Int. J. Nonlinear Anal. Appl. 5 (2014) No. 2, 60-66
ISSN: 2008-6822 (electronic)
http://www.ijnaa.semnan.ac.ir

Sharing Several Secrets based on Lagrange's Interpolation formula and Cipher Feedback Mode

Abbas Cheraghi*

Faculty of Mathematics & Computer, Khansar, University of Isfahan, Isfahan, Iran.

(Communicated by M. Eshaghi Gordji)

Abstract

In a multi-secret sharing scheme, several secret values are distributed among a set of n participants. In 2000 Chien et al.'s proposed a (t, n) multi-secret sharing scheme. Many storages and public values required in Chien's scheme. Motivated by these concerns, some new (t, n) multi-secret sharing schemes are proposed in this paper based on the Lagrange interpolation formula for polynomials and cipher feedback mode (CFB), which are easier than Chien's scheme in the secret reconstruction and require fewer number of public values and storages than Chien's scheme. Also our schemes don't need any one-way function and any simultaneous equations.

Keywords: Multi-secret sharing, Lagrange interpolation, Cipher feedback mode.
2010 MSC: Primary 94A62; Secondary 65D05.

1. Introduction and preliminaries

Secret sharing scheme plays an significant role in protecting important information from getting lost, annihilated or in to wrong hands. In a secret sharing scheme one secret value is distributed into shares among a set of participants in such a way that only the authorized subsets of participants can reconstruct the secret from their shares, while the participants in a forbidden subset cannot obtain any information about the secret value. In 1979, the first (t, n) threshold secret sharing scheme is proposed by Shamir [6] and Blakley [1] independently. In this kind of scheme a secret can be share among n participants in which at least t or more participants can reconstruct the secret, but $(t-1)$ or fewer participants can obtain nothing about the secret.

*Corresponding author
Email address: a.cheraghi@khn.ui.ac.ir (Abbas Cheraghi)

Received: August 2013 *Revised:* February 2014

Afterwards, several multi-secret sharing schemes were proposed ([2]–[5], [8]). In a multi-secret sharing scheme, there are several secrets to be shared during one secret sharing process. In 1994, Jakson et al. [4] classified multi-secret sharing schemes into two types: the one-time-use scheme and the multi-use scheme. In a one-time-use scheme, when some particular secrets have been reconstructed, the secret holder must redistribute fresh shares to every participant. On the other hand, in a multi-use scheme, every participant only needs to keep one share. Chien et al. [2] proposed a (t, n) multi-secret sharing scheme . In their paper at least t of the n participants can easily reconstruct m secrets at the same time. But the secret reconstruction needs to solve simultaneous equations, which is a complex process, in other words Chien's scheme is not very efficient, because Chien solved $(n + m - t)$ simultaneous equations. In order to reduce the complexity of the secret reconstruction, Yang et al. [8] proposed an alternative implementation of Chien's scheme based on Shamir's secret sharing [6]. The reconstruction in Yang's scheme is easier toward the Chien's scheme, but more public values are required in Yang's scheme than in Chien's scheme. Some new (t, n) multi-secret sharing schemes are proposed in this paper based on the Lagrange interpolation for polynomial and cipher feedback mode (CFB), which are easier than Chien's scheme in the secret reconstruction costs and require fewer number of public values and storages than Chien's scheme. Also our schemes don't need any one-way function and any simultaneous equations. We will present the unconditional security of secret sharing schemes. That is, we do not place any limit on the amount of computation that can be performed by any forbidden subset of participants. We first study a special type of secret sharing scheme called a threshold scheme. Here is an informal definition [7].

