Note

Some democratic secret sharing schemes

Marco Carpentieri

Istituto per la Ricerca sui Sistemi Informatici Paralleli, Consiglio Nazionale delle Ricerche, Via Pietro Castellino 111, 80123 Napoli (Na), Italy

Received 1 March 1994; revised 8 August 1994

Abstract

In this paper, we consider the problem of constructing secret sharing schemes without the assistance of a Dealer. We show how to implement Brickell’s Vector space construction as a democratic secret sharing scheme. As a special case, we construct democratic threshold schemes by using Shamir’s method. In our democratic secret sharing schemes, the participants need no more information to be kept secret (shares) than they would need in the case where the schemes are constructed by a Dealer.

1. Introduction

Let \( P = \{P_1, \ldots, P_n\} \) be a finite set of \( n \) participants and \( \Gamma \) be a set of subsets of \( P \). A secret sharing scheme is a method to distribute partial information or shares to the participants in \( P \) in such a way that

- any set of participants \( A \in \Gamma \) can determine a secret \( s \),
- no subset of participants \( A' \notin \Gamma \) can do so.

The set \( \Gamma \) is called the access structure and the subsets in \( \Gamma \) are called authorized subsets. A secret sharing scheme is said to be “Perfect” if no subset of participants \( A' \notin \Gamma \) can determine any partial information regarding the secret \( s \) (in an information theoretic sense) even with infinite computational resources. Blakley [3] and Shamir [15] introduced independently perfect \((k, n)\) threshold secret sharing schemes in 1979. A perfect \((k, n)\) threshold secret sharing scheme realizes a special access structure such that:

- any \( k \) participants can determine the secret \( s \),
- no subset of \( k - 1 \) participants or less can determine any partial information regarding \( s \).
Secret sharing schemes have received considerable attention in the last few years because of their many applications to several fields, such as data security, secure computation and others [11]. For an extensive bibliography and illustration of the main results in the area, the reader is referred to [18, 19].

In secret sharing classical literature, all schemes depend, in their realization, on the existence of a Dealer whose function is, first, to choose the secret \( s \) and, then, to determine and distribute the shares to the participants in \( \mathcal{P} \). Recently, various researchers have considered the possibility that the Dealer may attempt to cheat, distributing an inconsistent set of shares, so that the secret cannot be determined correctly or so that different subsets of participants in \( \Gamma \) would calculate different secrets from the shares they possess. Some papers that addressed the problem are [1, 2, 7].

For many applications, no one can be trusted to know the secret. Therefore, Ingemarsson and Simmons [12] considered the problem of constructing secret sharing schemes without the assistance of a Dealer. For example, "Unanimous consent secret sharing scheme" [12] realizes an access structure \( \Gamma \) where the only subset of participants that can determine the secret \( s \) is the set of all the participants in \( \mathcal{P} \). To implement a perfect unanimous consent secret sharing scheme, each of the participants in \( \mathcal{P} \) could choose his share to be a random element of a finite field \( GF(q) \) with \( q \) elements, where \( q \) is a prime power (throughout the paper we refer such a field by \( GF(q) \)). The sum over \( GF(q) \) of the shares of the participants in \( \mathcal{P} \) could be taken as the secret \( s \) of the scheme. Unanimous consent secret sharing schemes are well known schemes in literature [13, 19] and they have been used for several years to ensure unanimous consent before a controlled action can be initiated [17]. Unfortunately, unanimous consent secret sharing schemes are the only known example of schemes that can be implemented in such a way that the participants can define the secret \( s \) by a random choice of their shares. However, Ingemarsson and Simmons gave a protocol to construct secret sharing schemes realizing any access structures without the assistance of a Dealer. Briefly, in Ingemarsson and Simmons' protocol, the participants first construct a unanimous consent secret sharing scheme and then they share the random information chosen among other participants by using private secret sharing schemes. Ingemarsson and Simmons referred their schemes as "Democratic secret sharing schemes". Democratic secret sharing only permits the sharing of a "random" secret among the participants, whereas in a traditional secret sharing scheme the Dealer can share any secret he desires.

