Optimization of zero leakage helper data systems

Nur Andini, F.

Award date:
2015

Master Thesis

Optimization of Zero Leakage Helper Data Systems

Fitria Nur Andini

Supervisor:
Boris Škorić (TU/e)

Department of Mathematics and Computer Science
Security Research Group
Eindhoven University of Technology
2015

Abstract

Biometric authentication is a promising solution for secure authentication. However, the storage of biometric data may lead to security and privacy problems. A Helper Data System (HDS) is introduced to solve these problems. HDS offers the capability to extract information from noisy data while maintaining the confidentiality. There are two types of HDS, which are Fuzzy Extractor (FE) and Secure Sketch (SS). The difference between FE and SS is, a Secure Sketch allows reconstruction of the enrolled biometric from a noisy measurement, whereas a Fuzzy Extractor derives a stable uniform key or secret. In this thesis, we consider a general Helper Data System (HDS), which extracts secret from the enrollment data, but with non-uniform probability of secret. This thesis explore the optimal secret reconstruction procedure in Zero Leakage Helper Data System (ZLHDS). The main goal is to maximize the amount of information that can be extracted from noisy data. The optimization of ZLHDS is done by maximizing the mutual information of the generated secret and the reconstruction secret given helper data. The optimization of ZLSS consists of two phase. First is the analysis to formulate the optimum reconstruction boundary. Second is the numerical analysis to find the optimum probability to obtain the maximum mutual information. The result confirmed that ZLHDS gives a higher mutual information than Zero Leakage Fuzzy Extractor (ZLFE) for a certain amount of noise. This thesis also explored the theoretical approach for the optimization of ZLHDS in a more general case, which is for arbitrary source and arbitrary noise distribution. This approach was done using Lagrange Multiplication, which resulted in a more complicated formula.

Acknowledgement

I would like to express my sincere gratitude to my supervisor dr. Boris Skoric for the continuous support of my thesis study and research, for his patience, motivation, enthusiasm, and immense knowledge. Besides my supervisor, I would like to thank the rest of my thesis committee: dr.ir. L.A.M. (Berry) Schoenmakers and dr. Tanya Ignatenko for their cooperation, insightful comments, and hard questions.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A reliable authentication scheme is crucial to allow secure access. Authentication is a process of determining whether a certain identity that is claimed by someone is actually true. If the claimed identity matches the database of the authorized users, then the user will be granted access.

1.1 Types of Authentication

There are three types of authentication schemes which are distinguished based on the category of the resources used. They are the authentication scheme that are based on *what you know*, *what you have*, and *what you are*.

What you know-based authentication distinguishes the authorized user from all other users from the knowledge of a secret. The authentication scheme simply checks whether a person who claims to be the authorized user, knows the secret. An example of *what you know*-based authentication is the password-based authentication scheme. This authentication scheme verifies that a user knows a password that nobody else does.

In the password-based authentication scheme, the system checks whether an identification data, e.g. username and password entered by the user is valid. The validity is done by comparing that username and password with the list of authorized identification data that stored in the database. Since the identification data is a confidential information, the storage needs to be secured.

Storing this identification data in a plain database without applying any cryptographic algorithm is not a wise thing to do. Once the database is compromised, the authentication system becomes vulnerable to attack. This problem can not be solved by simply encrypting the database, since it is susceptible to an *insider attack*. If an attacker possessed the decryption key, then the attacker can impersonate any users that are listed on that database.

A common solution to securely store passwords is by applying a cryptographic *hash* function to the stored password. Hash is a one-way-function that is computationally hard to invert. Therefore, even if the attackers can obtain the hashed data, it is difficult to revert the original password. Hence, it prevents the attacker from deriving any useful information from the hashed value.

Even though the database is secure, password-based authentication still has a weakness. Because of the limitation in human memory, people tend to choose a password that is easy to remember. Thus, making it easy for an attacker to guess the password.

On the contrary, if the password is difficult to guess, there is a high possibility that a user will forget the password. If the user writes down the password somewhere, it will raise the possibility

of leakage. Moreover, stealing passwords is often becoming the target of social engineering attack.

Another type of authentication scheme is the *what you have*-based authentication scheme. In this scheme, the identity of a user is verified based on an object that belongs to a certain user. For example, ID-card, biometric passport, RFID-card, and security token.

There are two types of identification that can be used in *what you have*-based authentication scheme. First is the authentic physical object, e.g. ID Card, having physical authenticity marks such as special microstructures, inks, etc. that are difficult to clone. Second is the hard-to-hack specialized hardware tokens that employ a cryptographic key.

The *what you have*-based authentication might have solved the risk of human memory limitation. However, it does not eliminate the risk of careless human behavior. If the authentication object (the passport, or the token) is lost or stolen, then anyone could easily impersonate the authorized user. Due to this limitation, an authentication technique based on *what you are* is developed.

The idea of *what you are*-based authentication corresponds to the natural way of how people recognize each other. People are not identified using some secret exchange protocol or certain belonging. People recognize each other because of their look, their sound, their human characteristic or in other words, *what you are*.

However, in order to utilize human characteristics in an authentication scheme, it is crucial to choose characteristics that are easy to measure and difficult to spoof. The characteristic that is often used in *what you are*-based authentication is the biometric information, such as fingerprint, iris, face, etc. This form of authentication is called biometric authentication.

Recently, the concept of biometric authentication has been applied to authenticate physical object. It becomes possible because of the implementation of physical unclonable function (PUF). PUF has similar characteristics as biometric, which are unique, measurable, and unclonable. Hence, PUF objects are generally known as device biometrics. Physical object authentication that uses PUF as its identifier is called PUF-based authentication.

This thesis is focused on *what you are*-based authentication.

1.2 Biometric authentication

Biometric authentication scheme has a promising potential as a solution for secure authentication scheme because of its unique characteristics. Biometric data is bound to the user identity and cannot be forgotten. Biometric authentication utilizes the physiological or behavioral characteristic of a person, such as fingerprint, iris, retina, handprint, face, DNA, signature and voice. This biometric information is called biometric identifier.

Generally, biometric authentication consists of two phases: enrollment and authentication. During the enrollment phase, a biometric template is extracted from the biometric identifier of a user. Biometric template is a form of features that best characterizes the biometric sample. This biometric template is then stored in the database as the enrollment data.

In the authentication phase, the system scans another biometric sample of a user, extracts the biometric feature, and then compares it against the enrollment data. A user is authenticated if the new sample produces high similarity with the enrollment data in the database.

In a general biometric authentication scheme, the extracted biometric template usually contains confidential information of the user. Therefore, if the storage of this biometric template is not secured, it may lead to several security and privacy problems.

1.2.1 Problems in Biometric Authentication

Security problems occur when an attacker is able to obtain sufficient information to produced fake biometrics, e.g. rubber finger, face mask, fake DNA, or fake iris. Using these fake biometrics, an attacker might be able to impersonate a certain user to gain unauthorized access to a system or to leave fake evidence at a crime scene.

Privacy problems occur when some personal information can be derived from the biometric template. For example, a biometric template may reveal disease information. Once leaked, an attacker may misuses the health information of a certain user for malicious intentions. Another privacy risk occurs when an attacker is able to perform cross-correlation between databases, so that an attacker could observe that someone is enrolled in both databases. Hence, the storage of biometric data needs to be highly secured.

In the password-based authentication, the database is secured using hash functions. However, hash functions are very sensitive to noise. A minor change in the source results in a totally different hash value. In contrast, biometric information is prone to noise. It is impossible to reproduce two exact similar biometric information. Therefore, applying a straightforward implementation of hash to biometric information is not possible. It is necessary to perform a noise-correction procedure to the biometric information for further processing.

1.3 PUF-Based Authentication

Another form of *what you are*-based authentication is the implementation of Physical Unclonable Function (PUF). It was first introduced by [12]. They developed a physical one-way function which was easy to evaluate on every input but hard to revert when only the output is known.

PUF is a random function that is embodied in a physical structure. PUF performs a unique challenge-response behavior which is hard to predict, but reliable and easy to evaluate. PUF is also unique and unclonable. These properties are caused by the uncontrollable manufacture of their physical microstructure.

When the microstructure is challenged by a physical stimulus, the response is unpredictable. This unpredictable response is caused by the complex interaction between the stimulus and the physical microstructure of the device. However, this response is reliable. When PUF is queried with the same challenge, the corresponding responses are relatively similar and only differ by a minor variation. Thus, the response can be evaluated.

It is impossible to construct two PUFs with the exact same challenge-response behavior, even though those PUFs were manufactured with the same process as a similar device. Therefore, PUFs can be used as a unique and a tamper-evident device identifier.

PUFs can also generate and store secure key for authentication. The responses of the PUFs act as the authentication data. In order to derive a reproducible bit strings for the authentication data, a noise-correction algorithm is required. Because PUF is unique and prone to noise, it is also known as device biometrics.

PUF-based authentication also has similar problems as biometric authentication. Those problems are the noisy response and the highly-secured storage requirement.

1.4 Approaches for Protecting Privacy

Both biometric and PUF data contain confidential information, either it is the personal data or the secure key. Therefore, this information needs to be stored securely. There are several algorithms that not only provides secure storage, but also enable the stored data to be further

processed. The latest feature is important for authentication. Those algorithms are homomorphic encryption and helper data system.

Homomorphic encryption was first introduced by [13]. It is a cryptographic scheme that enables a computation to be performed directly on the encrypted data without decrypting it first. The result of this algorithm is a ciphertext where the decryption matches the result of the same operations performed on the original plaintext. Homomorphic cryptosystem is *malleable* by design.

In general, there are two types of homomorphic algorithm. They are the partially homomorphic [6][1] [11]; e.g. as unpadded RSA, El Gamal, Goldwasser-Micali, Benaloh, and Paillier; and the fully homomorphic encryption scheme [5]. The difference is that the first algorithm only allows certain operations on their cipertext computation, e.g. addition, and multiplication. On the other hand, fully-homomorphic algorithm supports both addition and multiplication to be performed on the encrypted values. However, homomorphic cryptosystems require enormous computational resources.

Another approach is the helper data system, as proposed by [7], [10] and [4]. Helper data system offers a security primitive that can extract information from noisy sources while maintaining the confidentiality of the data. Moreover, helper data system requires less resources and less complex computation, compared to the homomorphic cryptosystem. Hence, helper data system is convenient for biometric based authentication.

1.5 Helper Data System

Helper data system is a cryptographic primitive that extracts high-entropy noise-free bit strings from noisy sources. Helper data system is attractive because the extracted information hides the confidential information of the source data. Another advantage of the helper data system is that it can be combined with various cryptographic algorithms, including hash functions. Thus, it can be used in a biometric authentication scheme.

In general, helper data system consists of two phase. They are the Generation phase and the Reconstruction phase. The Generation phase obtains the noisy biometric data as input and generates two values, the secret and the helper data. The secret contains the *most significant bits* of the input, while the helper data contains the *least significant bits*. Therefore, the helper data contains only the required information to reconstruct the secret without actually leaking any confidential information of the biometric input.

The Reconstruction phase obtains another noisy biometric data, that correlated to the input of the Generation phase, and helper data as its input. The output of this phase is the reconstructed secret. In the ideal case, the reconstructed secret from the Reconstruction phase should be similar with the generated secret from the Generation phase.

There are two types of helper data system, they are Fuzzy Extractors and Secure Sketches. Fuzzy extractor produces a uniform and an error-tolerant bit string as the extraction result. Fuzzy extractors are mostly used to generate keys. On the other hand, secure sketches focus more on extracting entropy without requiring uniformity constraint.

Helper data algorithm was first introduced by [7], [10], and [4]. Their work, however, was focused only on the discrete metric spaces. The definition of fuzzy extractor was then extended by [15], where a generic construction of fuzzy extractor for noisy continuous sources is introduced.

1.6 Zero Leakage Helper Data System

Helper data is considered as a public data, thus it should not reveal any confidential information of its input data. Zero leakage property is defined as a condition where the mutual information between the helper data and the secret extracted is equal to zero [3]. Their proposed zero leakage properties ensure that the helper data is independent from the secret. Thus, knowing the helper data never leaks any information about the secret. For instance, the proposed scheme of [15] and [3] are zero leakage.

