A new threshold multi secret sharing scheme

Massoud Hadian Dehkordi[i] and Samaneh Mashhadi[ii]

ABSTRACT

We present a new multi-secret sharing based on non-homogeneous linear recursion. Compared with the previous schemes, it has two easier methods for the recovery phase and fewer public values. Also, it has a simple construction phase. Altogether, it is a very efficient scheme and provides many functions for practical applications.

KEYWORDS

Threshold scheme, Multi-secret sharing, Non-homogeneous linear recursion, Public value.

1. INTRODUCTION

Secret sharing plays an important role in protecting important information from getting lost, destroyed, or into wrong hands. It has been an interesting branch of modern cryptography. In 1979, the first (t,n) threshold secret sharing scheme is proposed by Shamir [12] and Blakley [2] independently. Shamir's scheme [12] is based on the Lagrange interpolating polynomial, while Blakley's scheme [2] is based on the linear projective geometry. In a (t,n) threshold scheme, a secret can be shared among n participants. At least t or more participants can reconstruct the secret, but $(t-1)$ or fewer participants can obtain noting about the secret.

Later, several multi-secret sharing schemes were proposed. In a multi-secret sharing scheme, there are multiple secrets to be shared during one secret sharing process. In 2000, Chien et al. [3] proposed a multi-secret sharing scheme based on the systematic block codes. Chien's scheme has several merits:

1. It allows parallel secret reconstruction;
2. The dealer can dynamically determine the number of the distributed secrets;
3. It is a multi-use scheme;
4. Compared with previous multi-secret sharing schemes, it has fewer public values.

But Chien's scheme is not very efficient, because the reconstruction costs $n+k-t$ simultaneous equations, a complex process. In order to reduce the complexity of the secret reconstruction, Yang et al. [13] proposed an alternative implementation of Chien's scheme based on Shamir's secret scheme in 2004.

In the recovery phase of Yang's scheme, participants must reconstruct a $(t-1)$th degree polynomial (when $k \le t$), or a $(k-1)$th degree polynomial (when $t < k$). Although the reconstruction in Yang's scheme is easier than that in Chien's scheme, but more public values are required in Yang's scheme when $k < t$. One of the main efficiency parameters is the number of public values, which affects the storage and communication complexity of the scheme. Motivated by these concerns, a (t,n) multi-secret sharing scheme is proposed by Pang et al. [11], in 2005. Pang's scheme is based on shamir's scheme as Yang's scheme and requires the same number of public values as Chien's scheme.

In this paper, we will propose a new scheme, based on non-homogeneous linear recursion. We propose two easy ways for secret reconstruction and a simple method for the construction phase. In addition, our scheme requires the same number of public values as Chien's and Pang's schemes. Altogether, the new scheme we shall propose overcomes the drawback of the previous schemes and provides great capabilities for many applications. This paper is organized into six sections. In section 2, we review Chien's, Yang's and Pang's schemes. Section 3 introduces the non-homogeneous linear recursion. In section 4, we propose our scheme. Section 5 poses

i Dr M. Hadian Dehkordi, Department of Mathematics, Iran University of Science and Tecnology, Narmak, Tehran, Iran (e-mail: mhadian@iust.ac.ir)

ii S. Mashhadi, Ph. D. student, Department of Mathematics, Iran University of Science and Tecnology, Narmak, Tehran, Iran (e-mail: smashhadi@mathdep.iust.ac.ir)

discussion and analysis. Finally, we give conclusion in section 6.

2. REVIEW OF CHIEN'S, YANG'S AND PANG'S SCHEMES

A. Chien's scheme:

I. System parameters:

$P_1, P_2, \ldots, P_k$ denote k secrets to be shared among n participants. $f(r,s)$ denotes any two-variable one-way function. Let $GF(2^m)$ be a large finite field and all the numbers are elements in it. Let g be a primitive element in $GF(2^m)$ and $G(N,L)$ denotes a special type of systematic block codes generator matrix $\left(I, P^T\right)^T_{L\times N}$ where I is a $L\times L$ identity matrix and P is $(N-L)\times L$ matrix $\left(g^{(i-1)(j-1)}\right)$ for $i=1,2,\ldots,N-L$; $j=1,2,\ldots,L$. Let the superscript T mean vector transposition. The dealer D randomly chooses n secret shadows $s_1, s_2, \ldots, s_n$ and distributes s_i to participant M_i for $i=1,2,\ldots,n$ by a secure channel.

