

# A Verifiable and Detectable Secret Sharing Scheme by Using a New Geometric Approach\*

Justie Su-tzu Juan<sup>†</sup> and Yu-Lin Chuang

Department of Computer Science and Information Engineering

National Chi Nan University

Puli, Nantou 545, TAIWAN

## Abstract

*Secret sharing schemes are methods for distributing a secret among  $n$  participants in such a way that any qualified subsets of participants can recover the secret, and unqualified participants can not. In 1979, secret sharing schemes were first independently introduced by Blakley and Shamir. In 1987, Feldman proposed a verifiable secret sharing scheme based on Shamir's Scheme, that every participant can verify their share is true or not. Wu and He proposed a geometric approach for sharing secrets by using a hyperspherical polynomial in 1995. The secret can hide in any one of the coefficients of a hyperspherical polynomial.*

*This paper propose a new geometric approach for sharing secrets based on a hyperelliptic function that is efficient than Wu and He's Scheme. Moreover, we modify it to be a practical scheme that can verify the shares and detect the cheater, which is more efficient than Feldman's scheme.*

**Keywords:** secret sharing scheme, hyperelliptic,  $(k, n)$ -threshold scheme, online, multi-secret.

## 1 Introduction

A *secret sharing scheme* is a method for distributing a secret among several participants in such a way that only qualified subsets of the participants can reconstruct it and unqualified subsets receive no information about the secret. Another view of a secret sharing scheme is a pair of efficient algorithms: *distribution algorithm* and *reconstruction algorithm* run by a *dealer* and some participants. The distribution algorithm is executed by a dealer who, given a secret, computes some *shares* and gives them to the participants. The reconstruction algorithm is executed by a qualified subset of participants who, by putting together their own shares, can therefore reconstruct the secret.

In 1979, secret sharing schemes were first independently introduced by Blakley [1] and Shamir [12], who considered the important case that the set of qualified subsets of  $n$  participants is the

---

\*This research was supported in part by the National Science Council under grant NSC93-2213-E260-022.

<sup>†</sup>Corresponding author. Email: jsjuan@ncnu.edu.tw

set of all subsets of size at least  $t$ , for some integer  $t$ . It was called the  $(t, n)$ -threshold scheme. In 1987, Ito et al. [9] proposed a general method of secret sharing called secret sharing scheme which allows a secret (or *master key*) to be shared among a finite set of participants in such a way that only certain pre-specified subsets of participants can recover the secret.

Let  $P$  be the set of participants. The collection of subsets of participants that can reconstruct the secret in this way is called *access structure* (denoted by  $\Gamma$ ). The collection of subsets of participants that cannot reconstruct the secret is called *prohibited structure* (denoted by  $\Delta$ ) [14]. Let  $\mathcal{K}$  be the master key space and  $\mathcal{S}$  be the share space. The *information rate* of the secret sharing scheme is defined as  $\log_2 |\mathcal{K}| / \log_2 |\mathcal{S}|$  [2]. A secret sharing scheme is *perfect* if any set of participants in the prohibited structure obtains no information regarding the secret [5,10,16,21].

Feldman presented a verifiable secret sharing scheme in 1987 [5]. This scheme can verify the authenticity of the shares of Shamir's  $(t, n)$ -threshold scheme. It also can detect the cheater when some participants try to recover the secret together. Wu and He presented a  $(t, n)$  threshold scheme for sharing a secret in 1995 [15]. The scheme is based on some geometric properties. They give a practical algorithm to solve the problem of dividing the secret into  $n$  shares efficiently.

This paper is organized as follows. In Section 2, we first propose a  $(t, n)$ -threshold scheme by using a hyperelliptic polynomial, called HE-TS. In Section 3, We propose a verifiable and detectable secret sharing scheme based on HE-TS. And in Section 4, we will make the conclusion and give some suggestions what we can do in the future.