The theory of zero leakage helper data system was then refined by [3]. They focused on the quantization and proved that the zero leakage scheme requires quantile helper data. Their result also provided an optimal reconstruction algorithm minimizing the reconstruction error probability. However, the optimal reconstruction for a ZL HDS with a not-uniformly-distributed secret remains an open question.

The uniformity constraint of the fuzzy extractor has a negative impact on the amount of entropy extracted from the source. In the fuzzy extractor algorithm, the input data is partitioned into certain number of equiprobable regions. The choice of the number of the equiprobable regions depends on the noise characteristic. If the chosen number of regions is too large, then the error correction may fail. If it is too small, then the helper data system will not give the correct reconstruction.

1.7 Research Questions

This thesis explores the optimization of zero leakage Helper Data System (ZLHDS). There are two questions that become the main focus of this research. They are:

- finding the best reconstruction algorithm in ZLHDS
- how to optimize the quantization intervals so that the maximum amount of entropy is extracted from the source.

1.8 Contributions and Outline

This thesis is focused on the optimization of ZLHDS. We have modified the reconstruction boundaries proposed by [3] to suit the secure sketch requirements.

Our approach consists of two phases. First is to obtain the generalized formula to produce the optimum reconstruction boundary. Second is to perform numerical analysis to define the optimum quantization intervals that maximizes the bit of information extracted. The numerical analysis is applied under assumption of Gaussian source and Gaussian noise with zero mean, and a perfect enrollment.

Chapter 2 gives the preliminaries; including the helper data system, information theory, zero leakage, and the results of [3]. Chapter 3 focus on the detailed analysis of the proposed algorithm, including the optimal quantization boundary and the optimization of the quantization intervals. Chapter 4 elaborates the numerical analysis of the algorithm proposed. Chapter 5 describes the analytical approach for general case with arbitrary source and noise. Finally, chapter 6 summarizes and concludes the results of this thesis.

Chapter 2

Preliminaries

2.1 Information Theory

2.1.1 Expected Value, PMF, PDF, and CDF

The expected value of a random variable is the average of all possible values. Consider a discrete random variable X and a function $h(X)$. The expected value of $h(X)$ is defined as

$$\mathbb{E}[h(x)] = \sum_{x \in \mathcal{X}} Pr[X = x]h(x). \tag{2.1}$$

A probability mass function (PMF) is a function that gives the probabilities of the possible value x for a *discrete* random variable X.

A probability density function (PDF) is a function which describes the probability that a *continuous* random variable X is close to a given value.

A Cumulative Distribution Function (CDF) describes the probability that a real-valued random variable X with a given probability distribution will be found to have a value less than or equal to X.

2.1.2 Shannon Entropy

The Shannon entropy of a discrete random variable X is a measure of the amount of the uncertainty that is associated with X.

$$H(X) = -\sum_{x \in \mathcal{X}} p_x \log p_x \tag{2.2}$$

The joint entropy of two random variables, X and Y, is the entropy of their joint distribution.

$$H(X, Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p_{xy} \log p_{xy}. \tag{2.3}$$

The conditional entropy measures how much the uncertainty about X exist if Y is known.

$$H(X|Y) = -\sum_{y \in \mathcal{Y}} p_y \sum_{x \in \mathcal{X}} p_{x|y} \log p_{x|y}. \tag{2.4}$$

2.1.3 Mutual Information

Mutual information between two random variables measures the amount of information that can be obtained about one random variable by observing another. The mutual information of discrete random variable X relative to Y is given by:

$$I(X;Y) = \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} p_{xy} \log \frac{p_{xy}}{p_x p_y}. \tag{2.5}$$

For continuous random variables, the mutual information is:

$$I(X;Y) = \int_{x\in\mathcal{X}} \mathrm{d}x \int_{y\in\mathcal{Y}} \mathrm{d}y\, p_{xy} \log \frac{p_{xy}}{p_x p_y}. \tag{2.6}$$

Mutual information can be represented as:

$$I(X;Y) = H(X) - H(X|Y) \tag{2.7}$$
$$= H(Y) - H(Y|X) \tag{2.8}$$
$$= H(X) + H(Y) - H(X,Y). \tag{2.9}$$

2.2 Helper Data System

Helper data system (HDS) is a cryptographic primitive that can extract a reproducible bit strings from noisy sources while maintaining its privacy. HDS consists of two phases, Generation and Reconstruction. There are two special algorithms that have been developed for HDS, they are Fuzzy Extractor (FE) and Secure Sketches (SS). In FE the probability distribution of the extracted secret given the helper data is (nearly) uniform. On the other hand, the probability distribution of the extracted secret in SS is not necessarily uniform. In SS, however, the entropy of the secret given the helper data is generally higher than for a FE.

2.2.1 Fuzzy Extractor

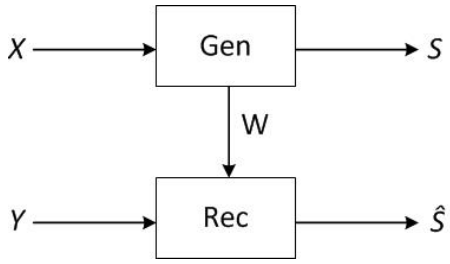


Figure 2.1: Fuzzy Extractor Scheme

Definition 2.2.1 (Fuzzy Extractor)**.** Taken from Definition 6.1 in [14].
A *Fuzzy Extractor* for a source space $\mathcal{X}$ and target space $\{0,1\}^l$ consists of a (possibly non-deterministic) procedure:

- `Gen`: $\mathcal{X} \to \{0,1\}^l \times \{0,1\}^* : x \mapsto (s_x, w_x)$ ("generate") which extracts a secret s_x and helper data w_x from x, and

- `Rec`: $\mathcal{X} \times \{0,1\}^* \to \{0,1\}^l : (y, w) \mapsto \hat{s}_x$ ("reconstruction") which tries to reconstruct the secret from the helper data and a fresh measurement y.

A Fuzzy Extractor must satisfy the following properties:

- Correctness: The probability that $\hat{S}_x = S_x$ must be close to 1.
- Security: The random variable S_x must be close to uniform, given knowledge of W_x.

In the `Gen` phase, FE extracts a uniform random bit string S from an enrollment data X. The `Gen` phase also outputs a helper data W that can be safely made public since it does not contain any confidential information of the secret S.

The `Rec` phase takes Y as its input. Y is the noisy value that correlated to X, which is also known as the authentication measurement. Hence, the secret bit string S can be reconstructed as $\hat{S}$ from Y and W. The helper data W helps the reconstruction of secret S.

2.2.2 Secure Sketch

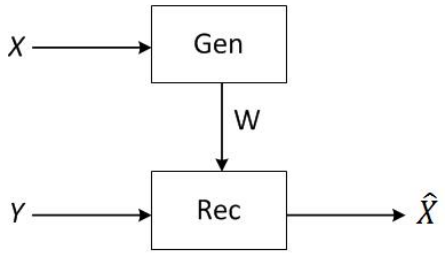


Figure 2.2: Secure Sketch Scheme

Definition 2.2.2 (Secure Sketch)**.** Taken from Definition 6.2 in [14].
A *Secure Sketch* for a source space $\mathcal{X}$ consists of two algorithms,

- `Gen`: $\mathcal{X} \to \{0,1\}^* : x \mapsto w_x$ ("sketch"), and
- `Rec`: $\mathcal{X} \times \{0,1\}^* \to \mathcal{X} : (y, w_x) \mapsto \hat{x}$ ("reconstruct").

A Secure Sketch must satisfy the following properties:

- Correctness: The probability that $\hat{X} = X$ must be close to 1.
- Security: X given W_x must have high entropy.

It is always possible to construct a FE from SS.

2.2.3 General Helper Data System

Another scheme is the general HDS where the algorithm is similar to FE but with non-uniform probability of secret s.

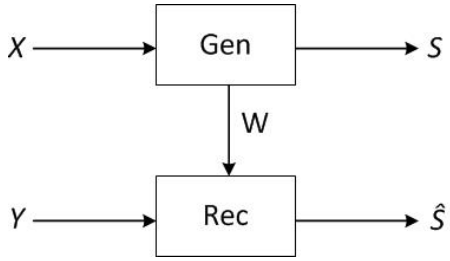


Figure 2.3: General HDS

2.3 Zero Leakage

Although secure sketches leave entropy in W and fuzzy extractors extract uniform randomness from it, they may leak some information about the secret s during the error correction. Zero Leakage (ZL) algorithm was developed by [2] to resolve this problem.

The work of [2] introduced a constraint on the conditional helper data as

$$f_W(W|S=s) = f_W(w) \quad \forall_S \in \{0,\ldots,N-1\} \tag{2.10}$$

so that $I(W;S)=0$. f_W is the probability density function of W and N is the total number of secret.

They defined ZL as a condition where helper data does not reveal privacy of the source. This condition can be achieved if the mutual information between W and S is equal to zero.

Definition 2.3.1 (Zero Leakage)**.** Taken from Definition 2.1 [3].
Let $W \in \mathcal{W}$, we call a helper data system *Zero Leakage* if and only if

$$\forall_{\mathcal{V}\subseteq\mathcal{W}} \quad \mathbb{P}[S=s|W\in\mathcal{V}] = \mathbb{P}[S=s] \tag{2.11}$$

Def. 2.3.1 implies $I(W;S)=0$.

In ZL the helper data W contains only the *least significant digits* of source X, while S contains the *most significant digits*. Thus, S does not depend on W.

2.4 Noise Model

The correlation $\rho \in [-1,1]$ between the enrollment measurement X and the authentication measurement Y is defined as

$$\rho = \frac{\mathbb{E}[XY]-\mathbb{E}[X]\mathbb{E}[Y]}{\sigma_X\sigma_Y} \tag{2.12}$$

where σ_X and σ_Y denotes the variance of the enrollment sample and the authentication sample respectively. Later, we also introduce σ_R as the variance of the additive noise.

Let the noise-free measurement is notated as Z, then we have the noisy enrollment and noisy authentication measurements as

$$X = Z + \mathcal{N}_{\mathrm{e}} \tag{2.13}$$
$$Y = Z + \mathcal{N}_{\mathrm{Rec}} \tag{2.14}$$

where $\mathcal{N}_{\mathrm{e}}$ is the enrollment noise and $\mathcal{N}_{\mathrm{Rec}}$ is the authentication noise. Thus, we have

$$Y = X - \mathcal{N}_{\mathrm{e}} + \mathcal{N}_{\mathrm{Rec}} \tag{2.15}$$

Without loss of generality, we consider X and Y to have zero mean. Thus, as defined in [3], the authentication sample Y which related to the enrollment sample X and the independent noise R is

$$Y = \lambda X + R \tag{2.16}$$

where $\lambda \in [0, 1]$ is the attenuation parameter. R is the zero-mean additive noise that is *uncorrelated* with X.

