i \in \mathcal{P}$ and $\pi \in [i]_\nu$. Notice that π is a tuple $\pi = (\pi_Y)_{Y \subseteq \mathcal{X}}$ and that $\pi_Y \in [i]_{\nu^Y}$ for $Y \subseteq \mathcal{X}$. By (5.1)

$$\nu_i(\pi) = \sum_{\tilde{\pi} \in [\mathcal{X}]_{\tilde{\nu}}} \tilde{\nu}_{\mathcal{X}}(\tilde{\pi}) \prod_{Y \subseteq \mathcal{X}} \nu^Y_{i|s}(\pi_Y|\tilde{\pi}_Y).$$

Notice that ν_i is a probability measure on tuples indexed by the elements of $2^{\mathcal{X}}$. Therefore the *restriction* $(\nu_i)_Z$, $Z \subseteq 2^{\mathcal{X}}$, of ν_i to Z is well-defined by

$$(\nu_i)_Z(\pi_Z) = \sum_{\{\hat{\pi} \in [2^{\mathcal{X}}]_{\nu_i} : \hat{\pi}_Z = \pi_Z\}} \nu_i(\hat{\pi})$$

(notice the similarity with the definition of ν_A in Section 1.2.2). We define for $Z \subseteq 2^{\mathcal{X}}$

$$Z_{\nu_i}$$

as a random variable with probability measure $(\nu_i)_Z$ (notice the similarity with the definition of A_ν in Section 1.2.3). Thus $(\nu_i)_{2^{\mathcal{X}}} = \nu_i$, $[2^{\mathcal{X}}]_{\nu_i} = [i]_\nu$, and $(2^{\mathcal{X}})_{\nu_i} = i_\nu$. Together with (5.2) we obtain

$$c_i(\nu) = H(i_\nu)/H(s_\nu) = H((2^{\mathcal{X}})_{\nu_i})/H(s_{\tilde{\nu}}). \tag{5.3}$$

5. The bound: In the next two steps of this proof we derive

$$H(Y_{\nu_i}) = H(i_{\nu^Y}), \tag{5.4}$$
$$H(\{Y : i \in \Gamma^Y\}_{\nu_i}) = H(\mathcal{X}(i)_{\tilde{\nu}}). \tag{5.5}$$

Hence,

$$\begin{aligned} H((2^{\mathcal{X}})_{\nu_i}) &\leq H(\{Y : i \in \Gamma^Y\}_{\nu_i}) + H(\{Y : i \notin \Gamma^Y\}_{\nu_i}) \\ &\leq H(\{Y : i \in \Gamma^Y\}_{\nu_i}) + \sum_{\{Y : i \notin \Gamma^Y\}} H(Y_{\nu_i}) \\ &= H(\mathcal{X}(i)_{\tilde{\nu}}) + \sum_{\{Y : i \notin \Gamma^Y\}} H(i_{\nu^Y}) \\ &\leq \sum_{Y \subseteq \mathcal{X}} H(i_{\nu^Y}). \end{aligned}$$

Together with (5.3) we can derive the bounds stated in the theorem.

6. The derivation of (5.4): We derive for tuples π indexed by the elements of $2^{\mathcal{X}}$ and for $Y \subseteq \mathcal{X}$ (notice that Y is an element of $2^{\mathcal{X}}$ where Z is a subset of $2^{\mathcal{X}}$)

$$\begin{aligned}(\nu_i)_Y(\pi_Y) &= \sum_{\{\hat{\pi}\in[i]_\nu : \hat{\pi}_Y = \pi_Y\}} \sum_{\tilde{\pi}\in[\mathcal{X}]_{\tilde{\nu}}} \tilde{\nu}_{\mathcal{X}}(\tilde{\pi}) \prod_{V\in 2^{\mathcal{X}}} \nu^V_{i|s}(\hat{\pi}_V|\tilde{\pi}_V) \\ &= \sum_{\tilde{\pi}\in[\mathcal{X}]_{\tilde{\nu}}} \tilde{\nu}_{\mathcal{X}}(\tilde{\pi})\nu^Y_{i|s}(\pi_Y|\tilde{\pi}_Y) \\ &= \sum_{\tilde{\pi}\in[Y]_{\tilde{\nu}}} \tilde{\nu}_Y(\tilde{\pi})\nu^Y_{i|s}(\pi_Y|\tilde{\pi}) \\ &= \sum_{\tilde{\pi}\in[s]_{\nu^Y}} \nu^Y_s(\tilde{\pi})\nu^Y_{i|s}(\pi_Y|\tilde{\pi}) \\ &= \sum_{\tilde{\pi}\in[s]_{\nu^Y}} \nu^Y_{is}(\pi_Y\tilde{\pi}) \\ &= \nu^Y_i(\pi_Y).\end{aligned}$$

So, $(\nu_i)_Y = \nu^Y_i$, $[Y]_{\nu_i} = [i]_{\nu^Y}$, $Y_{\nu_i} = i_{\nu^Y}$, and

$$H(Y_{\nu_i}) = H(i_{\nu^Y}).$$

7. The derivation of (5.5): Let $\pi \in [2^{\mathcal{X}}]_{\nu_i}$ and $\tilde{\pi} \in [\mathcal{X}]_{\tilde{\nu}}$. Let $Y \subseteq \mathcal{X}$ with $i \in \Gamma^Y$. Then $\pi_Y \in [Y]_{\nu_i} = [i]_{\nu^Y}$ and $\tilde{\pi}_Y \in [Y]_{\tilde{\nu}} = [s]_{\nu^Y}$. See Lemma 5.4.1 and its consequence, w.l.o.g.

$$\nu^Y_{i|s}(\pi_Y|\tilde{\pi}_Y) = \begin{cases} 1, & \text{if } \pi_Y = \tilde{\pi}_Y, \\ 0, & \text{if } \pi_Y \neq \tilde{\pi}_Y. \end{cases} \tag{5.6}$$

So, for $Z = \{Y : i \in \Gamma^Y\}$

$$\begin{aligned}(\nu_i)_Z(\pi_Z) &= \sum_{\{\hat{\pi}\in[i]_\nu : \hat{\pi}_Z = \pi_Z\}} \sum_{\tilde{\pi}\in[\mathcal{X}]_{\tilde{\nu}}} \tilde{\nu}_{\mathcal{X}}(\tilde{\pi}) \prod_{Y\in 2^{\mathcal{X}}} \nu^Y_{i|s}(\hat{\pi}_Y|\tilde{\pi}_Y) \\ &= \sum_{\tilde{\pi}\in[\mathcal{X}]_{\tilde{\nu}}} \tilde{\nu}_{\mathcal{X}}(\tilde{\pi}) \prod_{\{Y : i\in\Gamma^Y\}} \nu^Y_{i|s}(\pi_Y|\tilde{\pi}_Y) \\ &= \sum_{\{\tilde{\pi}\in[\mathcal{X}]_{\tilde{\nu}} : \tilde{\pi}_Y = \pi_Y \text{if } i\in\Gamma^Y\}} \tilde{\nu}_{\mathcal{X}}(\tilde{\pi}) \\ &= \sum_{\{\tilde{\pi}\in[\mathcal{X}(i)]_{\tilde{\nu}} : \tilde{\pi}_Y = \pi_Y \text{if } i\in\Gamma^Y\}} \tilde{\nu}_{\mathcal{X}(i)}(\tilde{\pi}).\end{aligned}$$

Hence, if there exists $\omega \in [\mathcal{X}(i)]_{\tilde{\nu}}$ with $\pi_Y = \omega_Y$ for all $Y \subseteq \mathcal{X}$ with $i \in \Gamma^Y$ then $(\nu_i)_Z(\pi_Z) = \tilde{\nu}_{\mathcal{X}(i)}(\omega)$. If there does not exist such an ω then $(\nu_i)_Z(\pi_Z) = 0$. Thus

$$H(\{Y : i \in \Gamma^Y\}_{\nu_i}) = H(Z_{\nu_i}) = H(\mathcal{X}(i)_{\tilde{\nu}}).$$

Chapter 6

Unconditionally Secure Group Authentication

In conventional authentication theory [94] two trusting parties, say Alice and Bob, want to communicate securely over an insecure channel. If Bob receives a message he wants to be able to detect with high probability whether the message came from Alice or not, and if he concludes that the message came from Alice he wants to be sure that the message equals the original message sent by Alice. An eavesdropper enemy could have intercepted the message sent by Alice and he could have substituted another message. This is called a *substitution attack.* The enemy can also pretend to be Alice by transmitting a message to Bob. This is called a *impersonation attack.* Bob wants to be able to detect both type of attacks with high probability if one occurred. So, if Alice sends a message it should contain a sort of stamp or signature saying she is the one who transmits the message. The stamp should be difficult to copy by an enemy. In other words the message should be authenticated by Alice. Conventional authentication theory deals with this problem. This problem can be extended to the case where the *capability* to authenticate a message is given to groups instead of a single person. This setting has not attracted much attention. In this chapter we deal with a scenario where among a group of participants only certain subsets of the group are able to authenticate a message in order to send it to a trustable receiver. For example, the group could be bank clerks authorizing a large transaction for a bank (the receiver). We only consider unconditionally secure schemes, that is the security does not rely on any computational complexity assumption. As pointed out in [38] the problem is not solved by simply combining a secret sharing and an authentication scheme because such a solution would give the users of a qualified group not only the capability to authenticate after they combined their shares, but also full knowledge of the underlying secret. We use an approach where we extend existing secret sharing schemes to unconditionally secure group authentication schemes.

Boyd [23] introduced the problem of the construction of a scheme for which more than one person is needed to sign a message. In his paper he gave a 2 out of n RSA [92] conditionally secure signature scheme. Later Desmedt and Frankel [39] introduced a threshold signature scheme by combining schemes for secret sharing and authentication. Their paper deals almost only with conditionally secure schemes. In their paper an unconditionally secure scheme, based on a geometrical approach, is briefly discussed. The problem is further developed and discussed by Desmedt in [37] and [38].

In Section 6.1 we describe the conventional authentication model. In Section 6.2 we define the group authentication model and we give measures of the security in accordance with the conventional authentication model. Sections 6.3 and 6.4 analyse group authentication schemes based on perfect secret sharing schemes obtained by the generalized vector space construction (see Chapter 3) and authentication schemes using maximum rank distance codes. This chapter is joint work with Christian Gehrmann and Ben Smeets and is submitted to Designs, Codes and Cryptography [49]. In [78] the situation considered in this chapter is independently addressed and contains different results.

6.1 Systematic Authentication Codes

In conventional authentication a sender wants to transmit messages over an insecure channel to a receiver in the presence of a malicious adversary. The sender and receiver trust each other. The adversary can insert a message into the channel, which is called an *impersonation attack*, or observe a transmitted message and then replace it with another message, which is called a *substitution attack*. The receiver wants to detect false messages sent by the adversary. For this purpose the sender and receiver use a so-called authentication code.

We consider *systematic authentication codes*, also called Cartesian authentication codes. Sender and receiver select securely a secret key $s \in \mathcal{S}$ (also called the encoding rule). The random variable representing the selection of the secret key $s \in \mathcal{S}$ is denoted by S. The information the sender can transmit is called a message $m \in \mathcal{M}$ (also called a source state). A systematic authentication code can be described by a publicly known *authentication function* F which produces an *authentication tag* $F(m, s)$. The authenticated message that is sent to the receiver will be equal to $(m, F(m, s))$. The receiver will detect a false message if the authentication tag does not correspond to the message and secret key.

The probability of a successful impersonation attack is denoted by P_I. It equals the highest possible (worst case) probability that an authentication tag $F(m, s')$ and message m correspond to oneanother:

$$P_I = \max_{m \in \mathcal{M}} \max_{s' \in \mathcal{S}} P(F(m, S) = F(m, s')).$$

The probability of a successful substitution attack is denoted by P_S. It equals the highest possible (worst case) probability that an authentication tag $F(\hat{m}, s')$ and message $\hat{m}$ correspond to oneanother given the knowledge of an intercepted authenticated message $(m, F(m, s))$, $m \neq \hat{m}$:

$$P_S = \max_{\substack{\hat{m}, m \in \mathcal{M}, \\ m \neq \hat{m}}} \max_{s' \in \mathcal{S}} Pr(F(\hat{m}, S) = F(\hat{m}, s') | F(m, S) = F(m, s')).$$

The primary goal of authentication is to construct codes maximizing $|\mathcal{M}|$ given upper bounds on P_I, P_S, and $|\mathcal{S}|$. A secondary goal is to construct codes with small *message expansion*

$$\frac{\log |\{(m, F(m, s)) : m \in \mathcal{M}, s \in \mathcal{S}\}|}{\log |\mathcal{M}|}.$$

We finish this section by recalling the following lower bound on P_I due to Simmons

$$P_I \geq 2^{-I(S;M,F(M,S))}, \qquad (6.1)$$

where M is the random variable representing the selection of messages by the sender. If we want the probability of impersonation to be small this implies automatically that we have to tolerate that an authenticated message provides outsiders with at least $-\log P_I$ bits of information about the key! It was shown in [64] that for systematic codes (as in this section) we have

$$P_S \geq P_I. \qquad (6.2)$$

This implies that for systematic codes, when we want to have P_S small, we also have to tolerate that at least $-\log P_S$ bits secret key information will leak.

6.2 USGA-Schemes

An unconditionally secure group authentication scheme (USGA-scheme) is a method for certain predefined subsets of participants $\mathcal{P}$ to compute authentication tags by combining shares of a secret key. Let $\mathcal{P}$ denote the set of participants. The set of all groups qualified to compute correct authentication tags is denoted by Γ, and is called the access structure as in secret sharing. Again, only monotone access structures are considered. Any non-qualified subset should not be able to compute a correct tag. Further we want to achieve that the participants of a qualified set can compute a correct tag but only without getting too much knowledge of the underlying key. Otherwise a non-qualified subgroup of a qualified set may be able to authenticate another message. Since the lower bounds (6.1) and (6.2) are also valid for USGA-schemes our wish to have low values of P_I and P_S forces that we have to tolerate a leak of secret key information of at least $-\log P_I$ bits.

Let $\mathcal{M}$ denote the set of messages and let $\mathcal{S}$ denote the set of possible secret keys. The receiver of the authenticated messages also plays the role of dealer of the secret key. To share a secret $s \in \mathcal{S}$ he selects an auxiliary arbitrary element a from a set $\mathcal{A}$ in order to compute for participant $i \in \mathcal{P}$ its share

$$S_i(s, a),$$

which is transmitted securely to participant i. In what follows random variable A represents the selection of the auxiliary variable $a \in \mathcal{A}$ by the receiver/dealer. Functions S_i, $i \in \mathcal{P}$, are called *sharing functions.* The receiver/dealer does not need a after this setup phase. If the participants of a qualified group $X \in \Gamma$ want to send an authenticated message $m \in \mathcal{M}$ to the receiver they need to compute the authentication tag $F(m, s)$ by combining their shares. The computation is done in two phases. Firstly, each participant i in X calculates

$$F_i^X(m, S_i(s, a)).$$

Secondly, each participant in X transmits this to a combiner. The combiner calculates the authentication tag by evaluating $C_X(F_i^X(m, S_i(s, a)); i \in X)$, which will equal $F(m, s)$. In what follows C_X simply adds, that is the combiner calculates

$$C_X(F_i^X(m, S_i(s, a)); i \in X) = \sum_{i \in X} F_i^X(m, S_i(s, a)).$$

The output of the combiner is the authentication tag $F(m, s)$ of message m. Now, group X transmits $(m, F(m, s))$ to the receiver. The receiver accepts the message if the tag corresponds to the message and the secret key, i.e., he computes the correct tag from the received m and private secret s and he verifies whether the received tag and correct tag are the same. Note that the receiver can do the computation of the tag directly because he knows the private secret s (which is unknown to each individual participant).

Functions S_i, F_i^X, C_X, and F, and sets $\mathcal{S}$, $\mathcal{A}$, and $\mathcal{M}$ are known to all participants, that is the USGA-scheme is public domain.

The combiner need not to be secure, that is all its inputs can be revealed to each participant in $\mathcal{P}$. We notice that this situation corresponds to the situation described in [39]. The combiner can be seen as a device build by the receiver. In some practical situations the combiner and receiver might be one and the same person (for example, if the participants, combiner, and receiver communicate by means of a computer network). In that case the receiver essentially receives a larger authentication tag, $F_i^X(m, S_i(s, a))$ for $i \in X$, such that impersonation and substitution attacks become in general less successful. However, as pointed out in [37], there are two advantages of the separation of the combiner and the receiver. Firstly, it decreases the communication cost between the sender group and the receiver. Secondly, it gives the possibility to have an anonymous sender group. Besides these two advantages we have a third advantage; the authentication function only depends on the secret key and the message as in ordinary single authentication. Hence, all the properties of the message checking process for the receiver side are the same as for those of the receiver side of a single authentication scheme with the same authentication function.

As in ordinary single authentication schemes we measure the security of a scheme by the probabilities of successful impersonation and substitution attacks. The probability of a successful impersonation attack is denoted by P_I. It equals the highest possible (worst case) probability that an authentication tag $F(m, s')$ and message m correspond to oneanother given the knowledge of the shares $S_i(s, a), i \in Y$, of a non-qualified group Y:

$$P_I = \max_{Y \notin \Gamma} \max_{m \in \mathcal{M}} \max_{\substack{s' \in \mathcal{S}, \\ a' \in \mathcal{A}}} P\left(F(m, S) = F(m, s') \,|S_i(S, A) = S_i(s', a') \text{ for } i \in Y\right).$$

The probability of a successful substitution attack is denoted by P_S. It equals the highest possible (worst case) probability that an authentication tag $F(\hat{m}, s')$ and message $\hat{m}$ correspond to one another given the knowledge of the shares $S_i(s, a), i \in Y$, of a non-qualified group Y, and the knowledge of (intercepted) inputs of the combiner $F_i^X(m, S_i(s, a)), i \in X$, transmitted by a qualified group X, and the output $F(m, s)$ of the combiner:

$$P_S = \max_{\substack{Y \notin \Gamma, \\ X \in \Gamma}} \max_{\substack{\hat{m}, m \in \mathcal{M}, \\ m \neq \hat{m}}} \max_{\substack{s' \in \mathcal{S}, \\ a' \in \mathcal{A}}} P\left(\begin{array}{c} F(\hat{m}, S) \\ = F(\hat{m}, s') \end{array} \middle| \begin{array}{l} S_i(S, A) = S_i(s', a'), \text{ for } i \in Y, \\ F_i^X(m, S_i(S, A)) = \\ F_i^X(m, S_i(s', a')), \text{ for } i \in X \end{array} \right).$$

We notice that given the combiners input the output of the combiner can be calculated, which is the reason for not including the output of the combiner in the definition of P_S.

In the remainder of this chapter we assume for reasons of simplicity that S and A are uniformly distributed. Hence,

$$P_I = \max_{Y \notin \Gamma} \max_{m \in \mathcal{M}} \max_{\substack{s' \in \mathcal{S}, \\ a' \in \mathcal{A}}} \frac{\left| \left\{ \begin{array}{c} (s, a) \in \\ \mathcal{S} \times \mathcal{A} \end{array} \middle| \begin{array}{l} F(m, s) = F(m, s'), \\ S_i(s, a) = S_i(s', a'), \\ \text{for } i \in Y \end{array} \right\} \right|}{\left| \left\{ \begin{array}{c} (s, a) \in \\ \mathcal{S} \times \mathcal{A} \end{array} \middle| \begin{array}{l} S_i(s, a) = S_i(s', a'), \\ \text{for } i \in Y \end{array} \right\} \right|}, \qquad (6.3)$$

$$P_S = \max_{\substack{Y\notin\Gamma,\\ X\in\Gamma}} \max_{\substack{\hat{m},m\in\mathcal{M},\\ m\neq\hat{m}}} \max_{\substack{s'\in\mathcal{S},\\ a'\in\mathcal{A}}} \frac{\left|\left\{ \begin{array}{c} (s,a)\in \\ \mathcal{S}\times\mathcal{A} \end{array} \;\middle|\; \begin{array}{l} F(\hat{m},s)=F(\hat{m},s'),\\ S_i(s,a)=S_i(s',a'),\\ \text{for } i\in Y,\\ F_i^X(m,S_i(s,a)) = \\ F_i^X(m,S_i(s',a')), i\in X \end{array}\right\}\right|}{\left|\left\{ \begin{array}{c} (s,a)\in \\ \mathcal{S}\times\mathcal{A} \end{array} \;\middle|\; \begin{array}{l} S_i(s,a)=S_i(s',a'),\\ \text{for } i\in Y,\\ F_i^X(m,S_i(s,a)) = \\ F_i^X(m,S_i(s',a')), i\in X \end{array}\right\}\right|},$$

and the size of i's share is

$$\log|\{S_i(s,a)|s\in\mathcal{S}, a\in\mathcal{A}\}|$$

and equals $H(S_i(S,A))$.

The primary goal of group authentication is to construct schemes maximizing $|\mathcal{M}|$ given upper bounds on P_I, P_S, and the maximal size of a share. A secondary goal is to construct schemes with small message expansion

$$\frac{\log|\{(m,F(m,s)) : m\in\mathcal{M}, s\in\mathcal{S}\}|}{\log|\mathcal{M}|}.$$

6.3 Linear USGA-Schemes

We consider the situation in which the receiver uses a perfect secret sharing scheme obtained by the generalized vector space construction of Chapter 3 (Section 3.1) to share the key. In what follows $\mathcal{P}=\{1,\ldots,n\}$, $\mathcal{S}=GF(q)^{mk}$, and $\mathcal{A}=GF(q)^{m(l-k)}$, where l is some integer $l\geq k$. Thus the size of a possible secret key is mk q-ary bits. Let each participant have an $l\times p_i$ matrix G_i over $GF(q)$. These matrices are not secret, they are publicly accessible.

We recall some definitions and notations from Section 3.1. For $X=\{i_1,\ldots,i_w\}\subseteq\mathcal{P}$, with $i_1<\ldots<i_w$, we define the $l\times p[X]$ matrix $G[X]$ over $GF(q)$, with $p[X]=\sum_{i\in X}p_i$, by $G[X]=(G_{i_1}|\ldots|G_{i_w})$. By $G^1[X]$ we denote the matrix consisting of the first k rows of $G[X]$, and by $G^2[X]$ we denote the matrix consisting of the last $l-k$ rows of $G[X]$. Matrices G_i^1 and G_i^2, $i\in\mathcal{P}$, are defined in a similar way. We assume that the set of q-ary matrices G_i, $i\in\mathcal{P}$, is suitable for Γ on $\mathcal{P}$ with set of possible secrets $GF(q)^k$. Note that the set of possible secret keys in our USGA-scheme is $GF(q)^{mk}$ (and not $GF(q)^k$). Thus [V1] and [V2] hold:

[V1] for all $X\in\Gamma$ the unit vectors $\mathbf{e}^i\in GF(q)^l$ for $1\leq i\leq k$ can be expressed as a linear combination of the columns of matrix $G[X]$, and

[V2] for all $X\notin\Gamma$ none of the non-zero linear combinations of $\{\mathbf{e}^1,\ldots,\mathbf{e}^k\}$ can be expressed as a linear combination of the columns of matrix $G[X]$.

As explained in Theorem 3.1.2 [V1] and [V2] are sufficient and necessary conditions to construct a perfect secret sharing scheme for access structure Γ on $\mathcal{P}$ with set of possible secrets $GF(q)^k$ by means of the generalized vector space construction. Such a scheme has worst-case information rate k/p, where $p = \max_{i \in \mathcal{P}} p_i$.

[V1] implies that for all $X = \{i_1, \ldots, i_w\} \in \Gamma$ there exists a (possibly more than one) matrix $B[X] = (B[X]_{i_1}^T | \ldots | B[X]_{i_w}^T)^T$ such that

$$\begin{pmatrix} I_k \\ O \end{pmatrix} = G[X]B[X] = \begin{pmatrix} \sum_{i \in X} G_i^1 B[X]_i \\ \sum_{i \in X} G_i^2 B[X]_i \end{pmatrix}, \tag{6.4}$$

where $B[X]_{i_j}$ is a $p_{i_j} \times k$ matrix over $GF(q)$. For each $X \in [\Gamma]^-$ we fix a solution $B[X]$ of Equation (6.4). These solutions are not secret, they are publicly accessible (e.g. there is a publicly accessible deterministic algorithm which computes $B[X]$ given G_i, $i \in X$).

For matrices E and D we define their Kronecker product $E \otimes D$ as the matrix

$$E \otimes D = \begin{pmatrix} d_{1,1}E & d_{1,2}E & \cdots \\ d_{2,1}E & d_{2,2}E & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}, \text{ where } D = \begin{pmatrix} d_{1,1} & d_{1,2} & \cdots \\ d_{2,1} & d_{2,2} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}.$$

To share a secret key $\mathbf{s} \in \mathcal{S}$ the dealer/receiver selects an arbitrary element $\mathbf{a} \in \mathcal{A}$, and transmits securely to $i \in \mathcal{P}$

$$S_i(\mathbf{s}, \mathbf{a}) = \mathbf{s}(G_i^1 \otimes I_m) + \mathbf{a}(G_i^2 \otimes I_m).$$

Thus, the size of i's share is mp_i q-ary bits.

Let the set of messages $\mathcal{M}$ be a set with $m \times r$ matrices with entries in $GF(q)$. For matrices $M \in \mathcal{M}$ we define

$$M^* = I_k \otimes M.$$

The authentication tag of a message $M \in \mathcal{M}$ is given by

$$F(M, \mathbf{s}) = \mathbf{s}M^*.$$

Let $X' \in \Gamma$. Suppose that the participants in X' want to compute the authentication tag corresponding to message M. Then they select a subgroup $X \subseteq X'$ such that $X \in [\Gamma]^-$. Each participant $i \in X$ computes

$$F_i^X(M, S_i(\mathbf{s}, \mathbf{a})) = S_i(\mathbf{s}, \mathbf{a})(B[X]_i \otimes I_m)M^*,$$

which they transmit to the combiner. The combiner calculates and outputs

$$C_X(F_i^X(M, S_i(\mathbf{s}, \mathbf{a})); i \in X),$$

which equals

$$
\begin{aligned}
& \sum_{i\in X} F_i^X(M, S_i(\mathbf{s},\mathbf{a})) \\
= & \sum_{i\in X} S_i(\mathbf{s},\mathbf{a})(B[X]_i \otimes I_m)M^* \\
= & \sum_{i\in X} (\mathbf{s}(G_i^1 \otimes I_m) + \mathbf{a}(G_i^2 \otimes I_m))(B[X]_i \otimes I_m)M^* \\
= & \sum_{i\in X} (\mathbf{s}(G_i^1 B[X]_i \otimes I_m) + \mathbf{a}(G_i^2 B[X]_i \otimes I_m))M^* \\
= & \ \mathbf{s}\left[\left(\sum_{i\in X} G_i^1 B[X]_i\right) \otimes I_m\right] M^* + \mathbf{a}\left[\left(\sum_{i\in X} G_i^2 B[X]_i\right) \otimes I_m\right] M^* \\
= & \ \mathbf{s}(I_k \otimes I_m)M^* \\
= & \ \mathbf{s}M^* \\
= & \ F(M,\mathbf{s}),
\end{aligned}
\tag{6.5}
$$

as required. Now group X' transmits $(M, F(M,\mathbf{s}))$ to the receiver.

The following theorem is the main result concerning the size parameters, P_I, and P_S. The left null space of matrix M is denoted by $N(M)$ and defined as

$$N(M) = \{\mathbf{x} : \mathbf{x}M = \mathbf{0}\}.$$

Theorem 6.3.1 *Let a collection of $l \times p_i$ q-ary matrices G_i, $i \in \mathcal{P}$, be a suitable set of matrices for Γ on $\mathcal{P}$ with set of possible secrets $GF(q)^k$ and define $p = \max_{i\in\mathcal{P}} p_i$. Let $\mathcal{M}$ be a set of $m\times r$ matrices with entries in $GF(q)$. Then we can construct an USGA-scheme for Γ on $\mathcal{P}$ with*

- *$\mathcal{M}$ as the set of messages,*
- *q^{mk} possible secret keys,*
- *maximal share size pm q-ary symbols,*
- $P_I = \max_{M\in\mathcal{M}} \left(\frac{|N(M)|}{q^m}\right)^k$,
- $P_S = \max_{M,\hat{M}\in\mathcal{M},\hat{M}\neq M} \left(\frac{|N(\hat{M})\cap N(M)|}{|N(M)|}\right)^k$, *and*
- *message expansion* $1 + \frac{rk\log q}{\log|\mathcal{M}|}$.

In the next sections we will apply this theorem for sets of messages representing maximum rank distance codes.