## 2 The New Secret Sharing Scheme

In 1995, Wu and He [15] proposed a  $(t, n)$ -threshold scheme for sharing a secret based on a hyperspherical function. We call it HS-TS. They use the equation  $\sum_{i=1}^{t-1} (x_i - a_i)^2 = s \pmod{p}$  and create a  $(t, n)$ -threshold scheme, where  $p$  is a prime. They gave the following theorem and corollary at first.

**Theorem 1 [15]** *Let  $p$  be an odd prime number. If 2 is a quadratic non-residue modulo  $p$ , then every integer  $r \in [0, p)$  can be expressed in the form  $r = x^2 + y^2 \pmod{p}$  with integers  $x, y \in [0, p)$ .*

**Corollary 1 [15]** *Let  $p$  be an odd prime number. If 2 is not a quadratic residue modulo  $p$ , then every integer  $z \in [0, p)$  can be expressed as the sum of  $t$  ( $t \geq 2$ ) integer squares (modulo  $p$ ).*

We use a hyperelliptic equation to improve HS-TS. It can enhance the information rate. The original hyperelliptic equation is  $\sum_{i=1}^t \frac{(x_i - a_i)^2}{b_i^2} = 1 \pmod{p}$ . For convenience, we change the form to be  $\sum_{i=1}^t b_i^2 (x_i - a_i)^2 = 1 \pmod{p}$  and create a  $(2t, n)$ -threshold scheme. If we want to create a  $(2t - 1, n)$ -threshold scheme, then we publish a selected coefficient of the polynomial to each participant, for example,  $b_1$ . So we say it is a  $(2t, n)$ -threshold scheme without loss of generality. This  $(t, n)$ -threshold scheme is called HE-TS, and the algorithm is stated as follows.

### Initial Phase

Step 1 : For  $i = 0, 1, 2, \dots, (p - 1)/2$ , compute  $z_i = i^2 \pmod{p}$ . Put the pair  $(z_i, i)$  in the directory file.

Step 2 : Publish the directory file.

### Divide Secret Phase

For  $i = 1, 2, \dots, n$ , do the following :

Step 1 : For  $j = 1, 2, \dots, t - 2$ , do the following:

(1.1) Randomly choose a pair in the directory file and let it be  $(r_{ij}, w_{ij})$ .

(1.2) Set  $x_{ij}$  to be either  $b_i^{-1}w_{ij} + a_j \pmod{p}$  or  $p - b_i^{-1}w_{ij} + a_j \pmod{p}$ .

Step 2 : Choose two pairs  $(r_{i(t-1)}, w_{i(t-1)})$  and  $(r_{it}, w_{it})$  from the directory file, such that

$$r_{i(t-1)} + r_{it} = 1 - \sum_{j=1}^{t-2} r_{ij} \pmod{p}.$$

Step 3 : Set  $x_{i(t-1)}$  to be either  $b_i^{-1}w_{i(t-1)} + a_{t-1} \pmod{p}$  or  $p - b_i^{-1}w_{i(t-1)} + a_{t-1} \pmod{p}$ . Set

$x_{it}$  to be either  $b_i^{-1}w_{it} + a_t \pmod{p}$  or  $p - b_i^{-1}w_{it} + a_t \pmod{p}$ .

Step 4 : Let  $E_i = (x_{i1}, x_{i2}, \dots, x_{it})$  and  $E'_i = (x_{i1}^2, x_{i1}, x_{i2}^2, x_{i2}, \dots, x_{it}^2, x_{it})$ .

Step 5 : If  $i \leq 2t$  and  $E'_1, E'_2, \dots, E'_i$  are linear dependent, then repeat Step 1 to 4. If  $i > 2t$  and any  $2t$  of  $E'_1, E'_2, \dots, E'_i$  are linear dependent, then repeat Step 1 to 4.

Step 6 : Output  $E_i$ .