Definition 1.1. *Let t, n be positive integers, $t \leq n$. A (t, n) threshold scheme is a method of sharing a secret S among a set of n participants $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$, in such a way that any t participants can compute the value of S, but any subset of $t-1$ or fewer participants does not obtain any information about the secret.*

The value of S is chosen by a special person called the *dealer*. The dealer is denoted by D and we assume $D \notin \mathcal{P}$. When D wants to share the secret S among the set of participants in $\mathcal{P}$, he gives each participant some partial information called a share. The shares should be distributed secretly, so no participant knows the share given to another participant. In a multi-secret sharing scheme, several secret values are distributed among a set of n participants. In this paper some new methods are proposed based on the Lagrange interpolation formula and cipher feedback mode, which are easier than Chien's scheme.

The rest of this paper is organized as follows. In Section 1.1, we will briefly review Chien et al.'s multi-secret sharing scheme. In Section 2.1, we will present our first multi-secret sharing scheme base on Shamir's scheme. In Section 2.2, we will present our second multi-secret sharing scheme base on cipher feedback mode. Finally, in section 3, we will compare our methods with Chien et al.'s scheme in terms of the number of public values and the storages.

1.1. Review of Chien et al.'s scheme

At first gives a definition of a one-way function $f(r, x)$ with two variables r and x [2]. The one-way function has been used in Chien's scheme.

Definition 1.2. *Function $f(r, x)$ denotes any two-variables one-way function that maps any r and x onto a bit string $f(r, x)$ of a fixed length. The two-variable one-way function has several properties: (1) Given r and x it is easy to compute $f(r, x)$. (2) Given x and $f(r, x)$, it is hard to compute r. (3) Having no knowledge of x, it is hard to compute $f(r, x)$ for any r. (4) Given x, it is hard to find two different values r_1 and r_2 such that $f(r_1,x) = f(r_2,x)$. (5) Giving r and $f(r, x)$, it is hard to compute x. (6) Given pairs of r_i and $f(r, x)$, it is hard to compute $f(r', x)$ for $r' \neq r_i$.*

The properties of the two-variable one-way function have been proven in [3]. On the other hand, $G(N,K)$ denotes a special type of systematic block code generator matrix $G(N,K) = \begin{pmatrix} I \\ P \end{pmatrix}$, where I is a $K \times K$ identity matrix and P is a $(N-K) \times K$ matrix $[g^{(i-1)(j-1)}]$ for $1 \leq i \leq N-K$ and $1 \leq j \leq K$ with g being a primitive element in $GF(2^w)$ and $K < 2^w$. Here, $(S_1, S_2, \ldots, S_m)$ denotes m secrets to be shared among n participants. Before the secret sharing, D randomly chooses n secret shares or share $x_1, x_2, \ldots, x_n$ and distributes them to every participant over a secret channel. Then D performs the following steps:

1. Randomly choose an integer r and compute $f(r, x_i)$ for $i = 1, 2, ..., n$
2. Construct the generator matrix $G(2(n+m)-t, n+m)$ and $n+m < 2^w$.
3. Let $U = (S_1, S_2, ..., S_m, f(r,x_1), f(r,x_2), ..., f(r,x_n))^T$ be a vector and let the superscript T mean vector transposition.
4. Compute $V = G \times U = \begin{pmatrix} I \\ P \end{pmatrix} \times U$. The vector V can be expressed as

$$V = (S_1, S_2, ..., S_m, f(r,x_1), ..., f(r,x_n), c_1, c_2, ..., c_{n+m-t})^T, \quad (1)$$

where

$$c_i = \sum_{j=1}^{m} g^{(i-1)(j-1)} S_j + \sum_{j=m+1}^{n+m} g^{(i-1)(j-1)} f(r, x_{j-m}), 1 \leq i \leq m+n-t \quad (2)$$

5. Publish $(r, c_1, c_2, ..., c_{n+m-t})$ in any authenticated manner and so on.

If at least t participants pool their pseudo shares $f(r,x_i)$ (for $i = 1, 2, ..., t$), then the $(n+m-t)$ equations in Eq. (2) will contain only $(n+m-t)$ unknown symbols. Therefore, the secrets $(S_1, ..., S_m)$ and other participants' pseudo shares $f(r,x_i)$ (for $i = t+1, ..., n$) can be obtained by solving $(n+m-t)$ simultaneous equations in Eq. (2). According to the properties of the two-variable one-way function, dealer does not need to redistribute fresh secret shares to every participants in the next secret sharing session. The secret holder only has to choose and publish another random integer r. In Chien et al.'s scheme, there are $(n+m-t+1)$ public values required.