Proof of Theorem 6.3.1: We will show that the USGA-scheme described in this section has the properties as listed in Theorem 6.3.1. Clearly, the properties concerning the set of messages, the number of possible secret keys, maximal share size, and message expansion hold. It remains to verify the expressions for P_I and P_S. So, we will subsequently analyse for $X \in \Gamma$, $Y \notin \Gamma$, $M, \hat{M} \in \mathcal{M}$, $M \neq \hat{M}$, $\mathbf{s}' \in \mathcal{S}$, and $\mathbf{a}' \in \mathcal{A}$ the quantities

$$\left|\{(\mathbf{s},\mathbf{a}) \in \mathcal{S} \times \mathcal{A} \mid S_i(\mathbf{s},\mathbf{a}) = S_i(\mathbf{s}',\mathbf{a}'), \text{ for } i \in Y \ \}\right|, \tag{6.6}$$

$$\left|\left\{(\mathbf{s},\mathbf{a}) \in \mathcal{S} \times \mathcal{A} \,\middle|\, \begin{array}{l} F(M,\mathbf{s}) = F(M,\mathbf{s}'), \\ S_i(\mathbf{s},\mathbf{a}) = S_i(\mathbf{s}',\mathbf{a}'), \text{ for } i \in Y \end{array}\right\}\right|, \tag{6.7}$$

$$\left|\left\{ \begin{array}{c} (\mathbf{s},\mathbf{a}) \in \\ \mathcal{S} \times \mathcal{A} \end{array} \,\middle|\, \begin{array}{l} S_i(\mathbf{s},\mathbf{a}) = S_i(\mathbf{s}',\mathbf{a}'), \text{ for } i \in Y, \\ F_i^X(M, S_i(\mathbf{s},\mathbf{a})) = F_i^X(M, S_i(\mathbf{s}',\mathbf{a}')), i \in X \end{array}\right\}\right|, \tag{6.8}$$

$$\left|\left\{ \begin{array}{c} (\mathbf{s},\mathbf{a}) \in \\ \mathcal{S} \times \mathcal{A} \end{array} \,\middle|\, \begin{array}{l} F(\hat{M},\mathbf{s}) = F(\hat{M},\mathbf{s}'), \\ S_i(\mathbf{s},\mathbf{a}) = S_i(\mathbf{s}',\mathbf{a}'), \text{ for } i \in Y, \\ F_i^X(M, S_i(\mathbf{s},\mathbf{a})) = F_i^X(M, S_i(\mathbf{s}',\mathbf{a}')), i \in X \end{array}\right\}\right|, \tag{6.9}$$

being the numerators and denominators in (6.3).

In order to evaluate P_I let us start by analysing (6.6). Let $Y \notin \Gamma$. From [V2] we infer that if $G^2[Y]\mathbf{b}^T = \mathbf{0}^T$ then $G[Y]\mathbf{b}^T = \mathbf{0}^T$. Thus the rank of matrix $G[Y]$ equals the rank of matrix $G^2[Y]$. Hence, the rows of matrix $G^1[Y]$ are linear combinations of the rows of matrix $G^2[Y]$. This proves that there exists a matrix L such that $G[Y]^1 = LG[Y]^2$. So

$$S_i(\mathbf{s},\mathbf{a}) = S_i(\mathbf{s}',\mathbf{a}'), \text{ for all } i \in Y, \tag{6.10}$$

is equivalent to each of the following statements

$$\begin{array}{l}
\mathbf{s}(G_i^1 \otimes I_m) + \mathbf{a}(G_i^2 \otimes I_m) = \mathbf{s}'(G_i^1 \otimes I_m) + \mathbf{a}'(G_i^2 \otimes I_m) \text{ for all } i \in Y, \\
\mathbf{s}(G[Y]^1 \otimes I_m) + \mathbf{a}(G[Y]^2 \otimes I_m) = \mathbf{s}'(G[Y]^1 \otimes I_m) + \mathbf{a}'(G[Y]^2 \otimes I_m), \\
\mathbf{s}(LG[Y]^2 \otimes I_m) + \mathbf{a}(G[Y]^2 \otimes I_m) = \mathbf{s}'(LG[Y]^2 \otimes I_m) + \mathbf{a}'(G[Y]^2 \otimes I_m), \\
(\mathbf{a} - \mathbf{a}' + (\mathbf{s} - \mathbf{s}')(L \otimes I_m))(G^2[Y] \otimes I_m) = \mathbf{0}.
\end{array}$$

Thus for fixed $\mathbf{s}$, $\mathbf{s}'$, and $\mathbf{a}'$, we have $|N(G^2[Y] \otimes I_m)|$ solutions $\mathbf{a}$ to the equations given by (6.10). Hence, the expression in (6.6) equals

$$|\mathcal{S}||N(G^2[Y] \otimes I_m)| \tag{6.11}$$

$(|\mathcal{S}| = q^{mk})$.

We continue by analysing (6.7). We notice that

$$F(M,\mathbf{s}) = F(M,\mathbf{s}') \tag{6.12}$$

is equivalent to the statements

$$\begin{array}{l}
\mathbf{s}M^* = \mathbf{s}'M^*, \\
(\mathbf{s} - \mathbf{s}')M^* = \mathbf{0}.
\end{array}$$

So, for fixed $\mathbf{s}'$ we have $|N(M^*)|$ solutions $\mathbf{s}$ to the equation given by (6.12). This shows that (6.7) equals

$$|N(M^*)||N(G^2[Y] \otimes I_m)|. \tag{6.13}$$

From (6.11) and (6.13) we infer that

$$\begin{aligned} P_I &= \max_{Y \notin \Gamma} \max_{M \in \mathcal{M}} \frac{|N(M^*)||N(G^2[Y] \otimes I_m)|}{|\mathcal{S}||N(G^2[Y] \otimes I_m)|} \\ &= \max_{M \in \mathcal{M}} \frac{|N(M^*)|}{q^{mk}} = \max_{M \in \mathcal{M}} \left(\frac{|N(M)|}{q^m} \right)^k . \end{aligned}$$

In order to obtain P_S we proceed analysing (6.8). Suppose $X' \in \Gamma$ reconstructed $F(M, \mathbf{s}) = \mathbf{s}M^*$. Let $X \in [\Gamma]^-$ be the subgroup responsible for the reconstruction. We derive for $i \in X$

$$\begin{aligned} & F_i^X(M, S_i(\mathbf{s}, \mathbf{a})) \\ = \; & S_i(\mathbf{s}, \mathbf{a})(B[X]_i \otimes I_m)M^* \\ = \; & ((\mathbf{s}G_i^1 B[X]_i + \mathbf{a}G_i^2 B[X]_i) \otimes I_m)M^* \\ = \; & \mathbf{s}(G_i^1 B[X]_i \otimes I_m)M^* + \mathbf{a}(G_i^2 B[X]_i \otimes I_m)M^* \\ = \; & \mathbf{s}\left[\left(G_i^1 - LG_i^2\right) B[X]_i \otimes I_m\right] M^* + \\ & (\mathbf{a} + \mathbf{s}(L \otimes I_m))(G_i^2 B[X]_i \otimes I_m)M^*. \end{aligned}$$

Also, see (6.5),

$$\sum_{i \in X} F_i^X(M, S_i(\mathbf{s}, \mathbf{a})) - F_i^X(M, S_i(\mathbf{s}', \mathbf{a}')) = F(M, \mathbf{s}) - F(M, \mathbf{s}') = (\mathbf{s} - \mathbf{s}')M^*.$$

Hence,

$$F_i^X(M, S_i(\mathbf{s}, \mathbf{a})) = F_i^X(M, S_i(\mathbf{s}', \mathbf{a}')), \text{ for } i \in X \tag{6.14}$$

is equivalent to

$$\begin{aligned} & (\mathbf{a} - \mathbf{a}' + (\mathbf{s} - \mathbf{s}')(L \otimes I_m))(G_i^2 B[X]_i \otimes I_m)M^* \\ & = -(\mathbf{s} - \mathbf{s}')((G_i^1 - LG_i^2)B[X]_i \otimes I_m)M^*, \text{ for } i \in X, \\ & \text{and } (\mathbf{s} - \mathbf{s}')M^* = \mathbf{0}. \end{aligned} \tag{6.15}$$

By definition $M^* = I_k \otimes M$ and M is a $m \times r$ q-ary matrix. Let

$$A = (G_i^1 - LG_i^2)B[X]_i.$$

Matrix A is a $k \times k$ q-ary matrix. Therefore

$$(A \otimes I_m)(I_k \otimes M) = A \otimes M = (I_k \otimes M)(A \otimes I_r).$$

We conclude that

$$((G_i^1 - LG_i^2)B[X]_i \otimes I_m)M^* = M^*((G_i^1 - LG_i^2)B[X]_i \otimes I_r). \qquad (6.16)$$

By substituting (6.16) in (6.15) we conclude that (6.14) is equivalent to

$$\begin{aligned}&(\mathbf{a} - \mathbf{a}' + (\mathbf{s} - \mathbf{s}')(L \otimes I_m))(G_i^2 B[X]_i \otimes I_m)M^* \\ &= -(\mathbf{s} - \mathbf{s}')M^*((G_i^1 - LG_i^2)B[X]_i \otimes I_r), \text{ for } i \in X, \\ &\text{and } (\mathbf{s} - \mathbf{s}')M^* = \mathbf{0},\end{aligned}$$

which is clearly equivalent to

$$\begin{aligned}&(\mathbf{a} - \mathbf{a}' + (\mathbf{s} - \mathbf{s}')(L \otimes I_m))(G_i^2 B[X]_i \otimes I_m)M^* = \mathbf{0}, \text{ for } i \in X \\ &\text{and } (\mathbf{s} - \mathbf{s}')M^* = \mathbf{0}.\end{aligned}$$

Thus for fixed $\mathbf{s}$, $\mathbf{s}'$, and $\mathbf{a}'$ such that $(\mathbf{s} - \mathbf{s}')M^* = \mathbf{0}$ we have

$$\left| N(G^2[Y] \otimes I_m) \cap \bigcap_{i \in X} N((G_i^2 B[X]_i \otimes I_m)M^*) \right|$$

solutions $\mathbf{a}$ to the equations given by (6.10) and (6.14). If $(\mathbf{s} - \mathbf{s}')M^* \neq \mathbf{0}$ then there are no solutions $\mathbf{a}$ to the equations given by (6.14). For fixed s' we have $|N(M^*)|$ solutions $\mathbf{s}$ to the equation $(\mathbf{s} - \mathbf{s}')M^* = \mathbf{0}$. Hence, (6.8) equals

$$|N(M^*)| \left| N(G^2[Y] \otimes I_m) \cap \bigcap_{i \in X} N((G_i^2 B[X]_i \otimes I_m)M^*) \right| . \qquad (6.17)$$

We notice that $F(\hat{M}, \mathbf{s}) = F(\hat{M}, \mathbf{s}')$ is equivalent to $(\mathbf{s} - \mathbf{s}')\hat{M}^*$. Thus for fixed $\mathbf{s}'$ we have $|N(M^*) \cap N(\hat{M}^*)|$ solutions $\mathbf{s}$ to the equations $(\mathbf{s} - \mathbf{s}')M^* = \mathbf{0}$, and $F(\hat{M}, \mathbf{s}) = F(\hat{M}, \mathbf{s}')$. This implies that (6.9) equals

$$|N(\hat{M}^*) \cap N(M^*)| \left| N(G^2[Y] \otimes I_m) \cap \bigcap_{i \in X} N((G_i^2 B[X]_i \otimes I_m)M^*) \right| . (6.18)$$

From equations (6.17) and (6.18) we infer that

$$P_S = \max_{\substack{M, \hat{M} \in \mathcal{M} \\ \hat{M} \neq M}} \frac{|N(\hat{M}^*) \cap N(M^*)|}{|N(M^*)|} = \max_{\substack{M, \hat{M} \in \mathcal{M} \\ \hat{M} \neq M}} \left(\frac{|N(\hat{M}) \cap N(M)|}{|N(M)|} \right)^k .$$

□

6.4 Maximum Rank Distance Codes

In this section we discuss linear maximum rank distance codes (MRD-codes) as studied by Gabidulin in [53]. In Section 6.5 they will be used to construct the set of messages $\mathcal{M}$ such that the expressions for P_I and P_S in Theorem 6.3.1 are easy to evaluate. A linear MRD-code is a set of matrices over $GF(q)$ closed under addition. They can be constructed in the following manner. Let $Q_{s,t}$, $0 < s \leq t$, denote the set of so called "linearized" polynomials of the form

$$F(z) = \sum_{i=0}^{s-1} f_i z^{q^i},\ z \in GF(q^t),$$

where $f_i \in GF(q^t)$. Let $s \leq r \leq t$, and let $g_j \in GF(q^t)$, $1 \leq j \leq r$, be linearly independent over $GF(q)$ (such elements do exist since $r \leq t$). Further, let ϕ be an isomorphism from $GF(q^t)$ to $GF(q)^t$. Gabidulin [53] showed that

$$\mathcal{R}_{s,r,t} = \{(\phi(F(g_1))|\ldots|\phi(F(g_r))) : F \in Q_{s,t}\} \tag{6.19}$$

is a linear MRD-code consisting of $t \times r$ matrices over $GF(q)$ with $|\mathcal{R}_{s,r,t}| = |Q_{s,t}| = q^{ts}$ elements such that

$$rank(R) \geq r - s + 1$$

for $R \in \mathcal{R}_{s,r,t}$. Its proof is as follows. Let $\alpha_i \in GF(q)$, $1 \leq i \leq r$, such that $\sum_{1\leq i\leq r} \alpha_i \phi(F(g_i)) = 0$. Then

$$\begin{aligned} 0 &= \sum_{1\leq i\leq r} \alpha_i \phi(F(g_i)) \\ &= \phi(\sum_{1\leq i\leq r} \alpha_i F(g_i)), \end{aligned}$$

hence, $\sum_{1\leq i\leq r} \alpha_i F(g_i) = 0$. We derive

$$\begin{aligned} 0 &= \sum_{1\leq i\leq r} \alpha_i F(g_i) \\ &= \sum_{0\leq j\leq s-1} f_j \sum_{1\leq i\leq r} \alpha_i g_i^{q^j} \quad (\alpha_i^q = \alpha_i) \\ &= \sum_{0\leq j\leq s-1} f_j \left(\sum_{1\leq i\leq r} \alpha_i g_i \right)^{q^j} \\ &= F\left(\sum_{1\leq i\leq r} \alpha_i g_i \right). \end{aligned}$$

Polynomial $F(z)$ has at most q^{s-1} zero points. Elements g_i, $1 \leq i \leq r$, are linearly independent over $GF(q)$. Hence, there are at most q^{s-1} tuples

$(\alpha_1, \ldots, \alpha_r)$ such that $F(\sum_{1\leq i\leq r} \alpha_i g_i) = 0$. We conclude that there are at most q^{s-1} tuples $(\alpha_1, \ldots, \alpha_r)$ such that $0 = \sum_{1\leq i\leq r} \alpha_i \phi(F(g_i)) = (\phi(F(g_1))| \ldots |\phi(F(g_r)))(\alpha_1, \ldots, \alpha_r)^T$. Thus matrix

$$(\phi(F(g_1))| \ldots |\phi(F(g_r)))$$

has column rank (= row rank) at least $r - s + 1$, its row length minus $s - 1$. This finishes the proof.

6.5 A construction using MRD codes.

In this section we discuss a special class of linear group authentication schemes. We will define $\mathcal{M}$ by means of the MRD codes described in the previous section. For the sake of completeness we notice that in [65] it was shown how these can be used to construct authentication codes for non-trusting parties.

Let

$$0 < s \leq m/2 - |m/2 - r|.$$

Then, $s \leq r \leq m - r$, if $r \leq m/2$, and $s \leq m - r \leq r$, if $r \geq m/2$. We define the set of $m \times r$ matrices $\mathcal{M}_{s,r}$ by

$$\mathcal{M}_{s,r} = \begin{cases} \{(I_r|R^T)^T : R \in \mathcal{R}_{s,r,m-r}\}, & \text{if } r < m/2, \\ \{(I_r|R)^T : R \in \mathcal{R}_{s,m-r,r}\}, & \text{if } r \geq m/2. \end{cases}$$

We notice that

$$|\mathcal{M}_{s,r}| = q^{s(m/2+|m/2-r|)}. \tag{6.20}$$

Let $\mathcal{M}_{s,r}$ be the set of messages $\mathcal{M}$ in Theorem 6.3.1. Let us analyse the expressions for P_I and P_S. Let $M \in \mathcal{M}$. Its column rank is r, so

$$|N(M)| = q^{m-r},$$

hence,

$$P_I = q^{-rk}. \tag{6.21}$$

Let $M \neq \hat{M} \in \mathcal{M}$. Suppose that $r < m/2$. Then $M = (I_r|R^T)^T$ and $\hat{M} = (I_r|\hat{R}^T)^T$ for some $R, \hat{R} \in \mathcal{R}_{s,r,m-r}$, $R \neq \hat{R}$. We derive

$$\begin{aligned} |N(\hat{M}) \cap N(M)| &= |\{\mathbf{s} : \mathbf{s}\hat{M} = \mathbf{0}, \mathbf{s}M = \mathbf{0}\}| \\ &= |\{(\mathbf{s}^0, \mathbf{s}^1) : \mathbf{s}^0 + \mathbf{s}^1\hat{R} = \mathbf{s}^0 + \mathbf{s}^1 R = \mathbf{0}\}| \\ &= |\{(\mathbf{s}^0, \mathbf{s}^1) : \mathbf{s}^0 = -\mathbf{s}^1 R, \mathbf{s}^1(R - \hat{R}) = \mathbf{0}\}| \\ &= |N(R - \hat{R})| \\ &= q^{(m-r)-rank(R-\hat{R})} \\ &\leq q^{(m-r)-(r-s+1)}, \end{aligned}$$

where the inequality follows from the fact that $R - \hat{R} \in \mathcal{R}_{s,r,m-r}$, hence, $rank(R - \hat{R}) \geq r - s + 1$. We have obtained that

$$\frac{|N(\hat{M}) \cap N(M)|}{|N(M)|} \leq q^{-(r-s+1)k} = q^{-(m/2-|m/2-r|-s+1)k}.$$

Similarly, for $r \geq m/2$, $M = (I_r|R)^T$ and $\hat{M} = (I_r|\hat{R})^T$ for some $R, \hat{R} \in \mathcal{R}_{s,m-r,r}$, $R \neq \hat{R}$, and so

$$\begin{aligned} |N(\hat{M}) \cap N(M)| &= |N(R^T - \hat{R}^T)| \\ &= q^{(m-r)-rank((R-\hat{R})^T)} \\ &= q^{(m-r)-rank(R-\hat{R})} \\ &\leq q^{(m-r)-(m-r-s+1)}. \end{aligned}$$

Hence,

$$\frac{|N(\hat{M}) \cap N(M)|}{|N(M)|} \leq q^{-(m-r-s+1)k} = q^{-(m/2-|m/2-r|-s+1)k}.$$

In both cases we obtain

$$P_S = q^{-(m/2-|m/2-r|-s+1)k}. \tag{6.22}$$

What are the best choices of m, r, and s to achieve our primary goal? To answer this let $r+b = \lfloor m/2 \rfloor$. From $0 < s \leq m/2 - |m/2-r| = r$ we conclude that

$$\begin{aligned} &0 < s + b \leq r + b = \lfloor m/2 \rfloor = m/2 - |m/2 - (r+b)|, \\ &s \leq r \leq \lceil m/2 \rceil = m - r - b. \end{aligned}$$

From the first formula we infer that we are allowed to choose a new r and s by taking $r + b$ and $s + b$ respectively. From the second formula we obtain

$$s(m-r) \leq s(m-r) + b(m-r-s) = (s+b)(m-(r+b)).$$

We conclude that if we increase both r and s with b then the number of messages increases (cf. (6.20)), P_I decreases (cf. (6.21)), while P_S (cf. (6.22)), and the maximal share size remain the same. Choosing $r = \lfloor m/2 \rfloor$ leads to $q^{s\lceil m/2 \rceil}$ messages, $P_I = q^{-\lfloor m/2 \rfloor k}$, and $P_S = q^{-(\lfloor m/2 \rfloor - s+1)k}$. Choosing $r = \lceil m/2 \rceil$ leads to $q^{s\lceil m/2 \rceil}$ messages, $P_I = q^{-\lceil m/2 \rceil k}$, and $P_S = q^{-(\lfloor m/2 \rfloor - s+1)k}$. Our primary goal is to maximise $|\mathcal{M}|$ given upper bounds on P_I, P_S, and the maximal size of a share. We conclude that we should choose $r \geq m/2$.

Theorem 6.5.1 *Let a collection of $l \times p_i$ q-ary matrices G_i, $i \in \mathcal{P}$, be a suitable set of matrices for Γ on $\mathcal{P}$ with set of possible secrets $GF(q)^k$. Let $p = \max_{i \in P} p_i$ and let r, s, and m be integers such that $0 < s \leq m - r$ and $r \geq m/2$. Then we can construct an USGA-scheme for Γ on $\mathcal{P}$ with*

- *q^{sr} messages,*
- *maximal share size pm q-ary symbols,*
- *$P_I = q^{-rk}$,*
- *$P_S = q^{(m-r-s+1)k}$, and*
- *message expansion $1 + k/s$.*

Suppose that the conditions of Theorem 6.5.1 hold and let $r - b = \lceil m/2 \rceil$. Then $0 < s \leq m - r \leq \lceil m/2 \rceil = r - b$. Hence,

$$\begin{aligned} &0 < (s+b) \leq m - (r-b), \\ &sr \leq sr + b(r-b-s) = (s+b)(r-b). \end{aligned}$$

From the first formula we infer that we are allowed to choose a new r and s by taking $r - b$ and $s + b$ respectively. We conclude from the second formula that if we decrease r with b and increase s with b then the number of messages increases (cf. (6.20)), P_I increases (cf. (6.21)), and P_S (cf. (6.22)), and the maximal share size remain the same. We recall that $P_S \geq P_I$. So if we are only interested in the *probability of deception* $P_D = \max\{P_I, P_S\}$ then we should choose $r = \lceil m/2 \rceil$.

Corollary 6.5.2 *Let a collection of $l \times p_i$ q-ary matrices G_i, $i \in \mathcal{P}$, be a suitable set of matrices for Γ on $\mathcal{P}$ with set of possible secrets $GF(q)^k$. Let $p = \max_{i \in \mathcal{P}} p_i$ and s and m such that $0 < s \leq \lfloor m/2 \rfloor$. Then we can construct an USGA-scheme for Γ on $\mathcal{P}$ with*

- *$q^{s\lceil m/2 \rceil}$ messages,*
- *maximal share size pm q-ary symbols,*
- *$P_S = P_D = q^{-(\lfloor m/2 \rfloor - s + 1)k}$ and $P_I = q^{-\lceil m/2 \rceil k}$.*

Let a collection of $l \times p_i$ q-ary matrices G_i, $i \in \mathcal{P}$, be a suitable set of matrices for Γ on $\mathcal{P}$ with set of possible secrets $GF(q)^k$. Let us construct USGA-schemes by means of Corollary 6.5.2 for which the probability of deception P_D is upper bounded by q^{-dk}, where $d > 0$ is a designed security parameter, and the maximal share size is upper bounded by pN for some integer $N \geq d$. Hence, m and s need to be chosen such that $\lfloor m/2 \rfloor - s + 1 \geq d$ and $m \leq N$ (notice that the maximal share size does not depend on s). We like the number of messages to be as large as possible. Therefore we choose $s = \lfloor m/2 \rfloor - d + 1$ as large as possible. Then the message size is $(\lfloor m/2 \rfloor - d + 1)\lceil m/2 \rceil \log_2 q$ binary bits and the maximal share size is $pm \log_2 q$

binary bits. Therefore we choose $m = N$, which maximizes the message size ($N \geq d$). Thus, for N approaching infinity we obtain

$$\frac{\text{message size}}{(\text{maximal share size})^2} \approx \frac{1}{4p^2 \log_2 q}, \tag{6.23}$$

which only depends on parameters concerning the design of the suitable set of matrices. It is not possible, when using MRD codes, to get an exponential dependence between the number of message and key bits, which is known from constructions for single authentication [66].

Let a collection of $l \times p_i$ q-ary matrices G_i, $i \in \mathcal{P}$, be a suitable set of matrices for Γ on $\mathcal{P}$ with set of possible secrets $GF(q)^k$. Let us consider the concatenation of this set with itself, that is we consider the set of matrices

$$\bar{G}_i = \begin{pmatrix} G_i^1 & 0 \\ 0 & G_i^1 \\ G_i^2 & 0 \\ 0 & G_i^2 \end{pmatrix}, \ i \in \mathcal{P}.$$

The reader can check [V1] and [V2] to conclude that the set of matrices $\bar{G}_i$, $i \in \mathcal{P}$, is suitable for Γ on $\mathcal{P}$ with set of possible secrets $GF(q)^{2k}$. For this new set p is twice as big. From (6.23) we infer that it is unwise to consider such concatenations. We should try to find small sized matrices defining a suitable set for Γ.

We finish this section and chapter by giving an example of a construction of a threshold authentication scheme.

Example 6.5.3 Let $\mathcal{P} = \{1, \ldots, n\}$. A (t, n)-threshold scheme is a secret sharing scheme for the access structure $\Gamma = \{X \subseteq P : |X| \geq t\}$. In Example 1.2.6 we have presented a scheme for Γ with set of possible secrets $GF(q)$, where q is a prime power at least $n + 1$. The construction is linear and can be translated in terms of a suitable set of matrices G_i, by defining

$$G_i = (x_i^{t-1}, \ldots, x_i^2, x_i, 1)^T$$

for n distinct non zero elements $x_i \in GF(q)$. Notice that $p = 1$.

To construct a (t, n)-threshold authentication scheme we apply Corollary 6.5.2. Let $m = 2r$ and s be positive integers. Now let

$$\mathcal{M} = \{(I_r|R)^T : R \in \mathcal{R}_{s,r,r}\},$$

where $\mathcal{R}_{s,r,r}$ is the set of MRD codes defined by (6.19). This gives us a linear (t, n)-threshold authentication scheme with a key and share size of $2r$ q-ary symbols and with $|\mathcal{M}| = q^{sr}$, $P_I = q^{-r}$, and $P_S = q^{-(r-s+1)}$.

In Table 6.1 we give the parameters of various constructions made over $GF(8)$. We have listed for various values of r and s, the key size (which

r	s	key size	$\log_2 \lvert\mathcal{M}\rvert$	P_I	P_S	τ
4	1	24	12	2^{-12}	2^{-12}	48
4	2	24	24	2^{-12}	2^{-9}	
4	3	24	36	2^{-12}	2^{-6}	
8	1	48	24	2^{-24}	2^{-24}	
8	2	48	48	2^{-24}	2^{-21}	
8	3	48	72	2^{-24}	2^{-18}	
8	4	48	96	2^{-24}	2^{-15}	
8	5	48	120	2^{-24}	2^{-12}	19.2
16	13	96	624	2^{-48}	2^{-12}	14.77
32	29	192	2784	2^{-96}	2^{-12}	13.24
64	61	384	11712	2^{-192}	2^{-12}	12.59
128	125	768	48000	2^{-384}	2^{-12}	12.29

Table 6.1: Performance of (t, n)-threshold schemes

equals each share size), the size of the message ($= \log_2 |\mathcal{M}|$), parameters P_I and P_S, and in the last column τ the square of the key size divided by the message size. All sizes are measured in binary bits. Notice that τ tends to $4 \log_2 q = 12$ if r tends to infinity and $r - s$ remains constant, see (6.23).

From (6.23) we infer that we like to have a linear (t, n)-threshold scheme with as set of possible secrets $GF(q)$ where q should be as small as possible. Therefore we mention for the sake of completeness the lower bounds $q \geq t + 1$ and $q \geq n - t + 2$ if $0 < t < n$ [13]. If these lower bounds are not satisfied then there does not exist a linear (t, n)-threshold scheme.

Part II

Secret Key Generation

Chapter 7

Unconditionally Secure Secret Key Generation

The second part of this thesis addresses the problem how two persons can generate a secret key while having at their disposal a noisy communication channel eavesdropped by an adversary. We will explain how to generate a secret key in an unconditionally secure way. That is the security of the key does not rely on the amount of computing time and resources that are available when attempting to obtain information about the secret key by unauthorized means. We consider and discuss the *broadcast channel with confidential messages* (BCC) in Section 7.1. In Section 7.2 we extend this model by allowing public discussion.

7.1 The BCC without Public Discussion

The situation we consider is the BCC introduced by Csiszár and Körner [36]. This model generalizes earlier models by Wyner [100] and Körner and Marton [69]. It involves three participants: two legitimate users Alice (X) and Bob (Y), and an enemy cryptanalyst Eve (Z). Alice can communicate to Bob by using a discrete memoryless channel (DMC). It also produces side information to the enemy cryptanalyst Eve. We denote this channel by $X\to(Y,Z)$. It is depicted in Figure 7.1. Channel $X\to(Y,Z)$ and the channels $X\to Y$ and $X\to Z$ from Alice to Bob and Alice to Eve, induced by it, see Table 7.1, are discrete and memoryless. The random variables X, Y, and Z are assumed to take values in the finite sets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$.