An important issue in the implementation of secret sharing schemes is the size of shares distributed to participants since the security of a system degrades as the amount of the information that must be kept secret increases. Recently, several papers studied this topic and both upper bounds and lower bounds on the size of the shares have been provided [4, 5, 8–10, 20]. In Ingemarsson and Simmons' proposals to implement democratic secret sharing schemes, the participants keep secret all the private information distributed by other participants. Consequently, so far, the main disadvantage of democratic secret sharing schemes, with respect to the schemes...
constructed by a Dealer, appeared to be the size of shares distributed to participants. In this paper, we show how to implement the Vector space construction due to Brickell [6] as a democratic secret sharing scheme. As a special case, we construct \((k, n)\) threshold democratic schemes by using Shamir's method [15]. In our democratic secret sharing schemes the participants need no more information to be kept secret (shares) than they would need in the case where the schemes are constructed by a Dealer.

2. The vector space democratic construction

Let \(\Gamma \neq \{\varnothing\}\) be the access structure that the participants in \(\mathcal{P}\) would like to realize and \(GF(q)^t\) be the \(t\)-dimensional vector space over \(GF(q)\), where \(t \geq 2\). Suppose there exists a function, known to all the participants,

\[
\psi: \mathcal{P} \cup \{X\} \rightarrow GF(q)^t,
\]

where \(X\) denotes an undetermined participant not in \(\mathcal{P}\) such that the following property is satisfied

1. the row vector \(\psi(X)\) can be expressed as a linear combination of the row vectors in the set \(\{\psi(P_i)\}: P_i \in A\) if and only if \(A\) is an authorized subset of the access structure \(\Gamma\).

To construct a democratic secret sharing scheme realizing \(\Gamma\) the participants in \(\mathcal{P}\) proceed as follows.

(i) Each participant \(P_j\) in \(\mathcal{P}\) chooses uniformly at random an element \(a_j\) in \(GF(q)\).

The secret is

\[
s = \sum_{j=1}^{n} a_j.
\]

(ii) Each participant \(P_i\) in \(\mathcal{P}\) chooses uniformly at random a row vector \(v_i\) in \(GF(q)^t\) such that \(a_i = v_i \cdot \psi(X)\), where "\cdot" is the inner product in \(GF(q)^t\). Then, \(P_i\) gives the element \(s_{i,j} = v_i \cdot \psi(P_j)\) to participant \(P_j\), for \(j = 1, \ldots, n\). Indeed, each participant \(P_j\) is able to calculate his own share as

\[
s_j = \sum_{i=1}^{n} s_{i,j}.
\]

The properties of the described construction are summarized in the following lemma.

**Lemma 1.** Any subset of participants \(A \in \Gamma\) can calculate the secret \(s\), but no subset of participants \(A' \notin \Gamma\) can determine any partial information regarding \(s\).
Proof. Since property (1) holds, for each authorized subset of participants \( A \in \Gamma \) it results

\[
\psi(X) = \sum_{l: P_l \in A} c_l \psi(P_l),
\]

where the elements \( c_l \) are known to all the participants in \( \mathcal{P} \). For each \( P_l \) in \( \mathcal{P} \) we have

\[
a_l = v_l \cdot \psi(X)
\]

\[
= v_l \cdot \sum_{l: P_l \in A} c_l \psi(P_l)
\]

\[
= \sum_{l: P_l \in A} c_l v_l \cdot \psi(P_l) \quad \text{(by linearity of "·")}
\]

\[
= \sum_{l: P_l \in A} c_l S_{i,l}.
\]

Let us sum \( a_l \) over \( i = 1, \ldots, n \), to get

\[
S = \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} \sum_{l: P_l \in A} c_l S_{i,l}
\]

\[
= \sum_{l: P_l \in A} \sum_{i=1}^{n} c_l S_{i,l} \quad \text{(by commutativity)}
\]

\[
= \sum_{l: P_l \in A} c_l \sum_{i=1}^{n} S_{i,l} \quad \text{(by linearity)}
\]

\[
= \sum_{l: P_l \in A} c_l S_l.
\]

Consequently, the participants in \( A \) can calculate the secret \( s \) as a linear combination of their own shares. Let \( A' \) be a nonauthorized subset of participants. For all \( P_j \) in \( A' \), we have

\[
S_j = \sum_{i=1}^{n} s_{i,j} = \sum_{i=1}^{n} v_l \cdot \psi(P_j)
\]

\[
= \sum_{i=1}^{n} \psi(P_j) \cdot v_l \quad \text{(by symmetry of "·")}
\]

\[
= \psi(P_j) \cdot \sum_{i=1}^{n} v_l \quad \text{(by linearity of "·")}
\]

\[
= \psi(P_j) \cdot \sum_{l: P_l \in A'} v_l + \psi(P_j) \cdot \sum_{l: P_l \in \mathcal{P} - A'} v_l.
\]
Likewise,

\[ s = \sum_{i=1}^{n} a_i = \psi(X) \cdot \sum_{i : P_i \in A'} v_i + \psi(X) \cdot \sum_{i : P_i \in \mathcal{P} - A'} v_i. \]