According to the consistency requirements for the second order statistic:

1. Eq.(2.16) squared: $\mathbb{E}[Y^2] = \mathbb{E}(\lambda X + R)^2$
2. Eq.(2.16) times X: $\mathbb{E}[XY] = \mathbb{E}(\lambda X^2 + RX)$

since $\sigma_{XR} = 0$, where σ_{XR} is the covariance between X and R, then we have the variances as

1. $\sigma_Y^2 = \lambda^2 \sigma_X^2 + \sigma_R^2$
2. $\rho\, \sigma_X \sigma_Y = \lambda \sigma_X^2$

The unknown variables are λ and σ_R. Using the equation above, we solve them as

$$\lambda = \rho \frac{\sigma_Y}{\sigma_X} \tag{2.17}$$

and

$$\sigma_R^2 = \sigma_Y^2 - \lambda^2 \sigma_X^2 \tag{2.18}$$

$$= \sigma_Y^2 - \rho^2 \frac{\sigma_Y^2}{\sigma_X^2} \sigma_X^2 \tag{2.19}$$

$$\sigma_R^2 = \sigma_Y^2 (1 - \rho^2). \tag{2.20}$$

As defined on [3], λ can also be expressed as

$$\lambda^2 = \frac{\rho^2}{1 - \rho^2} \frac{\sigma_R^2}{\sigma_X^2}. \tag{2.21}$$

The ratio of the enrollment data to the noise is defined as the Signal to Noise Ratio (SNR), such that

$$\mathrm{SNR} = \frac{\lambda^2 \sigma_X^2}{\sigma_R^2} \tag{2.22}$$

In this noise model, there are two limiting situations exist [3]

1. Perfect Enrollment, occurs when the enrollment noise is negligible.

$$\sigma_Y^2 = \sigma_X^2 + \sigma_R^2 \quad \Longleftrightarrow \quad \lambda = 1 \tag{2.23}$$

$$\sigma_R^2 = \sigma_Y^2 - \sigma_X^2. \tag{2.24}$$

2. Identical conditions, occurs when the enrollment and the authentication noise are identical.

$$\sigma_Y^2 = \sigma_X^2 \iff \lambda = \rho \tag{2.25}$$

$$\sigma_R^2 = (1-\rho^2)\sigma_X^2. \tag{2.26}$$

Definition 2.4.1 (Symmetric Fading Noise)**.** Taken from Definition 2.2 [3].
The noise is called *symmetric fading noise* if for all x, y_1, y_2 holds

$$|y_1 - \lambda x| > |y_2 - \lambda x| \Rightarrow \psi(y_1|x) < \psi(y_2|x) \tag{2.27}$$

Gaussian noise is an example of symmetric fading noise.

2.5 Results from De Groot et.al.[3]

The work of [3] observed the ZL property of HDS in the case of a one dimensional continuous source X and continuous helper data W.

Consider a random variable $X \in \mathbb{R}$. The Probability Density Function (PDF) of X is denoted as f, while the Cumulative Distribution Function (CDF) is denoted as F.

The secret S is an integer in the range $\mathcal{S} = \{0, \ldots, N-1\}$ where S is a result of a quantization function Q such that $S = Q(X)$. The probability mass function of secret s is denoted as p_s.

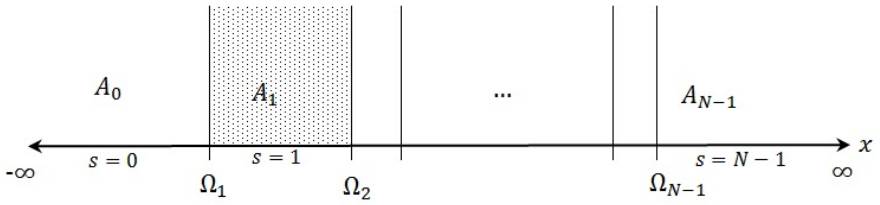


Figure 2.4: Quantization regions and Quantization boundaries for enrollment phase

The quantization regions is defined as $A_s = \{x \in \mathbb{R} : Q(x) = s\}$. One quantization region represents a single value of s. The left boundary of a quantization region A_s is the quantization boundary Ω_s where $\Omega_s = F^{-1}\left(\sum_{t=0}^{s-1} p_t\right)$. In the Figure 2.4, the shaped area represents the quantization regions and the vertical lines represent the quantization boundaries for enrollment phase.

The continuous helper data is represented as $W \in \mathcal{W} \subset \mathbb{R}$ where $\mathcal{W} = [0, 1)$. The helper data is computed using a function g such that $W = g(X)$. g is an invertible function on each quantization interval A_s.

2.5.1 Sibling Points

Sibling points are a point x that corresponds to a different secret s but gives rise to the same helper data w.

Definition 2.5.1 (Sibling Points)**.** Taken from Definition 2.1 [3].
Two points $x, x' \in \mathbb{R}$, with $x \neq x'$ are called sibling points if $g(x) = g(x')$.

Lemma 3.4 from [3] proved that for each quantization interval A_s there exists only one point x that is compatible with w. Theorem 3.6 from [3] proved that g is differentiable on each quantization interval, it has to be either monotonously increasing on all intervals or monotonously decreasing on all intervals.

2.5.2 Quantile Relationship between Sibling Points

De Groot et al.[3] proved that zero leakage is equivalent to quantile relationship between sibling points.

Theorem 2.5.2 (Quantile Sibling Points)**.** *Taken from Theorem 3.8 in [3].*
Let g be monotonously increasing on each interval A_s with $g(A_0) = \cdots = g(A_{N-1}) = \mathcal{W}$. Let $s, t \in \mathcal{S}$. Let $x_s \in A_s, x_t \in A_t$ be sibling points as defined in Def. 2.5.1. In order to satisfy Zero Leakage we have the following necessary and sufficient condition on the sibling points,

$$\frac{F(x_s) - F(\Omega_s)}{p_s} = \frac{F(x_t) - F(\Omega_t)}{p_t}. \tag{2.28}$$

According to the Theorem 2.5.2, the enrollment phase can be defined as

$$s = Q(x) \tag{2.29}$$

$$w = g(x) = \frac{F(x) - F(\Omega_s)}{p_s}. \tag{2.30}$$

The helper data w is represented as a quantile distance between x and Ω_s and normalized to p_s.

2.5.3 Optimal Reconstruction Boundary of ZLFE

The work of [3] discovered how maximum likelihood reconstruction is done for ZLFE.

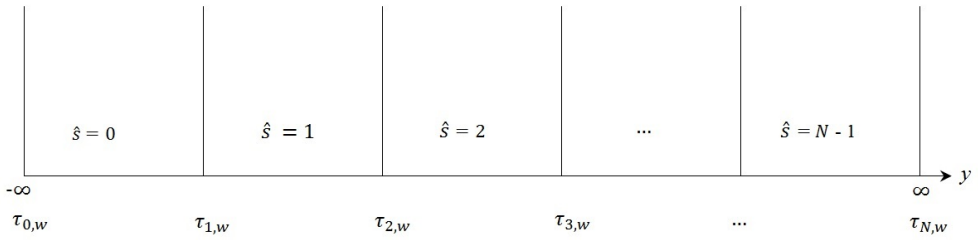


Figure 2.5: Reconstruction boundaries for some given w

Lemma 2.5.3 (Optimal Reconstruction FE)**.** *Taken from Lemma 4.1 [3]. Let* $\mathrm{Rec}(y, w)$ *be the reconstruction algorithm of a ZL FE system. Let g_s^{-1} be the inverse of the helper data generation function for a given secret s. Then optimal reconstruction is achieved by*

$$\mathrm{Rec}(y, w) = \arg\max_{s \in S} v(y|g_s^{-1}(w)). \tag{2.31}$$

They [3] also found where the reconstruction boundary lie that follow from Eq.(2.31) by finding a point $y = \tau_s$ that gives the equal probability of $v(y|g_s^{-1}(w))$ for s and $s-1$. The threshold τ_s represents the lower boundary of the decision region. The optimal reconstruction where $\hat{s} = s$ can be achieved if $\tau_{s,w} \leq y < \tau_{s+1,w}$.

Theorem 2.5.4 (Optimal Reconstruction Boundary in ZL FE System)**.** *Taken from Theorem 4.2 [3]. Let $\psi(y|x)$ represent symmetric fading noise. Then the optimal reconstruction in a FE scheme is obtained by the following choice of thresholds*

$$\tau_s = \lambda \frac{g_s^{-1}(w) + g_{s-1}^{-1}(w)}{2}. \tag{2.32}$$

2.6 Lagrange Multipliers

Lagrange multipliers is an algorithm on finding the extrema of a function $m(x, y)$ where one or more constraints, e.g. $c(x, y) = 0$, have to be satisfied. A new variable λ is introduced. A new function $L[x, y, \lambda]$ is constructed as

$$L[x, y, \lambda] = m(x, y) + \lambda\, c(x, y).$$

The extrema are found by calculating the partial derivatives of L w.r.t. x, y, and λ, and demanding each derivative to be equal to zero.

2.7 Implicit Function Theorem (IFT)

Let $G(\vec{p}, \tau) : \mathbb{R}^{N+1} \to \mathbb{R}$ be a function where $\vec{p} = \{p_0, p_1, \ldots, p_{N-1}\}$. Denoting points (p_α, τ) that satisfies $G(\vec{p}, \tau) = 0$ and $\frac{\partial G}{\partial \tau} \neq 0$ at p_α.

Thus the calculation of the implicit function can be done as follows:

$$\frac{\partial \tau}{\partial p_\alpha} = -\frac{\partial G / \partial p_\alpha}{\partial G / \partial \tau}. \tag{2.33}$$

2.8 Summary of Notations

There are several notations used in this thesis, they are:

Kronecker Delta		
$\delta_{s,\alpha}$		$\delta_{s,\alpha} = \begin{cases} 0, & s \neq \alpha \\ 1, & s = \alpha \end{cases}$.
Step Function		
$\mathbf{1_{s-1}}(\alpha)$	$\sum_{i=0}^{s-1} \delta_{i,\alpha}$	$\mathbf{1_{s-1}}(\alpha) = \begin{cases} 1, & \alpha \leq s-1 \\ 0, & \alpha > s-1 \end{cases}$.
Gaussian Noise		
$\varphi_\sigma(z)$	$\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{z^2}{2\sigma^2}}$	Probability distribution function of a Gaussian random variable with zero mean and variance σ^2.
$\varphi'_\sigma(z)$	$-\frac{z}{\sigma}\varphi_\sigma(z)$	First derivative of Gaussian.
$\Phi_\sigma(z)$	$\int_{-\infty}^{z} \mathrm{d}z' \varphi_\sigma(z')$	Error function: $-\frac{1}{2}\operatorname{erf}(\frac{-z}{\sqrt{2}\sigma})$.
Enrollment Measurements		
X	$(-\infty, \infty)$	Enrollment measurement of the generation phase.

$f(x)$		Probability density function of X.
$F(x)$	$\int_{-\infty}^{x} \mathrm{d}x'\, f(x')$	Cumulative distribution function of X.
s	$Q(x)$	The generated secret $s \in \mathcal{S}$, where $\mathcal{S} = \{0, \ldots, N-1\}$.
Ω_s	$F^{-1}\left(\sum_{t=0}^{s-1} p_t\right)$	Quantization boundary of the Generation Phase.
w	$\left(F(x) - \sum_{i=0}^{s-1} p_i\right) / p_s$	$w = g(x)$ where $w \in \mathcal{W}$ in which $\mathcal{W} = [0, 1)$.
$\xi_{s,w}$	$F^{-1}\left(\sum_{i=0}^{s-1} p_i + w p_s\right)$	x-value that corresponds to s, w.
Authentication Measurements		
Y	$(-\infty, \infty)$	Authentication measurement of the reconstruction phase. It is the noisy value correlated to the source X.
$\psi(y\|x)$	$v(y - \lambda x)$	Probability density function of y given x.
$V(z)$	$\int_{-\infty}^{z} \mathrm{d}y\, v(y)$	Cumulative density function.
$\tau_{s,w}$	$\frac{\sigma_R^2 \ln \frac{p_s}{p_{s-1}}}{\lambda(\xi_{s-1,w} - \xi_{s,w})} + \lambda \frac{(\xi_{s-1,w} + \xi_{s,w})}{2}$	Reconstruction boundary for certain s and w.
$q_{\hat{s}}$	$\int_{-\infty}^{\infty} \mathrm{d}x\, f(x) \int_{\tau_{\hat{s},w(x)}}^{\tau_{\hat{s}+1,w(x)}} \mathrm{d}y\, \psi(y\|x)$	$\Pr[\hat{S}{=}\hat{s}]$ which also equal to $\mathbb{E}_w\, \Lambda_{\hat{s}\|w}$.
Conditional Probabilities		
$\Upsilon_{\hat{s}\|s,w}$	$V(\tau_{\hat{s}+1,w} - \lambda\xi_{s,w}) - V(\tau_{\hat{s},w} - \lambda\xi_{s,w})$	$\int_{\tau_{\hat{s},w}}^{\tau_{\hat{s}+1,w}} \mathrm{d}y\, \psi(y\|\xi_{s,w})$.
$\Pi_{s,\hat{s}\|w}$	$p_s \Upsilon_{\hat{s}\|s,w}$	
$\Gamma_{s\|\hat{s},w}$	$\frac{\Pi_{s,\hat{s}\|w}}{\Lambda_{\hat{s}\|w}}$	
$\Lambda_{\hat{s}\|w}$	$\sum_s p_s \Upsilon_{\hat{s}\|s,w}$	$\sum_s \Pi_{s,\hat{s}\|w}$.
Noise		
λ	$\rho \frac{\sigma_Y}{\sigma_X}$	The attenuation parameter where $\lambda \in [0, 1]$.
Mutual Information		
$I(S; \hat{S}, W)$	$\sum_{s,\hat{s}} \mathbb{E}_w p_s \Upsilon_{\hat{s}\|s,w} \ln \frac{\Upsilon_{\hat{s}\|s,w}}{\Lambda_{\hat{s}\|w}}$	Mutual information.
Error Reconstruction		
$\Pr[\hat{S} = S]$	$\sum_s p_s \mathbb{E}_w \Upsilon_{s\|s,w}$	Probability of correct reconstruction.
E_{Rec}	$1 - \Pr[\hat{S} = S]$	Error probability of the reconstruction phase.