Alice and Bob want to generate a secret key in such a way that the information that Eve can obtain about it is minimal. In order to generate such a secret key, Alice and Bob first agree upon a specific block code with encoding rule $\mathcal{E}$ and decoding rule $\mathcal{D}$ that they will use. It is assumed that Eve has complete knowledge of the situation. She knows the strategy (including the encoding and decoding algorithms $\mathcal{E}$ and $\mathcal{D}$) used by Alice and Bob, and

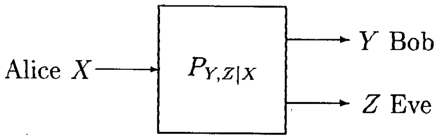


Figure 7.1: The broadcast channel with confidential messages

Channel	Transition Probabilities
$X \rightarrow (Y,Z)$	$P_{Y,Z\|X}(y,z\|x)$
$X \rightarrow Y$	$P_{Y\|X}(y,x) = \sum_{z \in \mathcal{Z}} P_{Y,Z\|X}(y,z\|x)$
$X \rightarrow Z$	$P_{Z\|X}(z,x) = \sum_{y \in \mathcal{Y}} P_{Y,Z\|X}(y,z\|x)$

Table 7.1: Transition probabilities

she knows the transition probabilities $P_{Y,Z|X}$ of $X \rightarrow (Y,Z)$. Alice and Bob are completely aware of the situation as well. In particular, they know that an enemy (Eve) receives information. During secret key generation, no feedback is allowed from Bob to Alice.

In order to generate a shared secret key, Alice encodes k source symbols S^k into X^n, which is the input to the discrete memoryless channel (DMC) $X \rightarrow (Y,Z)$. Bob produces an estimate $\hat{S}^k$ based on Y^n, the output of the channel from Alice to Bob. The *block error probability* is defined as

$$P_B = P(\hat{S}^k \neq S^k).$$

The coding situation can be characterized by a pair (R, Δ), where R is the *rate* at which information is sent by Alice to Bob, i.e.

$$R = H(\hat{S}^k)/n,$$

and where Δ is the enemy's per bit *equivocation* about this information, i.e.

$$\Delta = H(\hat{S}^k|Z^n)/H(\hat{S}^k).$$

The enemy's per bit equivocation Δ is the *fraction* of the total information that Alice seeks to transmit to Bob which remains secret for Eve.

Of course, Alice and Bob want P_B to be small, while keeping R and Δ as large as possible. The rate-equivocation pair (r, δ), $r \geq 0, \delta \geq 0$, is said to be *achievable* if, for all $\varepsilon > 0$, there exists an encoder-decoder pair $(\mathcal{E}, \mathcal{D})$ such that Alice and Bob can use this pair to generate a secret key at rate

$$R \geq r - \varepsilon$$

while

$$\Delta \geq \delta - \varepsilon$$

and

$$P_B \leq \varepsilon.$$

The *capacity region* is the set of all achievable rate-equivocation pairs. The *secrecy capacity* C_s is the supremum of all information rates at which Alice and Bob can generate a key that remains essentially entirely secret for Eve, i.e., it equals the supremum of information rates r such that $(r, 1)$ is achievable. The secrecy capacity of a BCC $X \rightarrow (Y, Z)$ can be viewed as a function of the transition probabilities $P_{Y,Z|X}$ defining channel $X \rightarrow (Y, Z)$. Therefore, we prefer to write $C_s(P_{Y,Z|X})$ instead of C_s.

We started the definition of capacity region by noting that Alice and Bob want P_B to be small, while keeping R and Δ as large as possible. A natural question arises. Note that the rate $R = H(\hat{S}^k)/n$ and equivocation $\Delta = H(\hat{S}^k|Z^n)/H(\hat{S}^k)$ are defined by using $\hat{S}^k$, Bob's estimate of the source bits encoded and transmitted by Alice. Also note that Bob's estimate $\hat{S}^k$ is equal to S^k with high probability since P_B is small. So, the information contained in $\hat{S}^k$ is approximately the information contained in S^k. This should imply that R and Δ can also be defined as $H(S^k)/n$ and $H(S^k|Z^n)/H(S^k)$ respectively. Is this true? Yes, the following simple lemma can be applied to show that if $P_B \approx 0$ then $H(S^k) \approx H(\hat{S}^k)$ and $H(S^k|Z^n) \approx H(\hat{S}^k|Z^n)$. Hence, the capacity region stays the same when using the alternative definitions of R and Δ.

Lemma 7.1.1 *Let $A, \hat{A}$, and B be random variables such that $P(A \neq \hat{A}) \leq \varepsilon \leq 1/2$. Let $\mathcal{A}$ be the range of random variables A and $\hat{A}$. Then*

$$|H(A|B) - H(\hat{A}|B)| \leq 2h(\varepsilon) + 2\varepsilon \log |\mathcal{A}|$$

where h denotes the binary entropy function

$$h(x) = -x \log x - (1-x)\log(1-x), \quad \textit{for } 0 \leq x \leq 1.$$

Proof: We notice that $H(A|B) + H(\hat{A}|AB) = H(A\hat{A}|B) = H(\hat{A}|B) + H(A|\hat{A}B)$, and hence $|H(A|B) - H(\hat{A}|B)| = |H(A|\hat{A}B) - H(\hat{A}|AB)| \leq H(A|\hat{A}B) + H(\hat{A}|AB) \leq H(A|\hat{A}) + H(\hat{A}|A)$. Define random variable U to be equal to 1 if $A \neq \hat{A}$ and equal to 0 if $A = \hat{A}$. Then

$$\begin{aligned}
&H(A|\hat{A}) \leq H(AU|\hat{A}) \leq H(U) + H(A|U\hat{A}),\\
&H(A|U\hat{A}) = P_U(0)H(A|\hat{A}, U=0) + P_U(1)H(A|\hat{A}, U=1),\\
&P_U(1) = P(A \neq \hat{A}) \leq \varepsilon,\\
&H(U) = h(P_U(1)) \leq h(\varepsilon),\\
&H(A|\hat{A}, U=0) = 0, \quad \text{and}\\
&H(A|\hat{A}, U=1) \leq \log |\mathcal{A}|.
\end{aligned}$$

Hence, $H(A|\hat{A}) \leq h(\varepsilon) + \varepsilon \log|\mathcal{A}|$. By interchanging the role of A and $\hat{A}$ in the previous arguments we obtain $H(\hat{A}|A) \leq h(\varepsilon) + \varepsilon \log|\mathcal{A}|$, and the lemma follows. Notice that this proof is similar to the proof of Fano's inequality.

□

Csiszár and Körner [36] characterized the capacity region in terms of information theoretical expressions. In particular, they proved that the secrecy capacity equals $I(V;Y) - I(V;Z)$ maximized over all possible probability distributions $P_{V,X}$ where V is a random variable with range $\mathcal{V}$, finitely bounded by $|\mathcal{V}| \leq |\mathcal{X}| + 1$. Notice that $P_{V,X} = P_V P_{X|V}$ where P_V defines random variable P_V and $P_{X|V}$ defines the transition probabilities of a channel $V \rightarrow X$. Thus,

$$C_s(P_{Y,Z|X}) = \max_{V, V \longrightarrow X} [I(V;Y) - I(V;Z)].$$

Clearly, the bounds

$$C(P_{Y|X}) - C(P_{Z|X}) \leq C_s(P_{Y,Z|X}) \leq C(P_{Y|X})$$

hold where $C(P_{Y|X})$ and $C(P_{Z|X})$ denote the channel capacities of channels $X \rightarrow Y$ and $X \rightarrow Z$, respectively.

It costs quite some computing time to determine whether a tuple (r, δ) is achievable or not using Csiszár's and Körner's characterization. For example to find out whether $(r, 1)$ is achievable we need to find out whether $r \leq C_s(P_{Y,Z|X})$, hence $I(V;Y) - I(V;Z)$ needs to be computed for all possible probability distributions $P_{V,X}$ with $|\mathcal{V}| \leq |\mathcal{X}| + 1$. In Chapter 8 we describe a special class of BCC's with easier to compute characterizations for the capacity region and secrecy capacity. The result presented in Chapter 8 generalizes the results of Leung [74] where the situation of the *wire-tap channel* introduced by Wyner [100] is discussed. In Wyner's model X, Y, and Z form a Markov chain $X \rightarrow Y \rightarrow Z$. Wyner proved that $C_s(P_{Y,Z|X})$ equals $I(X;Y|Z)$ maximized over all probability distributions P_X;

$$C_s(P_{Y,Z|X}) = \max_{P_X} I(X;Y|Z), \quad \text{for } P_{Y,Z|X} = P_{Y|X} P_{Z|Y}. \tag{7.1}$$

For the sake of completeness we mention that Massey [79] gave a simplified treatment of Wyner's wire-tap channel. It is advised to read Massey's paper before starting to study Csiszár's and Körner's characterizations of the BCC. Piret [91] showed that for Wyner's wire-tap channel $C_s(P_{Y,Z|X})$ can be achieved by using binary linear codes in the case where $X \rightarrow Y$ and $Y \rightarrow Z$ are binary symmetric channels.

In the model of the BCC the ranges of random variables X, Y, and Z are finite and channel $X \rightarrow (Y, Z)$ is discrete and memoryless. We can consider more general models by relaxing these conditions. For example Leung and Hellman [75] discuss the more realistic situation in which X, Y, and Z form a continuous Markov chain $X \rightarrow Y \rightarrow Z$ where $X \rightarrow Y$ and $Y \rightarrow Z$ are additive white Gaussian noise (AWGN) channels, and input $X = (X_1, \ldots, X_l) \in I\!R^l$ is power limited, that is for some fixed power P

$$\frac{1}{l} \sum_{1 \le i \le l} E(X_i) \le P$$

where $E(X_i)$ is the expected (average) value taken by X_i. This model is called the *AWGN wire-tap channel.* They showed that the secrecy capacity equals the difference between the capacities of $X \rightarrow Y$ and $X \rightarrow Z$, that is

$$C_s(P_{Y,Z|X}) = C(P_{Y|X}) - C(P_{Z|X}).$$

Yamamoto [102] extended the AWGN wire-tap channel by considering two wire-tappers (two enemies Eve).

Another interesting generalization is the following. In the BCC we assume that channel $X \rightarrow Z$ is memoryless and that its characteristics are known to Alice and Bob. Suppose that $X \rightarrow Z$ has memory in the sense that its characteristics varies according to a pre-specified strategy implemented by Eve and known to Alice and Bob. In other words, based on received messages over channel $X \rightarrow Z$ Eve eavesdrops in an active way by changing the characteristics of channel $X \rightarrow Z$ to optimize her situation. Of course, Eve has her restrictions, she can not arbitrarily vary the characteristics of channel $X \rightarrow Z$. For example, let $X \rightarrow (Y, Z)$ be such that $X \rightarrow Y$ is noiseless with an n-dimensional binary input and output alphabet $\mathcal{X} = \mathcal{Y} = GF(2)^n$, and such that $X \rightarrow Z$ is a channel outputting a selection of m bits Shannon information about X. The selection of these m bits is based on the memory of channel $X \rightarrow Z$ and is programmed by Eve. Wire-tap channel II introduced by Ozarow and Wyner [89] is an example of this situation. A different way of describing the situation is the following. The original BCC is described by channel $X \rightarrow (Y, Z)$ with transition probabilities $P_{Y,Z|X} = P_{Y|X} P_{Z|X,Y}$ where $P_{Y|X}$ defines a channel $X \rightarrow Y$ and $P_{Z|X,Y}$ defines a channel $(X, Y) \rightarrow Z$. Hence, we can equivalently use channels $X \rightarrow Y$ and $(X, Y) \rightarrow Z$ to describe the original BCC. In the new situation $(X, Y) \rightarrow Z$ varies according to Eve's strategy. So, the new situation can be described by a channel $X \rightarrow Y$ and a collection of *eavesdropping* channels $(X, Y) \rightarrow Z$ from which Eve selects (depending on her knowledge at that moment in time) the one optimizing her situation. This resembles the situation of the original BCC in which Alice and Bob only know the characteristics of $X \rightarrow Y$ and a collection of possible characteristics of eavesdropping channels $(X, Y) \rightarrow Z$ out of which they need to take into account the channel optimizing Eve's situation (which depends on the moment in time). We will continue this type of discussions in Section 7.3 where we generalize the BCC by allowing tampering by Eve.

We have not yet discussed the following very important generalization of the BCC. We can generalize the BCC by allowing public communication by Alice and Bob. We introduce this concept by analyzing the following situation of Korzhik [71]. Suppose Alice and Bob communicate over a wire with the property that no enemy can come near to the wire. In other words they secured the area around the wire. For example, no enemy can come within a radius of 1 meter distance to the wire. This means that there can be an enemy who planted a device just outside the 1 meter area to receive all electro-magnetic radiation. Hence, if Alice transmits a signal to Bob over this wire then the enemy obtains information about this signal from his device. This describes a BCC $X \rightarrow (Y, Z)$ where $X \rightarrow Y$ represents the wire and $X \rightarrow Z$ represents the channel from Alice to the electro-magnetic detector of the enemy Eve. In this situation communication over the BCC by Alice and Bob is expensive since they need to secure the area within a radius of 1 meter from the wire. Public communication is much cheaper. So, to generate a secret key in a cheaper way Alice and Bob should use their BCC in combination with public communication. This leads to the concept of the *BCC with public discussion.* It was introduced by Kahn and Hellman in [67], by Maurer in [82], and by Ahlswede and Csiszár in [1]. In the next section we describe and consider the BCC with public discussion.

Suppose Alice and Bob want to generate a secret key at a certain information rate R in Korzhik's situation. The more area they secure the more expensive communication over $X \rightarrow Y$ becomes. Hence, Alice and Bob want to find the cheapest BCC with which they can achieve a certain secrecy capacity, that is they are interested in the minimal amount of area around the wire they need to secure. This is the type of question Korzhik considered in [71].

Yamamoto discussed in [101] the following variation on the BCC model. Suppose there is an information service generating source symbols represented by a random variable S with the property that S consists of two correlated parts A and B. Thus $S = (A, B)$ and $P_S = P_{A,B}$. The information service encodes $S^k = (A^k, B^k)$ into X^n, which is the input to a DMC $X \rightarrow Y$ from the information service to Bob, a client. Suppose that Bob paid the information service to receive the information contained in B^k within a certain prescribed distortion tolerance, but who did not pay the information service to obtain information contained in A^k. Then the encoding must be done in such a way that Bob can produce an estimate $\hat{B}^k$ based on Y^n within the prescribed distortion tolerance, and such that the equivocation $H(A^k|Y^n)/H(A^k)$ about A^k is as large as possible. Yamamoto studied this situation, he investigated the maximal achievable equivocation and minimal rate necessary to attain the prescribed distortion and equivocation tolerances.

We end this section by reconsidering the security measures introduced in this section. Alice and Bob want to generate a secret key at maximal information rate, that is they want to achieve $(C_s(P_{Y,Z|X}), 1)$. By the definition of achievable rate-equivocation pairs we have that for all $\varepsilon > 0$ there exists an encoder-decoder pair $(\mathcal{E}, \mathcal{D})$ such that Alice and Bob can use this pair to generate a secret key at rate $C_s(P_{Y,Z|X}) \geq R \geq C_s(P_{Y,Z|X}) - \varepsilon$ while $P_B \leq \varepsilon$, and $\Delta \geq 1 - \varepsilon$, i.e. $H(S^k|Z^n) \geq (1-\varepsilon)H(S^k)$. By choosing ε arbitrarily close to 0 Alice and Bob can generate a secret key about which Eve has only an arbitrarily small fraction ε of the total amount of information. In the definition of achievable rate-equivocation pairs it is possible that this fraction $\epsilon = 1/\sqrt{H(S^k)}$ since $1/\sqrt{H(S^k)}$ goes to 0 as n goes to infinity $(1/\sqrt{H(S^k)} = 1/\sqrt{nR})$. Hence, it is possible that Eve's total amount of information about the secret key grows with $\varepsilon H(S^k) = \sqrt{H(S^k)}$, which is unbounded as n grows to infinity. This was noted by Maurer [83] and he introduced the notion of *strong secrecy capacity.* He defined the enemy's total amount of information about the secret key by

$$\bar{\Delta} = H(S^k) - H(S^k|Z^n) = I(S^k; Z^n).$$

The strong secrecy capacity is the supremum of all information rates r for which for all $\varepsilon > 0$ there exists an encoder-decoder pair $(\mathcal{E}, \mathcal{D})$ such that Alice and Bob can use this pair to generate a secret key at rate $R \geq r - \varepsilon$ while $\bar{\Delta} \leq \varepsilon$, and $P_B \leq \varepsilon$. It is strongly believed that the strong secrecy capacity equals the secrecy capacity.

7.2 The BCC with Public Discussion

In the BCC with public discussion Alice and Bob generate a secret key as follows. They first agree upon a specific protocol $\mathcal{P}$ that they will use. It is assumed that Eve has complete knowledge of the situation. She knows the protocol $\mathcal{P}$ used by Alice and Bob, and she knows the transition probabilities $P_{Y,Z|X}$ of the DMC $X \rightarrow (Y, Z)$. Alice and Bob are completely aware of the situation as well. In particular, they know that an enemy (Eve) receives information. Protocol $\mathcal{P}$ makes use of a public channel. As explained in the previous section we assume that public communication is very cheap, therefore a highly redundant error-correcting code with large minimal distance can be used during the communication over this public channel. So, we assume that Alice and Bob can communicate over a noiseless public channel, and, hence, Eve receives full knowledge about this communication.

In order to generate a shared secret key, Alice transmits n source symbols X^n over the DMC $X \rightarrow (Y, Z)$. Bob receives Y^n and Eve receives Z^n. Alice and Bob will use a protocol $\mathcal{P}$ to extract a common secret key as follows. Based on Y^n Bob computes a public message P_1 according to protocol $\mathcal{P}$, which he transmits over the public channel to Alice. Based on X^n and P_1 Alice computes a public message P_2 according to $\mathcal{P}$, which she transmits over the public channel to Bob. Based on X^n, P_1, and P_2 Bob computes a public message P_3 etc. Before computing a public message Alice and Bob decide, based on their received information during the protocol, whether to stop transmitting public messages or not. If they decide to stop, say after

t transmissions, then Alice extracts a secret key S^k from X^n, $P_1, \ldots, P_t$ according to a decoding rule $\mathcal{D}_A$, and Bob extracts a secret key $\hat{S}^k$ from Y^n, $P_1, \ldots, P_t$ according to a decoding rule $\mathcal{D}_B$ (decoding rules $\mathcal{D}_A$ and $\mathcal{D}_B$ are part of protocol $\mathcal{P}$). By P we denote the collection of all public messages, P_1, $\ldots, P_t$, together with the fact that based on $X^n, P_1, \ldots, P_t$ and $Y^n, P_1, \ldots, P_t$, respectively, Alice and Bob decided to stop their public communication.

As for the BCC without public discussion The *block error probability* is defined as $P_B = P(S^k \neq \hat{S}^k)$. The coding situation can be characterized by a pair (R, Δ), where R is the *rate* at which information is sent by Alice to Bob over the (expensive) BCC $X \rightarrow (Y, Z)$, i.e.

$$R = H(S^k)/n,$$

and where Δ is the enemy's per bit *equivocation* about this information, i.e.

$$\Delta = H(S^k | Z^n P)/H(S^k).$$

The enemy's per bit equivocation Δ is the fraction of the total information that Alice seeks to transmit to Bob which remains secret for Eve. We notice that in the definition of the information rate public communication plays no role. This is because public transmissions are assumed to be very cheap compared to transmissions over the channel $X \rightarrow (Y, Z)$. Like the BCC we can define achievable rate-equivocation pairs and a capacity region. The secrecy capacity with public discussion $\bar{C}_s(P_{Y,Z|X})$ is the supremum of information rates r such that $(r, 1)$ is achievable. Clearly,

$$C_s(P_{Y,Z|X}) \leq \bar{C}_s(P_{Y,Z|X}) \leq C(P_{Y|X}).$$

The reader is encouraged to study [82, 1, 28] for well written deep discussions on the BCC with public discussion. Here we only summarize the main results and idea's.

Ahlswede and Csiszár found characterizations of the secrecy capacity in the restricted situation where only one public message is allowed to contain data. In the case where this public message is sent from Alice to Bob the secrecy capacity is called the *forward key-capacity* and it appears to be equal to $C_s(P_{Y,Z|X})$. Intuitively, this is clear since Alice can not use any information sent by Bob in order to construct her public message, simply because there are no messages sent by Bob to Alice. Hence, the public message $\mathcal{I}$ contains only information about the selection of the n source bits X^n. This information is transmitted to Bob and more important also to Eve. Hence, Alice and Bob are not allowed to use the part of information in X^n respectively Y^n which is dependent on $\mathcal{I}$ to extract a secret key. If they break this rule the secret key will depend on $\mathcal{I}$, and Eve will obtain information about it. We conclude that the public message has only a negative effect on Alice's and Bob's situation. Not using a public message is better. This proves intuitively that the forward key capacity equals $C_s(P_{Y,Z|X})$. In the case where the non-empty public message is sent from Bob to Alice the secrecy capacity is called the *backward key-capacity*, and its characterization is unknown.

Both Maurer [82] (who was the first) and Ahlswede and Csiszár [1] found that $\bar{C}_s(P_{Y,Z|X})$ is upper bounded by $I(X;Y|Z)$ maximized over all possible probability distributions P_X. If X, Y, and Z form a Markov chain in some order then equality holds. Thus equality holds if $X \rightarrow Y \rightarrow Z$, i.e. $P_{Y,Z|X} = P_{Y|X}P_{Z|Y}$, or $Z \leftarrow X \rightarrow Y$, i.e. $P_{Y,Z|X} = P_{Y|X}P_{Z|X}$, or $X \rightarrow Z \rightarrow Y$, i.e. $P_{Y,Z|X} = P_{Y|Z}P_{Z|X}$ (in the last case $I(X;Y|Z) = 0$). In particular, see (7.1),

$$\begin{aligned} \bar{C}_s(P_{Y,Z|X}) = C_s(P_{Y,Z|X}) = \max_{P_X} I(X;Y|Z), \\ \text{for } P_{Y,Z|X} = P_{Y|X}P_{Z|Y}. \end{aligned} \tag{7.2}$$

Ahlswede and Csiszár noted that $\bar{C}_s(P_{Y,Z|X})$ is more generally upper bounded by $I(X;Y|U)$ maximized over all possible probability distributions P_X and $P_{U|Z}$ where U is some random variable;

$$\bar{C}_s(P_{Y,Z|X}) \leq \max_{X,Z \rightarrow U} I(X;Y|U)$$

(this result was independently noted in [42] as well).

Example 7.2.1 Let X be a binary random variable and let $X \rightarrow (Y,Z)$ be defined by

$$Y = (B, BD + (1+B)X)$$

and

$$Z = (B, BD + X)$$

where B and D are uniformly distributed binary random variables and $+$ is the addition modulo 2. Define $Z = (Z_0, Z_1) \rightarrow U$ by

$$U = (Z_0, Z_0(E + Z_1) + Z_1)$$

where E is a uniformly distributed binary random variable. We will show that $I(X;Y) = I(X;Y|Z) = H(X)/2$ and $I(X;Y|U) = 0$. Hence, the more general upper bound gives $\bar{C}_s(P_{Y,Z|X}) = 0$, the less general upper bound gives $\bar{C}_s(P_{Y,Z|X}) \leq 1/2$, and the other known upper bound, $\bar{C}_s(P_{Y,Z|X}) \leq C(P_{Y|X})$, gives $\bar{C}_s(P_{Y,Z|X}) \leq 1/2$ as well.

Equality $I(X;Y) = H(X)/2$ is derived by

$$\begin{aligned} I(X;Y) &= I(X;B, BD + (1+B)X) \\ &= I(X;B) + I(X;BD + (1+B)X|B) \\ &= 0 + I(X;BD + (1+B)X|B) \\ &= P_B(0)I(X;BD + (1+B)X|B=0) + \\ &\quad\; P_B(1)I(X;BD + (1+B)X|B=1) \\ &= I(X;X)/2 + I(X;D)/2 \\ &= H(X)/2 + 0. \end{aligned}$$

We obtain $I(X;Y|Z) = H(X)/2$ from

$$\begin{aligned} I(X;Y|Z) &= I(X;B,BD+(1+B)X|B,BD+X) \\ &= I(X;B|B,BD+X)+ \\ &\quad I(X;BD+(1+B)X|B,BD+X) \\ &= 0+I(X;BD+(1+B)X|B,BD+X) \\ &= P_B(0)I(X;BD+(1+B)X|BD+X,B=0)+ \\ &\quad P_B(1)I(X;BD+(1+B)X|BD+X,B=1) \\ &= I(X;X|X)/2+I(X;D|D+X)/2 \\ &= 0+H(X)/2. \end{aligned}$$

Finally, we prove $I(X;Y|U) = 0$. We notice that if $B = 0$ then $U = (0, X)$ and if $B = 1$ then $U = (1, E)$. Hence,

$$U = (B, BE + (1 + B)X),$$

with which we derive

$$\begin{aligned} I(X;Y|U) &= I(X;B,BD+(1+B)X|B,BE+(1+B)X) \\ &= I(X;B|B,BE+(1+B)X)+ \\ &\quad I(X;BD+(1+B)X|B,BE+(1+B)X) \\ &= 0+I(X;BD+(1+B)X|B,BE+(1+B)X) \\ &= P_B(0)I(X;BD+(1+B)X|BE+(1+B)X,B=0)+ \\ &\quad P_B(1)I(X;BD+(1+B)X|BE+(1+B)X,B=1) \\ &= I(X;X|X)/2+I(X;D|E)/2 \\ &= 0+0. \end{aligned}$$

In the situation of the BCC with public discussion only upper bounds on $\bar{C}_s(P_{Y,Z|X})$ and no precise characterizations of $\bar{C}_s(P_{Y,Z|X})$ are known. Orlitsky and Widgerson [88] discussed under which circumstances the secrecy capacity with public discussion is positive. Kahn and Hellman in [67] where the first to discuss methods to achieve rate-equivocation pairs beyond the capacity region of the BCC without public discussion. In present literature, see especially Cachin's and Maurer's paper[28], the generation of a secret key is split into three phases:

- advantage distillation,
- information reconciliation, and
- privacy amplification.

These phases are described in the coming subsections.

By considering the enemy's total information about the secret key Maurer [83] defined the strong secrecy capacity with public discussion in a similar way as he defined the strong secrecy capacity, see the previous section. He proved that all bounds on the secrecy capacity with public discussion also hold for the strong secrecy capacity with public discussion. It is believed that both capacities are equal to oneanother.

7.2.1 Advantage Distillation

In this phase Alice and Bob create a random variable W about which either Alice has full knowledge and Bob has more information than Eve or Bob has full knowledge and Alice has more information than Eve. The reason to create such a W is that Alice and Bob need an advantage over Eve in order to generate a secret key. Hence, advantage distillation is only needed when such a W is not available from the moment Alice and Bob start their public communication. Alice and Bob create W by exchanging messages, jointly denoted by random variable C, over the public channel. By creating W Alice and Bob distill an advantage over Eve;

$$H(W|XC) = 0, \ H(W|YC) < H(W|ZC)$$

or

$$H(W|YC) = 0, \ H(W|XC) < H(W|ZC).$$

The following example from [81] illustrates a technique to achieve this goal.

Example 7.2.2 Let us consider the situation in which $X \rightarrow (Y, Z)$ is such that both $X \rightarrow Y$ and $X \rightarrow Z$ are AWGN channels. Let $X \rightarrow Z$ be superior to channel $X \rightarrow Y$. Hence, a random variable W about which both Alice and Bob have more information than Eve is not available. Suppose Alice uses binary antipodal signaling to transmit an uncoded sequence of independent random bits. Bob receives an analog signal s with mean $+1$ or -1 according to the bit sent by Alice. In order to convert the enemy's advantage into a disadvantage Bob picks only those bits out of the data stream that he receives very reliable. For example, he picks s iff $|s| \geq t$ where t is a predefined reliability threshold. He discards less reliable bits. By using the public channel he informs Alice about which bits he selected, and Alice will select the corresponding bits out of the data stream she transmitted to Bob. Of course Eve gets to know which bits Alice and Bob picked and, hence, Eve knows which bits were reliably transmitted to Bob. This is information about the additive white Gaussian noise caused by channel $X \rightarrow Y$. Since Eve received the signal transmitted by Alice over a (partially) different channel $X \rightarrow Z$, this information gives Bob more additional information about the signal transmitted by Alice than it gives Eve additional information about the signal transmitted by Alice. Hence, Bob can obtain an advantage over Eve. Since Eve's channel $X \rightarrow Z$ is superior to channel $X \rightarrow Y$ Bob's bit error probability is on the average worse than Eve's bit error probability, but it is better when averaged only over the selected bits. Let W be the random variable representing the selected bits of Alice. The random variable C representing the public communication between Alice and Bob is a list of indices of all the bits picked by Bob. Then $H(W|XC) = 0$ and $H(W|YC) < H(W|ZC)$.