II. Construction phase:

The dealer D performs the following steps:

- Randomly choose an integer r and compute $f(r,s_i)$ for $i=1,2,\ldots,n$;
- Construct the generator matrix $G(2(n+k)-t, n+k)$;
- Let $E=(P_1,\ldots,P_k, f(r,s_1), \ldots, f(r,s_n))^T$;

Compute $V=G\times E$, so $V=(P_1,\ldots,P_k, f(r,s_1), \ldots, f(r,s_n), c_1,\ldots,c_{n-k-t})^T$ where

$$c_i=\sum_{j=1}^{k} g^{(i-1)(j-1)}P_j+\sum_{j=k}^{n+k} g^{(i-1)(j-1)} f(r,s_{j-k}) \qquad (1)$$

- Publish $(r, c_1, c_2, \ldots, c_{n-k-t})$.

III. Recovery phase:

In order to reconstruction these k secrets, at least t participants pool their share $f(r,s_i)$'s, and then the $(n+k-t)$ equations in (1) will be obtained with only $(n+k-t)$ unknown symbols contained. Therefore, the k secrets, can be obtained by solving simultaneous equations in (1).

B. Yang's scheme:

I)

I. System parameters:

$P_1, P_2, \ldots, P_k$ and $f(r,s)$ in this scheme are the same as those in Chien's scheme. Let q be a large prime and all the numbers are elements in the finite field $GF(q)$. The dealer D randomly chooses n secret shadows $s_1, s_2, \ldots, s_n$ and distributes s_i to participant M_i for $i=1,2,\ldots,n$ by a secure channel.

II. Construction phase:

The dealer D performs the following steps:

1. If $(k \le t)$

- Randomly choose an integer r and compute $f(r,s_i)$ for $i=1,2,\ldots,n$;
- Construct $(t-1)$th degree polynomial $h(x) \bmod q$ as follows:

$$h(x)=P_1+P_2x+\cdots+P_kx^{k-1}+a_1x^k+a_2x^{k+1}+\cdots+a_{t-k}x^{t-1} \bmod q; \quad (2)$$

- Compute $y_i=h(f(r,s_i)) \bmod q$ for $i=1, 2,\ldots,n$;
- Publish $(r, y_1, y_2, \ldots, y_n)$.

2. If $(t<k)$

- Randomly choose an integer r and compute $f(r,s_i)$ for $i=1,2,\ldots,n$;
- Construct $(k-1)$th degree polynomial $h(x) \bmod q$ as follow

$$h(x)=P_1+P_2x+\cdots+P_kx^{k-1} \bmod q; \quad (3)$$

- Compute $y_i=h(f(r,s_i)) \bmod q$ for $i=1, 2,\ldots,n$;
- Compute $h(i) \bmod q$ for $i=1,2,\ldots,k-t$;
- Publish $(r, h(1),\ldots,h(k-t), y_1, y_2, \ldots, y_n)$.

III. Recovery phase:

At least t participants pool their shares $f(r,s_i)$'s.

1. If $(k \le t)$

By using the Lagrange interpolation polynomial, with the knowledge of t pairs of $(f(r,s_i), y_i)$ the $(t-1)$th degree polynomial $h(x)$ can be uniquely determined.

2. If $(t<k)$

By using the Lagrange interpolation polynomial, with the knowledge of t pairs of $(f(r,s_i), y_i)$ and $(k-t)$ pairs of $(i, h(i))$ the $(k-1)$th degree polynomial $h(x)$ can be uniquely determined.

From the obtained polynomial, we can easily get the secrets.

C. Pang's scheme:

[1] System parameters:

$P_1, P_2, \ldots, P_k, q$ and $f(r,s)$ in this scheme are the same as those in Yang's scheme. The dealer D randomly chooses n secret shadows $s_1, s_2, \ldots, s_n$ and distributes s_i to participant M_i for $i=1,2,\ldots,n$ by a secure

channel. Also, D selects n distinct integers, $u_1,u_2,\ldots,u_n$ from $[k,q-1]$ as participants' public identity information.

II. Construction phase:

The dealer D performs the following steps:

1. Randomly choose an integer r and compute $f(r,s_i)$ for $i=1,2,\ldots,n$;
2. Use the $(n+k)$ pairs of $(0,P_1),(1,P_2),\ldots,(k-1,P_k)$ and $(u_i,f(r,s_i))$ for $i=1,2,\ldots,n$; to construct a $(n+k-1)$th degree polynomial

$$h(x)=a_0+a_1x+\cdots+a_{n+k-1}x^{n+k-1} \bmod q; \quad (4)$$

3. Take out the $(n+k-t)$ minimum integers $d_1,d_2,\ldots,d_{n+k-t}$ from $[k,q-1]-\{u_i \mid 1\le i\le n\}$ and compute $h(d_i)$ for $1\le i\le n+k-t$;
4. Publish $(r,h(d_1),h(d_2),\ldots,h(d_{n+k-t}))$.