Table 2.1: Summary of Notations

Chapter 3

Optimization of Zero Leakage Helper Data System

This chapter first introduces the problem formulation. The first problem that will be elaborated on this chapter is on defining the optimal reconstruction boundaries.

Followed by the optimization of the quantization boundaries. The optimization of Zero Leakage Helper Data System (ZLHDS) is computed by maximizing the mutual information.

3.1 Problem Formulation

There are two main problems on the optimization of ZLHDS. They are:

- finding the optimal reconstruction boundaries for ZLHDS algorithm
- optimize the quantization intervals so that $I(S;\hat{S}|W)$ is maximized; while maintaining a reasonable error rate

These problems is elaborated further on the following sections.

3.2 Determining The Optimal Reconstruction Boundaries

The lower boundary of a reconstruction region of a certain secret s is defined as a threshold $\tau_{s,w}$. The reconstruction boundaries is constructed with the main objective is to obtain $\hat{s} = s$. This can be attained when the authentication data y satisfy $\tau_{s,w} \leq y < \tau_{s+1,w}$. The illustration of this reconstruction boundaries is displayed on Figure 2.5. The lowest and the highest boundaries are fixed, $\tau_{0,w} = -\infty$ and $\tau_{N,w} = \infty$.

In order to produce an exact reconstruction of secret s, maximum likelihood algorithm is utilized to determine the most probable $\hat{s}$ given known y and w.

Lemma 3.2.1. *The optimal reconstruction of secret s is*

$$\mathrm{Rec}(y, w) = \arg\max_{s \in S} \psi(y|\xi_{s,w}) p_s. \tag{3.1}$$

Proof. This is a slight modification of Lemma 4.1 from [3] with the same starting point

$$\mathrm{Rec}(y, w) = \arg\max_{s \in S} f(s|y, w) \tag{3.2}$$

$$= \arg\max_{s \in S} \frac{f(s,y,w)}{f(y,w)}. \tag{3.3}$$

Since the denominator does not depend on s, it can be eliminated

$$\mathrm{Rec}(y,w) = \arg\max_{s \in S} f(s,y,w) \tag{3.4}$$

$$= \arg\max_{s \in S} f(y|s,w)\, f(w|s)\, p_s \tag{3.5}$$

and since for every enrollment data there is a corresponding w-value, it results in $f(w|s) = 1$ (see Appendix A.1 for the proof), then it yields

$$\mathrm{Rec}(y,w) = \arg\max_{s \in S} f(y|s,w)\, p_s. \tag{3.6}$$

Since knowing s and w is equal as knowing $\xi_{s,w}$ and given $\psi(y|\xi_{s,w})$ as the probability density function of $y|\xi_{s,w}$, then the Eq. (3.6) becomes Eq. (3.1) □

From Eq.(3.1) we can derive a general lemma of $\tau_{s,w}$ for general noise.

Lemma 3.2.2. *The reconstruction boundary $\tau_{s,w}$ that gives equal probability for s and $s-1$ can be defined as*

$$p_s \psi(\tau_{s,w}|\xi_{s,w}) = p_{s-1}\psi(\tau_{s,w}|\xi_{s-1,w}). \tag{3.7}$$

Proof. Using Lemma 3.2.1 to reconstruct the secret that gives equal probability for s and $s-1$, we define y as the boundary $\tau_{s,w}$.

$$p_s \psi(y|\xi_{s,w}) = p_{s-1}\psi(y|\xi_{s-1,w}) \tag{3.8}$$

□

In the fuzzy extractor, the value of p_s is not depend on s due to its uniformity distribution. However, in this general helper data system, similar to secure sketch, the value of p_s needs to be considered.

In the case of Gaussian noise, we have:

$$\psi(y|\xi_{s,w}) = \varphi_{\sigma_R}(y - \lambda\xi_{s,w}). \tag{3.9}$$

Theorem 3.2.3. *Let the noise be Gaussian with zero mean and variance σ_R^2, then the optimal placement of reconstruction boundaries is*

$$\tau_{s,w} = \frac{\sigma_R^2 \ln \frac{p_s}{p_{s-1}}}{\lambda\,(\xi_{s-1,w} - \xi_{s,w})} + \lambda\frac{(\xi_{s-1,w} + \xi_{s,w})}{2}. \tag{3.10}$$

Proof. The proof for Theorem 3.2.3 closely follows Theorem 4.2 from [3]. We apply Gaussian noise on $\psi(y|\xi_{s,w})$, under Eq. (3.1), to define a point $y = \tau_{s,w}$ that gives equal probability for s and $s-1$.

$$\varphi_{\sigma_R}(y - \lambda\xi_{s-1,w})p_{s-1} = \varphi_{\sigma_R}(y - \lambda\xi_{s,w})p_s \tag{3.11}$$

$$\iff \qquad \frac{1}{\sigma_R\sqrt{2\pi}} e^{-\frac{(y-\lambda\xi_{s-1,w})^2}{2\sigma_R^2}} p_{s-1} = \frac{1}{\sigma_R\sqrt{2\pi}} e^{-\frac{(y-\lambda\xi_{s,w})^2}{2\sigma_R^2}} p_s \tag{3.12}$$

$$\iff \ln\left(e^{-\frac{(y-\lambda\xi_{s-1,w})^2}{2\sigma_R^2}} p_{s-1}\right) = \ln\left(e^{-\frac{(y-\lambda\xi_{s,w})^2}{2\sigma_R^2}} p_s\right) \tag{3.13}$$

$$\iff \frac{-(y-\lambda\xi_{s-1,w})^2}{2\sigma_R^2} + \ln p_{s-1} = \frac{-(y-\lambda\xi_{s,w})^2}{2\sigma_R^2} + \ln p_s \tag{3.14}$$

$$\iff 2y\lambda\xi_{s-1,w} - \lambda^2\xi_{s-1,w}^2 + 2\sigma_R^2 \ln p_{s-1} = 2y\lambda\xi_{s,w} - \lambda^2\xi_{s,w}^2 + 2\sigma_R^2 \ln p_s \tag{3.15}$$

$$\iff 2y\lambda\left(\xi_{s-1,w} - \xi_{s,w}\right) = 2\sigma_R^2 \ln\frac{p_s}{p_{s-1}} + \lambda^2\left(\xi_{s-1,w}^2 - \xi_{s,w}^2\right) \tag{3.16}$$

$$\iff 2y = \frac{2\sigma_R^2 \ln\frac{p_s}{p_{s-1}} + \lambda^2\left(\xi_{s-1,w}^2 - \xi_{s,w}^2\right)}{\lambda\left(\xi_{s-1,w} - \xi_{s,w}\right)} \tag{3.17}$$

$$\iff y = \frac{\sigma_R^2 \ln\frac{p_s}{p_{s-1}}}{\lambda\left(\xi_{s-1,w} - \xi_{s,w}\right)} + \lambda\frac{\xi_{s-1,w} + \xi_{s,w}}{2} \tag{3.18}$$

by notating the threshold as $y = \tau_{s,w}$ thus we have the result in Eq. (3.10). □

Remark. In the case of Fuzzy Extractor algorithm, the Eq. (3.10) is reduced to the result of [3].

$$\tau_{s,w} = \lambda\frac{\xi_{s-1,w} + \xi_{s,w}}{2}. \tag{3.19}$$

Lemma 3.2.1 and Theorem 3.2.3 are new results.

3.3 Optimization of the Quantization Intervals

Interval of quantization regions under curve $\psi(y|x)$ is defined as the probability of the reconstructed secret $p_{\hat{s}}$. The optimization of the quantization intervals is obtained by maximizing the mutual information between S and $\hat{S}$ given W, which can be notated as $I(S;\hat{S}|W)$.

Lemma 3.3.1. *For zero leakage helper data system the mutual information can be formulated as*

$$I(S;\hat{S}|W) = H(S) - H(S|\hat{S},W) = I(S;\hat{S},W). \tag{3.20}$$

Proof of Lemma 3.3.1.

$$I(S;\hat{S}|W) = H(S|W) - H(S|\hat{S},W) \tag{3.21}$$

for ZL, it holds that $H(S|W) = H(S)$. □

Since S and W are independent, Lemma 3.3.1 can also be re-written into the following lemma.

Lemma 3.3.2.

$$I(S;\hat{S},W) = \sum_{s,\hat{s}} \mathbb{E}_w p_s \Upsilon_{\hat{s}|s,w} \ln\frac{\Upsilon_{\hat{s}|s,w}}{\Lambda_{\hat{s}|w}} \tag{3.22}$$

The proof is in Appendix A.2.

The aim of this thesis is to maximize $I(S;\hat{S}|W)$. The numerics of Lemma 3.3.2 are presented in Chapter 4, in the case of Gaussian source and Gaussian noise, along with the discussion of the analytical approach.

3.4 Reconstruction Error Probability

The error rate is calculated as the probability of the incorrect secret reconstruction. Since

$$\Pr[\hat{S} = Q(x)|X = x] = \int_{\tau_{Q(x),g(x)}}^{\tau_{Q(x)+1,g(x)}} \mathrm{d}y\, \psi(y|x) \tag{3.23}$$

$$= V(\tau_{Q(x)+1,g(x)} - \lambda\xi_{Q(x),g(x)}) - V(\tau_{Q(x),g(x)} - \lambda\xi_{Q(x),g(x)}). \tag{3.24}$$

then the probability of the correct reconstruction is

$$\Pr[\hat{S} = S] = \mathbb{E}_x \int_{\tau_{Q(x),g(x)}}^{\tau_{Q(x)+1,g(x)}} \mathrm{d}y\, \psi(y|x) \tag{3.25}$$

with $s = Q(x)$ and $w = g(x)$, we have

$$= \sum_s p_s \mathbb{E}_w [V(\tau_{s+1,w} - \lambda\xi_{s,w}) - V(\tau_{s,w} - \lambda\xi_{s,w})] \tag{3.26}$$

$$= \sum_s p_s \mathbb{E}_w \Upsilon_{s|s,w}. \tag{3.27}$$

The Average Reconstruction Error Probability is defined as

$$E_{\mathrm{Rec}} = 1 - \Pr[\hat{S} = S]. \tag{3.28}$$

Such that it becomes

Definition 3.4.1.

$$E_{\mathrm{Rec}} = 1 - \sum_s p_s \mathbb{E}_w \Upsilon_{s|s,w}. \tag{3.29}$$

Chapter 4

Numerical Analysis of Zero Leakage Helper Data System

This section describes the numerical analysis for the optimization of Zero Leakage Helper Data System (ZLHDS) algorithm. The numerics were done in Mathematica 10.0 Student Edition. To simplify the calculation, the source is assumed to be Gaussian with zero mean and a variance equal to one. The noise is also assumed to be a zero mean Gaussian, which modeled under perfect enrollment where $\lambda = 1$. The adjustable parameters for our numerical analysis are the number of secret, N, and the noise variance, σ_R. The objective of this numerical analysis is to find the optimum $\vec{p}$ that maximize $I(S;\hat{S}|W)$. We also compare the result of ZLHDS with the result Zero Leakage Fuzzy Extractor (ZLFE).