In next section two new (t,n) multi-secret sharing schemes are proposed based on the Lagrange interpolation for polynomial and cipher feedback mode (CFB).

2. New (t,n) multi-secret sharing schemes

In this section we will use the following notation. Let $\mathcal{P} = \{P_i : 1 \leq i \leq n\}$ be the set of n participants. The Shamir threshold scheme is presented as cryptosystem. In this scheme, the dealer constructs a random polynomial $f(x)$ of degree at most $t-1$. Every participant P_i obtains a distinct point (x_i, y_i) on this polynomial [7].

2.1. The scheme base on Lagrange's interpolation

The first scheme is based on Shamir (t,n) threshold scheme [6] and Lagrange's interpolation formula. Since the values of the secrets are usually chosen by the dealer, the first scheme can be described as follows:

Initialization Phase; Let dealer D decide to distribute m secrets among a set of n participants and how to choose the secrets and their values are not important. (for example suppose that these secrets are the m passwords of a complex safe deposit.) D select a large prime number q in which $q \geq n+m+1$.

- D independently at random and secretly chooses t elements of $\mathbb{Z}_q$, which are denoted $a_0, a_1, ..., a_{t-1}$.
- For $0 \leq i \leq m-1$, D computes the set of m secrets $S_i = f(i)$ where $f(x) = \sum_{j=0}^{t-1} a_j x^j \bmod q$.
- D chooses n distinct, non-zero elements of $\mathbb{Z}_q$, denoted x_i where $x_i \geq m$ and D gives the value x_i to P_i for $1 \leq i \leq n$. The values x_i are public.

Share Distribution; Suppose D wants to share m secrets $S_0, \ldots, S_{m-1} \in \mathbb{Z}_q$ among a set of n participants.

- For $1 \leq i \leq n$, D computes $y_i = f(x_i)$.
- For $1 \leq i \leq n$, D secretly gives the share y_i to P_i.

Finally, a subset of participants $B \subseteq \mathcal{P}$ will pool their shares in an attempt to compute the set of m secrets $\{S_0, \ldots, S_{m-1}\}$. (Alternatively, they could give their shares to a trusted authority which will perform the computation for them.) If $|B| \geq t$, then they should be able to compute the values of $S_0, \ldots, S_{m-1}$ as a function of the shares they collectively hold; if $|B| < t$, then they should not be able to compute none of them.

Reconstruction Phase; Let's look at how a subset B of t participants can reconstruct the secrets. This is basically accomplished by means of polynomial interpolation [7]. Suppose that participants $P_{r_1}, ..., P_{r_t}$ want to determine all of the secrets. They know that $y_{r_j} = f(x_{r_j})$. Since $f(x)$ has degree at most $t-1$, $f(x)$ can be written as $f(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1}$ where the coefficients $a_o, ..., a_{t-1}$ are unknown elements of $\mathbb{Z}_q$ and $S_i = f(i)$ are the secrets for $0 \leq i \leq m-1$. Since $y_{r_j} = f(x_{r_j})$, $1 \leq j \leq t$, the subset B can obtain t linear equations in the t unknowns $a_o, ..., a_{t-1}$, where all arithmetic is done in $\mathbb{Z}_q$. If the equations are linearly independent, there will be a unique solution. Clearly, it is important that the system of t linear equations has a unique solution. There are various ways to show that this is always the case. Perhaps the nicest way to address this question is to appeal to the Lagrange interpolation formula for polynomials. The formula for $f(x)$ is as follows:

$$f(x) = \sum_{j=1}^{t} (y_{r_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_{r_k}}{x_{r_j} - x_{r_k}}) \bmod q.$$