The technique demonstrated in the previous example is called *reliability estimation* and was introduced by Maurer [82]. It can also be formulated in terms of error correcting codes. The trick is that Alice encodes k bits into a code word of n bits using a linear error correcting code. She transmits this codeword to Bob, who makes a public reliability decision based on the syndrome of his received word. In Chapter 10 we generalize Maurer's [82] reliability estimation technique and we generalize Gander's and Maurer's [55] improvement of Maurer's reliability estimation technique. The only other known technique [81, 82] is demonstrated in the next example and we call it *channel rotation.*

Example 7.2.3 Let us consider the situation in which $X \rightarrow (Y, Z)$ is such that Z, X, and Y form the Markov chain $Z \leftarrow X \rightarrow Y$, thus $P_{Y,Z|X} = P_{Y|X}P_{Z|X,Y} = P_{Y|X}P_{Z|X}$. Suppose that $X \rightarrow Y$ is a binary symmetric channel $BSC(p)$ with cross-over probability p, and suppose that $X \rightarrow Z$ is a $BSC(q)$ with $p > q$. Hence, channel $X \rightarrow Z$ is superior to channel $X \rightarrow Y$, and a random variable W about which both Alice and Bob have more information than Eve is not available. We will show that Alice and Bob can create a *rotated* BCC $Y' \rightarrow (X', Z')$ from Bob to Alice and Eve for which $P_{X',Z'|Y'} = P_{X'|Y'}P_{Z'|X'}$ with $P_{X'|Y'} = P_{Y|X}$ and $P_{Z'|X'} = P_{Z|X}$. Hence, $Y' \rightarrow X'$ is a $BSC(p)$ and $Y' \rightarrow Z'$ is $Y' \rightarrow X'$ cascaded with a $BSC(q)$. This means that the advantage of Eve is turned around because Alice's and Bob's rotated channel $Y' \rightarrow X'$ is superior to Eve's rotated channel $Y' \rightarrow Z'$. This implies that by taking $W = Y'$ Bob has full knowledge of W and Alice has more information about W than Eve, and we have reached the purpose of the advantage distillation phase.

Alice and Bob create the rotated BCC by using public communication. Alice creates a uniformly distributed binary random variable X which she sends over the BCC $X \rightarrow (Y, Z)$ to Bob. Bob receives $Y = X + A$, and Eve receives $Z = X + E$, where A is the noise bit generated in the $BSC(p)$ $X \rightarrow Y$ and E is the noise bit generated in the $BSC(q)$ $X \rightarrow Z$. Bob selects Y' the random variable he wants to transmit over the rotated BCC to Alice, and he adds Y to it. He obtains $C = Y + Y' = Y' + X + A$, which he transmits publicly to Alice. Alice adds X to C to obtain $X' = Y' + A$. Alice forgets X and C and Bob forgets Y and C, hence, their situation is as if Bob transmitted Y' and Alice received $X' = Y' + A$ over a $BSC(p)$ $Y' \rightarrow X'$ from Bob to Alice.

Eve knows $Z = X + E$ and $C = Y' + X + A$. Since $(Z, C) \rightarrow (Z + C, Z)$ is a bijective function we can describe Eve's knowledge completely by the random variables $Y' + A + E$ and $X + E$. Because X is uniformly distributed and independent of (Y', A, E) random variable $X + E$ is also uniformly distributed and independent of (Y', A, E). So, without losing knowledge Eve can disregard $X + E$. This means that the situation of Eve is as if Eve received $Z' = Y' + A + E$ over the rotated channel $Y' \rightarrow X' \rightarrow Z'$. This is how Alice and Bob creat a rotated BCC and how they reach the goal of the advantage distillation phase; $H(W|YC) = H(W|Y') = 0$ and $H(W|XC) \leq H(W|X') < H(W|Z') = H(W|ZC)$ where $W = Y'$ (the first inequality is actually an equality).

We conclude this subsection by noting that in current literature the advantage distillation phase is also called the coding gain phase since Alice and Bob achieve coding gain towards Eve.

7.2.2 Information Reconciliation

Suppose w.l.o.g. that during the advantage distillation phase Alice and Bob created a random variable W by publicly exchanging information C about which Alice has full knowledge, i.e. $H(W|XC) = 0$, and Bob has more information than Eve, i.e. $H(W|YC) < H(W|ZC)$, see Subsection 7.2.1. In the reconciliation phase Alice and Bob exchange publicly redundant error-correction information U (e.g. a sequence of parity checks) such that Bob can determine W with high probability and such that Eve has only partial knowledge about W. During this phase Alice and Bob reconcile the shared string W in such a way that

$$H(W|YCU) \approx 0$$

while Eve has a substantial amount of uncertainty about W, i.e.

$$H(W|ZCU) > 0.$$

Notice that $H(U) \geq H(U|YC) \approx H(U|YC) + H(W|YCU) = H(WU|YC) \geq H(W|YC)$, see [28].

Suppose that W is a uniformly distributed random variable representing a binary string $(w_1, \ldots, w_n) \in GF(2)^n$ about which Alice has full knowledge. Further suppose that Bob knows the random variable $\bar{W}$ representing a noisy version $(w_1 + e_1, \ldots, w_n + e_n)$ of W where $e_i \in GF(2)$ and $+$ is the binary addition (e.g. e_i are generated by a $BSC(p)$). Then $H(W|XC) = 0$ and $H(\bar{W}|YC) = 0$. Let us assume that Bob uses $\bar{W}$ in the reconciliation phase and that he discards Y and C. Of course Alice and Bob can only agree on a secret key if Bob does not lose his advantage over Eve by discarding Y and C. So, we assume that $\bar{W}$ is such that

$$H(W|YC) \leq H(W|\bar{W}) < H(W|ZC). \tag{7.3}$$

Let us analyse $H(W|\bar{W})$. Let E be the random variable representing the noise bits $(e_1, \ldots, e_n)$. Then $\bar{W} = W + E$. Thus

$$H(W|\bar{W}) \quad = \quad H(W + \bar{W}|\bar{W}) = H(E|W + E).$$

Since W is uniformly distributed and independent of E random variable $W + E$ is also uniformly distributed and independent of E. Hence, $H(E|W+E) = H(E)$, and we obtain

$$H(W|\bar{W}) = H(E).$$

The interpretation of this formula is that Bob needs to know the noise E besides $\bar{W}$ in order to obtain full knowledge about W.

All known reconciliation procedures [5, 24] are based on the public exchange of parity checks by Alice and Bob. The idea is the following. Alice and Bob publicly select a set of indices $I_1 \subseteq \{1, \ldots, n\}$ based on their knowledge of probability distribution P_E. Then Alice computes $\sum_{i \in I_1} w_i$ the parity of the bits $\{w_i\}_{i \in I_1}$ and Bob computes $\sum_{i \in I_1}(w_i + e_i)$ the parity of the bits $\{w_i + e_i\}_{i \in I_1}$. They transmit these parities to oneanother and they compare both parities by computing

$$p_1 = \sum_{i \in I_1} w_i + \sum_{i \in I_1}(w_i + e_i) = \sum_{i \in I_1} e_i.$$

Based on P_E and p_1 Alice and Bob publicly select a second set of indices $I_2 \subseteq \{1, \ldots, n\}$. Alice and Bob compute the parity of the bits $\{w_i\}_{i \in I_2}$ and $\{w_i + e_i\}_{i \in I_2}$. They publicly transmit those parities to oneanother and both Alice and Bob compute $p_2 = \sum_{i \in I_2} e_i$. Based on P_E, p_1, and p_2 Alice and Bob publicly select a third set of indices. They compute the corresponding parities which they transmit to one another and compare by calculating p_3. Alice and Bob iterate this procedure, say m times, until Bob has almost no uncertainty about random variable E, and hence W.

Let us describe the public communication by means of random variables. During the reconciliation phase Alice and Bob publicly transmitted parities. Actually, they constructed a binary parity check matrix D defined by

$$D_{i,j} = \begin{cases} 1 & \text{if } j \in I_i, \\ 0 & \text{if } j \notin I_i, \end{cases}$$

for $1 \leq j \leq n$ and $1 \leq i \leq m$. Alice transmitted $D(w_1, \ldots, w_n)^T$ to Bob and Bob transmitted $D(w_1 + e_1, \ldots, w_n + e_n)^T$ to Alice. Let $\mathcal{D}(\mathbf{x})$ be the function representing the binary multiplication of matrix H with the binary vector $\mathbf{x}^T$, and let $l(\mathcal{D})$ be the rank of matrix H. The construction of $\mathcal{D}$ depends on Alice's and Bob's knowledge of P_E and the values $p_i = \sum_{j \in I_i} e_j$. Hence, the construction of $\mathcal{D}$ can be seen as a random process which depends only on random variable E. Let random variable P correspond to parity check function $\mathcal{D}$ and let $\mathcal{P} = \{\mathcal{D} : P_P(\mathcal{D}) \neq 0\}$ be the range of random variable P.

We notice that P only depends on E and that W is independent of E and therefore independent of P. Thus, P is independent of W and independent of $\bar{\mathcal{D}}(W)$ for $\bar{\mathcal{D}} \in \mathcal{P}$. Since W is uniformly distributed $\bar{\mathcal{D}}(W)$, $\bar{\mathcal{D}} \in \mathcal{P}$, is uniformly distributed. We obtain for $\bar{\mathcal{D}} \in \mathcal{P}$

$$l(\bar{\mathcal{D}}) = H(\bar{\mathcal{D}}(W)) = H(\bar{\mathcal{D}}(W)|P = \bar{\mathcal{D}}) = H(P(W)|P = \bar{\mathcal{D}}),$$

and

$$H(P(W)|P) = \sum_{\mathcal{D} \in \mathcal{P}} P_P(\mathcal{D}) H(P(W)|P = \mathcal{D}) = \sum_{\mathcal{D} \in \mathcal{P}} P_P(\mathcal{D}) l(\mathcal{D}),$$

which represents the average number of independent parity checks Alice and Bob use in the reconciliation phase. Alice and Bob publicly select the sets of indices I_i leading to a parity check function $\mathcal{D}$ represented by random variable P. Furthermore, Alice and Bob exchange publicly parity check values $\mathcal{D}(W)$ and $\mathcal{D}(\bar{W})$. Thus, the public communication is described by random variable

$$U = (P(W), P(\bar{W}), P),$$

where P represents which parity checks Alice and Bob communicated to oneanother and where $P(W)$ and $P(\bar{W})$ represent the values of these parity checks.

In the reconciliation procedure Alice and Bob iterate selecting, transmitting, and comparing parities until Bob has almost no uncertainty about random variable E. At the end of this subsection we explain the reconciliation strategy of Bennett et al. [5] which shows that such a procedure does reach the situation in which Bob has almost no uncertainty about random variable E. Thus Alice and Bob construct $P = \mathcal{D}$ such that

$$\begin{aligned} 0 \approx H(E|\mathcal{D}(W)\mathcal{D}(\bar{W}), P = \mathcal{D}) &= H(E|P(W)P(\bar{W}), P = \mathcal{D}) \\ &= H(E|U, P = \mathcal{D}). \end{aligned} \tag{7.4}$$

Hence,

$$H(E|U) \approx 0$$

and therefore

$$\begin{aligned} 0 \leq H(W|YCU) &\leq H(W|\bar{W}U) = H(W\bar{W}|\bar{W}U) = H(E\bar{W}|\bar{W}U) \\ &= H(E|U\bar{W}) \leq H(E|U) \\ &\approx 0. \end{aligned}$$

Thus $H(W|YCU) \approx 0$ which means that Bob has almost no uncertainty about W. As noted before this follows from the fact that Bob has almost no uncertainty about E given U and Bob has full knowledge of $\bar{W}$. Hence, Bob has almost no uncertainty about $\bar{W} + E = W$.

We notice that

$$H(U) \approx H(U) + H(E|U) = H(EU) \geq H(E) = H(W|\bar{W}). \qquad (7.5)$$

We will analyse how U gives information about E. We will show that both P and $P(E) = P(W) + P(\bar{W})$ give information about E. If P takes on a value $\mathcal{D}$ then $\mathcal{D}$ represents a linear function, hence, $\mathcal{D}(\bar{W}) = \mathcal{D}(W) + \mathcal{D}(E)$. From (7.4) and the fact that W is independent of E and P we infer that

$$\begin{aligned} 0 &\approx H(E|\mathcal{D}(W)\mathcal{D}(\bar{W}), P = \mathcal{D}) \\ &= H(E|\mathcal{D}(W)\mathcal{D}(E), P = \mathcal{D}) \\ &= H(E|\mathcal{D}(E), P = \mathcal{D}) \\ &= H(E|P(E), P = \mathcal{D}). \end{aligned}$$

Hence,

$$\begin{aligned} H(\mathcal{D}(E)|P = \mathcal{D}) &= H(P(E)|P = \mathcal{D}) \\ &\approx H(P(E)|P = \mathcal{D}) + H(E|P(E), P = \mathcal{D}) \\ &= H(EP(E)|P = \mathcal{D}) \\ &= H(E|P = \mathcal{D}). \end{aligned}$$

By using the arguments with which we proved that $H(W|\bar{W}) = H(E)$ we can prove that $H(E|P = \mathcal{D}) = H(W|\bar{W}, P = \mathcal{D})$. We notice that $\mathcal{D}(E)$ takes on a value in a $l(\mathcal{D})$-dimensional subspace of $GF(2)^n$. Thus $l(\mathcal{D}) \geq H(\mathcal{D}(E)|P = \mathcal{D})$. By combining the formula's we obtain

$$l(\mathcal{D}) \geq H(\mathcal{D}(E)|P = \mathcal{D}) \approx H(W|\bar{W}, P = \mathcal{D}).$$

We conclude that on the average Bob needs at least

$$\begin{aligned} H(P(W)|P) &= \sum_{\mathcal{D} \in \mathcal{P}} P_P(\mathcal{D}) l(\mathcal{D}) \\ &\geq \sum_{\mathcal{D} \in \mathcal{P}} P_P(\mathcal{D}) H(W|\bar{W}, P = \mathcal{D}) = H(W|\bar{W}P) \qquad (7.6) \end{aligned}$$

parity checks in order to obtain almost full knowledge about W. For the sake of completeness we mention that

$$\begin{aligned} H(P(E)|P) &= \sum_{\mathcal{D} \in \mathcal{P}} P_P(\mathcal{D}) H(\mathcal{D}(E)|P = \mathcal{D}) \\ &\approx \sum_{\mathcal{D} \in \mathcal{P}} P_P(\mathcal{D}) H(W|\bar{W}, P = \mathcal{D}) = H(W|\bar{W}P). \qquad (7.7) \end{aligned}$$

We notice that

$$\begin{aligned} H(W|\bar{W}P) &= H(WP|\bar{W}) - H(P|\bar{W}) \\ &= H(W|\bar{W}) + H(P|W\bar{W}) - H(P|\bar{W}) \\ &= H(W|\bar{W}) + H(P|WE) - H(P|W + E). \end{aligned}$$

Since W is uniformly distributed and independent of E random variable $W+E$ is also uniformly distributed and independent of E. So, W and $W+E$ are independent of E and, hence, P. Thus $H(P|WE) = H(P|E)$ and $H(P|W+E) = H(P)$ and we conclude that

$$H(W|\bar{W}P) = H(W|\bar{W}) - I(P;E). \tag{7.8}$$

The combination of (7.6), (7.7), and (7.8) gives

$$\begin{aligned} H(P(W)|P) + I(P;E) &\geq H(P(E)|P) + I(P;E) \\ &\approx H(E) = H(W|\bar{W}), \end{aligned} \tag{7.9}$$

where $H(P(W)|P)$ represents the average number of independent parity check values needed by Bob to obtain almost full knowledge about W and where $I(P;E)$ measures the dependency of P on E. Random variable P represents Alice's and Bob's selection of the parity checks (the rows of parity check matrix D). For example, if the selection of the parity checks does not depend on E at all then $I(P;E) = 0$ and according to (7.9) Bob needs at least $H(W|\bar{W})$ independent parity check values in order to obtain almost full knowledge about W.

If there is a one to one correspondence between the selection of the $(i+1)$-th parity check and the value of the i-th parity check then the selection of the parity checks almost totally depends on E, that is $H(P|E) \approx 0$. Bob needs to use the values of the parity checks in order to compute the error values represented by E. But, it is sufficient for Bob to consider the structure of the parity check matrix (represented by P) because there is an almost one to one correspondence between the selection of the parity checks and their values. Bob can disregard the values of the parity checks communicated from Alice to him and from him to Alice. Hence, P already contains all the information about $P(E)$, that is $0 \approx H(P(E)|P)$. Thus $I(P;E) \approx H(E) = H(W|\bar{W}))$, see (7.9). Now, inequality (7.9) gives no lower bound on $H(P(W)|P)$, the number of independent parity check values needed by Bob.

Alice and Bob reach the purpose of the reconciliation phase if Eve still has a substantial amount of uncertainty about W. Eve's uncertainty about W equals

$$\begin{aligned} H(W|ZCU) &\geq H(W|ZCUE) = H(W|ZCEPP(W)) \\ &= H(WPP(W)|ZCE) - H(PP(W)|ZCE) \\ &= H(WP|ZCE) - H(P|ZCE) - H(P(W)|PZCE) \\ &= H(W|ZCE) + H(P|ZCEW) - H(P|ZCE) - \\ &\quad H(P(W)|PZCE), \end{aligned}$$

where $H(P|ZCE) = H(P|ZCEW) = H(P|E)$ since $ZCW \rightarrow E \rightarrow P$ is a Markov chain and where $H(P(W)|PZCE) \leq H(P(W)|P)$. We conclude that

$$\begin{aligned} H(W|ZCU) &\geq H(W|ZCE) - H(P(W)|P) \\ &= H(W|ZC) - H(P(W)|P) - I(E;W|ZC). \end{aligned}$$

Hence, if

$$H(P(W)|P) + I(E;W|ZC) < H(W|ZC) \tag{7.10}$$

then $H(W|ZCU) > 0$ and Eve has still a substantial amount of uncertainty about W.

Another condition implying that Eve has still a substantial amount of uncertainty about W is

$$H(U) < H(W|ZC) \tag{7.11}$$

since $H(W|ZCU) \geq H(W|ZC) - H(U)$. This condition can only hold if $H(W|\bar{W}) < H(W|ZC)$, see (7.5). That is Bob has not lost his advantage over Eve by discarding Y and C, see (7.3). Condition (7.11) appears to be weaker than (7.10). To show that condition (7.11) implies condition (7.10) we derive (from the arguments with which we proved that $H(W|\bar{W}) = H(E)$ we infer the first equality)

$$\begin{aligned} & H(P(W)|P) + I(E;W|ZC) \\ \leq\ & H(P(W)|P) + H(E) \\ \leq\ & H(P(W)|P) + H(P(E)|P) + H(P), \text{ by (7.9)} \\ =\ & H(P(W)|P) + H(P(\bar{W})|P(W)P) + H(P) \\ =\ & H(P(\bar{W})P(W)P) = H(U). \end{aligned}$$

We have seen that condition (7.11) can only hold if Bob has not lost his advantage over Eve by discarding Y and C. But, Alice and Bob reach their purpose of the reconciliation phase if (7.10) holds, which is a weaker condition than (7.11). Thus, it may be possible that Alice and Bob reach the purpose of the reconciliation phase even if Bob has lost his advantage over Eve by discarding Y and C. We conclude that during the reconciliation phase Alice and Bob indirectly distill an advantage over Eve.

We will explain the reconciliation strategy of Bennett et al. [5]. Alice and Bob start the reconciliation phase by publicly selecting a block size b and an arbitrary, randomly chosen, function $f:\ \{1,\ldots,n\}\rightarrow\{1\ldots r\}$ with the property that for all numbers $b_j = \{i : f(i) = j\}$, $1 \leq j \leq r$, either $b_j = b$ or $b_j = b-1$. The interpretation of f is that it partitions the set of indices $\{1,\ldots,n\}$ into r more or less equally sized blocks. Of each block Alice and Bob compute the parity which they compare publicly. Thus for $1 \leq j \leq r$ Alice computes the parity $\sum_{i:f(i)=j} w_i$ and Bob computes the parity $\sum_{i:f(i)=j}(w_i + e_i)$ which they transmit to oneanother over the public channel. Alice and Bob compare both parities by computing

$$p_j = \sum_{i:f(i)=j} w_i + \sum_{i:f(i)=j} (w_i + e_i) = \sum_{i:f(i)=j} e_i.$$

If $p_j = 1$ then they know that $e_i = 1$ for at least one i with $f(i) = j$ and they will perform publicly a bisective error search.

The bisective error search works as follows. Alice and Bob publicly split the set of indices $\{i : f(i) = j\}$ into two approximately equally sized ($\approx b/2$) disjunct non-empty parts. Of the first part Alice and Bob compute the parity which they communicate to oneanother over the public channel. For example, suppose w.l.o.g. that $\{i : f(i) = j\} = \{1, \ldots, b\}$ and that $\{1, \ldots, a\}$ is the first part. Alice and Bob compare the parities of the first part. So, they obtain $p'_j = \sum_{1 \leq i \leq a} e_i$, and also $p"_j = p_j + p'_j = \sum_{a+1 \leq i \leq b} e_i$. Either $p'_j = 1$ or $p"_j = 1$. If $p'_j = 1$ then they know that an error occurred in the first part and they perform a bisective error search for the first part. If $p"_j = 1$ then an error occurred in the second part and they perform a bisective error search for the second part. They continue the bisective error search until it is not possible to split the part containing at least one error into two non-empty disjunct pieces. Thus until the part containing at least one error consists of only one index. At that moment Alice and Bob located one error and Bob can correct it.

Example 7.2.4 Let Alice's block be

100101110111001

and Bob's block be

001101110111011.

Alice transmits publicly parity 1 and Bob transmits publicly parity 0. They detect one error. So, they start a bisective error search. Alice's first part is 1001011 and has parity 0. Bob's first part is 0011011 and has parity 0. They communicate these parities to each other and they conclude that Bob's second part contains an error. So Alice and Bob continue with their bisective search for their second parts 10111001 and 10111011, respectively. Alice's first halve is 1011 and has parity 1. Bob's first halve is 1011 and has parity 1. They communicate these parities to each other. Again Bob's second halve contains an error. Alice's second halve is 1001 which she splits into parts 10 and 01. Bob's second halve is 1011 which he splits into parts 10 and 11. They communicate the parities of the first parts to each other. They conclude that the error is in the second part. They continue with the bisective search and Alice and Bob obtain parts 0 and 1, and, parts 1 and 1, respectively. They conclude that an error is contained in the first part of Bob. They stop the search. They located the error (bit 14) at a cost of 4 additional public parity checks. Bob corrects the error.

Alice and Bob *repeat* the whole procedure consisting of choosing a partition function f and performing bisective error searches until with high probability Bob has corrected all errors. At that moment Bob has almost no uncertainty about E and, hence, W.

In the reconciliation strategy of Bennett et al. [5] bisective error searches are used to locate errors. To detect errors Alice and Bob partition the set of indices $\{1, \ldots, n\}$ into blocks of more or less equal size b of which they compare the parities. Brassard and Savail [24] improved the strategy by noting the following. Suppose the procedure of choosing a partition function f followed by bisective error searches is iterated k times. Further, suppose a bisective error search is performed in the k-th iteration and one error e_i is located. In each of the previous k iterations index i is an element of one of its blocks. Let set B be such a block and suppose Alice and Bob know that its parity equals $\sum_{j \in B} e_j = 0$. Since $e_i = 1$ and $i \in B$ Alice and Bob conclude that $\sum_{j \in B \setminus \{i\}} e_j = 1$. Hence, they detect an error for free, that is $e_j = 1$ for at least one index $j \in B \setminus \{i\}$. So, Alice and Bob can perform additional bisective error searches to locate such errors. Thus Brassard and Savail noted that whenever Alice and Bob locate an error they may detect other errors by reconsidering their public communication. This improves the efficiency of the reconciliation procedure.

In [5] and [24] it is not analysed how Alice and Bob can find the optimal choice for the block size b. Let us consider the strategy of Bennett et al. [5] Suppose Alice and Bob partition $\{1, \ldots, n\}$ into blocks of equal size b. Let $n = (m+m')b$, where m equals the expected number of blocks with matching parity. Then Alice and Bob are expected to locate and correct m' errors (in the strategy of Brassard and Savail more errors are expected to be located and corrected). They publicly compare the parity checks of each of the $m+m'$ blocks. In addition they compare $\approx m' \log_2 b$ parity checks during each of the m' bisective error searches. Hence, Alice and Bob correct m' errors at a cost of $\approx m'(1 + \log_2 b) + m$ parity checks. We have seen that each public parity check may give Eve information. Hence, a good strategy is to choose the b minimizing the expected rate between the number of parity checks and the number of corrected errors. Thus b should minimize

$$B(b) = \frac{m'(1 + \log_2 b) + m}{m'} \tag{7.12}$$

Let $\hat{p}$ be Alice's and Bob's estimate of the bit error probability. At the start of the reconciliation phase they know $\hat{p}$, but during the information reconciliation $\hat{p}$ will change when Bob corrects errors and when Alice and Bob find out that certain blocks have matching parity. The probability that a block has matching parity equals

$$h = \sum_{2i=0}^{b} \binom{b}{2i} \hat{p}^{2i}(1 - \hat{p})^{b-2i} = \frac{1 + (1 - 2\hat{p})^b}{2}.$$

Hence,

$$\begin{aligned} B(b) &= \log_2 b + \frac{m'+m}{m'} = \log_2 b + \frac{1}{1-h} \\ &= \log_2 b + \frac{2}{1-(1-2\hat{p})^b}. \end{aligned} \qquad (7.13)$$

So, if Alice and Bob can estimate the bit error probability $\hat{p}$ then they can compute the block length b minimizing $B(b)$. One method to estimate $\hat{p}$ is the following. For $0 \leq i \leq n$ we calculate the probability $P(i)$ that the to be reconciliated string contains i errors. Suppose that so far t errors have been detected, located, and corrected during the reconciliation phase. Let $P(i| \geq t)$ be the probability that the to be reconciliated string contains i errors given that it contains at least t errors, i.e.

$$P(i| \geq t) = \frac{P(i)}{\sum_{i \geq t} P(i)},$$

if $i \geq t$ and $P(i| \geq t) = 0$ if $i < t$. If the reconciliation string contains i errors and t errors have been corrected then the bit error probability $\hat{p}$ equals $(i-t)/n$. Therefore an estimate of $\hat{p}$ could be

$$\sum_{i \geq t} P(i| \geq t) \frac{i-t}{n}.$$

In [5] simulations of the reconciliation procedure were presented. No explanation of how to choose the block length b was given (by trial and error?). Interesting however is that their choices correspond to our analysis.

7.2.3 Privacy Amplification

Suppose w.l.o.g. that Alice and Bob created a random variable W by exchanging publicly information C and U such that Alice has full knowledge about W, i.e. $H(W|XCU) = 0$, Bob has almost full knowledge about W, i.e. $H(W|YCU) \approx 0$, and Eve has a substantial amount of uncertainty about W, i.e. $H(W|ZCU) > 0$. Let $\mathcal{G}$ be a class of compression functions and let G be the random variable corresponding to the random choice with uniform distribution of a member of $\mathcal{G}$. In the privacy amplification phase Alice and Bob will agree publicly on a compression function G to distill from W a shorter string $S = G(W)$ about which Bob still has almost full knowledge but Eve now has only a negligible amount of information. At the end of this phase Alice and Bob amplified their privacy;

$$H(S|XCUG) = 0,$$

$$H(S|YCUG) \approx 0,$$

and $H(S) \approx H(S|ZCUG)$, i.e.

$$\Delta = H(S|ZCUG)/H(S) \approx 1$$

(or the stronger version $\bar{\Delta} = I(S;ZCUG) \approx 0$). The concept of privacy amplification was introduced by Bennett et al. [7].