4.1 The Numerical Analysis

The first step is to define all of the required formulas to perform the numerical analysis. They are the mutual information formula based on Lemma 3.3.2 and the error probability based on Definition 3.4.1. The required definition for the error probability is only $\Upsilon_{\hat{s}|s,w}$. On the other hand, the mutual information requires several of definitions. These required definitions are given in the Figure 4.1 below. The detailed form of each definitions are given in Section 2.8.

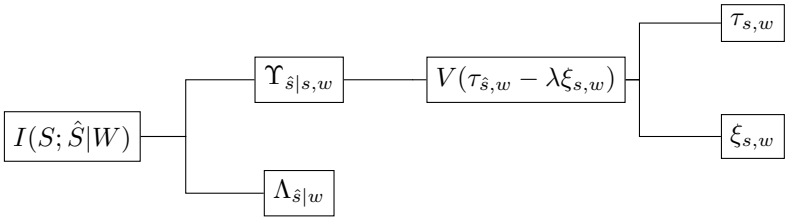


Figure 4.1: Chart of the required definitions for the numerics

For $\tau_{s,w}$, since it is fixed that $\tau_{0,w} = -\infty$ and $\tau_{N,w} = \infty$ then $\tau_{s,w}$ only need to be calculated for $s = \{1, \ldots, N-1\}$. When the p_{N-2} is very small compared to p_{N-3} and p_{N-1}, the order of $\tau_{s,w}$ may switched. For an illustration of this behavior, see Figure 4.2. There is no intersection between p_1 and p_2 because p_1 is too small. Instead, p_2 intersects with p_0, in which this intersection happens before the intersection between p_0 and p_1. Thus, the order of the boundary is switched.

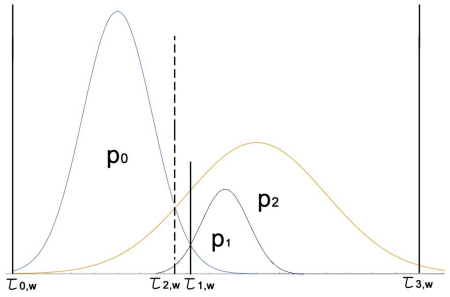
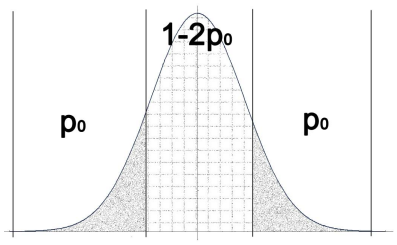


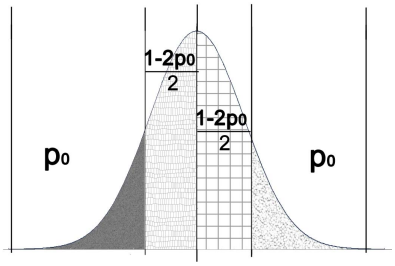
Figure 4.2: Illustration for the switched $\tau_{s,w}$ for $N = 3$. Each gaussian represents the distribution of the noise which is $v(y - \lambda\xi_{s,w})$ with $\lambda = 1$.

The optimum $\vec{p}$ that maximize the $I(S;\hat{S}|W)$ will never be this drastically different from each other. Hence, the pathological case as shown in Figure 4.2 will never occurs as the optimum $\vec{p}$. Lemma 3.2.2 will always hold in our numerics.

Since the Gaussian source and the Gaussian noise are centered at zero, we knew it in advance that the probability of $\vec{p}$ is symmetric. We used this symmetry to simplify the numerics. For example, for $N = 3$ the value of p_0 and p_2 are identical. Thus, the value of p_1 can easily be calculated as $p_1 = 1 - 2p_0$. We can expect that for $N = 4$, the $\vec{p} = \{p_0, p_1, p_1, p_0\}$, where $p_1 = (1 - 2p_0)/2$. These examples are depicted on Figure 4.3. For $N = 5$ we have $\vec{p} = \{p_0, p_1, 1-2(p_0+p_1), p_1, p_0\}$ and for $N = 6$ is $\vec{p} = \{p_0, p_1, 1-2(p_0+p_1)/2, 1-2(p_0+p_1)/2, p_1, p_0\}$.



(a) $N = 3$.



(b) $N = 4$.

Figure 4.3: Illustration of Symmetrical Probability for $N \in \{3, 4\}$. The gaussian represents the distribution of the source, $f(x)$.

The procedure of finding the maximum mutual information value and the optimum $\vec{p}$ is performed using `FindMaximum` in Mathematica. This command allows the searching of local maximum and its corresponding p values subject to certain constraint in a continuous domain.

Figure 4.4 shows an example of of mutual information with $N = 3$ and $\sigma_R = 0.5$ for p_0 and p_1 in range of $\{0.08, \ldots, 0.72\}$. As can be seen, the highest mutual information is above 0.8 for a combination of p_0 around 0.2 and $0.4 < p_1 < 0.6$. According to Table 4.1, the mutual information result for ZLFE with $N = 3$ and $\sigma_R = 0.5$ is 2% lower than the result of ZLHDS. Thus, the highest mutual information for ZLHDS is slightly above the result of the ZLFE with uniform probability.

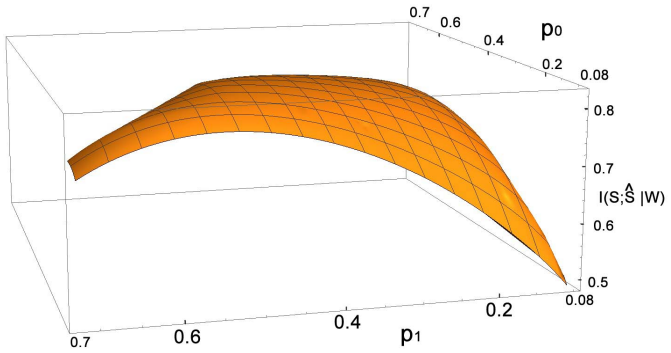


Figure 4.4: Example: $I(S;\hat{S}|W)$ for $N = 3$, $\sigma_R = 0.5$ as a function of p_0 and p_1.

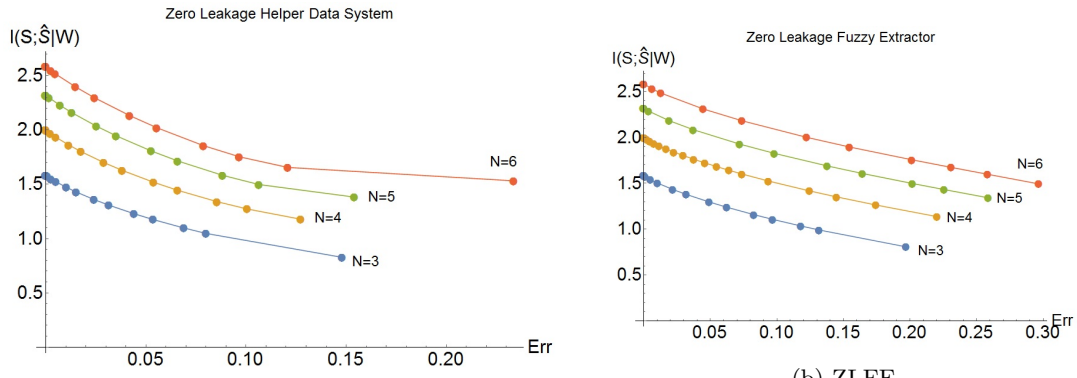
Table 4.1: Comparison of Secret Reconstruction between ZLHDS and ZLFE with N = 3

σ_R	**ZLHDS**			**ZLFE**	
	$\vec{p}$	$I(S;\hat{S}\|W)$	E_{Rec}	$I(S;\hat{S}\|W)$	E_{Rec}
0.01	$\{0.333, 0.334, 0.333\}$	1.585	1.1×10^{-15}	1.585	1.1×10^{-15}
0.03	$\{0.333, 0.334, 0.333\}$	1.585	1.1×10^{-15}	1.585	1.1×10^{-15}
0.05	$\{0.333, 0.334, 0.333\}$	1.585	1.1×10^{-15}	1.585	1.1×10^{-15}
0.08	$\{0.333, 0.334, 0.333\}$	1.585	1.1×10^{-15}	1.585	1.2×10^{-8}
0.10	$\{0.333, 0.334, 0.333\}$	1.585	3.2×10^{-6}	1.585	3.2×10^{-6}
0.13	$\{0.329, 0.342, 0.329\}$	1.583	0.0002	1.582	0.0002
0.15	$\{0.322, 0.355, 0.322\}$	1.575	0.0007	1.573	0.0011
0.18	$\{0.309, 0.382, 0.309\}$	1.551	0.003	1.539	0.005
0.20	$\{0.299, 0.400, 0.299\}$	1.525	0.005	1.504	0.010
0.23	$\{0.286, 0.428, 0.286\}$	1.473	0.010	1.433	0.022
0.25	$\{0.279, 0.442, 0.279\}$	1.430	0.015	1.380	0.032
0.28	$\{0.268, 0.464, 0.268\}$	1.360	0.024	1.290	0.049
0.30	$\{0.262, 0.476, 0.262\}$	1.310	0.032	1.240	0.062
0.33	$\{0.254, 0.491, 0.254\}$	1.230	0.044	1.159	0.083
0.35	$\{0.250, 0.499, 0.250\}$	1.176	0.053	1.107	0.097
0.38	$\{0.246, 0.508, 0.246\}$	1.098	0.069	1.036	0.118
0.40	$\{0.244, 0.512, 0.244\}$	1.048	0.080	0.991	0.132
0.50	$\{0.253, 0.494, 0.253\}$	0.827	0.148	0.808	0.197

4.2 The Result: Performance of ZLHDS

Table 4.1 displays the comparison of secret reconstruction between ZLHDS and ZLFE algorithm for $N = 3$. As shown on the table, when the noise variance is very low the ZLHDS coincides with the ZLFE. However, as the noise variance becomes larger, the ZLHDS is slightly better than the ZLFE. Further results for the comparison of ZLHDS and ZLFE are given in the Appendix B.

We analyze the ZLHDS and the ZLFE reconstruction performances for $N \in \{3, 4, 5, 6\}$ as shown in Figure 4.5. Every point in the graph corresponds to a σ_R value. According to Figure 4.5, the result of ZLHDS reconstruction algorithm is slightly better than the result of ZLFE.



(a) ZLHDS

(b) ZLFE

Figure 4.5: $I(S; \hat{S}|W)$ and Error probability for $N \in \{3, 4, 5, 6\}$ and $\sigma_R \in \{0.01, \ldots, 0.3\}$ for ZLHDS and ZLFE.

4.3 Discussion

The numerical analysis enables us to find the optimum $\vec{p}$ that maximize $I(S; \hat{S}|W)$. For a noise variance less than 0.10, the result of ZLHDS coincides with the result of ZLFE, regardless the number of N used. As the data becomes more noisy, the ZLHDS is able to extract information approximately 2%-5% better than ZLFE. This is because the non-uniform probability gives a noise resilient quantization region compared to those using the uniform probability. For a noise variance larger than 0.15 the error probability of ZLHDS is half of those of ZLFE.

Under the assumptions of zero mean Gaussian source and zero mean Gaussian noise distribution, the optimum probability of $\vec{p}$ is symmetrical. Thus, we can simplify the search range of $\vec{p}$ while finding the maximum $I(S; \hat{S}|W)$. For example, for $N = 3$ and $N = 4$, the search range of $\vec{p} = \{p_0, \ldots, p_{N-1}\}$ can be simplified into one dimensional region since $p_0 = p_{N-1}$. Therefore, p_1 can be calculated as $p_1 = 1 - 2p_0$ for $N = 3$ and $p_1 = (1 - 2p_0)/2$ for $N = 4$. Thus, it only need to search for p_0 value. While for $N = 5$ and $N = 6$, the search range is two dimensional. For $N = 7$ and above, the computation becomes labor intensive since the search range is larger than two dimensional space. For example, for $N = 7$ and $N = 8$ requires three dimensional search range, for $N = 9$ and $N = 10$ requires four dimensional search range and so on.