A group B of t participants can compute $f(x)$ by using the interpolation formula. But a simplification is possible, because the participants in B do not need to know the whole polynomial $f(x)$. It is sufficient for them to deduce the constant terms $S_i = f(i)$. Hence, they can compute the following expression, which is obtained by substituting $x = i$ into the Lagrange interpolation formula:

$$S_i = \sum_{j=1}^{t} (y_{r_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x_{r_k} - i}{x_{r_k} - x_{r_j}}) \bmod q \qquad (\text{for } 0 \leq i \leq m-1).$$

Suppose we define

$$b_{i,j} = \prod_{1 \le k \le t, k \ne j} \frac{x_{r_k} - i}{x_{r_k} - x_{r_j}} \bmod q,\ 1 \le j \le t \text{ and } 0 \le i \le m-1.$$

(Note that the $b_{i,j}$'s can be pre-computed, if desired, and their values are not secret.) Then we have $S_i = \sum_{j=1}^{t} b_{i,j} y_{r_j} \bmod q$. Hence, each secret is a linear combination (modulo q) of the t shares, so this scheme is easier than Chien's scheme in the secret reconstruction.

Security Analysis; Because our scheme is based on Shamir's scheme, at least t or more participants combining their shares will make it easy to reconstruct the secrets, but only $t-1$ or fewer participants will not do. In the information theoretic sense, our scheme is a perfect threshold scheme in which knowing only $t-1$ or fewer shares provides no more information about the secrets to an opponent than knowing no pieces.

The second our scheme is based on Cipher Feedback Mode which is also easier than Chien's scheme in the secret reconstruction and require fewer storages than Chien's scheme.

2.2. The scheme based on cipher feedback mode (CFB)

Like Chien's scheme, the second scheme is also based on Shamir's secret sharing. The rest of this section another new (t, n) multi-secret sharing scheme is proposed based on the Lagrange interpolation formula for polynomials and cipher feedback mode (CFB), which is easier than Chien's scheme in the secret reconstruction and requires fewer storages than Chien's scheme. We explain our method with CFB mode. At the first we define CFB mode and finally we describe our method and the secret construction. Let Addition modulo 2 corresponds to the exclusive-or operation and shown by $\oplus$ symbol. In this section all of the values are in binary representation.

2.2.1. CFB mode

Cipher feedback mode (CFB) was developed for DES. They were standardized in FTPS Publication 81 in December 1980. This mode of operation can be used (with minor change) for any block cipher. Here is short description of this mode of operation [7]. Let a sequence $S_1, S_2, \ldots, S_m$ of the secrets to produce a string of ciphertext, $c_1, c_2, \ldots, c_m$. Dealer starts with c_0=IV (an initialization vector as a first private value) and we produce the keystream element $I_1, I_2, \ldots, I_m$ by encrypting the previous ciphertext. That is, $I_i = e_k(c_{i-1})$ for all $1 \le i \le m$. Now we encrypt using the formula $c_i = S_i \oplus I_i$ for all $1 \le i \le m$. Note that the encryption function e_k is used for both encryption and decryption in CFB mode. Most popular encryption function are DES and AES [7]. Finally for decrypt we use the formula $S_i = c_i \oplus I_i$ for all $1 \le i \le m$.

2.2.2. Description of the second scheme

This scheme is also based on the Lagrange interpolation formula for polynomials and cipher feedback mode (CFB). It can be described as follows:

Initialization Phase; Let q be a large prime and all the numbers are elements in the finite field $GF(q)$ with binary representation of length $\lceil \log_2 q \rceil$. Let a sequence $S_1, S_2, \ldots, S_m$ of the m secrets. Dealer starts with c_0=IV as a first private value and a key k as a second private value for encryption and decryption functions. Then dealer D produces a string of ciphertext,

$c_1, c_2, \ldots, c_m$ corresponding to sequence $S_1, S_2, \ldots, S_m$ of the m secrets by CFB mode describe in section 2.2. Finally D publishes m public values $c_1, c_2, \ldots, c_m$.