Let us consider the situation in which $X \rightarrow (Y, Z)$ is such that $X \rightarrow Y$ is noiseless and $X \rightarrow Z$ is a $BSC(q)$. Then Alice and Bob do not need an advantage distillation phase or a reconciliation phase. In fact, this situation is a special case of the wire-tap channel model, and (7.2) states $C_s(P_{Y,Z|X}) = \bar{C}_s(P_{Y,Z|X})$. Hence, we do not even need public discussion to achieve $\bar{C}_s(P_{Y,Z|X})$. We notice that $\bar{C}_s(P_{Y,Z|X}) = h(q)$. In [31] Garleial and Hellman prove the following interesting result. Let B be an arbitrary but fixed binary $n \times r$ matrix having full rank. Define $\mathcal{G}_{r,n}$ as the class of functions $g_A \in GF(2)^n \rightarrow GF(2)^r$ with $g_A(\mathbf{x}) = \mathbf{x}AB$ where A is an invertible binary $n \times n$. Let $R \leq h(q)$ be a fixed information rate and let $0 \leq \Delta < 1$ be a fixed equivocation. Let r and n be integers such that $R = r/n$. Let G be the random variable corresponding to the random choice with uniform distribution of a member of $\mathcal{G}_{r,n}$. Then there exists a function $\varepsilon(n)$ with $\varepsilon(n) \rightarrow 0$ as n goes to infinity such that with probability at least $1 - \varepsilon(n)$

$$H(G(X^n)|Z^n) \geq \Delta H(G(X^n)).$$

This result of Garleial and Hellman shows that we can use a compression function represented by the random variable G to distill from X^n a shorter string $S^r = G(X^n)$ about which Eve has only a negligible amount of information; $H(S^r|Z^n) \approx H(S^r)$.

A more general method to distill a secret key is the following from Bennett et al. [6]. They define a class $\mathcal{G}$ of functions $\mathcal{A} \rightarrow \mathcal{B}$ to be *universal*$_2$, or *universal* for short, if for any distinct x_1 and x_2 in $\mathcal{A}$ the probability that $g(x_1) = g(x_2)$ is at most $1/|\mathcal{B}|$ when g is chosen at random from $\mathcal{G}$ according to the uniform distribution.

Example 7.2.5 [6] Let ϕ be an isomorphism from $GF(2)^n$ to $GF(2^n)$, and let $1 \leq r \leq n$. An example of a universal class of functions is the class consisting of functions $g_a : GF(2)^n \rightarrow GF(2)^r$, $a \in GF(2^n)$, where g_a assigns to an argument $\mathbf{x}$ the last r bits of the vector $\phi^{-1}(a\phi(\mathbf{x}))$.

Let $\mathcal{G}$ be a universal class of functions $GF(2)^n \rightarrow GF(2)^r$ and let G be the random variable corresponding to the random choice with uniform distribution of a member of $\mathcal{G}$. Let W_1 and W_2 represent two independent random variables both defined by probability distribution P_W with range $\mathcal{W} = GF(2)^n$. Define the *collision probability* $P_c(W)$ of W by

$$P_c(W) = P(W_1 = W_2) = \sum_{w \in \mathcal{W}} P_W(w)^2.$$

Hence, $P_c(W)$ is the probability that W takes on the same value twice. In [6] it is noted that

$$\begin{aligned} & P(G(W_1) = G(W_2)) \\ = \ & P(W_1 = W_2) + P(W_1 \neq W_2)P(G(W_1) = G(W_2)|W_1 \neq W_2) \\ \leq \ & P_c(W) + (1 - P_c(W))2^{-r} \leq P_c(W) + 2^{-r} \end{aligned}$$

by the definition of universality.

Let the *collision entropy* $H_c(W)$ be defined by

$$H_c(W) = -\log_2 P_c(W).$$

Notice that

$$H_c(W) \leq H(W)$$

by Jensen's inequality. Bennett et al. [6] proved

$$\begin{aligned} H(G(W)|G) & \geq H_c(G(W)|G) \\ & = \sum_{g \in \mathcal{G}} P_G(g) H_c(G(W)|G = g) \\ & = -\sum_{g \in \mathcal{G}} P_G(g) \log_2 P_c(G(W)|G = g) \\ & \geq -\log_2 \sum_{g \in \mathcal{G}} P_G(g) P_c(G(W)|G = g) \\ & = -\log_2 P(G(W_1) = G(W_2)) \\ & \geq -\log_2(P_c(W) + 2^{-r}) \\ & = r - \log_2(1 + 2^{r - H_c(W)}) \\ & \geq r - \frac{2^{r-H_c(W)}}{\ln 2}, \end{aligned} \tag{7.14}$$

since $\log_2(1 + 2^{r-H_c(W)}) \leq 2^{r-H_c(W)}/\ln 2$. This inequality tells us that

$$H(G(W)|G) \approx H(G(W))$$

if $H_c(W) < r$. Hence, G is an interesting compression function for generating a secret key. Inequality (7.14) also applies to conditional distributions such as $P_{W|ZCU=zcu}$.

Suppose Alice and Bob created a uniformly distributed random variable W with range $\mathcal{W} = GF(2)^n$ by exchanging public information C and U such that $H(W|XCU) = 0$ and $H(W|YCU) \approx 0$. Further, suppose that Alice and Bob know that with probability at least $1 - 2^{-s} \approx 1$ random variables Z, C, and U take on values z, c, and u such that Eve's collision entropy $H_c(W|ZCU = zcu)$ is at least t. Then by (7.14)

$$\begin{aligned} H(G(W)|ZCU = zcu) & \geq H_c(G(W)|G, ZCU = zcu) \\ & \geq r - 2^{r-t}/\ln 2 = H(G(W)) - 2^{r-t}/\ln 2 \end{aligned}$$

and we conclude that

$$H(G(W)|ZCU) \geq (1-2^{-s})(H(G(W)) - 2^{r-t}/\ln 2).$$

Hence, $S = G(W)$ can be used as secret key if $r < t$ is small enough.

The approach of Bennett et al. [6] is more general in the sense that Alice and Bob only need to know that with probability at least $1-2^{-s} \approx 1$ random variables Z, C, and U take on values z, c, and u such that Eve's collision entropy $H_c(W|ZCU = zcu)$ is at least t, that is

$$P_c(W|ZCU = zcu) \leq 2^t.$$

So, Alice and Bob only need to know a constraint on the probability distribution representing Eve's knowledge. Of course the approach of Bennet et al. may not be the best one since they only use that $H(W|ZCU = zcu) \geq H_c(W|ZCU = zcu) \geq t$ with probability at least $1-2^{-s} \approx 1$. If Alice and Bob know a sharper lower bound on Eve's Shannon information then there may exist a strategy with which they can generate a longer secret key.

Cachin and Maurer [28] describe what the influence is of the reconciliation phase on Eve's collision entropy. They prove that for $\hat{s} > 0$ with probability at least $1 - 2^{\hat{s}}$ random variable $U = (P(W), P(\bar{W}), P)$ takes on a value $u = (\mathcal{D}(w), \mathcal{D}(\bar{w}), \mathcal{D})$ such that the decrease in collision entropy by giving u is

$$H_c(W|ZCU = zcu) - H_c(W|ZC = zc) \leq 2l(\mathcal{D}) + 2\hat{s}.$$

Suppose that at the end of the advantage distillation phase Alice and Bob created the advantage that with probability at least $1 - 2^s$ random variables Z and C take on values z and c such that Eve's collision entropy $H_c(W|ZC = zc)$ is at least t. Then at the end of the reconciliation phase random variables Z, C, and U take on values z, c, and $u = (\mathcal{D}(w), \mathcal{D}(\bar{w}), \mathcal{D})$ such that

$$H_c(W|ZCU = zcu) \geq t - 2l(\mathcal{D}) - 2\hat{s}$$

with probability at least $(1-2^s)(1-2^{\hat{s}})$. Hence, if they choose $r < t - 2l(\mathcal{D}) - 2\hat{s}$ small enough then they can use $S = G(W)$ as secret key.

We conclude that collision information is a useful tool. Alice's and Bob's goal is to reduce Eve's Shannon information. They achieve this goal by using a universal class of functions. We have showed that a lower bound on Eve's collision information $H_c(W|ZCU = zcu)$ leads to a lower bound on Eve's Shannon information $H(W|ZCU)$. More generally, let V be some random variable dependent on $WZCU$ with range $\mathcal{V}$. Then a lower bound on $H_c(W|ZCUV = zcuv)$ leads to a lower bound on Eve's Shannon information $H(W|ZCUV) \leq H(W|ZCU)$. This may lead to a better lower bound on $H(W|ZCU)$ since unlike Shannon entropy

$$H_c(W|ZCUV = zcuv) > H_c(W|ZCU = zcu)$$

is possible! Such a random variable V is said to contain *spoiling knowledge* about W. This consideration is used in [6] to sharpen (7.14) into

$$H_c(G(W)|G) \geq r - \sum_{v \in \mathcal{V}} P_V(v) \min \left\{ r, \frac{2^{r-H_c(W|V=v)}}{\ln 2} \right\}.$$

7.3 Outline of the Second Part of the Thesis

In Chapter 8 we consider the BCC in which tampering is allowed by Eve. We discuss passive tampering [52] (joint work with Arie Koppelaar) and active tampering [45]. Chapter 9 [47] discusses a special class of BCC for which the secrecy capacity can be calculated. Finally, we discuss the advantage distillation phase in Chapter 10 [43]. Besides the results presented in Chapter 8, 9, and 10 we notice that the analysis of the reconciliation phase presented in Subsection 7.2.2 is own work as well.

Chapter 8

The BCC with Tampering

In this chapter we consider BCC's with tampering. In Section 8.1 [52] (joint work with Arie Koppelaar) we describe how Alice and Bob communicate over a quantum channel where Eve uses an intercept/resend strategy (so, Eve is not an active tamperer). Eve's eavesdropping causes tampering of the signal from Alice to Bob. The tampering effect of Eve's eavesdropping can not be controlled by her. A model in which Eve actively tampers the signal sent by Alice to Bob is discussed in Section 8.2 [45].

To detect impersonation and/or substitution of messages by an enemy (Eve) Alice and Bob use authentication codes (see Chapter 6). The idea is that before Alice encodes and transmits a message M, she appends an authentication tag $F(M, S)$. The authentication message $(M, F(M, S))$ is then encoded and sent to Bob. The tag depends on M and a secret key S known to Alice and Bob. Function F is public knowledge. Bob detects tampering if he receives a message with a not corresponding tag. In the case where Alice and Bob use authentication Alice and Bob need to agree on a secret key before they start using the BCC to generate a new secret key. Hence, in this situation we should not use the phrase secret key generation but secret key amplification.

We notice that Alice and Bob can use an authentication code to detect tampering of the information Alice sends to Bob. However, they will not be able to detect tampering of the noise generated in the channel from Alice to Bob. In Section 8.2 we will show that it can be interesting for Eve to actively tamper this noise.

8.1 Quantum Key Agreement

We consider quantum key agreement between two legal users Alice and Bob in which an eavesdropper Eve intercepts and resends photons. We show how Alice and Bob attain a probabilistic upper bound on Eve's knowledge.

8.1.1 Quantum Transmission

We consider the quantum key agreement method described by Bennett et al. [5] in which an eavesdropper uses the intercept/resend strategy. We derive the probability that an eavesdropper obtains at most l bits of information given the number of errors after the raw quantum transmission.

Bennett et al. considered quantum key agreement between two legal users Alice and Bob. It is based on Heisenberg's uncertainty principle. Alice sends a random sequence of the four canonical kinds of polarized photons to Bob, horizontal, vertical, left-circular, and right-circular. For each received photon Bob chooses randomly whether to measure the photon's rectilinear or circular polarization. Then Bob announces publicly which kind of measurement he made. Alice replies publicly whether the transmitted photon was rectilinear or circular polarized. Alice and Bob then discard all bit positions for which Bob's measurement did not match and all bit positions for which Bob did not detect any photon at all. The polarizations of the remaining photons are interpreted as bit 0 for horizontal or left-circular, and bit 1 for vertical and right-circular. These steps together are called a raw quantum transmission session.

In [5] different eavesdropping strategies are presented. We only consider the intercept/resend strategy during the raw quantum transmission. In this case the eavesdropper Eve intercepts selected pulses and reads them in bases of her choosing. Then Eve fabricates a pulse of the same polarization as she detected, which she sends to Bob. We assume that Eve uses rectilinear and circular bases only (there are more bases, see [5]). With probability 1/2 Eve measures the polarization of the intercepted photon in the correct base (that is the base agreed by Alice and Bob). Heisenberg's uncertainty principle implies that measuring a photon's linear polarization randomizes its circular polarization, and vice versa. Hence, with probability 1/2 Eve interprets intercepted photons measured by her in the wrong base correctly (that is Eve's interpretation coincides with Alice's interpretation). Similarly, with probability 1/2 Bob interprets intercepted photons measured by Eve in the wrong base correctly. For simplicity we assume that Bob and Eve have detectors of 100% quantum efficiency, that is measuring in the correct base imposes no errors (to Alice and Bob this is a worst case assumption since Eve is assumed to have a perfect detector and all errors occurred in Bob's detector are assumed to be caused by Eve). So after the agreement of the bases between Alice and Bob, both Eve and Bob have bit error probability 1/4 for the bits intercepted by Eve. There is a significant difference between the channel from Alice to Bob and the channel from Alice to Eve; Eve knows which intercepted photons were measured by her in correct base, where Bob does not know which intercepted photons were measured by Eve in correct base. This extra knowledge of Eve gives Eve information about whether her interpretation of an intercepted photon is correct or completely arbitrary (that is independent of Alice's interpretation). We conclude that Eve's channel is superior to Bob's channel.

Alice and Bob want to distill a secret key of a certain minimal length from each raw quantum transmission session despite eavesdropping by Eve. They remove all raw quantum transmission sessions for which it is not possible to distill a secret key of sufficient length. It is Eve's intention that Alice and Bob generate a secret key about which Eve gets some information. Hence, Eve's activities should not prevent Alice and Bob from generating a secret key. Therefore it can be better for Eve only to intercept a part of the pulses as otherwise Alice and Bob may not generate a secret key at all. Alice and Bob have to solve the following problems [70]:

1. Find with high probability the location of all, say t errors after agreement of their bases. This can be done by means of information reconciliation, see [5, 24]. During the information reconciliation, Alice and Bob reveal bits to Eve. The exact number b of bits revealed to Eve can be computed by Alice and Bob.

2. Given the number of errors t, compute an upper bound l, which holds with high probability, on the number of bits of information obtained by Eve during the raw quantum transmission session. This problem will be discussed in Subsection 8.1.2.

3. Generate a secret key given that Eve obtained at most $l + b$ bits of information, and compute the secret information leaking to Eve. This can be solved by means of privacy amplification, see [7, 6, 28].

8.1.2 Probabilistic Upper Bound

To solve the second problem we introduce some notation. By n we denote the number of bits shared between Alice and Bob after a raw quantum transmission session (n is fixed, Alice keeps on sending photons until Bob has received n photons in correct base). The random variable representing the number of bits intercepted/resent by Eve is denoted by K ($\leq n$). We notice that we only discus the intercept/resend eavesdropping strategy where intercepted photons are measured in rectilinear and circular base only. The random variable representing the number of deterministic bits of information of the raw quantum transmission session leaking to Eve is denoted by L, and the random variable representing the number of errors which Alice and Bob have after agreement of their bases is denoted by T. Notice that

$$L + T \leq K,$$

and that given $K = k$ the expected values of L and T are equal to $k/2$ and $k/4$, respectively.

Our goal is to find a function l_ε such that

$$P(L \leq l_\varepsilon(T)) > 1 - \varepsilon.$$

I.e., if $T = t$ is measured during information reconciliation then $l_\varepsilon(t)$ is an upper bound on L with probability at least $1-\varepsilon$. This means that in a fraction ε of all quantum transmission sessions Alice and Bob assume an incorrect upper bound. Thus they require ε to be small. We like to emphasize that l_ε describes a *probabilistic upper bound* on Eve's knowledge.

Random variable K represents Eve's strategy of partial intercept/resend eavesdropping. Probability distributions P_L and P_T depend on the value of K. The value taken on by K is not known to Alice and Bob. However, after the reconciliation phase they know with high probability the value taken on by T. In order to find a function l_ε Alice and Bob are interested in $P(L \geq l | T = t, K = k)$, for $0 \leq k, t, l \leq n$, which is the probability that the number of deterministic bits of information of the raw quantum transmission session leaking to Eve is at least l given the number of errors t which Alice and Bob have after agreement of their bases, calculated under the assumption that Eve intercepted k bits. Lemma 8.1.1 characterizes this quantity. As we will show, it leads to a probabilistic upper bound.

Before we state and prove the lemma we analyse a few probabilities. We have seen that with probability 1/2 Eve measures an intercepted photon in correct base. With probability 1/2 Bob interprets an intercepted and resent photon measured by Eve in the wrong base wrongly, and with probability 1/4 Bob interprets an intercepted and resent photon wrongly. Henceforward, taking our quantum transmission model into account we obtain

$$\begin{aligned} P_{L|K}(l|k) &= \binom{k}{l}(1/2)^k, \\ P_{T|L,K}(t|l,k) &= \binom{k-l}{t}(1/2)^{k-l}, \\ P_{T|K}(t|k) &= \binom{k}{t}(1/4)^t(3/4)^{k-t}, \end{aligned} \tag{8.1}$$

and

$$\begin{aligned} P_{L|T,K}(l|t,k) &= \frac{P_{L|K}(l|k)P_{T|L,K}(t|l,k)}{P_{T|K}(t|k)} \\ &= \binom{k-t}{l}(1/3)^{k-t-l}(2/3)^l. \end{aligned} \tag{8.2}$$

The binomial distribution can be upper bounded by, see [32, pp. 61–70],

$$\sum_{l=0}^{m} \binom{n}{l} p^l(1-p)^{n-l} < F\left((m - pn + 1/2)/\sqrt{np(1-p)}\right), \tag{8.3}$$

where $F(u) = e^{-u^2/2}$ if $u \leq 0$ and $F(u) = 1$ if $u \geq 0$. Later on we need the inverse function we define u_α defined by $F(u_\alpha) = \alpha$, for $0 < \alpha < 1$, i.e. $u_\alpha = -\sqrt{\ln(1/\alpha^2)}$.

Lemma 8.1.1 *Let $0 \leq l, t, k \leq n$ such that $l + t \leq k$. Then*

$$\begin{aligned} P(L \geq l | T = t, K = k) &= \sum_{j=0}^{k-t-l} \binom{k-t}{j} (2/3)^{k-t-j} (1/3)^j \\ &< F\left(\sqrt{2(k-t)} - 3(l-1/2)/\sqrt{2(k-t)}\right) \end{aligned}$$

and

$$\begin{aligned} P(T \leq t | K = k) &= \sum_{j=0}^{t} \binom{k}{j} (1/4)^j (3/4)^{k-j} \\ &< F\left(4(t+1/2)/\sqrt{3k} - \sqrt{k/3}\right). \end{aligned}$$

The upper bound on probability $P(L \geq l | T = t, K = k)$ is decreasing in l and increasing in $k - t$. The upper bound on probability $P(T \leq t | K = k)$ is decreasing in k and increasing in t.

Proof: Since $L + T \leq K$

$$\begin{aligned} P(L \geq l | T = t, K = k) &= \sum_{j=l}^{k-t} P_{L|T,K}(j|t,k) \\ &= \sum_{j=0}^{k-t-l} P_{L|T,K}(k-t-j|t,k), \text{ and} \qquad (8.4) \\ P(T \leq t | K = k) &= \sum_{j=0}^{t} P_{T|K}(j|k). \qquad (8.5) \end{aligned}$$

By substituting (8.1) and (8.2) in (8.4) and (8.5), respectively, and by using (8.3) we obtain the desired results.

□

For $\varepsilon > 0$ and $0 \leq t, k \leq n$ we define $\hat{l}_\varepsilon(t, k)$ as the minimal value l for which

$$F\left(\sqrt{2(k-t)} - 3(l+1/2)/\sqrt{2(k-t)}\right) \leq \varepsilon.$$

Thus if $T = t$ and $K = k$ then with probability at least $1 - \varepsilon$, the integer $\hat{l}_\varepsilon(t, k)$ is an upper bound of the number of deterministic bits leaked to Eve during the raw quantum transmission session. Alice and Bob will generate a short secret key during the privacy amplification phase if $\hat{l}_\varepsilon(t, k)$ is large. This is the reason why Alice and Bob are interested in the *minimal* value of l.

We notice that the upper bound on $P(L \geq l|T = t, K = k)$ is decreasing in l and increasing in $k-t$. Hence, $\hat{l}_\varepsilon(t,k)$ increases if $k-t$ increases. Suppose that Alice and Bob want to take the worst case (to them) strategy of Eve into account, that is $k = n$ (because $k = n$ maximizes the upper bound on $P(L > l|T = t, K = k)$ w.r.t. k). We derive

$$\begin{aligned} & P(L > \hat{l}_\varepsilon(T,n)) \\ = & \sum_{k,t} P(L > \hat{l}_\varepsilon(t,n)|K = k, T = t)P_{K,T}(k,t) \\ < & \sum_{k,t} F\left(\sqrt{2(k-t)} - 3(\hat{l}_\varepsilon(t,n) + 1/2)/\sqrt{2(k-t)}\right) P_{K,T}(k,t) \\ \leq & \sum_{k,t} F\left(\sqrt{2(n-t)} - 3(\hat{l}_\varepsilon(t,n) + 1/2)/\sqrt{2(n-t)}\right) P_{K,T}(k,t) \\ \leq & \sum_{k,t} \varepsilon P_{K,T}(k,t) \\ = & \varepsilon. \end{aligned}$$

Hence, $P(L \leq \hat{l}_\varepsilon(T,n)) > 1 - \varepsilon$ and we achieved our goal.

Suppose that in reality Eve does not intercept, that is $k = 0$ implying that $l = 0$. Then Alice and Bob will have $t = 0$. Since $\hat{l}_\varepsilon(t,k)$ increases if t decreases Alice and Bob compute $\hat{l}_\varepsilon(t,n) >> l = 0$. Their probabilistic upper bound $\hat{l}_\varepsilon(t,n)$ is not good. We conclude that Alice and Bob should not take a worst case situation ($k = n$) into account. Given $T = t$, it is better to estimate the value of K and to use this estimate to estimate L. In this way we will obtain a better upper bound to achieve our goal. This is considered in the following theorem.

Theorem 8.1.2 *Let $0 < \alpha, \beta < 1/2$. For real numbers $0 \leq t < n$ we define $k_\alpha(t)$ by*

$$k_\alpha(t) = \min\{k, n\},$$

where $k \in \mathbb{N}$ is the minimal value for which

$$u_\alpha \geq 4(t + 1/2)/\sqrt{3k} - \sqrt{k/3},$$

where $u_\alpha = -\sqrt{ln(1/\alpha^2)}$. We define $l_{\alpha,\beta}(t)$ as the minimal value $l \in \mathbb{N}$ for which

$$u_\beta \geq \sqrt{2(k_\alpha(t) - t)} - 3(l + 1/2)/\sqrt{2(k_\alpha(t) - t)},$$

and we define

$$l^*_\varepsilon(t) = \min_{\alpha+\beta=\varepsilon} l_{\alpha,\beta}(t).$$

Functions $k_\alpha(t)$, $l_{\alpha,\beta}(t)$, and $l^*_\varepsilon(t)$ are well defined and decreasing in α, α and β, and ε, respectively. We have that

$$P(L \leq l^*_\varepsilon(T)) > 1 - \varepsilon.$$

Proof: In this proof we denote $4(t+1/2)/\sqrt{3k} - \sqrt{k/3}$ by $f(t,k)$ and $\sqrt{2(k_\alpha(t)-t)} - 3(l+1/2)/\sqrt{2(k_\alpha(t)-t)}$ by $g_\alpha(t,l)$. Since $f(t,k) \to -\infty$ as k tends to infinity, $k_\alpha(t)$ is well defined. Because $u_\alpha < 0$ $(0 < \alpha < 1/2)$, $f(t,t) = \sqrt{3t} + (1/2)/\sqrt{3t} > 0$, and $t < n$, we have that $k_\alpha(t) > t$. Hence, inequality $u_\beta \geq g_\alpha(t,l)$ with which $l_{\alpha,\beta}(t)$ is defined makes sense. Furthermore $g_\alpha(t,l) \to -\infty$ as l tends to infinity, hence $l_{\alpha,\beta}(t)$ is well defined.

If α increases then u_α increases, and if t decreases then $f(t,k)$ decreases. Thus $k_\alpha(t)$ decreases if α increases or t decreases. If $k_\alpha(t)$ decreases then $g_\alpha(t,l)$ decreases. Thus, if α increases then $k_\alpha(t)$ decreases and $l_{\alpha,\beta}(t)$ decreases. Since u_β increases if β increases $l_{\alpha,\beta}(t)$ decreases if β increases. Summarizing, we have that $k_\alpha(t)$ and $l_{\alpha,\beta}(t)$, and, hence, $l^*_\varepsilon(t)$ are well defined and decreasing in α, α and β, and ε, respectively. Furthermore we have that $k_\alpha(t)$ is increasing in t.

We will first show that it is sufficient to prove

$$P(k_\alpha(T) < K) < \alpha \tag{8.6}$$

and

$$P(L \geq l_{\alpha,\beta}(t) | T = t, K = k) < \beta \;\text{ if } k_\alpha(t) \geq k. \tag{8.7}$$

Indeed, it follows from

$$\begin{aligned}
P(L > l_{\alpha,\beta}(T)) &= \sum_{k,t} P(L > l_{\alpha,\beta}(t)|K=k, T=t) P_{K,T}(k,t) \\
&= \sum_{k,t:k_\alpha(t)\geq k} P(L > l_{\alpha,\beta}(t)|K=k, T=t) P_{K,T}(k,t) \\
&\quad + \sum_{k,t:k_\alpha(t)<k} P(L > l_{\alpha,\beta}(t)|K=k, T=t) P_{K,T}(k,t) \\
&< \sum_{k,t:k_\alpha(t)\geq k} \beta P_{K,T}(k,t) + \sum_{k,t:k_\alpha(t)<k} P_{K,T}(k,t) \\
&= \beta P(k_\alpha(T) \geq K) + P(k_\alpha(T) < K) \\
&< \beta + \alpha,
\end{aligned}$$

hence, $P(L \leq l_{\alpha,\beta}(T)) > 1 - (\alpha + \beta)$. Thus,

$$P(L \leq l^*_\varepsilon(T)) > 1 - \varepsilon$$

which is what we need to prove. Notice that $l_{\alpha,\beta}(t)$ is decreasing in α and β and therefore $l^*_\varepsilon(t)$ is equal to $\min_{\alpha+\beta\leq\varepsilon} l_{\alpha,\beta}(t)$.

Let us prove (8.6). We define $t_\alpha(k)$ by

$$t_\alpha(k) = (u_\alpha\sqrt{3k} + k - 2)/4.$$

Then $u_\alpha = 4(t_\alpha(k) + 1/2)/\sqrt{3k} - \sqrt{k/3} = f(t_\alpha(k), k)$. Hence, the minimal value $\hat{k}$ for which $u_\alpha \geq f(t_\alpha(k), \hat{k})$ is at most k. Since $f(t_\alpha(k), \hat{k})$ is decreasing in $\hat{k}$ the minimal value for which $u_\alpha \geq f(t_\alpha(k), \hat{k})$ is equal to k. Hence,

$$k_\alpha(t_\alpha(k)) = \min\{k, n\}. \tag{8.8}$$

By using Lemma 8.1.1, (8.8), and the fact that $k_\alpha(t)$ is increasing in t we derive

$$\begin{aligned}
P(k_\alpha(T) < K) &= \sum_{0 \leq k \leq n} P(k_\alpha(T) < k | K = k) P_K(k) \\
&= \sum_k P(k_\alpha(T) < k_\alpha(t_\alpha(k)) | K = k) P_K(k) \\
&= \sum_k P(T < t_\alpha(k) | K = k) P_K(k) \\
&< \sum_k F\left(4(\lfloor t_\alpha(k) \rfloor + 1/2)/\sqrt{3k} - \sqrt{k/3}\right) P_K(k) \\
&\leq \sum_k F\left(4(t_\alpha(k) + 1/2)/\sqrt{3k} - \sqrt{k/3}\right) P_K(k) \\
&= \sum_k F(u_\alpha) P_K(k) = \alpha.
\end{aligned}$$

Let us prove (8.7). Suppose that $k_\alpha(t) \geq k$. Then by Lemma 8.1.1 and the fact that $P(L > l | T = t, K = k)$ is increasing in k we obtain

$$\begin{aligned}
& P(L > l_{\alpha,\beta}(t) | T = t, K = k) \\
\leq\ & P(L \geq l_{\alpha,\beta}(t) + 1 | T = t, K = k_\alpha(t)) \\
<\ & F\left(\sqrt{2(k_\alpha(t) - t)} - 3(l_{\alpha,\beta}(t) + 1/2)/\sqrt{2(k_\alpha(t) - t)}\right) \\
\leq\ & F(u_\beta) = \beta.
\end{aligned}$$

This completes the proof.