As the noise variance becomes larger, the computational time is also becomes longer. When the variance is less than 0.1 the numerics took about 5-10 minutes to execute. While for a variance larger than 0.20 the computational time took around 30 minutes or more, depends on the N values. On the other hand, sometimes the computation does not converge even after more

than several hours had passed. For example, for $N = 6$ and $\sigma_R = 0.33$ the computation does not converge even after three hours.

Chapter 5

Optimization Using Lagrange Multiplier and Implicit Function Theorem

This section describes our theoretical analysis approach in maximizing $I(S;\hat{S}|W)$ in Zero Leakage Helper Data System (ZLHDS) for more general case, which is for arbitrary source distribution and arbitrary noise distribution. We also aim to speed up the optimization by numerically solving a set of analytical equations.

In order to maximize $I(S;\hat{S}|W)$, Lagrange multiplication algorithm is applied with constraints $\sum_{\beta} p_\beta = 1$ and $E_{\text{Rec}} = \kappa$, where κ is a constant.

5.1 The Lagrange Multiplier Approach

The Lagrangian for our optimization problem is defined as

$$L[\vec{p}, c_1, c_2] = I(S;\hat{S}|W) + c_1 \left(\sum_{\beta=0}^{N-1} p_\beta - 1 \right) + c_2(E_{\text{Rec}} - \kappa) \tag{5.1}$$

where c_1 and c_2 are the Lagrange multipliers.

The unknown variables in Eq. (5.1) are c_1, c_2 and $\{p_\alpha\}$. Therefore, the partial derivatives over c_1, c_2 and p_α need to be calculated and need to be set to zero.

The derivation of $L[\vec{p}, c_1, c_2]$ over c_1 is quite straightforward and is given as follows:

$$0 = \frac{\partial L[\vec{p}, c_1, c_2]}{\partial c_1} = \sum_{\beta=0}^{N-1} p_\beta - 1 \tag{5.2}$$

which is precisely the conservation of the probability constraint.

Similar case goes for the derivative over c_2:

$$0 = \frac{\partial L[\vec{p}, c_1, c_2]}{\partial c_2} = E_{\text{Rec}} - \kappa \tag{5.3}$$

On the other hand, the partial derivatives of $L[\vec{p}, c_1, c_2]$ over p_α is very tedious.

We split the derivative of Eq.(5.1) into three parts; the derivative of mutual information and the derivative of the constraint terms; and solve it from the simplest thing first. The partial derivative of the normalization constraint over p_α is

$$\frac{\partial \left[c_1(\sum_\beta p_\beta - 1) \right]}{\partial p_\alpha} = c_1 \sum_\beta \frac{\partial p_\beta}{\partial p_\alpha} - 0 \tag{5.4}$$

$$= c_1 \sum_\beta \delta_{\beta,\alpha} \tag{5.5}$$

$$= c_1. \tag{5.6}$$

In order to solve the derivative of the mutual information over p_α, we need the following lemmas. The proofs of all lemmas are in the Appendix A.

Lemma 5.1.1. *The partial derivative of $H(S)$ over p_α is*

$$\frac{\partial H(S)}{\partial p_\alpha} = -\ln(ep_\alpha). \tag{5.7}$$

Lemma 5.1.2 ($\frac{\partial \Pi_{\hat{s},s|w}}{\partial p_\alpha}$)**.**

$$\frac{\partial \Pi_{\hat{s},s|w}}{\partial p_\alpha} = \delta_{s,\alpha} \Upsilon_{\hat{s}|s,w} + p_s \frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha}. \tag{5.8}$$

Lemma 5.1.3 ($\frac{\partial \Lambda_{\hat{s}|w}}{\partial p_\alpha}$)**.**

$$\frac{\partial \Lambda_{\hat{s}|w}}{\partial p_\alpha} = \Upsilon_{\hat{s}|\alpha,w} + \sum_s p_s \frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha}. \tag{5.9}$$

Proof.

$$\frac{\partial \Lambda_{\hat{s}|w}}{\partial p_\alpha} = \frac{\partial}{\partial p_\alpha} \sum_s \Pi_{\hat{s},s|w} \tag{5.10}$$

$$= \sum_s \frac{\partial}{\partial p_\alpha} \Pi_{\hat{s},s|w} \tag{5.11}$$

using Lemma 5.1.2, we have Eq. (5.9) as the result. □

Thus, we have the derivative of the mutual information on the following lemma.

Lemma 5.1.4 ($\frac{\partial I(S;\hat{S}|W)}{\partial p_\alpha}$)**.**

$$\frac{\partial I(S;\hat{S}|W)}{\partial p_\alpha} = -\ln(ep_\alpha) + \mathbb{E}_w \sum_{\hat{s}} \Upsilon_{\hat{s}|\alpha,w} \ln \Gamma_{\alpha|\hat{s},w} + \mathbb{E}_w \sum_{s,\hat{s}} p_s \frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha} \ln \Gamma_{s|\hat{s},w} \tag{5.12}$$

Until this stage, the unsolved derivative is $\frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha}$. In order to calculate $\frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha}$ we need the following lemmas:

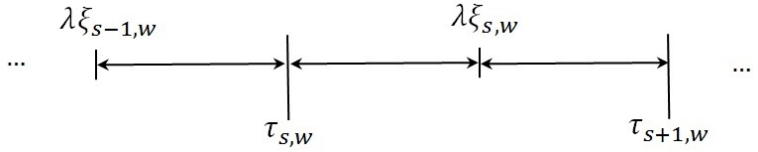


Figure 5.1: The relation between $\tau_{s,w}$ and $\xi_{s,w}$

Lemma 5.1.5 ($\frac{\partial \xi_{s,w}}{\partial p_\alpha}$)**.**

$$\frac{\partial \xi_{s,w}}{\partial p_\alpha} = \frac{1}{f(\xi_{s,w})}(\mathbf{1_{s-1}}(\alpha) + w\delta_{s,\alpha}). \tag{5.13}$$

Figure 5.1 illustrates the $\tau_{s,w}$ and the $\xi_{s,w}$. The $\tau_{s,w}$ represents the threshold of the reconstructed secret. The closed form expression for the general case is unknown. Thus, we will do the calculation of $\frac{\partial \tau_{s,w}}{\partial p_\alpha}$ using implicit function theorem.

Since $v()$ is an even function, where $v(\lambda\xi_{s,w} - \tau_{s,w}) = v(\tau_{s,w} - \lambda\xi_{s,w})$, then $G(\tau_{s,w}, \vec{p})$ can be defined as follows.

Definition 5.1.6 ($G(\tau_{s,w}, \vec{p})$)**.**

$$G(\tau_{s,w}, \vec{p}) = v(\tau_{s,w} - \lambda\xi_{s,w})p_s - v(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1} \tag{5.14}$$

Lemma 5.1.7 ($\frac{\partial \tau_{s,w}}{\partial p_\alpha}$)**.**

$$\begin{aligned}\frac{\partial \tau_{s,w}}{\partial p_\alpha} = &-\frac{1}{v'(\tau_{s,w} - \lambda\xi_{s,w})p_s - v'(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1}} \\ &\Bigg[\left(v(\tau_{s,w} - \lambda\xi_{s,w}) - \lambda w\frac{1}{f(\xi_{s,w})}v'(\tau_{s,w} - \lambda\xi_{s,w})p_s\right)\delta_{s,\alpha} \\ &-\left(v(\tau_{s,w} - \lambda\xi_{s-1,w}) - \lambda w\frac{1}{f(\xi_{s-1,w})}v'(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1}\right)\delta_{s-1,\alpha} \\ &-\lambda\frac{1}{f(\xi_{s,w})}v'(\tau_{s,w} - \lambda\xi_{s,w})p_s\mathbf{1_{s-1}}(\alpha) + \lambda\frac{1}{f(\xi_{s-1,w})}v'(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1}\mathbf{1_{s-2}}(\alpha)\Bigg].\end{aligned} \tag{5.15}$$

Remark. $\frac{\partial \tau_{s+1,w}}{\partial p_\alpha}$ is the $\frac{\partial \tau_{s,w}}{\partial p_\alpha}$ with shifted index from s to $s+1$.

As defined in the Section 2.8, we have

$$\Upsilon_{\hat{s}|s,w} = V(\tau_{\hat{s}+1,w} - \lambda\xi_{s,w}) - V(\tau_{\hat{s},w} - \lambda\xi_{s,w}). \tag{5.16}$$

Thus, $\frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha}$ is calculated below.

Lemma 5.1.8 ($\frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha}$)**.**

$$\frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha} = v(\tau_{\hat{s}+1,w} - \lambda\xi_{s,w})\frac{\partial \tau_{\hat{s}+1,w}}{\partial p_\alpha} - v(\tau_{\hat{s},w} - \lambda\xi_{s,w})\frac{\partial \tau_{\hat{s},w}}{\partial p_\alpha} + \Big(v(\tau_{\hat{s},w} - \lambda\xi_{s,w}) - v(\tau_{\hat{s}+1,w} - \lambda\xi_{s,w})\Big)\lambda\frac{\partial \xi_{s,w}}{\partial p_\alpha} \tag{5.17}$$

Proof.

$$\frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha} = \frac{\partial}{\partial p_\alpha}\Big(V(\tau_{\hat{s}+1,w} - \lambda\xi_{s,w}) - V(\tau_{\hat{s},w} - \lambda\xi_{s,w})\Big) \tag{5.18}$$

$$= v(\tau_{\hat{s}+1,w} - \lambda\xi_{s,w})\frac{\partial(\tau_{\hat{s}+1,w} - \lambda\xi_{s,w})}{\partial p_\alpha} - v(\tau_{\hat{s},w} - \lambda\xi_{s,w})\frac{\partial(\tau_{\hat{s},w} - \lambda\xi_{s,w})}{\partial p_\alpha} \tag{5.19}$$

$$= v(\tau_{\hat{s}+1,w} - \lambda\xi_{s,w})\left(\frac{\partial\tau_{\hat{s}+1,w}}{\partial p_\alpha} - \lambda\frac{\partial\xi_{s,w}}{\partial p_\alpha}\right) - v(\tau_{\hat{s},w} - \lambda\xi_{s,w})\left(\frac{\partial\tau_{\hat{s},w}}{\partial p_\alpha} - \lambda\frac{\partial\xi_{s,w}}{\partial p_\alpha}\right) \tag{5.20}$$

□

The partial derivative of the error constraint over p_α is:

Lemma 5.1.9 ($\frac{\partial[c_2(E_{\text{Rec}}-\kappa)]}{\partial p_\alpha}$)**.**

$$\frac{\partial\left[c_2(E_{\text{Rec}} - \kappa)\right]}{\partial p_\alpha} = -c_2\mathbb{E}_w\Bigg[V(\tau_{\alpha+1,w} - \lambda\xi_{\alpha,w}) - V(\tau_{\alpha,w} - \lambda\xi_{\alpha,w}) + \sum_s p_s\left(v(\tau_{s+1,w} - \lambda\xi_{s,w})\frac{\partial\tau_{s+1,w}}{\partial p_\alpha} - v(\tau_{s,w} - \lambda\xi_{s,w})\frac{\partial\tau_{s,w}}{\partial p_\alpha}\right)\Bigg] \tag{5.21}$$

Proof.

$$\frac{\partial\left[c_2(E_{\text{Rec}} - \kappa)\right]}{\partial p_\alpha} = c_2\frac{\partial(E_{\text{Rec}} - \kappa)}{\partial p_\alpha} + (E_{\text{Rec}} - \kappa)\frac{\partial c_2}{\partial p_\alpha} \tag{5.22}$$

$$= c_2\frac{\partial E_{\text{Rec}}}{\partial p_\alpha} + 0 \tag{5.23}$$

using E_{Rec} based on Definition 3.4.1, we have

$$= c_2\frac{\partial\left(1 - \sum_s p_s\mathbb{E}_w\left(V(\tau_{s+1,w} - \lambda\xi_{s,w}) - V(\tau_{s,w} - \lambda\xi_{s,w})\right)\right)}{\partial p_\alpha} \tag{5.24}$$

$$= -c_2\sum_s \mathbb{E}_w\frac{\partial\left(p_s\left(V(\tau_{s+1,w} - \lambda\xi_{s,w}) - V(\tau_{s,w} - \lambda\xi_{s,w})\right)\right)}{\partial p_\alpha} \tag{5.25}$$

$$= -c_2\sum_s \mathbb{E}_w\Bigg[\delta_{s,\alpha}\left(V(\tau_{s+1,w} - \lambda\xi_{s,w}) - V(\tau_{s,w} - \lambda\xi_{s,w})\right) + p_s\left(v(\tau_{s+1,w} - \lambda\xi_{s,w})\frac{\partial\tau_{s+1,w}}{\partial p_\alpha} - v(\tau_{s,w} - \lambda\xi_{s,w})\frac{\partial\tau_{s,w}}{\partial p_\alpha}\right)\Bigg] \tag{5.26}$$

then we have Eq.(5.21) as the result.