We show **Divide Secret Phase** is correct. In Step 2, from Theorem 1, there exist  $r_{i(t-1)}$  and  $r_{it}$  such that  $r_{i(t-1)} + r_{it} = 1 - \sum_{j=1}^{t-2} r_{ij} \pmod{p}$ . Hence  $[r_{i1} + r_{i2} + \dots + r_{i(t-2)}] + r_{i(t-1)} + r_{it} = 1 \pmod{p}$ . In Step 5, we ensure that any  $2t$  of  $n$  shares do not lie on a common  $(2t - 2)$  dimensional space. Hence we should verify  $\Delta \neq 0$ . For example, when we want to recover the secret by  $E_1, E_2, \dots, E_{2t}$ ,

$$\Delta = \det \begin{pmatrix} x_{11}^2 & x_{11} & x_{12}^2 & x_{12} & \cdots & x_{1t}^2 & x_{1t} \\ x_{21}^2 & x_{21} & x_{22}^2 & x_{22} & \cdots & x_{2t}^2 & x_{2t} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{(2t)1}^2 & x_{(2t)1} & x_{(2t)2}^2 & x_{(2t)2} & \cdots & x_{(2t)t}^2 & x_{(2t)t} \end{pmatrix}_{(2t \times 2t)}$$

We should confirm that  $E'_1, E'_2, \dots, E'_{2t}$  are linear independent. When we want to check that  $E'_1, E'_2, \dots, E'_{2t}$  are linear independent, one can compute the value of

$$\det \begin{pmatrix} E'_1 \\ E'_2 \\ \vdots \\ E'_{2t} \end{pmatrix}$$

and check the result is equal to zero or not.

### Recover Secret Phase

Any  $2t$  of  $n$  shares  $E_i$  by **Divide Secret Phase** can determine the secret  $K = (a_1, a_2, \dots, a_t, b_1^2, b_2^2, \dots, b_t^2)$ . Without loss of generality, let the  $2t$  shares be  $E_1, E_2, \dots, E_{2t}$ , and we can let equation

$$\sum_{i=1}^t b_i^2 (x_i - a_i)^2 = 1 \pmod{p}$$

be  $x_1^2 c_1 + x_1 c_2 + x_2^2 c_3 + x_2 c_4 + \dots + x_t^2 c_{2t-1} + x_t c_{2t} = 1$ . Using Cramer's Rule [6], we can determine

all  $c_i$  (for  $i = 1, 2, \dots, 2t$ ) as following :

for  $i$  is odd, let

$$\Delta_{c_i} = \det \begin{pmatrix} x_{11}^2 & x_{11} & \cdots & x_{1(\frac{i-1}{2})} & 1 & x_{1(\frac{i+1}{2})} & \cdots & x_{1t}^2 & x_{1t} \\ x_{21}^2 & x_{21} & \cdots & x_{2(\frac{i-1}{2})} & 1 & x_{2(\frac{i+1}{2})} & \cdots & x_{2t}^2 & x_{2t} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{(2t)1}^2 & x_{(2t)1} & \cdots & x_{(2t)(\frac{i-1}{2})} & 1 & x_{(2t)(\frac{i+1}{2})} & \cdots & x_{(2t)t}^2 & x_{(2t)t} \end{pmatrix},$$

for  $i$  is even, let

$$\Delta_{c_i} = \det \begin{pmatrix} x_{11}^2 & x_{11} & \cdots & x_{1(\frac{i}{2})} & 1 & x_{1(\frac{i}{2}+1)} & \cdots & x_{1t}^2 & x_{1t} \\ x_{21}^2 & x_{21} & \cdots & x_{2(\frac{i}{2})} & 1 & x_{2(\frac{i}{2}+1)} & \cdots & x_{2t}^2 & x_{2t} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{(2t)1}^2 & x_{(2t)1} & \cdots & x_{(2t)(\frac{i}{2})} & 1 & x_{(2t)(\frac{i}{2}+1)} & \cdots & x_{(2t)t}^2 & x_{(2t)t} \end{pmatrix},$$