□

Theorem 8.1.2 tells us that in a fraction $1 - \varepsilon$ of all raw quantum transmission sessions T and L attain values t and l such that $l \leq l^*_\varepsilon(t)$. Hence, in a fraction $1 - \varepsilon$ of all raw quantum transmissions $l^*_\varepsilon(t)$ upper bounds the number of bits leaking to Eve. The following lemma shows that $l^*_\varepsilon(t)$ is a better upper bound than $\hat{l}_\varepsilon(t, n)$. Figure 1 depicts this for $n = 10000$, where we used $l_{\varepsilon/2,\varepsilon/2}(t) \approx l^*_\varepsilon(t)$, which appears to be a good approximation (see also Example 8.1.5).

Lemma 8.1.3 *For all* $0 \leq t \leq n$ *and* $0 < \varepsilon < 1/2$

$$l^*_\varepsilon(t) \leq \hat{l}_\varepsilon(t, n).$$

Moreover, equality holds if $k_\varepsilon(t) = n$.

Proof: We first show that equality holds if $k_\varepsilon(t) = n$. By definition, $\hat{l}_\varepsilon(t,n)$ is the minimal l for which

$$F\left(\sqrt{2(n-t)} - 3(l+1/2)/\sqrt{2(n-t)}\right) \leq \varepsilon.$$

Hence, $\hat{l}_\varepsilon(t,n)$ is the minimal l for which $u_\varepsilon \geq \sqrt{2(n-t)} - 3(l+1/2)/\sqrt{2(n-t)}$. By definition, $l_{\alpha,\beta}(t)$ is the minimal value of l for which $u_\beta \geq \sqrt{2(k_\alpha(t)-t)} - 3(l+1/2)/\sqrt{2(k_\alpha(t)-t)}$. Theorem 8.1.2 states that $k_\alpha(t)$ is decreasing in α and at most n. So, if $k_\varepsilon(t) = n$ then $k_\alpha(t) = n$ for $0 < \alpha \leq \varepsilon$, and we have that $l_{\alpha,\varepsilon-\alpha}(t) = \hat{l}_{\varepsilon-\alpha}(t,n)$ for $0 < \alpha \leq \varepsilon$. Hence, $l^*_\varepsilon(t) = \min_{0<\alpha\leq\varepsilon} \hat{l}_{\varepsilon-\alpha}(t,n) = \hat{l}_\varepsilon(t,n)$, since $\hat{l}_\varepsilon(t,n)$ is decreasing in ε.

To show the inequality we notice that if $\alpha \downarrow 0$ then $u_\alpha \rightarrow -\infty$ and so $k_\alpha(t) = n$ if α is sufficiently small. Hence, $l_{\alpha,\varepsilon-\alpha}(t) \rightarrow \hat{l}_\varepsilon(t,n)$ as $\alpha \downarrow 0$, and we conclude that

$$l^*_\varepsilon(t) = \min_{\alpha+\beta=\varepsilon} l_{\alpha,\beta}(t) \leq \lim_{\alpha\downarrow 0} l_{\alpha,\varepsilon-\alpha}(t) = \hat{l}_\varepsilon(t,n).$$

□

The first example shows that it is possible that $l^*_\varepsilon(t) = \hat{l}_\varepsilon(t,n)$. The second example demonstrates that inequality $l^*_\varepsilon(t) < \hat{l}_\varepsilon(t,n)$ may hold in Lemma 8.1.3.

Example 8.1.4 Let $n = 1000$ and $t = 200$. Computer calculations give $P(L > 599|T = t, K = n) = 0.18798 \cdot 10^{-6}$, where the upper bound (8.3) gives $\varepsilon = 3.7267 \cdot 10^{-6}$. For $0 \leq \alpha \leq \varepsilon$ we have that $k_\alpha(t) = n$. Hence, $l^*_\varepsilon(t) = \hat{l}_\varepsilon(t,n) = 600$ by Lemma 8.1.3.

Example 8.1.5 Let $n = 1000$ and $t = 100$. Computer calculations give $P(L > 669|T = t, K = n) = 0.2553 \cdot 10^{-6}$, while the upper bound (8.3) gives $\varepsilon = 5.6967 \cdot 10^{-6}$. Let $\alpha = \beta = \varepsilon/2$. Then $k_\alpha(t) = 620$ and $l_{\alpha,\beta}(t) = 401$. Taking $\alpha = \varepsilon \cdot \theta$ and $\beta = \varepsilon \cdot (1-\theta)$ it turns out that $l_{\alpha,\beta}(t) = 401 \pm 2$ for $0.34 \leq \theta \leq 0.98$. We obtain the best bound $l^*_\varepsilon(t) = 399$ for $\theta \approx 0.74$. Hence, averaged over all raw quantum transmissions 399 upper bounds the number of bits leaking to Eve with probability at least $1 - \varepsilon$. We conclude that $l^*_\varepsilon(t) = 399 << 700 = \hat{l}_\varepsilon(t,n)$ (see also Figure 8.1).

As noted in [90] the binomial distribution can be approximated more closely by the Gaussian distribution than by the upper bound in (8.3). But, even if we replace F in Theorem 8.1.2 by the Gaussian distribution

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{-x^2/2} dx$$

we obtain almost the same bounds although $\varepsilon = 0.4453 \cdot 10^{-6}$ is a factor 13 smaller. We obtain $l_{\alpha,\beta}(t) = 401 \pm 2$ for $0.33 \leq \theta \leq 0.99$ and the best bound $l^*_\varepsilon(t) = 399$ is obtained by $\theta \approx 0.75$.

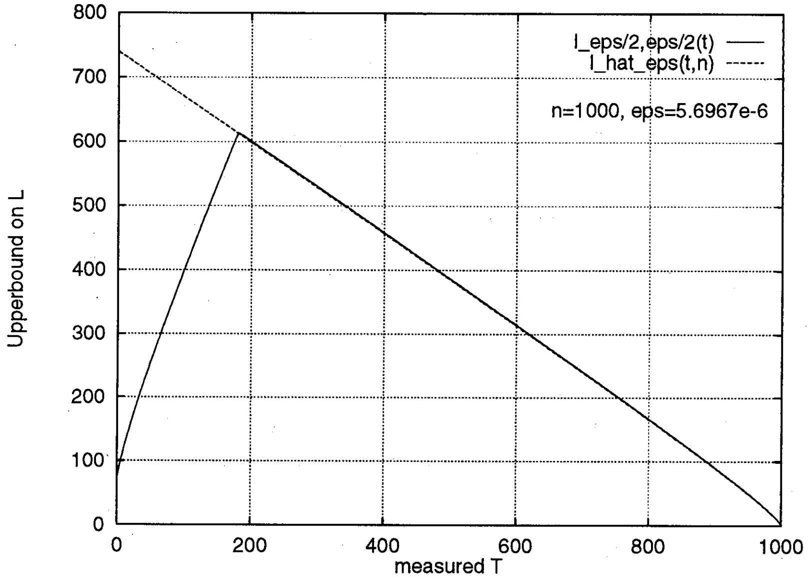


Figure 8.1: Upper bounds on the number of deterministic bits obtained by Eve.

An open problem is to strengthen Theorem 8.1.2 by using better upper bounds in (8.3), see [90], or by using the exact formula's in Lemma 8.1.1.

We conclude that Alice and Bob better take a worst case scenario into account where they estimate both K and L given T. We considered the situation in which Eve intercepts and resends a transmitted photon in rectilinear or circular base. An interesting exercise is to generalize the results in this section towards the situation in which Eve intercepts and resends a transmitted photon in any base of her choice.

8.2 Transmission Loss Manipulation

In this section we introduce the *BCC with tampering* (BCCT). Here, the enemy not only taps the wire but also actively tampers the signal communicated over the wire. We show that the legitimate users always have to take a certain worst case scenario into account.

Let A denote a random variable representing a parameter with which the BCC from Alice to Bob and Eve is described. For example, this parameter parameterizes into which extend the BCC is creating noise over the main channel. This parameter is partly unknown to Alice, Bob, and Eve. That is they know the distribution P_A of A. Further, suppose that before Alice and Bob start generating a secret key they have the means to measure the value

α taken on by A as accurately as they like. We assume that during the secret key generation the value of A does not change. Hence, Alice and Bob use the BCC $X \to (Y, Z)$ defined by $P_{Y,Z|X,A=\alpha}$ to generate a secret key.

This model is vulnerable for active tampering by Eve. Suppose that before and during the secret key generation Eve tampers by changing the parameter represented by A and suppose that initially (before generating a secret key) Alice and Bob are not aware of this. Let T be the random variable representing the tampering. Suppose it takes on value t before and during the secret key generation. Hence, Alice and Bob use $X' \to (Y', Z')$ defined by $P_{Y',Z'|X',T=t,A=\alpha}$. Suppose that there exists a function f such that

$$\begin{aligned} P_{Y'|X',T=t,A=\alpha} &= P_{Y|X,A=f(t,\alpha)} \text{ and} \\ P_{Z'|X',T=t,A=\alpha} &\neq P_{Z|X,A=f(t,\alpha)} \end{aligned} \tag{8.9}$$

and suppose further that

$$C_s(P_{Y',Z'|X',T=t,A=\alpha}) < C_s(P_{Y,Z|X,A=f(t,\alpha)}). \tag{8.10}$$

The property given by (8.9) states that the original BCC and the tampered BCC produce the same kind of noise over the main channel from Alice to Bob. The property given by (8.10) states that the original BCC and the tampered BCC produce a different kind of noise over the channel from Alice to Eve resulting in a gain towards Eve if she tampers.

Initially, Alice and Bob are not aware of Eve's tampering. Suppose Alice and Bob do not take tampering by Eve into account. Then they will think that they communicate over a BCC $X \to (Y, Z)$ defined by $P_{Y|X,A=\hat{\alpha}}$ for some value $\hat{\alpha} = f(t, \alpha)$. They will measure $\hat{\alpha}$ as accurate as they like before agreeing on their strategy to generate a secret key. During this measuring and during the generation of their secret key Alice and Bob will not notice anything strange because of the property given by (8.9). Hence, Alice and Bob use a strategy for generating a secret key over $X \to (Y, Z)$ at rate $C_s(P_{Y,Z|X,A=\hat{\alpha}})$. In reality, however, they use $X' \to (Y', Z')$ and their strategy will give Eve a non-negligible amount of information about the secret key since $C_s(P_{Y',Z'|X',T=t,A=\alpha}) < C_s(P_{Y,Z|X,A=\hat{\alpha}})$ where α is such that $\hat{\alpha} = f(t, \alpha)$, see (8.10). We conclude that Alice and Bob need to take tampering of Eve into account and we conclude that in this model Alice and Bob cannot detect the tampering of Eve, except possibly when Alice and Bob note that A takes on unlikely value according to distribution P_A.

We consider the following situation from [32, pp. 180–185,395]. If Alice wants to transmit a binary signal $\mathbf{a} \in \{0, 1\}^n$ then she converts it into a polar analog signal $a(t)$ with signal power S_A, which she transmits to Bob over a distortionless channel (i.e., the channel does not create noise) with length $l_A + l_B$ and attenuation coefficient α (the attenuation coefficient parameterizes into which extend the channel reduces the signal power). The first part of the main channel from Alice to the position where Eve taps the wire has length l_A, and, hence, the transmission loss L_A expressed in dB equals $(L_A)_{dB} = \alpha l_A$ (thus, $L_A = 10^{\alpha l_A/10}$). The second part of the main channel has length l_B and transmission loss $(L_B)_{dB} = \alpha l_B$. Bob uses an amplifier with noise figure n_B (the noise figure parameterizes into which extend the amplifier introduces noise) and power gain g_B (the power gain parameterizes into which extend the amplifier amplifies the signal power and noise power) to obtain an analog signal $b(t)$, which he converts to a binary signal $\mathbf{b} \in \{0,1\}^n$. The wire-tap channel of Eve causes transmission loss L_E. Eve uses an amplifier with noise figure n_E and power gain g_E, to obtain an analog signal $e(t)$, which she converts to a binary signal $\mathbf{e} \in \{0,1\}^n$. The noise caused in both amplifiers is additive white Gaussian noise with zero mean, independent of the signals $b(t)$ and $e(t)$. We assume that the electrical noise of the channels is negligible compared to the noise caused in both amplifiers. Suppose that Eve has inserted a tampering device which causes additional transmission loss $(L_T)_{dB} = \varepsilon_T(l_A + l_B)$ independent of her signal $e(t)$. Let T be the random variable representing ε_T.

Alice and Bob know S_A, n_B (which they can measure as accurate as they like), l_A, and l_B. Let A be the random variable representing the attenuation coefficient and suppose that Alice and Bob only know a probability distribution P_A of the attenuation coefficient. They know lower bounds $\bar{L}_E$ and $\bar{n}_E$ on L_E and n_E; $\bar{L}_E \leq L_E$ and $\bar{n}_E \leq n_E$. In the worst case for Alice and Bob $\bar{L}_E = L_E$ and $\bar{n}_E = n_E$. The tamper device introduces additional transmission loss L_T. Since, the exact value of the transmission loss over the main channel is unknown L_T is unknown. As we shall see Alice and Bob can not obtain any statistical information about L_T.

Suppose A takes on value α and T takes on value ε_T. The signal power of $b(t)$ is $S_A g_B / L_A L_T L_B$, and the corresponding noise power is $n_B g_B$. Hence, the signal to noise ratio $(S/N)_{AB}$ of the main channel equals

$$(S/N)_{AB} = S_A / L_A L_T L_B n_B = S_A / (n_B 10^{(\alpha+\varepsilon_T)(l_A+l_B)/10}).$$

This can be viewed as a decreasing function in $\alpha + \varepsilon_T$. Thus the channel from Alice to Bob with input $\mathbf{a}$ and output $\mathbf{b}$ is a $BSC(p_{AB}(\alpha + \varepsilon_T))$ with

$$p_{AB}(\alpha + \varepsilon_T) = Q(\sqrt{(S/N)_{AB}}),$$

that is a binary symmetric channel with cross-over probability $Q(\sqrt{(S/N)_{AB}})$, where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\lambda^2/2} d\lambda$. We notice that $p_{AB}(\alpha + \varepsilon_T)$ is increasing in $\alpha + \varepsilon_T$.

Suppose that A takes on value α. The signal power of $e(t)$ is $S_A g_E / L_A L_E$, and the corresponding noise power is $n_E g_E$. Hence, the signal to noise ratio of the channel from Alice to Eve $(S/N)_{AE}$ equals

$$(S/N)_{AE} = S_A / L_A L_E n_E \leq S_A / 10^{\alpha l_A/10} \bar{L}_E \bar{n}_E.$$

Thus the channel from Alice to Eve with input **a** and output **e** is a $BSC(p_{AE})$ with

$$p_{AE} = Q(\sqrt{(S/N)_{AE}}) \geq Q(\sqrt{S_A/10^{\alpha l_A/10}\bar{L}_E\bar{n}_E}) = \bar{p}_{AE}(\alpha).$$

Function $\bar{p}_{AE}(\alpha)$ is increasing in α.

We notice that all noise is generated in both amplifiers. Hence, the BCCT is equivalent to the binary symmetric BCC $Z \leftarrow X \rightarrow Y$, in which the main channel from Alice to Bob is a $BSC(p_{AB}(\alpha + \varepsilon_T))$ and the wire-tap channel is a $BSC(p_{AE})$ from Alice to Eve.

Suppose that prior to the secret key generation Alice transmits m zeroes to Bob. Let the random variable K_m be the number of 1s Bob receives over the main channel. Then we can derive the following known lemma.

Lemma 8.2.1

$$P\left(|p_{AB}(A+T) - K_m/m| \leq \varepsilon\right) \geq 1 - \frac{1}{4m\varepsilon^2}.$$

Proof: We derive by using Chebyshev's inequality

$$\begin{aligned}
&P\left(|p_{AB}(A+T) - K_m/m| \leq \varepsilon\right) \\
&= \int_\alpha P_A(\alpha) \int_{\varepsilon_T} P_{T|A}(\varepsilon_T|\alpha) \\
&\qquad P\left(|p_{AB}(A+T) - K_m/m| \leq \varepsilon | \, A = \alpha, T = \varepsilon_T\right) \, d\varepsilon_T d\alpha \\
&= \int_\alpha P_A(\alpha) \int_{\varepsilon_T} P_{T|A}(\varepsilon_T|\alpha) \\
&\qquad P\left(|p_{AB}(\alpha + \varepsilon_T) - K_m/m| \leq \varepsilon | \, A = \alpha, T = \varepsilon_T\right) \, d\varepsilon_T d\alpha \\
&\geq \int_\alpha P_A(\alpha) \int_{\varepsilon_T} P_{T|A}(\varepsilon_T|\alpha) \\
&\qquad \left(1 - \frac{p_{AB}(\alpha + \varepsilon_T)(1 - p_{AB}(\alpha + \varepsilon_T))}{m\varepsilon^2}\right) \, d\varepsilon_T d\alpha \\
&\geq \int_\alpha P_A(\alpha) \int_{\varepsilon_T} P_{T|A}(\varepsilon_T|\alpha) \left(1 - \frac{1}{4m\varepsilon^2}\right) \, d\varepsilon_T d\alpha \\
&= 1 - \frac{1}{4m\varepsilon^2}
\end{aligned}$$

from which the lemma follows.

□.

Hence, for m large enough Alice and Bob may approximate the value of $p_{AB}(A+T)$ by the value of K_m/m, which leads to an approximation of the value of $A+T$. More precisely, ($p_{AB}(y)$ is invertible and continuous)

$$P\left(|A + T - p_{AB}^{-1}(K_m/m)| \leq \varepsilon\right) \geq 1 - \frac{1}{4m\delta(\varepsilon)^2},$$

where $\delta(\varepsilon)\to 0$ as $\varepsilon\to 0$.

Suppose Alice and Bob measure $K_m = k$. Then $|A + T - p_{AB}^{-1}(k/m)| \leq \varepsilon$ with probability at least $1 - 1/4m\delta(\varepsilon)^2$. Hence, $p_{AB}(A + T) \leq p_{AB}(\varepsilon + p_{AB}^{-1}(k/m))$ with probability at least $1 - 1/4m\delta(\varepsilon)^2$. With probability $P(A \geq x)$ we have that $\bar{p}_{AE}(x) \leq \bar{p}_{AE}(A) \leq p_{AE}$. We conclude that with probability at least $(1 - 1/4m\delta(\varepsilon)^2)P(A \geq x)$ the worst-case scenario for Alice and Bob is a $BSC(p_{AB}(p_{AB}^{-1}(k/m)+\varepsilon))$ as main channel and a $BSC(\bar{p}_{AE}(x))$ as wire-tap channel. The BCCT is equivalent to the binary symmetric BCC $Z\leftarrow X\rightarrow Y$. Therefore, we have that the secrecy capacity of the worst-case scenario is equal to

$$h(\bar{p}_{AE}(x)) - h(p_{AB}(p_{AB}^{-1}(k/m) + \varepsilon)),$$

see Chapter 9 and [36]. We notice that a secret key generated by using a strategy based on the worst-case scenario is secret (for Eve) in the real situation.

The final conclusion is the following. Alice and Bob can not detect into which extend Eve tampers the noise generated by the main channel. In order to generate a secret key Alice and Bob need to take a worst-case scenario into account. They have to realize that k/m is an approximation of $\alpha + \varepsilon_T$ and not of α. Hence, k/m does not give any additional information about α than already known prior to the secret key generation. Therefore, Alice and Bob can only use P_A, which represents the knowledge about α known prior to the secret key generation, to find a proper worst-case scenario for Eve's eavesdropping channel: With probability at least $P(A \geq x)$ we have that $\bar{p}_{AE}(x) \leq p_{AE}$.

Chapter 9

On a Special Class of BCC

In this chapter based on [47] we show that Csiszár and Körner's characterization [36] of a discrete memoryless channel (DMC) $X \rightarrow Y$ as being less noisy than the DMC $X \rightarrow Z$ is equivalent to the condition that the mutual-information difference $I(X;Y) - I(X;Z)$ be a convex-$\cap$ function of the probability distribution for X. This result is used to obtain a simple determination of the capacity region of the broadcast channel with confidential messages (BCC), which is a DMC $X \rightarrow (Y, Z)$, when the DMC $X \rightarrow Y$ to the legitimate receiver is less noisy than the DMC $X \rightarrow Z$ to the enemy cryptanalyst and there is a probability distribution for X having strictly positive components that achieves capacity on both these channels. In particular, when these DMC's are both symmetric, then the secrecy capacity of the BCC is the difference of their capacities. It is further shown that the less-noisy condition in this result cannot be weakened to the condition that the DMC $X \rightarrow Y$ be more capable than the DMC $X \rightarrow Z$ in the sense of Csiszár and Körner [36].

9.1 Partial Orderings

In [68], Körner and Marton introduced two ways of partially ordering discrete memoryless channels with the same input alphabet. They defined a DMC $X \rightarrow Y$ to be *more capable* than a DMC $X \rightarrow Z$ in a manner they showed to be equivalent to the condition $I(X;Y) \geq I(X;Z)$ for every probability distribution on X. They defined a DMC $X \rightarrow Y$ to be *less noisy* than a DMC $X \rightarrow Z$ in a way that they showed to be equivalent to the condition that $I(U;Y) \geq I(U;Z)$ for every DMC $U \rightarrow X$ with finite input alphabet and for every probability distribution on U.

In [8], Bergmans defined the DMC $X \rightarrow Z$ to be a *degraded version* of the DMC $X \rightarrow Y$ to mean that there exists a DMC $Y \rightarrow Z$ (with probability distribution $P_{Z|Y}$) such that $X \rightarrow Z$ can be represented as the cascade of the channels $X \rightarrow Y$ and $Y \rightarrow Z$ (thus $P_{Z|X} = P_{Z|Y}P_{Y|X}$).

It is shown in [68] that being more capable is a strictly weaker condition than being less noisy in the sense that the latter implies the former and that being more noisy is a strictly weaker condition than being a degraded version.

In [36] the following theorem is proved.

Theorem 9.1.1 *If $X \to Y$ is less noisy than $X \to Z$, then the capacity region of the BCC $X \to (Y, Z)$ equals*

$$\left\{ (r,\delta) \;\middle|\; \begin{array}{l} r \geq 0, 0 \leq \delta \leq 1, \\ \textit{there exists a probability distribution } P_X \\ \textit{such that } r \leq I(X;Y) \textit{ and } r\delta \leq I(X;Y) - I(X;Z). \end{array} \right\}. \tag{9.1}$$

In particular, the secrecy capacity satisfies

$$C_s(P_{Y,Z|X}) = \max_{P_X} [I(X;Y) - I(X;Z)]. \tag{9.2}$$

Moreover, (9.2) also holds under the weaker condition that $X \to Y$ is more capable than $X \to Z$.

In Section 7.1 we have seen that for every BCC $X \to (Y, Z)$, the secrecy capacity satisfies

$$C_s(P_{Y,Z|X}) \geq C(P_{Y|X}) - C(P_{Z|X}). \tag{9.3}$$

In the sequel, we will say that the BCC $X \to (Y, Z)$ is *legitimate-users more capable* if $X \to Y$ is more capable than $X \to Z$. Similarly, a *legitimate-users less noisy* BCC will mean a BCC in which $X \to Y$ is less noisy than $X \to Z$, and *eavesdropper-degraded* BCC will mean a BCC in which $X \to Z$ is a degraded version of $X \to Y$. The degraded BCC is precisely the wire-tap channel model of Wyner [100].

In the next section we give a new characterization of the relation being less noisy. We show that for less noisy BCC's for which in addition both $X \to Y$ and $X \to Z$ are symmetric, $C_s(P_{Y,Z|X})$ equals the difference between the capacities of both channels. This generalizes a result by Leung [74], which states that for degraded BCC's in which both $X \to Y$ and $X \to Z$ are symmetric, $C_s(P_{Y,Z|X})$ equals $C(P_{Y|X}) - C(P_{Z|X})$. We show in Section 9.3 that the condition 'less noisy' in this new characterization cannot be replaced by 'more capable' by giving an example of a more capable BCC in which both $X \to Y$ and $X \to Z$ are symmetric but for which $C_s(P_{Y,Z|X})$ does not equal $C(P_{Y|X}) - C(P_{Z|X})$.

9.2 Less Noisy BCC's

We start with our main result, a new characterization of being less noisy.

Theorem 9.2.1 *The DMC $X \to Y$ is less noisy than the DMC $X \to Z$ if and only if $I(X;Y) - I(X;Z)$ is a convex-$\cap$ function of the input probability distribution P_X, i.e., for all α, $0 \le \alpha \le 1$, and all probability distributions P_X^a and P_X^b for X,*

$$\alpha f(P_X^a) + (1-\alpha) f(P_X^b) \le f(\alpha P_X^a + (1-\alpha) P_X^b)$$

where

$$f(P_X) = [I(X;Y) - I(X;Z)]_{P_X}$$

denotes the value of $I(X;Y) - I(X;Z)$ computed with the input probability distribution P_X.

Proof: For an arbitrary U with finite input alphabet $\mathcal{U}$, consider the Markov chain $U \to X \to (Y,Z)$. Each $u \in \mathcal{U}$ specifies a probability distribution P_X^u for X in the manner

$$P_X^u(x) = P_{X|U}(x|u), \; x \in \mathcal{X}.$$

We first note that

$$\begin{aligned} I(U;Y) &\overset{i)}{=} H(Y) - H(Y|U) = H(Y) - H(Y|X) \\ &\quad + H(Y|X) - H(Y|U) \\ &\overset{ii)}{=} H(Y) - H(Y|X) + H(Y|XU) - H(Y|U) \\ &\overset{iii)}{=} I(Y;X) - I(Y;X|U) \end{aligned}$$

where i) and iii) follow from the definition of mutual information, and where ii) follows from the fact that U, X, Y form a Markov chain so that

$$H(Y|X) - H(Y|XU) = I(U;Y|X) = 0.$$

From this and a similar derivation in which Y is replaced by Z, we infer that

$$I(U;Z) \le I(U;Y)$$

if and only if

$$I(X;Y|U) - I(X;Z|U) \le I(X;Y) - I(X;Z).$$

But

$$\begin{aligned} &I(X;Y|U) - I(X;Z|U) \\ &= \sum_{u \in U} P_U(u) \left[I(X;Y|U=u) - I(X;Z|U=u) \right] \\ &= \sum_{u \in U} P_U(u) \left[I(X;Y) - I(X;Z) \right]_{P_X^u}, \end{aligned}$$

and

$$I(X;Y) - I(X;Z) = [I(X;Y) - I(X;Z)]_{\sum\limits_{u \in U} P_U(u) P_X^u},$$

from which the theorem follows immediately.

□

From Theorems 9.1.1 and 9.2.1, we deduce that the secrecy capacity of a specific legitimate-users less noisy BCC can be found by standard nonlinear optimization techniques such as gradient search or maximization using the Kuhn-Tucker conditions [54, pp. 87–89]. In special cases, we can express the secrecy capacity explicitly as the difference of the capacities of the channels from Alice to Bob and Alice to Eve, respectively.

Theorem 9.2.2 *Let $X \to (Y, Z)$ be a BCC such that the DMC $X \to Y$ is less noisy than the DMC $X \to Z$ and such that there is a probability distribution P_X having all components strictly positive that maximizes both $I(X;Y)$ and $I(X;Z)$. Then*

$$C_s(P_{Y,Z|X}) = C(P_{Y|X}) - C(P_{Z|X}).$$

If both DMC's are symmetric then the uniform distribution maximizes both $I(X;Y)$ and $I(X;Z)$ [54, pp. 94].

Proof: Probability distribution P_X maximizes both $I(X;Y)$ and $I(X;Z)$. Since P_X has all components strictly positive it is a stationary point of both $I(X;Y)$ and $I(X;Z)$. Hence, P_X is a stationary point of $f(P_X) = [I(X;Y) - I(X;Z)]_{P_X}$. But as this difference has been shown to be convex-∩, it follows that P_X maximizes $I(X;Y) - I(X;Z)$.