□

5.2 Discussion

The optimization of ZLHDS approach using Lagrange Multiplier resulted in a more complicated formula compared to the original expression for $I(S;\hat{S}|W)$. Eq.(5.12) contains $\Upsilon_{\hat{s}|s,w} = \int_{\tau_{\hat{s},w}}^{\tau_{\hat{s}+1,w}} \mathrm{d}y\, v(y - \lambda\xi_{s,w})$ which is similar to the original expression of $I(S;\hat{S}|W)$ itself. We have not implemented the numerical analysis for this approach. Thus, it remains unclear for us whether the Lagrangian could optimize the performance of the numerical analysis at larger N.

Chapter 6

Summary

6.1 Conclusions

This thesis studied the general Helper Data System (HDS) and its particular zero leakage properties. The objective of this thesis is to maximize the extraction of information from a noisy data without leaking any confidential information.

There are three contributions of this thesis. The first contribution is the formulation for the optimal reconstruction boundaries. We have two new general formulas. They are Lemma 3.2.1 and Theorem 3.2.3. The second contribution is the maximization of the mutual information for zero leakage helper data system which described in Chapter 4. The numerical analysis assumed the source and the noise to be Gaussian with zero mean. We modeled the noise as perfect enrollment, where the attenuation parameter is equal to 1. The third contribution is the derivation of the analytical optimization equation, as described in Chapter 5.

In ZLHDS reconstruction, there is a possibility that the order of the $\tau_{s,w}$ is switched. This condition occurs when a small p_α is sandwiched between much larger $p_{\alpha-1}$ and $p_{\alpha+1}$, where α is a certain index in $\vec{p}$. This limits the search range when performing the numerical analysis. For a Gaussian source and Gaussian noise with zero mean, the optimum probability of $\vec{p}$ is symmetrical. This properties is useful to simplify the calculation of $\vec{p}$.

The numerical analysis of ZLHDS found the optimum $\vec{p}$ that maximizes the information extracted. The amount of the information extracted is decreases with increasing noise variance. This result is inline with the result of fuzzy extractor.

In conclusion, the performance of the ZLHDS is better than the ZLFE for certain noise variance. For a very small noise variance, the extracted information of ZLHDS algorithm coincides with the result of ZLFE. As the noise variance increases, the amount of of information extracted in ZLHDS is around 2%-5% better compared to ZLFE. While the error probability for a certain noise variance in ZLHDS even reaches half of the error probability in ZLFE.

We also perform an attempt to generalize the maximization of $I(S; S|W)$ using Lagrange Multiplier. This attempt produces complicated result and more formulas compared to our previous method. We have not perform the numerical analysis for this Lagrange optimization.

6.2 Future Work

ZLHDS algorithm is recommended for securely correcting noise in noisy data, as it can extract more information compared to ZLFE, for a certain range of noise variance. In this thesis, we have

studied the performance of ZLHDS for $N \in \{3, 4, 5, 6\}$, $\sigma_R \in \{0.01, \ldots, 0.3\}$. We only considered the perfect enrollment noise model where $\lambda = 1$. This thesis did not cover the problem for larger number of secret and larger noise variance.

In addition, there are several of open problems for future works, such as:

- explore the optimization of ZLHDS reconstruction for different noise model, e.g. where λ is not equal to one
- explore the optimization of ZLHDS reconstruction for a larger noise variance
- establish a generalized algorithm in maximizing the mutual information for arbitrary source distribution and arbitrary noise distribution.

Bibliography

[1] Josh Benaloh. Dense probabilistic encryption. In *Proceedings of the workshop on selected areas of cryptography*, pages 120–128, 1994. 4

[2] J.A. de Groot and J.-P.M.G. Linnartz. Zero leakage quantization scheme for biometric verification. In *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, pages 1920–1923, May 2011. 10

[3] Joep De Groot, Boris Škoric, Niels De Vreede, and Jean-Paul Linnartz. Information leakage of continuous-source zero secrecy leakage helper data schemes. *Gen*, 1:1, 2012. v, 5, 10, 11, 12, 13, 14, 17, 18, 19

[4] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM journal on computing*, 38(1):97–139, 2008. 4

[5] Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009. 4

[6] S Goldwasser and S Micali. Probabilistic encryption and how to play mental poker keeping secret all private information. In *Proceedings 14th ACM Symposium on the Theory of Computing*, 1982. 4

[7] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security*, pages 28–36. ACM, 1999. 4

[8] Steven G Krantz and Harold R Parks. *The implicit function theorem: history, theory, and applications*. Springer Science & Business Media, 2012.

[9] Stephen Lich-Tyler. Math for economic theory lecture notes. Implicit Function Theorem and Application, 2001.

[10] Jean-Paul Linnartz and Pim Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In *Audio-and Video-Based Biometric Person Authentication*, pages 393–402. Springer, 2003. 4

[11] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in cryptologyEUROCRYPT99*, pages 223–238. Springer, 1999. 4

[12] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–2030, 2002. 3

[13] Ronald L Rivest, Len Adleman, and Michael L Dertouzos. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978. 4

[14] Boris Škoric. Physical aspects of digital security lecture notes. Chapter 6 Fuzzy extractor and Secure Sketches, August 2014. 8, 9

[15] Evgeny Verbitskiy, Pim Tuyls, Chibuzo Obi, Berry Schoenmakers, and Boris Škorić. Key extraction from general nondiscrete signals. *Information Forensics and Security, IEEE Transactions on*, 5(2):269–279, 2010. 4, 5

Appendix A

Proofs

A.1 Proof of $f(w|s) = 1$

Proof of $f(w|s) = 1$. Knowing that

$$f(w|s)\mathrm{d}w = f(\xi_{s,w})\mathrm{d}\xi_{s,w}\frac{1}{p_s} \tag{A.1}$$

Thus we have

$$\begin{aligned} f(w|s) &= \frac{f(\xi_{s,w})}{p_s \mathrm{d}w/\mathrm{d}\xi_{s,w}} && \text{(A.2)}\\ &= \frac{f(\xi_{s,w})}{p_s \frac{\mathrm{d}}{\mathrm{d}\xi_{s,w}}\left[\frac{1}{p_s}F(\xi_{s,w}) - \sum_{j=0}^{s-1} p_j\right]} && \text{(A.3)}\\ &= \frac{f(\xi_{s,w})}{\mathrm{d}/\mathrm{d}\xi_{s,w}F(\xi_{s,w})} && \text{(A.4)}\\ &= \frac{f(\xi_{s,w})}{f(\xi_{s,w})} && \text{(A.5)}\\ &= 1 && \text{(A.6)} \end{aligned}$$

□

A.2 Proof of Lemma 3.3.2

Proof of $I(S;\hat{S},W)$.

$$\begin{aligned} I(S;\hat{S}|W) &= \sum_{s,\hat{s}} \mathbb{E}_w\, p_{s,\hat{s},w} \ln \frac{\Pi_{s,\hat{s}|w}}{p_s\, \Lambda_{\hat{s}|w}} && \text{(A.7)}\\ &= \sum_{s,\hat{s}} \mathbb{E}_w\, p_{s|w}\, p_w\, \Upsilon_{\hat{s}|s,w} \ln \frac{\Upsilon_{\hat{s}|s,w}\, p_s}{p_s\, \Lambda_{\hat{s}|w}} && \text{(A.8)} \end{aligned}$$

knowing that $p_w = 1$, ZL property $p_s = p_{s|w}$, we have Eq.(3.22) as the result. This Eq.(3.22) can also be written in the mutual information form such that:

$$I(S;\hat{S}|W) = I(S;\hat{S},W). \tag{A.9}$$

□

A.3 Proof of Lemma 5.1.1

Proof of $\frac{\partial H(S)}{\partial p_\alpha}$.

$$\frac{\partial H(S)}{\partial p_\alpha} = \frac{\partial \left(\sum_s p_s \ln \frac{1}{p_s} \right)}{\partial p_\alpha} \tag{A.10}$$

$$= -\sum_s \frac{\partial}{\partial p_\alpha} \left(p_s \ln p_s \right) \tag{A.11}$$

$$= -\sum_s \left(\ln p_s \frac{\partial p_s}{\partial p_\alpha} + p_s \frac{\partial \ln p_s}{\partial p_\alpha} \right) \tag{A.12}$$

knowing that $\frac{\partial p_s}{\partial p_\alpha} = \delta_{s,\alpha}$

$$= -\sum_s \left(\delta_{s,\alpha} \ln p_s + \delta_{s,\alpha} \frac{1}{p_s} p_s \right) \tag{A.13}$$

$$= -\sum_s \delta_{s,\alpha} (\ln p_s + 1) \tag{A.14}$$

finally we use $\sum_s \delta_{s,\alpha} \ln p_s = \ln p_\alpha$ and $\sum_s \delta_{s,\alpha} = 1$ which results the Eq. (5.7).

□

A.4 Proof of Lemma 5.1.2

Proof of $\frac{\partial \Pi_{\hat{s},s|w}}{\partial p_\alpha}$.

$$\frac{\partial \Pi_{\hat{s},s|w}}{\partial p_\alpha} = \frac{\partial \left(p_{s|w} \Upsilon_{\hat{s}|s,w} \right)}{\partial p_\alpha} \tag{A.15}$$

using ZL properties $p_{s|w} = p_s$ and chain rule

$$= \Upsilon_{\hat{s}|s,w} \frac{\partial p_s}{\partial p_\alpha} + p_s \frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha} \tag{A.16}$$

$$= \Upsilon_{\hat{s}|s,w} \delta_{s,\alpha} + p_s \frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha} \tag{A.17}$$

Thus, we have Eq. (5.8) as result. □

A.5 Proof of Lemma 5.1.4

Proof of $\frac{\partial I(S;\hat{S}|W)}{\partial p_\alpha}$.