and  $c_i = \Delta_{c_i}/\Delta$ . Then we can determine  $a_i$  and  $b_i^2$  by using  $c_j$  for all  $1 \leq i \leq t$ ,  $1 \leq j \leq 2t$ . For  $1 \leq i \leq t$ ,  $a_i = -c_{2i}/2c_{2i-1}$ , and

$$b_i^2 = \frac{\det \begin{pmatrix} 1 + \frac{c_2^2}{4c_1} & \cdots & \frac{c_1 c_{2i-2}^2}{4c_{2i-3}} & c_1 & \frac{c_1 c_{2i+2}^2}{4c_{2i+1}} & \cdots & \frac{c_1 c_{2t}^2}{4c_{2t-1}^2} \\ \frac{c_3 c_2^2}{4c_1^2} & \cdots & \frac{c_3 c_{2i-2}^2}{4c_{2i-3}} & c_3 & \frac{c_3 c_{2i+2}^2}{4c_{2i+1}} & \cdots & \frac{c_3 c_{2t}^2}{4c_{2t-1}^2} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{c_{2t-1} c_2^2}{4c_1^2} & \cdots & \frac{c_{2t-1} c_{2i-2}^2}{4c_{2i-3}} & c_{2t-1} & \frac{c_{2t-1} c_{2i+2}^2}{4c_{2i+1}} & \cdots & 1 + \frac{c_{2t-1} c_{2t}^2}{4c_{2t-1}^2} \end{pmatrix}_{(t \times t)}}{\det \begin{pmatrix} 1 + \frac{c_2^2}{4c_1} & \frac{c_1 c_4^2}{4c_3^2} & \cdots & \frac{c_1 c_{2t}^2}{4c_{2t-1}^2} \\ \frac{c_3 c_2^2}{4c_1^2} & 1 + \frac{c_4^2}{4c_3} & \cdots & \frac{c_3 c_{2t}^2}{4c_{2t-1}^2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{c_{2t-1} c_2^2}{4c_1^2} & \frac{c_{2t-1} c_4^2}{4c_3^2} & \cdots & 1 + \frac{c_{2t-1} c_{2t}^2}{4c_{2t-1}^2} \end{pmatrix}_{(t \times t)}}.$$

We will discuss our scheme, and compare it with HS-TS in the last section.

### 3 Verification and Detection

If some participants are dishonest, secret sharing scheme will not be in practice because of the following two reasons: (i) all participants can not check validity of the shares from the dealer, and (ii) participants can not verify validity of the shares from other participants. In order to resist malicious participants, Feldman proposed a verifiable and detectable secret sharing scheme

[5]. This scheme can verify and detect the authenticity of the shares of Shamir's  $(t, n)$ -threshold scheme. We propose a verifiable and detectable scheme that can verify and detect the authenticity of the shares of HE-TS. It is a  $(2t, n)$ -threshold scheme and this scheme is called by VDHE-TS. In the rest of this paper,  $p$  and  $q$  denote large primes such that  $p$  divides  $q - 1$ . Let  $Z_p$  be a finite field with  $p$  elements. Let  $g$  be an element of order  $p$  of multiplicative group  $Z_q^*$ . We described VDHE-TS as follows :

Step 1 : A dealer  $D$  chooses  $nk$  elements of  $Z_p$ , denoted by  $x_{ij}$ ,  $1 \leq i \leq n, 1 \leq j \leq t$ .

Step 2 :  $D$  chooses  $2t$  elements  $a_1, a_2, \dots, a_t, b_1, b_2, \dots, b_t$  from  $Z_p$  independently with the uniform distribution.

Step 3 :  $D$  use HE-TS to obtain  $E_i$  and distributes the shares  $E_i$  to  $Pt_i$  ( $1 \leq i \leq n$ ), where  $E_i = (x_{i1}, x_{i2}, \dots, x_{it})$  and  $\sum_{i=1}^t b_i^2 (x_i - a_i)^2 = 1$  over  $Z_p$ .