□

9.3 More Capable BCC's

Theorem 9.2.2 generalizes a result of Leung [74, Theorem 4], namely that it holds under the stronger assumption that $X \to Z$ is a degraded version of $X \to Z$. We now present an example to show that in Theorem 9.2.2 the condition of being less noisy cannot be replaced by the weaker condition of being more capable. For $0 \leq p < q \leq 1/2$, let the symmetric DMC $X \to Y$ be defined by the transition matrix

$$\frac{1}{2}\begin{pmatrix} 1-p & p & 1-q & q \\ p & 1-p & q & 1-q \\ 1-q & q & 1-p & p \\ q & 1-q & p & 1-p \end{pmatrix}.$$

For $0 \leq r < 1/2$, let the symmetric DMC $X \to Z$ be defined by the transition matrix

$$\frac{1}{2}\begin{pmatrix} 1-r & 1-r & r & r \\ 1-r & 1-r & r & r \\ r & r & 1-r & 1-r \\ r & r & 1-r & 1-r \end{pmatrix}.$$

P_X :	$[I(X;Y)]_{P_X}$:	$[I(X;Z)]_{P_X}$:
$P_0 = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$	$1 - \frac{1}{2}(h(p) + h(q)) = C(P_{Y\mid X})$	$1 - h(r) = C(P_{Z\mid X})$
$P_1 = (\frac{1}{2}, \frac{1}{2}, 0, 0)$, $P_2 = (0, 0, \frac{1}{2}, \frac{1}{2})$	$1-$ $\frac{1}{2}(h(p) + h(q))$	0
$P_3 = (\frac{1}{2}, 0, \frac{1}{2}, 0)$, $P_4 = (0, \frac{1}{2}, 0, \frac{1}{2})$	$1 - \frac{1}{2}(p+q)h(\frac{p}{p+q}) -$ $\frac{1}{2}(2-p-q)h(\frac{1-q}{2-p-q})$	$1 - h(r)$
$P_5 = (\frac{1}{2}, 0, 0, \frac{1}{2})$, $P_6 = (0, \frac{1}{2}, \frac{1}{2}, 0)$	$1 - \frac{1}{2}(1+p-q)h(\frac{p}{1+p-q}) -$ $\frac{1}{2}(1-p+q)h(\frac{q}{1-p+q})$	$1 - h(r)$
(a, b, c, d)	?	$h((a+b)(1-2r)+r)$ $-h(r) =$ $h((c+d)(1-2r)+r)$ $-h(r)$

Table 9.1: Expressions of some mutual informations

In Table 9.1 some computations for these DMC's are summarized, where h denotes the binary entropy function

$$h(x) = -x \log x - (1-x)\log(1-x),\text{ for } 0 \le x \le 1$$

(note that $d/dx[h(x)] = \log((1-x)/x)$). From Table 9.1 we see that for the BCC $X \to (Y, Z)$

$$\begin{aligned} C_s &= C(P_{Y|X}) = [I(X;Y) - I(X;Z)]_{P_1} \\ &> [I(X;Y) - I(X;Z)]_{P_0} = C(P_{Y|X}) - C(P_{Z|X}) \end{aligned}$$

(because $r \neq 1/2$). Hence, $X \to Y$ is not less noisy than $X \to Z$ (see Theorem 9.2.2).

Now take $P_X = (a, b, c, d)$ and put $t = \min\{a+b, c+d\}$. Then either $a \ge t/2$ or $b \ge t/2$, and either $c \ge t/2$ or $d \ge t/2$. Thus there exists a probability distribution P'_X and there exists an i, $3 \le i \le 6$, such that $P_X = tP_i + (1-t)P'_X$. Because $I(X;Y)$ is a convex-$\cap$ function of the input probability distribution P_X, we conclude that

$$[I(X;Y)]_{P_X} \ge t\,[I(X;Y)]_{P_i} \ge S \cdot t$$

where S is defined as

$$\min\{[I(X;Y)]_{P_i} : 3 \le i \le 6\}.$$

Therefore a sufficient condition for

$$[I(X;Y)]_{P_X} \ge [I(X;Z)]_{P_X}$$

is

$$S \cdot t \ge h(t(1-2r)+r) - h(r) = [I(X;Z)]_{P_X} \qquad (9.4)$$

(see Table 9.1). This inequality holds with equality for $t = 0$. Hence, (9.4) holds if

$$d/dt[S \cdot t] = S \geq d/dt[h(t(1-2r)+r) - h(r)]$$

for $0 \leq t \leq 1$. Since

$$\begin{aligned} \frac{d}{dt}[h(t(1-2r)+r) - h(r)] &= (1-2r)\log\frac{1-(t(1-2r)+r)}{t(1-2r)+r} \\ &\leq (1-2r)\log\frac{1-r}{r} \longrightarrow 0, \text{ as } r \longrightarrow \frac{1}{2} \end{aligned}$$

and $S > 0$ (because $p \neq q$ and $p \neq 1-q$), there exists an r close enough to 1/2 such that (9.4) holds. Thus, for suitable r, $I(X;Y) \geq I(X;Z)$ for all input probability distributions P_X. This proves the existence of a legitimate-users more capable BCC $X \longrightarrow (Y,Z)$ such that $X \longrightarrow Y$ and $X \longrightarrow Z$ are symmetric DMC's and $C_s > C(P_{Y|X}) - C(P_{Z|X})$. We summarize the above in the following theorem.

Theorem 9.3.1 *There exists a legitimate-users more capable BCC* $X \longrightarrow (Y,Z)$ *such that* $X \longrightarrow Y$ *and* $X \longrightarrow Z$ *are symmetric DMC's and* $C_s(P_{Y,Z|X}) > C(P_{Y|X}) - C(P_{Z|X})$.

Chapter 10

Advantage Distillation

In this chapter based on [43] we consider the following scenario, which is called the *binary symmetric* BCC or BSBCC for short. Two persons, Alice and Bob, communicate to each other by means of a noisy channel from Alice to Bob and a (bidirectional) noiseless public channel. This noisy channel is called the main channel. An enemy Eve taps the main channel using a binary symmetric wire-tap channel with error probability e_E. The first part of the main channel from Alice to the position where Eve made a connection to her wire-tap channel is a BSC(e_A), a binary symmetric channel with error probability e_A. The second part of the main channel from that position to Bob is a BSC(e_B). Suppose Alice transmits bit X over the main channel to Bob. Then Bob receives $X + A + B$, where A is a noise bit produced by the BSC(e_A) and B is a noise bit produced by the BSC(e_B). Eve will receive $X + A + E$, where bit E is a noise bit produced by her wire-tap channel, a BSC(e_E). By using channel rotation as described in Example 7.2.3 we can achieve the situation in which $e_A \geq e_B$.

We discuss the advantage distillation phase, see Subsection 7.2.1. We describe and generalize Maurer's reliability estimation technique [82] in Section 10.1. Section 10.2 contains the main contribution where we generalize the elegant efficiency improvement of Gander and Maurer [55].

10.1 Reliability Estimation

Maurer suggests in [82] to use the following technique which he calls reliability estimation. Alice and Bob start agreeing publicly upon a binary linear code $\mathcal{C}$ of dimension k and length n. To transmit a message of k bits Alice selects the unique code word $V^n \in \mathcal{C}$ representing the message, and she continues executing the following protocol, which we denote by $P(\mathcal{C})$, see Table 10.1. She chooses randomly a codeword $X^n \in \mathcal{C}$ which she transmits over the main channel to Bob. Then Bob receives a vector $X^n + A^n + B^n$ and Eve receives a vector $X^n + A^n + E^n$. Here and in the remainder of this paper A^n, B^n, and

E^n are noise vectors produced by n uses of the BSC(e_A), the BSC(e_B), and the BSC(e_E) respectively. Now Bob makes a reliability decision based on the Hamming distance between the received word and code $\mathcal{C}$. If this Hamming distance is small enough Bob calls his received word reliable. We consider the case where Bob's received word is reliable if and only if it is a code word, that is $X^n + A^n + B^n \in \mathcal{C}$ (the Hamming distance of the received word to the code equals 0). We notice that $X^n + A^n + B^n \in \mathcal{C}$ if and only if $A^n + B^n \in \mathcal{C}$ since $X^n \in \mathcal{C}$ and $\mathcal{C}$ is linear. Bob lets Alice know whether his received word is reliable or not. To this purpose he uses the public channel. Thus Eve receives this information as well. If Bob does not receive a reliable word then Alice chooses randomly a new code word $X^n \in \mathcal{C}$ which she transmits over the main channel to Bob who replies publicly whether his new received word is reliable enough or not. They repeat these actions until Bob receives a reliable word $X^n + A^n + B^n$. Then Bob chooses randomly a vector $\hat{X}^n \in \mathcal{C}$ and he transmits $\hat{X}^n + (X^n + A^n + B^n)$ over the public channel to Alice. At this moment X^n is known to Alice since she choose this vector herself. We notice that V^n is the code word representing the message of k bits Alice wants to transmit to Bob. Alice adds $X^n + V^n$ to the public message sent by Bob. She obtains $V^n + \hat{X}^n + A^n + B^n$ which she transmits over the public channel to Bob. He adds $\hat{X}^n$ and obtains $V^n + A^n + B^n$.

Protocol $P(\mathcal{C})$ creates a new BCC K from Alice to Bob and Eve, see Table 10.2. If Alice wants to transmit over BCC K a message of k information bits represented by $V^n \in \mathcal{C}$ then Bob receives $V^n + A^n + B^n$, where $A^n + B^n \in \mathcal{C}$. Eve receives over the first part of the main channel cascaded with her wire-tap channel $X^n + A^n + E^n$, and she receives by public communication $\hat{X}^n + X^n + A^n + B^n$, $V^n + \hat{X}^n + A^n + B^n$, and the knowledge that $A^n + B^n \in \mathcal{C}$. Vectors $\hat{X}^n$ and X^n are independent and uniformly chosen. Therefore Eve's information about V^n is the vector $(X^n + A^n + E^n) + (\hat{X}^n + X^n + A^n + B^n) + (V^n + \hat{X}^n + A^n + B^n) = V^n + A^n + E^n$ together with the knowledge that $A^n + B^n \in \mathcal{C}$, see Example 7.2.3 for a more precise argumentation. Therefore w.l.o.g. Eve receives over channel K vector $V^n + A^n + E^n$ and the knowledge that $A^n + B^n \in \mathcal{C}$.

The knowledge of $A^n + B^n \in \mathcal{C}$ gives Eve not as much additional information about V^n as it gives Bob additional information about V^n. The reason for this is the fact that the noise vectors $A^n + B^n$ and $A^n + E^n$ are into certain extend independent of each other (because B^n and E^n are independent). Therefore the knowledge whether $A^n + B^n \in \mathcal{C}$ or not gives more information about $A^n + B^n$ than information about $A^n + E^n$. This explains why the protocol achieves more coding gain towards Bob than coding gain towards Eve (Eve's advantage becomes smaller).

The expected number of bits transmitted over the main channel in order to transmit a message of k bits over the new BCC K equals

$$R(\mathcal{C}) = n/P(A^n + B^n \in \mathcal{C}).$$

Protocol $P(\mathcal{C})$:

- In order to transmit a message of k bits Alice selects the unique code word $V^n \in \mathcal{C}$ representing the message.
- Alice repeats until she receives over the public channel an acknowledgement of Bob the following procedure:
  - Alice chooses randomly $X^n \in \mathcal{C}$ which she transmits over the main channel to Bob.
  - Bob receives $X^n+A^n+B^n$ and Eve receives $X^n+A^n+E^n$.
  - Only if $X^n+A^n+B^n \in \mathcal{C}$ ($\equiv A^n+B^n \in \mathcal{C}$) Bob transmits over the public channel an acknowledgement to Alice. In that case Eve receives an acknowledgement as well, and hence the information that $A^n + B^n \in \mathcal{C}$.
- Bob chooses randomly $\hat{X}^n \in \mathcal{C}$ and computes $\hat{X}^n+(X^n+A^n+B^n)$ which he transmits over the public channel to Alice. Eve receives $\hat{X}^n + (X^n + A^n + B^n)$ as well.
- Alice computes $V^n + X^n + (\hat{X}^n + X^n + A^n + B^n) = V^n + \hat{X}^n + A^n + B^n$ which she transmits over the public channel to Bob. Eve receives $V^n + \hat{X}^n + A^n + B^n$ as well.
- Bob computes $\hat{X}^n + (V^n + \hat{X}^n + A^n + B^n) = V^n + A^n + B^n$ and he disregards all previously sent messages.

Table 10.1: Protocol $P(\mathcal{C})$

Channel K:

If Alice wants to transmit over channel K a message of k information bits represented by $V^n \in \mathcal{C}$ then Bob receives $V^n + A^n + B^n$, where $A^n + B^n \in \mathcal{C}$, and Eve receives $V^n + A^n + E^n$ together with the knowledge that $A^n + B^n \in \mathcal{C}$.

Table 10.2: The BCC K created by $P(\mathcal{C})$

Channel K is a discrete memoryless channel defined by the following transition probabilities. The probability that Bob receives $\mathbf{b}$ if Alice transmits $\mathbf{v} \in \mathcal{C}$ over BCC K equals

$$p_{B|A}(\mathbf{b}|\mathbf{v}) = \frac{P(A^n + B^n = \mathbf{v} + \mathbf{b})}{P(A^n + B^n \in \mathcal{C})}, \text{ for } \mathbf{b} \in \mathcal{C}.$$

The probability that Eve receives $\mathbf{e}$ if Alice transmits $\mathbf{v} \in \mathcal{C}$ over BCC K equals

$$p_{E|A}(\mathbf{e}|\mathbf{v}) = \frac{P(A^n + E^n = \mathbf{v} + \mathbf{e}, A^n + B^n \in \mathcal{C})}{P(A^n + B^n \in \mathcal{C})}.$$

Further

$$P(A^n + B^n = \mathbf{d}) = \prod_{i=1}^{n} \sum_{a \in \{0,1\}} P(A = a)P(B = a + d_i) \text{ and}$$

$$P(A^n + E^n = \mathbf{d}, A^n + B^n \in \mathcal{C}) =$$

$$\sum_{\mathbf{c} \in \mathcal{C}} \prod_{i=1}^{n} \sum_{a \in \{0,1\}} P(A = a)P(E = a + d_i)P(B = a + c_i),$$

where $\mathbf{d} = (d_1, \ldots, d_n)$, $\mathbf{c} = (c_1, \ldots, c_n)$, $P(A = 1) = e_A$, $P(B = 1) = e_B$, and $P(E = 1) = e_E$.

In Section 7.1 we have seen that the secrecy capacity of a BCC from Alice to Bob and Eve is at least the difference between the capacity of the channel from Alice to Bob and the channel from Alice to Eve. Since the channel from Alice to Bob and the channel from Alice to Eve are symmetric in the situation of BCC K, the capacities of both channels are achieved if $V^n \in \mathcal{C}$ is uniformly selected by Alice. We infer that the secrecy capacity of K is at least

$$I(\mathcal{C}) = \sum_{\mathbf{c} \in \mathcal{C}} \frac{P(A^n + B^n = \mathbf{c})}{P(A^n + B^n \in \mathcal{C})} \log \frac{P(A^n + B^n = \mathbf{c})}{P(A^n + B^n \in \mathcal{C})} -$$

$$\sum_{\mathbf{d} \in \mathbb{F}_2^n} \frac{P\left(\begin{array}{c} A^n + E^n = \mathbf{d}, \\ A^n + B^n \in \mathcal{C} \end{array}\right)}{P(A^n + B^n \in \mathcal{C})} \log \frac{P(A^n + E^n = \mathbf{d}, A^n + B^n \in \mathcal{C})}{P(A^n + E^n \in \mathbf{d} + \mathcal{C}, A^n + B^n \in \mathcal{C})}.$$

We conclude that the secrecy capacity with public discussion of the BSBCC is at least

$$I(\mathcal{C})/R(\mathcal{C}).$$

Example 10.1.1 [82] Let $\mathcal{C}^n = \{\mathbf{0}, \mathbf{1}\}$ be the repetition code with code word length n. Let $e = e_A(1 - e_B) + (1 - e_A)e_B = P(A + B = 1)$, $\alpha_{i,j} =$

$\sum_{a \in \{0,1\}} P(A = a)P(E = a + j)P(B = a + i)$, and $p_w^n = \alpha_{1,1}^w \alpha_{1,0}^{n-w} + \alpha_{0,1}^w \alpha_{0,0}^{n-w}$ for $0 \le w \le n$. Then

$$\begin{aligned} R(\mathcal{C}^n) &= \frac{n}{e^n + (1-e)^n} \text{ and} \\ I(\mathcal{C}^n) &= -h\left(\frac{e^n}{e^n + (1-e)^n}\right) + \\ & \sum_{w=0}^{n} \binom{n}{w} \frac{p_w^n}{e^n + (1-e)^n} h\left(\frac{p_w^n}{p_w^n + p_{n-w}^n}\right). \end{aligned}$$

It is possible to generalize the reliability estimation technique as follows. We notice that $A^n + B^n \in \mathcal{C}$ if and only if $(A^n + B^n)H = \mathbf{0}$ where H is the parity check matrix of $\mathcal{C}$. Suppose that Bob always transmits the syndrome $S^{n-k} = (A^n + B^n)H$ to Alice over the public channel instead of letting Alice know whether $A^n + B^n \in \mathcal{C}$ or not. The proposed change in protocol $P(\mathcal{C})$ leads to the creation of a channel K for which the following holds. If Alice transmits over channel K a message of k information bits represented by $V^n \in \mathcal{C}$ then Bob receives $V^n + A^n + B^n$ and $(A^n + B^n)H$, Eve receives $V^n + A^n + E^n$ and $(A^n + B^n)H$, and Alice receives $(A^n + B^n)H$. Suppose that Alice wants to transmit messages of k information bits each represented by $V_{\mathbf{s},i}^n$, $\mathbf{s} \in \mathbb{F}_2^{n-k}$, $i \in \{0, 1, \ldots\}$, as follows. Alice chooses randomly a code word $R^n \in \mathcal{C}$ which she transmits over channel K. If $\mathbf{s} = (A^n + B^n)H$ she selects a not yet transmitted message $V_{\mathbf{s},i}^n$ for some i, and she transmits over the public channel $R^n + V_{\mathbf{s},i}^n$ to Bob (and Eve). Bob receives $R^n + V_{\mathbf{s},i}^n$ and channel K outputted $R^n + A^n + B^n$ and $\mathbf{s} = (A^n + B^n)H$ to him. He adds $R^n + V_{\mathbf{s},i}^n$ and $R^n + A^n + B^n$ resulting in $V_{\mathbf{s},i}^n + A^n + B^n$. In this way channel K can be viewed as a collection of channels $K(\mathbf{s})$, $\mathbf{s} \in \mathbb{F}_2^{n-k}$, for which the following holds. If Alice transmits over channel $K(\mathbf{s})$ a message of k information bits represented by $V^n \in \mathcal{C}$ then Bob receives $V^n + A^n + B^n$ where $\mathbf{s} = (A^n + B^n)H$ and Eve receives $V^n + A^n + E^n$ and the knowledge that $(A^n + B^n)H = \mathbf{s}$. The expected number of bits transmitted over the main channel in order to transmit a message of k bits over channel $K(\mathbf{s})$ equals

$$R(\mathcal{C}, \mathbf{s}) = n / P(\mathbf{s} = (A^n + B^n)H),$$

and the secrecy capacity of BCC $K(\mathbf{s})$ is at least

$$I(\mathcal{C}, \mathbf{s}) = \sum_{\mathbf{c} \in \mathcal{C}} \frac{P(A^n + B^n = \mathbf{c})}{P(\mathbf{s} = (A^n + B^n)H)} \log \frac{P(A^n + B^n = \mathbf{c})}{P(\mathbf{s} = (A^n + B^n)H)} -$$

$$\sum_{\mathbf{d} \in \mathbb{F}_2^n} \frac{P\begin{pmatrix} A^n + E^n = \mathbf{d}, \\ \mathbf{s} = (A^n + B^n)H \end{pmatrix}}{P(\mathbf{s} = (A^n + B^n)H)} \log \frac{P\begin{pmatrix} A^n + E^n = \mathbf{d}, \\ \mathbf{s} = (A^n + B^n)H \end{pmatrix}}{P\begin{pmatrix} A^n + E^n \in \mathbf{d} + \mathcal{C}, \\ \mathbf{s} = (A^n + B^n)H \end{pmatrix}}.$$

We notice that $R(\mathcal{C}) = R(\mathcal{C}, \mathbf{0})$ and $I(\mathcal{C}) = I(\mathcal{C}, \mathbf{0})$. We conclude that the secrecy capacity with public discussion of the BSBCC is at least

$$\sum_{\mathrm{s} \in \mathbb{F}_2^n} \max\{0, I(\mathcal{C}, \mathrm{s})/R(\mathcal{C}, \mathrm{s})\}.$$

10.2 Efficiency Improvement

In this section we improve the lower bound $I(\mathcal{C})/R(\mathcal{C})$ by generalizing the smart and simple idea presented by Gander and Maurer [55]. Firstly, we introduce some notation. Secondly, we describe a protocol leading to the improved bound. Finally, we discuss some examples.

We call K an *appropriate* channel from Alice to Bob and Eve for code $\mathcal{C}$ of dimension k with word length n if K results from a protocol describing communication between Alice and Bob over the main channel and public channel, and if for K the following holds. If Alice transmits over channel K a message of k information bits represented by $V^n \in \mathcal{C}$ then Bob receives $V^n + A^n + B^n$ with $A^n + B^n \in \mathcal{C}$ and Eve receives $V^n + A^n + E^n$ and the knowledge that $A^n + B^n \in \mathcal{C}$. Let K be an appropriate channel for $\mathcal{C}$. Then $R(K)$ is defined as the expected number of bits transmitted over the main channel in order to transmit a message of k bits over channel K. From the analysis done in the previous section we infer that an appropriate channel K for $\mathcal{C}$ leads to the lower bound $\bar{C}_s \geq I(\mathcal{C})/R(K)$. We notice that protocol $P(\mathcal{C})$ produces an appropriate channel K for $\mathcal{C}$ for which $R(K) = R(\mathcal{C})$.

We call codes $\mathcal{C}_i$, $1 \leq i \leq h$, with code word lengths n_i, $1 \leq i \leq h$, a *partitioning* of code $\mathcal{C}$ with code word length n if $n = \sum_{i=1}^{h} n_i$ and if for all $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$ and for all $1 \leq i \leq h$ vector

$$(c_{m_i}, \ldots, c_{m_{i+1}-1}) \in \mathcal{C}_i,$$

where $m_i = \sum_{j=1}^{i-1} n_j$. In other words code $\mathcal{C}_i$ is the restriction of $\mathcal{C}$ to coordinates $m_i, \ldots, m_{i+1} - 1$. In what follows $\mathcal{C}_i$, $1 \leq i \leq h$, being a partitioning of $\mathcal{C}$ is denoted by $\mathcal{C}_1 \cdot \mathcal{C}_2 \cdots \mathcal{C}_h \models \mathcal{C}$. We write $\mathcal{C}^h$ for short for $\mathcal{C}_1 \cdot \mathcal{C}_2 \cdots \mathcal{C}_h$ if $\mathcal{C}_1 = \ldots = \mathcal{C}_h = \mathcal{C}$.

Example 10.2.1 Let $\mathcal{C}[]$ be the binary alphabet $\{0, 1\}$, and let $\mathcal{C}[r_1, \ldots, r_i]$ be recursively defined by

$$\mathcal{C}[r_1, \ldots, r_{i+1}] = \left\{ \left(\mathbf{c}^1, \ldots, \mathbf{c}^{r_{i+1}-1}, \sum_{j=1}^{r_{i+1}-1} \mathbf{c}^j \right) \middle| \, \mathbf{c}^1, \ldots, \mathbf{c}^{r_{i+1}-1} \in \mathcal{C}[r_1, \ldots, r_i] \right\}.$$

Then $\mathcal{C}[r_1, \ldots, r_i]^{r_{i+1}} \models \mathcal{C}[r_1, \ldots, r_{i+1}]$. We notice that $\mathcal{C}[r_1 = 2, \ldots, r_i = 2]$ is the repetition code of length 2^i and that $\mathcal{C}[r]$ is the parity check code of length r.

For $1 \leq i \leq h$ let K_i be an appropriate channel for code $\mathcal{C}_i$. Let $\mathcal{C}_1 \cdots \mathcal{C}_h \models \mathcal{C}$. For $1 \leq i \leq h$ let n_i be the code word length of $\mathcal{C}_i$, and let n be the code word length of $\mathcal{C}$. We will present a protocol which constructs an appropriate channel K for $\mathcal{C}$ for which in general $R(K) < R(\mathcal{C})$.

Suppose that Alice wants to transmit $V^n = (V^{n_1}, \ldots, V^{n_h}) \in \mathcal{C}$. Then she chooses randomly $X^n = (X^{n_1}, \ldots, X^{n_h}) \in \mathcal{C}$, and she transmits vector X^{n_i} over channel K_i for each $1 \leq i \leq h$. Then Bob receives $V^{n_i} + A^{n_i} + B^{n_i}$ with $A^{n_i} + B^{n_i} \in \mathcal{C}_i$ for $1 \leq i \leq h$ and Eve receives $V^{n_i} + A^{n_i} + E^{n_i}$ and the knowledge that $A^{n_i} + B^{n_i} \in \mathcal{C}_i$ for $1 \leq i \leq h$, see Table 10.2. The concatenation of Bob's received words $V^n + A^n + B^n = (V^{n_1} + A^{n_1} + B^{n_1}, \ldots, V^{n_h} + A^{n_h} + B^{n_h})$ is called reliable by Bob if and only if $V^n + A^n + B^n \in \mathcal{C}$. Bob lets Alice publicly know whether the concatenation of his received words is reliable or not. If Bob does not receive a reliable word then Alice chooses randomly a new code word $X^n \in \mathcal{C}$ which she transmits over the channels K_i to Bob who replies publicly whether his new concatenation of received words is reliable enough or not. They repeat these actions until Bob receives a reliable word $X^n + A^n + B^n$. Then Bob chooses randomly a vector $\hat{X}^n \in \mathcal{C}$ and he transmits $\hat{X}^n + (X^n + A^n + B^n)$ over the public channel to Alice. Alice adds $X^n + V^n$ to the public message sent by Bob. She obtains $V^n + \hat{X}^n + A^n + B^n$ which she transmits over the public channel to Bob. He adds $\hat{X}^n$ and obtains $V^n + A^n + B^n$. We notice that the last part of this protocol equals the last part of protocol $P(\mathcal{C})$. Again, w.l.o.g. Eve receives over the created channel K vectors $V^{n_i} + A^{n_i} + E^{n_i}$ and the knowledge that $A^{n_i} + B^{n_i} \in \mathcal{C}_i$ for $1 \leq i \leq h$, and she receives the knowledge that $A^n + B^n \in \mathcal{C}$. From $\mathcal{C}_1 \cdots \mathcal{C}_h \models \mathcal{C}$ we infer that $A^n + B^n \in \mathcal{C}$ implies that $A^{n_i} + B^{n_i} \in \mathcal{C}_i$ for $1 \leq i \leq h$. Thus w.l.o.g. Eve receives over channel K vector $V^n + A^n + E^n$ and the knowledge that $A^n + B^n \in \mathcal{C}$. Hence, the described protocol creates an appropriate channel K for $\mathcal{C}$.

The probability that the concatenation of Bob's received words is reliable equals

$$P(A^n + B^n \in \mathcal{C} | A^{n_i} + B^{n_i} \in \mathcal{C}_i \text{ for } 1 \leq i \leq h).$$

Hence, $R(K)$ equals $\sum_{i=1}^{h} R(K_i)$ divided by this probability. We notice that $A^{n_i} + B^{n_i}$, $1 \leq i \leq h$, are independent random variables and we notice that $A^n + B^n \in \mathcal{C}$ implies that $A^{n_i} + B^{n_i} \in \mathcal{C}_i$ for $1 \leq i \leq h$. Hence,

$$\begin{aligned} &P(A^n + B^n \in \mathcal{C} | A^{n_i} + B^{n_i} \in \mathcal{C}_i \text{ for } 1 \leq i \leq h) \\ &= \frac{P(A^n + B^n \in \mathcal{C}, A^{n_i} + B^{n_i} \in \mathcal{C}_i \text{ for } 1 \leq i \leq h)}{P(A^{n_i} + B^{n_i} \in \mathcal{C}_i \text{ for } 1 \leq i \leq h)} \\ &= \frac{P(A^n + B^n \in \mathcal{C})}{\prod_{i=1}^{h} P(A^{n_i} + B^{n_i} \in \mathcal{C}_i)}. \end{aligned}$$

From this we obtain the following relation

$$R(K) = \frac{\prod_{i=1}^{h} P(A^{n_i} + B^{n_i} \in \mathcal{C}_i) \sum_{i=1}^{h} R(K_i)}{P(A^n + B^n \in \mathcal{C})}.$$

W.lo.g. $R(K_i) \leq R(\mathcal{C}_i)$ (e.g. $P(\mathcal{C}_i)$ results into an appropriate channel K_i for $\mathcal{C}_i$ with $R(K_i) = R(\mathcal{C}_i)$). We notice that if $h > 1$ and if there exists an i such that $\mathcal{C}_i \neq \mathbb{F}_2^{n_i}$ then $R(K) < R(\mathcal{C})$. If $\mathcal{C}$ has minimal Hamming distance ≥ 3 then there exists a partitioning $\mathcal{C}_1 \cdots \mathcal{C}_h \models \mathcal{C}$ with $h > 1$ and $\mathcal{C}_i \neq \mathbb{F}_2^{n_i}$ for some $1 \leq i \leq h$. We conclude that if $\mathcal{C}$ has minimal Hamming distance ≥ 3 then there exists a partitioning of $\mathcal{C}$ leading to the lower bound $I(\mathcal{C})/R(K)$ on the secrecy capacity with public discussion of the BSBCC which improves the lower bound $I(\mathcal{C})/R(\mathcal{C})$.