$$\frac{\partial I(S;\hat{S}|W)}{\partial p_\alpha} = \frac{\partial H(S)}{\partial p_\alpha} - \frac{\partial H(S|\hat{S};W)}{\partial p_\alpha} \tag{A.18}$$

$$= -\ln(ep_\alpha) - \frac{\partial}{\partial p_\alpha}\Big(\mathbb{E}_w H(\hat{S};S|W=w) - \mathbb{E}_w H(\hat{S}|W=w)\Big) \tag{A.19}$$

$$= -\ln(ep_\alpha) - \mathbb{E}_w \sum_{s,\hat{s}} \frac{\partial H(\hat{S};S|W=w)}{\partial \Pi_{\hat{s},s|w}} \frac{\partial \Pi_{\hat{s},s|w}}{\partial p_\alpha} + \mathbb{E}_w \sum_{\hat{s}} \frac{\partial H(\hat{S}|W=w)}{\partial \Lambda_{\hat{s}|w}} \frac{\partial \Lambda_{\hat{s}|w}}{\partial p_\alpha} \tag{A.20}$$

$$= -\ln(ep_\alpha) + \mathbb{E}_w \sum_{s,\hat{s}} \ln(e\Pi_{\hat{s},s|w}) \frac{\partial \Pi_{\hat{s},s|w}}{\partial p_\alpha} - \mathbb{E}_w \sum_{\hat{s}} \ln(e\Lambda_{\hat{s}|w}) \frac{\partial \Lambda_{\hat{s}|w}}{\partial p_\alpha} \tag{A.21}$$

$$= -\ln(ep_\alpha) + \mathbb{E}_w \sum_{s,\hat{s}} \ln(e\Pi_{\hat{s},s|w}) \left(\delta_{s,\alpha} \Upsilon_{\hat{s}|s,w} + p_s \frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha}\right)$$
$$- \mathbb{E}_w \sum_{\hat{s}} \ln(e\Lambda_{\hat{s}|w}) \left(\Upsilon_{\hat{s}|\alpha,w} + \sum_s p_s \frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha}\right) \tag{A.22}$$

$$= -\ln(ep_\alpha) + \mathbb{E}_w \sum_{\hat{s}} \Upsilon_{\hat{s}|\alpha,w} \ln \frac{e\Pi_{\hat{s},\alpha|w}}{e\Lambda_{\hat{s}|w}} + \mathbb{E}_w \sum_{s,\hat{s}} p_s \frac{\partial \Upsilon_{\hat{s}|s,w}}{\partial p_\alpha} \ln \frac{e\Pi_{\hat{s},s|w}}{e\Lambda_{\hat{s}|w}} \tag{A.23}$$

Thus, we have Eq. 5.12 as the result. □

A.6 Proof of Lemma 5.1.5

Proof of $\frac{\partial \xi_{s,w}}{\partial p_\alpha}$.

$$\frac{\partial \xi_{s,w}}{\partial p_\alpha} = \frac{\partial F^{-1}\left(\sum_{i=0}^{s-1} p_i + w p_s\right)}{\partial p_\alpha} \tag{A.24}$$

$$= \frac{1}{f(\xi_{s,w})} \frac{\partial\left(\sum_{i=0}^{s-1} p_i + w p_s\right)}{\partial p_\alpha} \tag{A.25}$$

$$= \frac{1}{f(\xi_{s,w})} \left(\sum_{i=0}^{s-1} \delta_{i,\alpha} + w\delta_{s,\alpha}\right) \tag{A.26}$$

Thus, we have Eq.(5.13) as the result.

□

A.7 Proof of Lemma 5.1.7

Proof of $\frac{\partial \tau_{s,w}}{\partial p_\alpha}$.

$$\frac{\partial \tau_{s,w}}{\partial p_\alpha} = -\frac{\partial G/\partial p_\alpha}{\partial G/\partial \tau_{s,w}} \tag{A.27}$$

where

$$\frac{\partial G}{\partial p_\alpha} = \frac{\partial \left[v(\tau_{s,w} - \lambda\xi_{s,w})p_s - v(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1} \right]}{\partial p_\alpha} \tag{A.28}$$

$$\begin{aligned} &= v(\tau_{s,w} - \lambda\xi_{s,w})\frac{\partial p_s}{\partial p_\alpha} - \lambda\frac{\partial \xi_{s,w}}{\partial p_\alpha} v'(\tau_{s,w} - \lambda\xi_{s,w})p_s \\ &\quad - v(\tau_{s,w} - \lambda\xi_{s-1,w})\frac{\partial p_{s-1}}{\partial p_\alpha} + \lambda\frac{\partial \xi_{s-1,w}}{\partial p_\alpha} v'(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1} \end{aligned} \tag{A.29}$$

$$\begin{aligned} &= v(\tau_{s,w} - \lambda\xi_{s,w})\delta_{s,\alpha} - v(\tau_{s,w} - \lambda\xi_{s-1,w})\delta_{s-1,\alpha} \\ &\quad - \lambda\frac{1}{f(\xi_{s,w})}(\mathbf{1_{s-1}}(\alpha) + w\delta_{s,\alpha})v'(\tau_{s,w} - \lambda\xi_{s,w})p_s \\ &\quad + \lambda\frac{1}{f(\xi_{s-1,w})}(\mathbf{1_{s-2}}(\alpha) + w\delta_{s-1,\alpha})v'(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1} \end{aligned} \tag{A.30}$$

$$\begin{aligned} &= \left(v(\tau_{s,w} - \lambda\xi_{s,w}) - \lambda w\frac{1}{f(\xi_{s,w})} v'(\tau_{s,w} - \lambda\xi_{s,w})p_s \right) \delta_{s,\alpha} \\ &\quad - \left(v(\tau_{s,w} - \lambda\xi_{s-1,w}) - \lambda w\frac{1}{f(\xi_{s-1,w})} v'(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1} \right) \delta_{s-1,\alpha} \\ &\quad - \lambda\frac{1}{f(\xi_{s,w})} v'(\tau_{s,w} - \lambda\xi_{s,w})p_s\mathbf{1_{s-1}}(\alpha) + \lambda\frac{1}{f(\xi_{s-1,w})} v'(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1}\mathbf{1_{s-2}}(\alpha) \end{aligned} \tag{A.31}$$

$$\frac{\partial G}{\partial \tau_{s,w}} = \frac{\partial \left[v(\lambda\xi_{s,w} - \tau_{s,w})p_s - v(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1} \right]}{\partial \tau_{s,w}} \tag{A.32}$$

$$= v'(\tau_{s,w} - \lambda\xi_{s,w})p_s - v'(\tau_{s,w} - \lambda\xi_{s-1,w})p_{s-1} \tag{A.33}$$

Inputing Eq.(A.31) and Eq.(A.33) into Eq.(A.27), we have Eq.(5.15) as the result. □

Appendix B

Results

Table B.1: Comparison of Secret Reconstruction between ZLHDS and ZLFE with N = 4

σ_R	**ZLHDS**			**ZLFE**	
	$\vec{p}$	$I(S;\hat{S}\|W)$	E_{Rec}	$I(S;\hat{S}\|W)$	E_{Rec}
0.01	$\{0.250, 0.250, 0.250, 0.250\}$	2.0	1.1×10^{-15}	2.0	1.1×10^{-15}
0.03	$\{0.250, 0.250, 0.250, 0.250\}$	2.0	1.1×10^{-15}	2.0	1.1×10^{-15}
0.05	$\{0.250, 0.250, 0.250, 0.250\}$	1.99	2.7×10^{-11}	2.0	2.7×10^{-11}
0.08	$\{0.249, 0.251, 0.251, 0.249\}$	1.99	0.000015	1.99	0.000015
0.10	$\{0.244, 0.256, 0.256, 0.244\}$	1.99	0.00028	1.99	0.00037
0.13	$\{0.225, 0.275, 0.275, 0.225\}$	1.97	0.0022	1.96	0.0045
0.15	$\{0.211, 0.289, 0.289, 0.211\}$	1.94	0.0049	1.91	0.012
0.18	$\{0.189, 0.311, 0.311, 0.189\}$	1.86	0.0115	1.80	0.0299
0.20	$\{0.177, 0.323, 0.323, 0.177\}$	1.80	0.018	1.72	0.046
0.23	$\{0.161, 0.339, 0.339, 0.161\}$	1.70	0.029	1.60	0.074
0.25	$\{0.152, 0.348, 0.348, 0.152\}$	1.63	0.038	1.52	0.094
0.28	$\{0.141, 0.359, 0.359, 0.141\}$	1.52	0.054	1.42	0.125
0.30	$\{0.134, 0.366, 0.366, 0.134\}$	1.45	0.066	1.35	0.145
0.33	$\{0.128, 0.372, 0.372, 0.128\}$	1.34	0.086	1.26	0.175

Table B.2: Comparison of Secret Reconstruction between ZLHDS and ZLFE with N = 5

σ_R	**ZLHDS**			**ZLFE**	
	$\vec{p}$	$I(S;\hat{S}\|W)$	E_{Rec}	$I(S;\hat{S}\|W)$	E_{Rec}
0.01	$\{0.2, 0.2, 0.2, 0.2, 0.2\}$	2.32	1.1×10^{-15}	2.32	1.1×10^{-15}
0.03	$\{0.2, 0.2, 0.2, 0.2, 0.2\}$	2.32	1.1×10^{-15}	2.32	1.1×10^{-15}
0.05	$\{0.2, 0.2, 0.2, 0.2, 0.2\}$	2.32	7.3×10^{-15}	2.32	7.3×10^{-8}
0.08	$\{0.195, 0.200, 0.210, 0.200, 0.195\}$	2.32	0.0003	2.32	0.0004
0.10	$\{0.180, 0.206, 0.228, 0.206, 0.180\}$	2.29	0.0017	2.29	0.0036
0.13	$\{0.154, 0.218, 0.257, 0.218, 0.154\}$	2.23	0.007	2.18	0.019
0.15	$\{0.137, 0.225, 0.275, 0.225, 0.137\}$	2.16	0.013	2.08	0.037
0.18	$\{0.116, 0.235, 0.299, 0.235, 0.116\}$	2.04	0.025	1.92	0.072
0.20	$\{0.104, 0.239, 0.314, 0.239, 0.104\}$	1.95	0.035	1.83	0.098
0.23	$\{0.089, 0.245, 0.332, 0.245, 0.089\}$	1.81	0.053	1.69	0.138
0.25	$\{0.081, 0.247, 0.343, 0.247, 0.081\}$	1.72	0.07	1.61	0.16
0.28	$\{0.073, 0.249, 0.355, 0.249, 0.073\}$	1.58	0.09	1.49	0.20
0.30	$\{0.070, 0.252, 0.356, 0.252, 0.070\}$	1.49	0.11	1.43	0.23
0.33	$\{0.080, 0.259, 0.322, 0.259, 0.080\}$	1.38	0.15	1.34	0.26

Table B.3: Comparison of Secret Reconstruction between ZLHDS and ZLFE with N = 6

σ_R	**ZLHDS**			**ZLFE**	
	$\vec{p}$	$I(S;\hat{S}\|W)$	E_{Rec}	$I(S;\hat{S}\|W)$	E_{Rec}
0.01	$\{0.167, 0.167, 0.167, 0.167, 0.167, 0.167\}$	2.58	1.1×10^{-15}	2.58	1.1×10^{-15}
0.03	$\{0.167, 0.167, 0.167, 0.167, 0.167, 0.167\}$	2.58	3.1×10^{-13}	2.58	3.1×10^{-13}
0.05	$\{0.167, 0.167, 0.167, 0.167, 0.167, 0.167\}$	2.58	5.5×10^{-6}	2.58	5.5×10^{-6}
0.09	$\{0.143, 0.164, 0.193, 0.193, 0.164, 0.143\}$	2.55	0.003	2.53	0.007
0.10	$\{0.133, 0.165, 0.202, 0.202, 0.165, 0.133\}$	2.52	0.005	2.49	0.013
0.13	$\{0.105, 0.169, 0.226, 0.226, 0.169, 0.105\}$	2.39	0.015	2.31	0.045
0.15	$\{0.089, 0.170, 0.241, 0.241, 0.170, 0.089\}$	2.30	0.024	2.18	0.074
0.18	$\{0.069, 0.170, 0.261, 0.261, 0.170, 0.069\}$	2.13	0.042	2.0	0.122
0.20	$\{0.059, 0.169, 0.271, 0.271, 0.169, 0.059\}$	2.02	0.056	1.90	0.155
0.23	$\{0.049, 0.167, 0.284, 0.284, 0.167, 0.049\}$	1.86	0.079	1.76	0.202
0.25	$\{0.044, 0.166, 0.290, 0.290, 0.166, 0.044\}$	1.75	0.097	1.67	0.231
0.27	$\{0.042, 0.169, 0.289, 0.289, 0.169, 0.042\}$	1.66	0.12	1.60	0.26
0.30	$\{0.083, 0.222, 0.195, 0.195, 0.222, 0.083\}$	1.53	0.23	1.50	0.30