III. Recovery phase:

In order to reconstruction these k secrets, at least t participants pool their share $f(r,s_i)$'s, they can obtain t pairs of $(u_i,f(r,s_i))$. Then in the same way as in the construction phase, they find out the $(n+k-t)$ minimum integers $d_1,d_2,\ldots,d_{n+k-t}$. With the knowledge of the public values $h(d_1),h(d_2),\ldots,h(d_{n+k-t})$, they can obtain $(n+k-t)$ pairs of $(d_i,h(d_i))$, for $1\le i\le n+k-t$. Therefore, there are $(n+k)$ pairs obtained altogether and the $(n+k-1)$th degree polynomial can be uniquely determined. Subsequently, the secrets can be computed as $P_i=h(i-1)$ for $i=1,2,\ldots,k$, respectively.

3. Non-Homogeneous Linear Recursion

In this section, we will introduce mathematical background of our scheme. A detailed description of non-homogeneous linear recursion can be found in [1].

1. **Definition.** A non-homogeneous linear recursion of degree t is defined by the equations:

$$\begin{cases} u_0=c_0,u_1=c_1,\ldots,u_{t-1}=c_{t-1}, \\ u_{i+t}+a_1u_{i+t-1}+\cdots+a_tu_i=f(i) \quad (i\ge 0), \end{cases} \quad (5)$$

where $c_0,c_1,\ldots,c_{t-1}$ and $a_1,a_2,\ldots,a_t$ are constants.

2. **Theorem.** Let F be a field, and $h(x)$ is a polynomial in $F[x]$. Consider a typical fraction $h(x)/(1-\alpha x)^m$ where $\alpha\in F$ and $\deg h(x)<m$. Then

$$\frac{h(x)}{(1-\alpha x)^m}=\sum_{i=0}^{\infty}u_ix^i; \quad (6)$$

where $u_i=p(i)\alpha^i$ and $p(x)$ is a $(m-1)$th degree polynomial.

Proof. [1].

3. **Lemma.** Suppose sequence $(u_i)_{i\ge 0}$ is defined by [NHLR] as follows:

$$\begin{cases} u_0=c_0,u_1=c_1,\ldots,u_{t-1}=c_{t-1}, \\ \sum_{j=0}^{t}\binom{t}{j}u_{i+t-j}=(-1)^i \quad (i\ge 0), \end{cases} \quad (7)$$

where $c_0,c_1,\ldots,c_{t-1}$ are constants. Then $u_i=p(i)(-1)^i$ where, $p(x)$ is a tth degree polynomial.

Proof. By using (7), we calculate

$$\begin{aligned} \sum_{j=0}^{t}\binom{t}{j}x^j\sum_{i=0}^{\infty}u_ix^i &= u_0+\cdots+\left(\sum_{j=0}^{t}\binom{t}{j}u_{i-j}\right)x^i+\cdots \\ &= h(x)+x^t(1-x+x^2-x^3+\cdots) \\ &= h(x)+\frac{x^t}{1+x} \\ &= \frac{h(x)(1+x)+x^t}{1+x}; \end{aligned}$$

where, $h(x)$ is a polynomial with degree at most $t-1$. So $\sum_{i=0}^{\infty}u_ix^i=\frac{h(x)(1+x)+x^t}{(1+x)^{t+1}}$ and according to the previous theorem, we have $u_i=p(i)(-1)^i$ where, $p(x)$ is an expression of the form $A_0+A_1x+\cdots+A_tx^t$.

4. Our Scheme

In this section we propose our scheme.

A. System parameters:

Notations $P_1,P_2,\ldots,P_k$ and $f(r,s)$ in our scheme are the same as those in the Pang's scheme. q is a prime number, such that $q>\binom{t}{i}$ for $i=1,2,\ldots,t$. The dealer D randomly chooses n secret shadows $s_1,s_2,\ldots,s_n$ and distributes s_i to participant M_i for $i=1,2,\ldots,n$ by a secure channel.