Example 10.2.2 We continue with Example 10.2.1. Suppose that there exists an appropriate channel $K[r_1, \ldots, r_i]$ for $\mathcal{C}[r_1, \ldots, r_i]$. Since $\mathcal{C}[r_1, \ldots, r_i]^{r_{i+1}} \models \mathcal{C}[r_1, \ldots, r_{i+1}]$ there exists an appropriate channel $K[r_1, \ldots, r_{i+1}]$ for $\mathcal{C}[r_1, \ldots, r_{i+1}]$ such that

$$R(K[r_1, \ldots, r_{i+1}]) = \frac{r_{i+1} P(A^{n_i} + B^{n_i} \in \mathcal{C}[r_1, \ldots, r_i])^{r_{i+1}} R(K[r_1, \ldots, r_i])}{P(A^{n_{i+1}} + B^{n_{i+1}} \in \mathcal{C}[r_1, \ldots, r_{i+1}])},$$

where $n_i = \prod_{j=1}^{i} r_j$ is the code word length of $\mathcal{C}[r_1, \ldots, r_i]$. By induction $(R(K[]) = 1)$

$$\begin{aligned} R(K[r_1, \ldots, r_i]) &= \frac{n_i \prod_{j=1}^{i-1} P(A^{n_j} + B^{n_j} \in \mathcal{C}[r_1, \ldots, r_j])^{r_{j+1}-1}}{P(A^{n_i} + B^{n_i} \in \mathcal{C}[r_1, \ldots, r_i])} \\ &\ll \frac{n_i}{P(A^{n_i} + B^{n_i} \in \mathcal{C}[r_1, \ldots, r_i])} \\ &= R(\mathcal{C}[r_1, \ldots, r_i]). \end{aligned}$$

Example 10.2.3 We continue with Example 10.1.1. We notice that $\mathcal{C}^{\lfloor n/2 \rfloor} \cdot \mathcal{C}^{\lceil n/2 \rceil} \models \mathcal{C}^n$. Suppose that there exists an appropriate channel $K^{\lfloor n/2 \rfloor}$ for $\mathcal{C}^{\lfloor n/2 \rfloor}$ and suppose that there exists an appropriate channel $K^{\lceil n/2 \rceil}$ for $\mathcal{C}^{\lceil n/2 \rceil}$. Then there exists an appropriate channel K^n for $\mathcal{C}^n$ such that $R(K^n) = q_{\lfloor n/2 \rfloor} q_{\lceil n/2 \rceil} (R(K^{\lfloor n/2 \rfloor}) + R(K^{\lceil n/2 \rceil}))/q_n$, where $q_n = P(A^n + B^n \in \mathcal{C}^n) = e^n + (1-e)^n$.

By using induction we obtain $R(K^{2^i}) = (2^i \prod_{j=1}^{i-1} q_{2^j})/q_{2^i}$, which is the result presented by Gander and Maurer [55]. We can simplify this formula as follows

$$\begin{aligned} \prod_{j=1}^{i-1} q_{2^j} &= \prod_{j=0}^{i-1} \left(e^{2^j} + (1-e)^{2^j} \right) \\ &= \sum_{a_0 \in \{0,1\}} \cdots \sum_{a_{i-1} \in \{0,1\}} e^{\sum_{j=0}^{i-1} (1-a_j) 2^j} (1-e)^{\sum_{j=0}^{i-1} a_j 2^j} \\ &= e^{2^i - 1} \sum_{j=0}^{2^i - 1} \left(\frac{1-e}{e} \right)^j \\ &= \left((1-e)^{2^i} - e^{2^i} \right) / ((1-e) - e). \end{aligned}$$

Hence, $R(K^{2^i}) \approx 2^i/|1-2e| \ll 2^i/|(1-e)^{2^i}+e^{2^i}| = R(\mathcal{C}^{2^i})$. This shows the enormous efficiency improvement realized by Gander and Maurer.

Bibliography

[1] R. Ahlswede and I. Csiszár. "Common randomness in information theory and cryptography – Part I: secret sharing". *IEEE Trans. Inform. Theory*, Vol. IT-39(4):1121–1132, July 1993.

[2] M. Atici. "Optimal information and average information rates of the connected graphs on six vertices". Master's thesis, University of Nebraska, May 1994.

[3] B. Awerbuch, B. Chor, S. Goldwasser, and S. Micali. "Veriable secret sharing and achieving simultaneity in the presence of faults". In *Proceedings of the 26th Annual IEEE Symposium of Foundations of Computer Science*, pages 383–395. IEEE, New York, 1986.

[4] P. Beguin and A. Cresti. "General short computational secret sharing schemes". In *Adv. in Cryptology – EUROCRYPT '95, Lecture Notes in Comput. Sci.*, volume 921, pages 194–208, 1995.

[5] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. "Experimental quantum cryptography". *J. Cryptology*, 5:3–28, 1992.

[6] C.H. Bennett, G. Brassard, C. Crépeau, and U.M. Maurer. "Generalized privacy amplification". *IEEE Trans. Inform. Theory*, Vol. IT-41(6):1915–1923, 1995.

[7] C.H. Bennett, G. Brassard, and J.-M. Robert. "Privacy amplification by public discussion". *SIAM J. Comput.*, 17(2):210–229, April 1988.

[8] P.P. Bergmans. "Coding theorem for broadcast channels with degraded components". *IEEE Trans. Inform. Theory*, Vol. IT-19:197–207, 1973.

[9] M. Bertilsson. *"Linear Codes and Secret Sharing".* PhD thesis, Linköping University, 1993.

[10] M. Bertilsson and I. Ingemarsson. "A construction of practical secret sharing schemes using linear block codes". In *Adv. in Cryptology – AUSCRYPT '92, Lecture Notes in Comput. Sci.*, volume 718, pages 67–79, 1993.

[11] A. Beutelspacher. "How to say no". In *Adv. in Cryptology – Proceedings of EUROCRYPT '89, Lecture Notes in Comput. Sci.*, volume 434, pages 491–496, 1990.

[12] G. R. Blakley. "Safeguarding cryptographic keys". In *Proc. AFIPS 1979 Nat. Computer Conf.*, volume 48, pages 313–317. New York, June 1979.

[13] G.R. Blakley and G.A. Kabatianskii. "Linear algebra approach to secret sharing schemes". In *Error Control, Cryptology, and Speech Compression, Lecture Notes in Comput. Sci.*, volume 829, pages 33–40, 1994. It also appeared in the PreProceedings of the Workshop on Information Protection, Moscow, December, 1993.

[14] G.R. Blakley and C. Meadows. "Security of ramp schemes". In *Adv. in Cryptology – CRYPTO '84, Lecture Notes in Comput. Sci.*, volume 196, pages 242–268, 1985.

[15] C. Blundo. "Secret sharing schemes for access structures based on graphs". Tesi di Laurea, 1991. (in Italian).

[16] C. Blundo, A. Cresti, A. De Santis, and U. Vaccaro. "Fully dynamic secret sharing schemes". *Theoretical Computer Science*, 155:407–410, 1996. A preliminary version appeared in Adv. in Cryptology – CRYPTO '93, Lecture Notes in Comput. Sci., volume 773, pages 110–125, 1994.

[17] C. Blundo, A. De Santis, R. De Simone, and U. Vaccaro. "Tight bounds on the information rate of secret sharing schemes". *Designs, Codes and Cryptography*, 11:107–122, 1997.

[18] C. Blundo, A. De Santis, G. Di Crescenzo, A. Giorgio Gaggia, and U. Vaccaro. "Multisecret sharing schemes". In *Adv. in Cryptology – CRYPTO '94, Lecture Notes in Comput. Sci.*, volume 839, pages 150–163, 1994.

[19] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. "On the information rate of secret sharing schemes". *Theoretical Computer Science*, 154:283–306, 1996. A preliminary version appeared in Adv. in Cryptology – CRYPTO '92, Lecture Notes in Comput. Sci., volume 740, pages 148–167, 1993.

[20] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. "Perfectly-secure key distribution for dynamic conferences". In *Adv. in Cryptology – CRYPTO'92, Lecture Notes in Comput. Sci.*, volume 740, pages 471–481, 1993.

[21] C. Blundo, A. De Santis, D.R. Stinson, and U. Vaccaro. "Graph decompositions and secret sharing schemes". *J. Cryptology*, 8:39–64, 1995. A preliminary version appeared in Adv. in Cryptology – Proceedings of EUROCRYPT '92, Lecture Notes in Comput. Sci., volume 658, pages 1–24, 1993.

[22] C. Blundo, A. Giorgio Gaggia, and D.R. Stinson. "On the dealer's randomness required in secret sharing schemes". *Designs, Codes and Cryptography*, 11:107–122, 1997.

[23] C. Boyd. *"Digital multisignatures"*. In Cryptography and coding, H. Beker and F. Piper, eds., Clarendon Press, 1989.

[24] G. Brassard and L. Salvail. "Secret-key reconciliation by public discusssion". In *Adv. in Cryptology – Proceedings of EUROCRYPT '93, Lecture Notes in Comput. Sci.*, volume 765, pages 410–423, 1994.

[25] E.F. Brickell. "Some ideal secret sharing schemes". *J. Combin. Math. and Combin. Comput.*, 6:105–113, 1989.

[26] E.F. Brickell and D.M. Davenport. "On the classification of ideal secret sharing schemes". *J. Cryptology*, 4:123–134, 1991.

[27] E.F. Brickell and D.R. Stinson. "Some improved bounds on the information rate of perfect secret sharing schemes". *J. Cryptology*, 5:153–166, 1992.

[28] C. Cachin and U.M. Maurer. "Linking information reconciliation and privacy amplification". *J. Cryptology*, 10:97–110, 1997. A preliminary version appeared in Proc. of EUROCRYPT '94, Lecture Notes in Comput. Sci., volume 950, pages 266–274, 1995.

[29] R.M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. "A note on secret sharing schemes". In *In Sequences II: Methods in Communications, Security and Computer Science*, pages 335–344. Springer Verlag, 1993.

[30] R.M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. "On the size of shares for secret sharing schemes". *J. Cryptology*, 6:157–167, 1993.

[31] Aydano B. Carleial and Martin E. Hellman. "A note on Wyner's wiretap channel". *IEEE Trans. Inform. Theory*, pages 387–390, May 1977.

[32] A.B. Carlson. *"Communication Systems (An Introduction to Signals and Noise in Electrical Communication)"*. McCraw-Hill Book Company, 1986. third edition.

[33] M. Carpentieri, A. De Santis, and U. Vaccaro. "Size of shares and probability of cheating in threshold schemes". In *Adv. in Cryptology – EUROCRYPT '93, Lecture Notes in Comput. Sci.*, volume 765, pages 126–141, 1994.

[34] T.M. Cover and J.A. Thomas. *"Elements of Information Theory"*. John Wiley and Sons, Inc., 1991.

[35] L. Csirmaz. "The size of a share must be large". In *Adv. in Cryptology – EUROCRYPT '94, Lecture Notes in Comput. Sci.*, volume 950, pages 13–22, 1995.

[36] I. Csiszár and J. Körner. "Broadcast channels with confidential messages". *IEEE Trans. Inform. Theory*, Vol. IT-24(3):339–348, May 1978.

[37] Y Desmedt. "Threshold cryptography". In *Proceedings of the 3-rd Symposium on State and Progress of Research in Cryptography*, pages 110–122, February 1993.

[38] Y. Desmedt. "Threshold cryptography". *European Trans. on Telecommunications*, Vol. 5:449–457, 1994.

[39] Y. Desmedt and Y. Frankel. "Shared generation of authenticators and signatures". In *Proceedings of CRYPTO '91, Lecture Notes in Comput. Sci.*, volume 576, pages 457–469, 1992.

[40] W. Diffie and M.E. Hellman. "New directions in cryptography". *IEEE Trans. Inform. Theory*, Vol. IT-22:644–654, November 1976.

[41] M. van Dijk. "A linear construction of secret sharing schemes". *Designs, Codes and Cryptography*, 12:161–201, 1997. A preliminary version titled "A linear construction of perfect secret sharing schemes" appeared in the Proceedings of EUROCRYPT '94, Lecture Notes in Comput. Sci., volume 950, pages 23–34, 1995.

[42] M. van Dijk. "Wyner's wire-tap channel and its cryptographic application". Master's thesis, Eindhoven University of Technology, February 1993.

[43] M. van Dijk. "Coding gain strategies for the binary symmetric broadcast channel with confidential messages". In *Proceedings of the 16th Symposium on Information Theory in the Benelux, May 18 - 19*, pages 53–60, 1995.

[44] M. van Dijk. "On the information rate of perfect secret sharing schemes". *Designs, Codes and Cryptography*, 6:143–169, 1995.

[45] M. van Dijk. "The binary symmetric broadcast channels with confidential messages, with tampering". In *Proceedings of ISIT'95, September 17-22*, page 487, 1995.

[46] M. van Dijk. "More information theoretical inequalities to be used in secret sharing?". *Information Processing Letters*, 63:41–44, 1997.

[47] M. van Dijk. "On a special class of broadcast channels with confidential messages". *IEEE Inform. Theory*, 43:712–714, 1997.

[48] M. van Dijk. "The optimal linear worst-case information rate". In *Proceedings of ISIT'97, June 28 – July 4*, page 89, 1997. Extended version submitted to Designs, Codes and Cryptography (in July 1996).

[49] M. van Dijk, C. Gehrmann, and B. Smeets. "Unconditionally secure group authentication". Submitted to Designs, Codes and Cryptography (in November 1995).

[50] M. van Dijk, W.-A. Jackson, and K. M. Martin. "A general decomposition construction for incomplete secret sharing schemes". Submitted to Designs, Codes and Cryptography (in November 1995).

[51] M. van Dijk, W.-A. Jackson, and K. M. Martin. "A note on duality in linear secret sharing schemes". *Bulletin of the Institute of Combinatorics and its Application*, Vol. 19:93–101, 1997.

[52] M. van Dijk and A. Koppelaar. "Quantum key agreement". In *Proceedings of the 18th Symposium on Information Theory in the Benelux, May 15 - 16*, pages 97–104, 1997.

[53] E.M. Gabidulin. "Theory of codes with maximum rank distance". *Problems of Information Transmission*, Vol. 21, no. 1:1–12, July 1985.

[54] R.G. Gallager. *"Information Theory and Reliable Communications"*. John Wiley, New York, 1968.

[55] M.J. Gander and U.M. Maurer. "On the secret-key rate of binary random variables". In *Proceedings of ISIT'94*, page 351, 1994.

[56] I. Ingemarsson and G.J. Simmons. "A protocol to set up shared secret schemes without the assistance of a mutually trusted party". In *Adv. in Cryptology – EUROCRYPT '90, Lecture Notes in Comput. Sci.*, volume 473, pages 266–282, 1991.

[57] W.-A. Jackson and K. Martin. "Geometric secret sharing schemes and their duals". *Designs, Codes and Cryptography*, 4:83–95, 1994.

[58] W.-A. Jackson and K. M. Martin. "Combinatorial models for perfect secret sharing schemes". To appear in Journal of Combin. Math. and Combin. Comput.

[59] W.-A. Jackson and K. M. Martin. "A combinatorial interpretation of ramp schemes". *Australasian Journal on Combinatorics*, 14:51–60, 1996.

[60] W.-A. Jackson and K. M. Martin. "Perfect secret sharing schemes on five participants". *Designs, Codes and Cryptography*, 9:267–286, 1996.

[61] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe. "Multisecret threshold schemes". In *Adv. in Cryptology – CRYPTO '93, Lecture Notes in Comput. Sci.*, volume 773, pages 126–135, 1994.

[62] W.-A. Jackson, K. M. Martin, and C. M. O'Keefe. "Efficient secret sharing without a mutually trusted authority". In *Adv. in Cryptology – EUROCRYPT '95, Lecture Notes in Comput. Sci.*, volume 921, pages 183–193, 1995.

[63] W.-A. Jackson and K.M. Martin. "An algorithm for efficient geometric secret sharing schemes". Submitted (in 1995).

[64] T. Johansson. *"Contributions to Unconditionally Secure Authentication"*. PhD thesis, Lund University, 1994.

[65] T. Johansson. "Authentication codes for nontrusting parties obtained from rank metric codes". *Designs, Codes and Cryptography*, 6:205–218, 1995.

[66] T. Johansson, G. Kabatanskii, and B. Smeets. "On the relation between A-codes and codes correcting independent errors". In *Proceedings of EUROCRYPT '93, Lecture Notes in Comput. Sci.*, volume 765, pages 1–11, 1994.

[67] R.M. Kahn and M.E. Hellman. "On the wiretap channel with feedback". Appeared as preprint before 1982.

[68] J. Körner and K. Marton. "Comparison of two noisy channels". In *Transactions on the Colloquium on Information Theory*, pages 411–423, Keszthely, Hungary, 1975.

[69] J. Körner and K. Marton. "General broadcast channels with degraded message sets". *IEEE Trans. Inform. Theory*, Vol. IT-23(1):60–64, January 1977.

[70] V. Korzhik and D. Kushnir. Personal communication.

[71] V.I. Korzhik and V.A. Yakovlev. "Capacity of a communication channel with inner random coding". *Problemy Peredachi Informatsii*, 28(4):24–34, 1992. English translation.

[72] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii. "Nonperfect secret sharing schemes and matroids". In *Adv. in Cryptology – EUROCRYPT '93, Lecture Notes in Comput. Sci.*, volume 765, pages 126–141, 1994.

[73] P. Lancaster and M. Tismenetsky. *"The Theory of Matrices"*. Academic Press, 1985.

[74] S.K. Leung-Yan-Cheong. "On a special class of wiretap channels". *IEEE Trans. Inform. Theory*, Vol. IT-23(6):625–390, September 1977.

[75] S.K. Leung-Yan-Cheong and M.E. Hellman. "The Gaussian wire-tap channel". *IEEE Trans. Inform. Theory*, Vol. IT-24(4):451–456, July 1978.

[76] K.M. Martin. *Discrete Structures in the Theory of Secret Sharing.* PhD thesis, Royal Holloway and Bedford New College, University of London, 1991.

[77] K.M. Martin. "New secret sharing schemes from old". *Journal of Combin. Math. and Combin. Comput.*, 14:65–77, 1993.

[78] K.M. Martin and R. Safavi-Naini. "Unconditionally secure authentication systems with shared generation of authenticators". Preprint.

[79] J.L. Massey. "A simplified treatment of Wyner's wire-tap channel". In *Proc. 21st Annual Allerton Conf. on Communication, Control and Computing*, pages 268–276, Monticello, IL., Oct. 1983.

[80] J.L. Massey. "Minimal codewords and secret sharing". In *Proc. 6th Joint Swedish-Russian Int. Workshop on Inf. Th.*, pages 276–279, 1993.

[81] U.M. Maurer. "Perfect cryptographic security from partially independent channels". In *Proc. 23st Annual ACM symposium on Theory of Computing*, pages 561–571, New Orleans, Louisiana, May 1991.

[82] U.M. Maurer. "Secret key agreement by public discussion from common information". *IEEE Trans. Inform. Theory*, Vol. IT-39:733–742, May 1993.

[83] U.M. Maurer. "The strong secret key rate of discrete random triples". In *Proceedings of the International Symposium on Communications, Coding and Cryptography, held in honor of J.L. Massey on the occasion of his 60th birthday, Ascona, Switzerland, Feb. 10 - 13*, 1994.

[84] C. Meadows. "Some threshold schemes without central key distributors". *Congressus Numerantium*, Vol. 46:187–199, 1985.

[85] S. Micali. "Fair public-key cryptosystems". In *Proc. of CRYPTO '92, Lecture Notes in Comput. Sci.*, volume 740, pages 113–138, 1993.

[86] W. Ogata, K. Kurosawa, and S. Tsujii. "Nonperfect secret sharing schemes". In *Adv. in Cryptology - AUSCRYPT '92, Lecture Notes in Comput. Sci.*, volume 718, pages 56–66, 1993.

[87] K. Okada and K. Kurosawa. "Lower bound on the size of shares of nonperfect secret sharing schemes". In *Proceedings of ASIACRYPT '94, Lecture Notes in Comput. Sci.*, pages 33–41, 1995.

[88] A. Orlitsky and A. Wigderson. "Secrecy enhancement via public discussion". In *Proceedings of ISIT'91*, page 155, 1991.

[89] L.H. Ozarow and A.D. Wyner. "Wire-tap channel II". *Bell System Tech. J.*, 63:2135–2157, 1984.

[90] N. Palmieri. "Graphs decomposition for secret sharing schemes". Tesi di Laurea, 1993. (in Italian).

[91] P. Piret. "Wire-tapping of a binary symmetric channel". *Philips J. Res. 35*, pages 251–258, 1980.

[92] R.L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public key cryptosystems". *Comm. of the ACM*, Vol. 21:294–299, 1978.

[93] A. Shamir. "How to share a secret". *Comm. of the ACM*, 22:612–613, 1979.

[94] G.J. Simmons. *"A survey of information authentication"*. In *Contemporary Cryptology, The Science of Information Integrity*, G.J. Simmons, ed., IEEE Press, 1992.

[95] G.J. Simmons. *"An introduction to shared secret and/or shared control schemes and their application"*. In *Contemporary Cryptology, The Science of Information Integrity*, G.J. Simmons, ed., IEEE Press, 1992.

[96] G.J. Simmons, W.-A. Jackson, and K. Martin. "The geometry of shared secret schemes". *Bulletin of the Institute of Combinatorics and its Application*, pages 71–88, 1991.

[97] D.R. Stinson. "An explication of secret sharing schemes". *Designs, Codes and Cryptography*, 2:357–390, 1992.

[98] D.R. Stinson. "New general lower bounds on the information rate of secret sharing schemes". In *Adv. in Cryptology - CRYPTO '92, Lecture Notes in Comput. Sci.*, volume 740, pages 168–182, 1993.

[99] D.R. Stinson. "Decomposition constructions for secret sharing schemes". *IEEE Trans. Inform. Theory*, Vol. IT-40:118–125, January 1994.

[100] A.D. Wyner. "The wire-tap channel". *Bell System Tech. J.*, 54:1355–1387, 1975.

[101] H. Yamamoto. "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers". *IEEE Trans. Inform. Theory*, Vol. IT-29(6):918–923, November 1983.

[102] H. Yamamoto. "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels". *IEEE Trans. Inform. Theory*, Vol. IT-37(3):634–638, May 1991.

Index

Samenvatting

Dit proefschrift bestaat uit twee delen. Het tweede gedeelte gaat over hoe een geheime sleutel gegenereerd kan worden door twee personen die met elkaar kunnen communiceren over een ruisig kanaal die afgeluisterd wordt door een vijand.

[Deel I] *Het eerste gedeelte gaat over hoe een geheime sleutel over een groep mensen verdeeld kan worden.* Elk persoon in de groep krijgt een deel van deze sleutel. Alleen vooraf gespecificeerde groepen deelnemers moeten het geheim kunnen reconstrueren als zij hun delen combineren. Andere vooraf gespecificeerde groepen deelnemers mogen juist helemaal geen informatie over het geheim krijgen als zij hun delen combineren.

Bij het verdelen van een geheim wil je de delen die aan de deelnemers gegeven worden zo klein mogelijk houden. Dan kunnen de deelnemers hun deel beter onthouden. Een fundamenteel probleem is hoe het geheim te verdelen opdat de delen zo klein mogelijk zijn. Een methode om ondergrenzen voor de grootte van de delen te vinden is besproken. Bij toepassing van deze methode blijkt soms dat de gespecificeerde groepen deelnemers op een onpraktische manier zijn gekozen. Dat wil zeggen, de ondergrenzen die met de methode zijn afgeleid laten dan zien dat de grootte van de delen in verhouding met de grootte van het geheim onpraktisch groot zijn.

Methodes om een geheim te verdelen kunnen worden opgesplitst in twee klassen: basis-constructies en decompositie-constructies. Basis-constructies gebruiken niet al bestaande schema's om geheimen te verdelen. M.b.v. een matrix benadering kunnen lineaire basis-constructies beschreven worden. Dit leidt tot een dualiteitsresultaat zoals met gemeenschappelijk werk met Wen-Ai Jackson en Keith Martin is gebleken, en tot ondergrenzen voor de grootte van de delen in lineaire schema's, resp. tot een algoritme om lineaire schema's te vinden. Dit algoritme (door Perry Moerland geïmplementeerd) werd gebruikt om voor speciale situaties optimale schema's te vinden.

Decompositie-constructies gebruiken wel al bestaande schema's om geheimen te verdelen. Samen met Wen-Ai Jackson en Keith Martin zijn alle bekende decompositie-constructies gegeneraliseerd.

Een applicatie van het gebruik van bovenstaande schema's in authenticatie-theorie is beschreven. Samen met Christian Gehrmann en Ben Smeets is het scenario bekeken, waarin van een groep personen alleen bepaalde subgroepen in staat zijn om berichten te authenticeren en naar een betrouwbare ontvanger toe te zenden. Lineaire schema's om geheimen te verdelen kunnen worden uitgebreid tot zogenaamde "onconditioneel veilige groep authenticatieschema's".

[Deel II] *Het tweede gedeelte gaat over hoe twee personen, Alice en Bob, een geheime sleutel kunnen genereren door over een ruisig kanaal met elkaar te communiceren.* De situatie is echter niet zo eenvoudig: Er is namelijk een vijand, Eve, die de communicatie afluistert. Voor een speciale klasse van ruisige kanalen is bepaald wat de maximale snelheid is, waarop Alice en Bob een geheime sleutel kunnen genereren.

Het scenario is bekeken waarin Eve het signaal, dat Alice en Bob over hun ruisige kanaal zenden, ook nog kan veranderen. Twee voorbeelden zijn bekeken. In de eerste is Eve passief (gemeenschappelijk werk met Arie Koppelaar). In de tweede is Eve actief.

Een ander scenario is bekeken, waarin Alice en Bob extra gebruik kunnen maken van een publiek kanaal. Dan is het genereren van een geheime sleutel onder te verdelen in drie stappen: het extraheren van een voordeel, het overeen laten komen van informatie, het versterken van de geheimhouding. De eerste stap werd geanalyseerd en de techniek van Maurer en haar verbetering van Gander en Maurer is veralgemeend.

STELLINGEN

behorende bij het proefschrift

Secret Key Sharing and Secret Key Generation

van

Marten van Dijk

Eindhoven, 9 december 1997

1. There exist access structures with the property that in any secret sharing scheme for such an access structure all shares need to be impractically large compared to the size of the secret [1].

   [1] M. van Dijk. "On the information rate of perfect secret sharing schemes". *Designs, Codes and Cryptography*, Vol. 6:143–169, 1995.

2. Linear secret sharing schemes are the most interesting to study for the following reasons. Firstly, all known optimal information rates can be achieved by linear secret sharing schemes. Secondly, all ideal schemes are linear [1], and thirdly, in linear schemes qualified groups can reconstruct the secret in an efficient manner.

   [1] K.M. Martin. *Discrete Structures in the Theory of Secret Sharing.* PhD thesis, Royal Holloway and Bedford New College, University of London, 1991.

3. The definition of *average* information rate in terms of the entropy function is more natural than the definition of *worst-case* information rate in terms of the entropy function.

4. There is a correspondence between duality in coding theory and duality in secret sharing [1].

   [1] M. van Dijk. "A linear construction of secret sharing schemes". *Designs, Codes and Cryptography*, Vol. 12:161–201, 1997.

5. During information reconciliation not only information is reconciled but also an advantage is distilled.

6. We call a 0/1-matrix M of size $n \times k$ to be locally invertible if there exists a function $\mathcal{M} : \mathbb{N}^k \rightarrow \mathbb{N}^n$ such that for all vectors $y \in \{0,1\}^n$

   $$\mathcal{M}(yM) = y.$$

   Let $k(n)$ denote the minimal value of k for which a locally invertible $n \times k$ 0/1-matrix M exists. Then $k(n) \geq n/\log_2(n+1)$, and a *non constructive* proof of Chvátal [1] shows that $k(n)$ is at most $7n/\log_2 n$ for sufficiently large n. We can *construct* an infinite sequence of locally invertible $k_l \times n_l$ 0/1-matrices such that k_l is at most $n_l/\log_2\log_2 n_l$.

   [1] V. Chvátal. "Mastermind". *Combinatorica*, 3(3–4):325–329, 1983.

7. Een publiek geheim is geen geheim.

8. De psychoanalyse bestaat uit het decrypten van het onbewuste.

9. Je vraagt je af hoe het in godsnaam mogelijk is, dat een sekte in Gods naam leden kan werven.

10. Vaak is netwerken niet hetzelfde als net werken.

11. De waarheid moet gezegd kunnen worden, maar blijft te vaak in het midden liggen.