Denote

\[ v_{A'} = \sum_{i : P_i \in A'} v_i \quad \text{and} \quad v_{\mathcal{P} - A'} = \sum_{i : P_i \in \mathcal{P} - A'} v_i, \]

where \( v_{\mathcal{P} - A'} \) is a row vector in \( GF(q^f) \) unknown to all the participants in \( A' \). The best that the participants in \( A' \) can do to determine any information regarding the secret \( s \) is to consider the system of equations

\[ \psi(P_j) \cdot v_{\mathcal{P} - A'} = s_j - \psi(P_j) \cdot v_{A'}, \]

for all \( P_j \) in \( A' \), and

\[ \psi(X) \cdot v_{\mathcal{P} - A'} = s - \psi(X) \cdot v_{A'}. \]

Let \( d \) be the dimension of the subspace generated by the vectors \( \psi(P_j) \), for all \( P_j \) in \( A' \). Since property (1) holds, it results in \( d < t \) and, independently from the value of the secret \( s \), both the coefficient matrix and the augmented matrix of the system of equations have rank \( d + 1 \). Therefore, for each possible secret \( s \) there are \( q^{t-d-1} \) possible solutions for \( v_{\mathcal{P} - A'} \) and no information about \( s \) can be computed by the participants in \( A' \). \( \square \)

**Remark.** As a simple consequence of Lemma 1 the participants in \( \mathcal{P} \) can construct a \((k, n)\) threshold democratic scheme, where \( k < n \), as follows. The participants choose the elements \( a_i \) and the secret \( s \) is defined in \( GF(q) \), where \( q > n \), as in (i). Let \( a_1, \ldots, a_n \) be distinct, nonnull elements in \( GF(q) \) known to all the participants. Each participant \( P_i \) in \( \mathcal{P} \) chooses uniformly at random the elements \( a_{i,1}, \ldots, a_{i,k-1} \) in \( GF(q) \). If \( q_i(x) \) is the polynomial \( a_i + a_{i,1}x + \cdots + a_{i,k-1}x^{k-1} \), then \( P_i \) gives the element \( s_{i,j} = q_i(a_j) \) to participant \( P_j \), for \( j = 1, \ldots, n \). Indeed, each participant \( P_j \) is able to calculate his own share \( s_j \) as in (ii). Let \( q(x) \) be the sum of polynomials \( q_i(x) \), for \( i = 1, \ldots, n \), over \( GF(q) \). The secret \( s \) of the scheme is the constant term of the polynomial \( q(x) \) that any \( k \) participants can calculate by interpolation \([11,14]\).

**Acknowledgements**

The author thanks Professors Ugo Vaccaro, Alfredo De Santis, Roberto Vaccaro and Pasquale Lucio Scandizzo for their helpful suggestions and comments.
References

[1] B. Awerbuck, B. Chor, S. Goldwasser and S. Micali, Verifiable secret sharing and achieving simultane-
ity in the presence of faults, in: Proceedings of the 26th IEEE Symposium on Foundations of
[2] M. Ben-Or and T. Rabin, Verifiable secret sharing and multiparty protocols with honest majority, in:
schemes, in: Advances in Cryptology – CRYPTO ’92, Lecture Notes in Computer Science 740
schemes, in: Advances in Cryptology – EUROCRYPT ’92, Lecture Notes in Computer Science 658
105–113.
[8] E.F. Brickell and D.R. Stinson, Some improved bounds on the information rate of perfect secret
schemes, in: Advances in Cryptology – CRYPTO ’91, Lecture Notes in Computer Science 576
schemes, in: Advances in Cryptology – EUROCRYPT ’91, Lecture Notes in Computer Science 765
[12] I. Ingemarsson and G.J. Simmons, A protocol to set up shared secret schemes without the assistance
of a mutually trusted party, in: Advances in Cryptology – CRYPTO ’90, Lecture Notes in Computer
[16] G.J. Simmons, Robust shared secret schemes or “How to be sure you have the right answer even
[17] G.J. Simmons, Prepositioned shared secret schemes and/or shared control schemes, in: Advances in
436–467.
[18] G.J. Simmons, An introduction to shared secret and/or shared control schemes and their application,