B. Construction phase:

The dealer D performs the following steps:

- Randomly choose an integer r and compute $f(r,s_i)$ for $i=1,2,\ldots,n$;
- Consider [NHLR] which is defined by the

equations,

$$\begin{cases} u_0 = f(r,s_1), u_1 = f(r,s_2), \ldots, u_{t-1} = f(r,s_t), \\ \sum_{j=0}^{t} \binom{t}{j} u_{i+t-j} = (-1)^i \mod q \quad (i \geq 0); \end{cases}$$

- Compute u_i, $t \leq i \leq n+k+1$;
- Compute $y_i = f(r,s_i) - u_{i-1}$ for $t < i \leq n$ and $r_i = P_i - u_{i+n-1}$ for $1 \leq i \leq k$;
- Publish $(r, r_1, \ldots, r_k, y_{t+1}, \ldots, y_n, u_{n+k+1})$.

C. Recovery phase:

Now we propose two new ways for secret reconstruction and show how t honest participants can recover the secrets:

– Suppose t arbitrary participants $\{M_i\}_{i \in I}$, $(I \subseteq \{1,2,\ldots,n\}, |I| = t)$ pool their secret shares. They compute t terms of [NHLR] by their shares in the following way:

$$u_{j-1} = \begin{cases} f(r,s_j) & 1 \leq j \leq t, \\ f(r,s_j) - y_j & t < j \leq n. \end{cases} \quad (8)$$

Therefore, they obtain t pairs of $(i-1, (-1)^{i-1} u_{i-1})$ where $i \in I$ and public pair of $(n+k+1, (-1)^{n+k+1} u_{n+k+1})$. We use (X_i, Y_i) for $i \in I'$ where $I' = I \bigcup \{n+k+1\}$ to denote these $t+1$ pairs, respectively. Now, by using the Lagrange interpolation polynomial, the t th degree polynomial $p(x)$ can be uniquely determined as:

$$p(x) = \sum_{i \in I'} Y_i \prod_{j \in I', j \neq i} \frac{x - X_j}{X_i - X_j} \mod q \quad (9)$$
$$= A_0 + A_1 x + \cdots + A_t x^t \mod q.$$

Now, $u_j = p(j)(-1)^j \mod q$ for all $j \geq t$, and the k secrets can be computed as

$$P_i = u_{i+n-1} + r_i, \quad 1 \leq i \leq k. \quad (10)$$

–Suppose t participants $\{M_i, M_{i+1}, \ldots, M_{i+t-1}\}$ where $1 \leq i \leq n-t+1$ pool their secret shares $f(r,s_j)$ for $i \leq j \leq i+t-1$. In other words, suppose the t participants indexes are successive. Besides previous method, they can compute secrets as follows:

They compute t terms of [NHLR] by their shares in the following way:

$$u_{j-1} = \begin{cases} f(r,s_j) & 1 \leq j \leq t, \\ f(r,s_j) - y_j & t < j \leq n. \end{cases} \quad (11)$$

Now the secrets can be uniquely determined by using the following process:

$$u_{m+t} = (-1)^m - \sum_{j=1}^{t} \binom{t}{j} u_{m+t-j} \mod q. \quad (12)$$

This process is repeated as often as needed, starting with $m = i-1$ and proceeding to $m = k+n-t-1$. Then,

$$P_i = u_{i+n-1} + r_i, \quad 1 \leq i \leq k. \quad (13)$$

5. ANALYSIS AND DISCUSSION

In this section, we will prove that our scheme is a multi-use scheme and then we shall analysis the security and performance of it.

D. Multi-use scheme:

In our scheme, each participant M_i just polls his/her secret share $f(r,s_i)$ in the recovery phase, so that the real shadow s_i will not be disclosed and reuse of it is secure by the properties of the two-variable one-way function.

E. Security analysis:

Attaks: $t-1$ or fewer participants try to recover secrets or another's secret share.

Analysis: Recovery phase of our scheme is based on one of the following ways:

1. Using the Lagrange interpolation polynomial.
2. Using [NHLR] of degree t.

In the first way, the security of the proposed scheme is based on the security of Shamir's scheme as Yang's and Pang's schemes, in this point.

In the second way, each term u_i depends on the previous t terms. So, If m participants $\{M_i, \ldots, M_{i+m-1}\}$ where $1 \leq i \leq n+1-m$ and $1 \leq m < t$ pool their secret shares they can not reveal any previous terms u_j for $j < i-1$ or any forward terms u_j for $j > i+m-2$ by using [NHLR]. Therefore, the secrets and others' secret shares can not be obtained in this way.