Share distribution; D gives the shares to every participants as describe in section 2.1 as follows;

- D secretly chooses (independently at random) $t-2$ elements of $\mathbb{Z}_q$, which are denoted $a_2, ..., a_{t-1}$.
- For $1 \leq i \leq n$, D computes $y_i = f(x_i)$ where
  $f(x) = c_0 + kx + \sum_{j=2}^{t-1} a_j x^j \bmod q.$
- For $1 \leq i \leq n$, D gives the share (x_i, y_i) to each participants.

Reconstruction phase; A group B of t participants can compute $f(x)$ by using the Lagrange interpolation formula as follows:

$$f(x) = \sum_{j=1}^{t} (y_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}}) \bmod q$$

Subsequently, the secrets c_0 and k can be computed as $c_0 = f(0)$ and k as coefficient of x in $f(x)$. Finally the group B can reconstruct m secrets $S_1, S_2, \ldots, S_m$ from $(c_0, c_1, c_2, \ldots, c_m, k)$ by using the formula $S_i{=}c_i \oplus I_i$ for all $1 \leq i \leq m$ described in section 2.2.1.

Security Analysis; The security of this method depends on the security of $c_0 = IV$ and the value k, that both of them are coefficients of $f(x)$. Because of Shamir's scheme, at least t or more participants can reconstruct the values c_0 and k and finally reconstruct m secrets $S_1, S_2, \ldots, S_m$ from $(c_0, c_1, c_2, \ldots, c_m, k)$. On the other hands $t-1$ or fewer participants will not do, so this scheme is perfect.

3. Performance and analysis

Chien et al. used $(n+m-t+1)$ public values, $(2(n+m)-t) \times (n+m)$ storages, and solved $(n+m-t)$ simultaneous equations to share m secrets, while our first scheme uses n public values, t storages and no simultaneous equations, also each secret is a linear combination of the t shares. Moreover the second scheme uses $n+m$ public values, t storages and no simultaneous equations. Altogether when the first scheme apply for the number of the secrets more than $t-1$ then it needs the number of public values less than the Chien's scheme and less storages in all of the cases. Also the second scheme require fewer storages than Chiens scheme. Finally both of our schemes don't need any one-way function and any simultaneous equations. Moreover they are easier than Chien's scheme in the secret reconstruction.

References

[1] G. Blakley, *Safeguarding cryptographic keys,* in: Proc. AFIPS 1979 Natl. Conf., New York, (1979) 313–317.

[2] H.-Y. Chien, J.-K. Jan and Y.-M. Tseng, *A practical* (t, n) *multi-secret sharing scheme*, IEICE Transactions on Fundamentals E83-A 12 (2000) 2762–2765.

[3] L. Harn, *Efficient sharing (broadcasting) of multiple secret*, IEE Proceedings Computers and Digital Techniques 142 (3) (1995) 237–240.

[4] W.-A. Jackson, K.M. Martin and C.M. O'Keefe, *On sharing many secrets*, Asiacrypt'94 (1994) 42–54.

[5] L.-J. Pang and Y.-M. Wang, *A new* (t, n) *multi-secret sharing scheme based on Shamir's secret sharing*, Applied Mathematics and Computation 167 (2005) 840–848.

[6] A. Shamir, *How to share a secret*, Communications of the ACM 22 (1979) 612–613.
[7] Douglas R. Stinson, *Cryptography: Theory and Practice, 3rd Edition*, Chapman & Hall/CRC, (2006).
[8] C.-C. Yang, T.-Y. Chang and M.-S. Hwang, *A* (t, n) *multi-secret sharing scheme*, Applied Mathematics and Computation 151 (2) (2004) 483–490.