Step 4 :  $D$  publishes  $g, g^{b_1^2} \bmod q, g^{b_2^2} \bmod q, \dots, g^{b_t^2} \bmod q, g^{-2a_1 b_1^2} \bmod q, g^{-2a_2 b_2^2} \bmod q, \dots, g^{-2a_t b_t^2} \bmod q, g^{\sum_{j=1}^t (a_j b_j)^2} \bmod q$ .

In VDHE-TS, all  $Pt_\alpha$  can verify the authenticity of  $E_i$  by checking

$$g = (g^{b_1^2})^{x_{i1}^2} \dots (g^{b_t^2})^{x_{it}^2} (g^{-2a_1 b_1^2})^{x_{i1}} \dots (g^{-2a_t b_t^2})^{x_{it}} (g^{\sum_{j=1}^t (a_j b_j)^2}) \pmod{q} \quad (1 \leq i \leq n).$$

All participants also can detect cheaters by using above equation. Note that a verifiable and detectable scheme based on HS-TS can be obtained easily in the same way, and we call it is a VDHS-TS. We shall compare VDHE-TS, VDHS-TS with Feldman's scheme in terms of the number of published values, and the computing time in next section.

## 4 Conclusion and Future Work

In this paper, we proposed a new geometric approach for sharing secrets by using hyperelliptic function, called HE-TS, in Section 2. It is more flexible to hide the secrets and the information rate is better than Wu and He's scheme, called HS-TS. For HS-TS, there exist a practical algorithm to share a secret [15]. Here we propose a new scheme based on hyperelliptic function and also give a practical algorithm. We present a  $(2t, n)$  threshold scheme for sharing secrets. The computing time of **Recover Secret Phase** in HE-TS is equal to the time complexity of HS-TS. They both need to determine the  $2t \times 2t$  matrices. Note that, if secret  $K$  be hidden in only one coefficient  $a_i$  of the hyperspherical function of the HS-TS, then this scheme is perfect. Otherwise it is not. So we suppose the secret  $K = a_i$  for some  $i$  in both HS-TS and HE-TS. The length of the share that each participant be distributed is  $(2t-1)|K|$  in HS-TS. And the length of the share that each participant be distributed is  $t|K|$  in HE-TS, almost half the amount. Hence, HE-TS is more efficient when the dealer sends the shares to the participants. The information rate of HE-TS is better than HS-TS. That are  $\frac{1}{t}$  and  $\frac{1}{2t-1}$  for  $(2t, n)$ -threshold scheme, respectively.

In Section 3, we proposed one verifiable secret sharing schemes, VDHE-TS. In this scheme, all participant gets their shares can verify their shares is true or not, and can detect the cheater. We compare VDHE-TS and Feldman's scheme, these two verifiable and detectable secret sharing schemes are computationally secure. For  $(2t, n)$ -threshold scheme, storing published information needs  $2t + 1$  storages in Feldman's scheme. It need  $2t + 2$  storages to store published information

in VDHE-TS. To consider the computing time for the participants to verify the authenticity or detect cheater in one time, we calculate the number of the power, multiplication of exponent, addition of exponent, and multiplication of the equation separately. We list these comparisons in Table 1. Our results are better than Feldman’s scheme. The computing time of the dealer, we calculate the number of the power, multiplication of exponent, addition of exponent, and the inverse of exponent separately. When we consider the computing time of the dealer, our results are weaker than Feldman’s scheme. But the dealer only computes one time. The participants must compute many times including verification and detection. Hence, VDHE-TS is more efficient than VDHS-TS, and VDHS-TS is more efficient than Feldman’s scheme.