F. Performance analysis:

In this subsection, we shall propose a comparison of the Chien's, Yang's and Pang's schemes and ours in the following two aspects: public values and computational complexity.

1. Public value:

In Chien's and Pang's schemes, it is required to publish $(n+k-t+1)$ public values. In our scheme, $(n+k-t+2)$ public values are needed. While, Yang's scheme has $(n+k-t+\ )$ public values when $(t < k)$ and $(n+\ )$ public values when $(k \leq t)$. Therefore, our scheme almost requires the same number of public values as Chien's and Pang's schemes. Moreover, compared with

Yang's scheme number of public values in ours is less.

2. Computational complexity:

It is obvious that the most time consuming phase in these schemes is the recovery phase. The Gauss's algorithm for solving n simultaneous equations has running time of $O(n^3)$. So, the recovery phase in Chien's scheme can be done in time $O(n+k-t)^3$. Lagrange interpolation for construction a n th degree polynomial has running time of $O(n^2)$. Therefore, secrets are reconstructed in time $O(t-1)^2$ for $k \le t$ or $O(k-1)^2$ for $k > t$ in Yang's scheme. Similarly Pang's scheme has running time of $O(n+k-1)^2$.

The recovery phase in our scheme is based on one of the following ways:

1. Using the Lagrange interpolation polynomial.
2. Using [NHLR] of degree t.

The second way is faster than the first way. The former can be done in $O(t^2)$. It is obvious that when $k \le t$, $O(t-1)^2 \approx O(t^2) \le O(n+k-1)^2 \le O(n+k-t)^3$ and $O(t^2) \le O(k-1)^2 \le O(n+k-1)^2 \le O(n+k-t)^3$ when $k > t$. So compared with the previous schemes, our scheme is the fastest.

6. CONCLUSION

Based on the mathematical concept non-homogeneous linear recursion, we propose a new and efficient multi-secret sharing scheme in this paper. The proposed scheme provides many functions for practical applications. Analyses show that it is computationally secure and efficient scheme. It overcomes the drawback of the previous schemes and has all merits of previous schemes such as: it allows parallel secret reconstruction; the dealer can dynamically determine the number of the distributed secrets and this scheme is a multi-use scheme. Moreover, it has following advantages:

1. It is very efficient and easy to implement;
2. It has two ways for recovery phase and a new simple construction phase.
3. Needs few public values;
4. Compared with previous multi-secret sharing schemes, it needs the least storage as well as computing time.

3. REFERENCES

[1] N. L. Biggs, Discrete mathematics, Revised edition, Oxford university press, New York, 1989.

[2] G. Blakley, Safeguarding cryptographic keys, Proc AFIPS 1979 National Computer Conferance,AFIPS Press, New York, 1979, pp. 313 317.

[3] H.-Y. Chien, J.-K. Jan, Y.-M. Tseng, A practical (t,n) multi-secret sharing scheme, IEICE Transactions on Fundamentals of Electronics, Communications and Computer 83-A, 12, 2000,pp. 2762-2765.

[4] L. Chen, D. Gollman, C. J. Mitchell, P. Wild, Secret sharing with reusable polynomials, Proceeding of the Second Australisian Conferance on Information Security and Privacy ACISP, Australia,1997.

[5] M. Hadian Dehkordi, S. Mashhadi, An efficient threshold verifiable multi-secret sharing, Computer Standards & Interfaces 30, 3, 2008, pp. 187-190.

[6] M. Hadian Dehkordi, S. Mashhadi, New efficient and practical verifiable multi-secret sharing schemes, Information Sciences 178,9, 2008, pp. 2262-2274.

[7] M. Hadian Dehkordi, S. Mashhadi, Verifiable multi secret sharing verifiable secret sharing schemes based on non homogeneous linear recursions and elliptic curves, Computer Communications, Preprint.

[8] L. Harn, Efficient sharing (broadcasting) of multiple secret, IEEE Proc. Computers and Digital Techniques 142, 3, 1995, pp. 237-240.

[9] J. He, E. Dawson, Multistage secret sharing based on one-way function, Electronics Letters 30, 19, 1994, pp. 1591-1592.

[10] J. He, E. Dawson, Multistage secret sharing based on one-way function, Electronics Letters 31, 2, 1995, pp. 93-95.

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

[12] A. Shamir, How to share a secret, Communications of ACM 22, 11, 1979, pp. 612-613.

[13] C.-C. Yang, T.-Y. Chang, M.-S. Hwang, A (t,n) multi-secret sharing scheme, Applied Mathematics and Computation 151, 2004,pp.483-490.