Table 1: Comparison of the Feldman’s Scheme, VDHS-TS and VDHE-TS

$(2t, n)$ -threshold scheme			
	Feldman	VDHS-TS	VDHE-TS
public values	$2t + 1$	$2t + 2$	$2t + 2$
Computing time of the participants (each time)			
power operation	$2t$	$2t$	$2t$
multiplication of exponent	$2t - 2$	0	0
addition of exponent	0	$2t - 2$	0
multiplication	$2t - 1$	$2t$	$2t$
Computing time of the dealer			
power operation	$2t$	$2t + 1$	$2t + 1$
multiplication of exponent	0	0	$2t$
addition of exponent	0	$4t - 3$	$2t - 1$
inverse of exponent	0	$2t - 1$	$t$

In Section 2, the Step 5 of **Divide Secret Phase** in HS-TS needs to check  $E'_1, E'_2, \dots, E'_i$  are linear independent or not. This problem also appear in most of our schemes. We expect to propose a algorithm which can avoid  $E'_1, E'_2, \dots, E'_i$  linear dependent in finite steps in the future. In Section 4, the Step 2 of **Divide Secret Phase** in OHE-TS needs to check  $\sqrt{T}$  exist in the directory file or not. We can improve it by using more  $n$  public values or send one more share to each participant. The method will similar to HE-TS that stated in Section 2.

Wu and He proposed a secret sharing scheme based on a hyperspherical function. We proposed a secret sharing scheme based on a hyperelliptic function in Section 2. We guess there also exist a new geometric approach about hyperbole function or other geometric function on secret sharing scheme. That will be a interesting problem as the future work.

## References

- [1] G. Blakley, “Safeguarding cryptographic keys”, in *Proceedings of the National Computer Conference*, New York, pp.313-317, 1979.

- [2] E.F. Brickell and D.R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes", *Journal of Cryptology* 5, pp.153-166, 1992.
- [3] D.E.R. Denning, *Cryptography and data security*, Addison-Wesley, Reading, MA, 1983.
- [4] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory IT-31*, pp.469-472, 1985.
- [5] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing", in *Proceedings of 28th Foundations of Computer Science*, pp.427-437, 1987.
- [6] S.H. Friedberg, A.J. Insel and L.E. Spence, *Linear algebra*, Prentice Hall, 2002.
- [7] H. Ghodosi, J. Pieprzyk, G.R. Chaudhry and J. Seberry, "How to prevent cheating in Pinch's scheme", *Electronics Letters* Vol.33, pp.1453-1454, 1997.
- [8] R.W. Hamming, *Coding and Information Theory*, Englewood Cliffs, Reading, Prentice-Hall, 1986.
- [9] M. Ito, A. Satio and T. Nishizeki, "Secret sharing scheme realizing general access structure", *Journal of Cryptology* 6, pp.15-20, 1993.
- [10] W.A. Jackson, K.M. Martin and C.M. O'Keefe, "Multisecret threshold schemes", in *Proceedings of Advances in Cryptology-Crypto'93, Notes in Computer Science*, Vol. 773, Springer-Verlag, Berlin, pp.126-135, 1994.
- [11] R.L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", *Communications of the ACM* 21, pp.120-126, 1978.
- [12] A. Shamir, "How to share a secret", *Communications of the ACM* 22, pp.612-613., Nov. 1979.
- [13] C.E. Shannon, "Communication theory of secrecy systems", *Computer Security Journal*, VI(2) 7-66, 1990.
- [14] H.-M. Sun and S.-P. Shieh, "Secret sharing schemes for graph-based prohibited structures", *Computers and mathematics with Applications*, Vol. 36, No. 7, New York, pergamon Press, pp.131-140, 1998.
- [15] T.-C. Wu and W.-H. He, "A geometric approach for sharing secrets", *Computer & Security*, pp.135-145, 1995.
- [16] C.-Y. Yeun, *Design, analysis and applications of cryptographic techniques*, Ph.D. Thesis, Department of Mathematics, University of London, England, 2001.