Cheater Detection and Cheating Identification by Using Shamir Scheme

Prof. Svapnil M Vakharia

Assistant Professor
Information Technology Department
Gandhinagar Institute of Technology, Gandhinagar, India

Abstract: In cryptography, a secret sharing scheme is a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own. The study of secret sharing schemes was independently initiated by Shamir and Blakely in 1979. Since then several other secret sharing schemes Ire introduced. When shareholders present their shares in the secret reconstruction phase, dishonest shareholder(s) (i.e. cheater(s)) can always exclusively derive the secret by presenting faked share(s) and thus the other honest shareholders get nothing but a faked secret. Cheater detection and identification are very important to achieve fair reconstruction of a secret. My proposed scheme uses the shares generated by the dealer to reconstruct the secret and, at the same time, to detect and identify cheaters My proposed scheme is an extension of Shamir's secret sharing scheme.

Index Terms - **Attacks, Consistency, Detection, Identification, Majority voting, Secret sharing scheme**

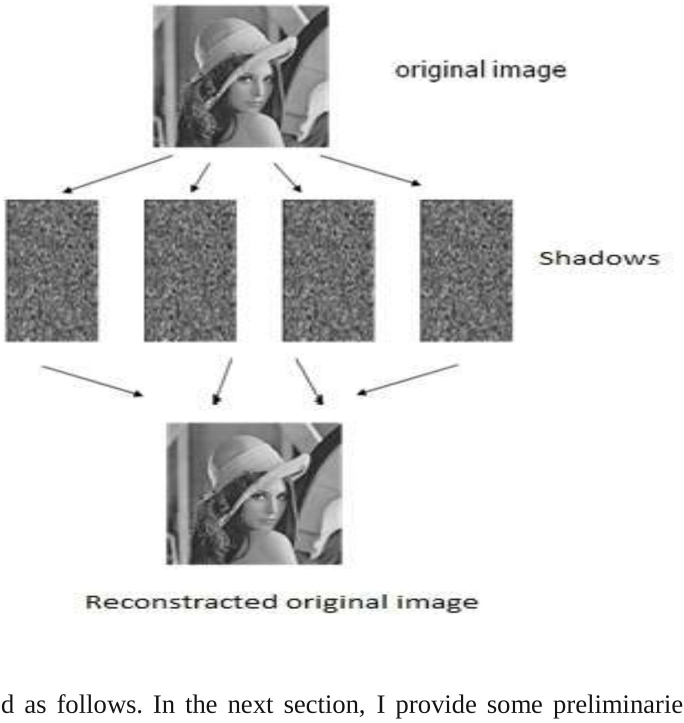
I. Introduction

Shamir's *(t, n)*-SS scheme is very simple and efficient to share a secret among *n* shareholders. However, when the shareholders present their shares in the secret reconstruction phase, dishonest shareholder(s) (i.e. cheater(s)) can always exclusively derive the secret by presenting faked share(s) and thus the other honest shareholders get nothing but a faked secret.

It is easy to see that the Shamir's original scheme does not prevent any malicious behavior of dishonest shareholders during secret reconstruction. Cheater detection and identification are very important to achieve fair reconstruction of a secret.

In this paper, I use a different approach to prevent cheaters. I consider the situation that there are more than *t* shareholders participated in the secret reconstruction. Since there are more than *t* shares (i.e. it only requires *t* shares) for reconstructing the secret, the redundant shares can be used for cheater detection and identification. My proposed scheme uses the shares generated by the dealer to reconstruct the secret and, at the same time, to detect and identify cheaters. Simmons [11] has suggested using the same method to detect cheaters.

In this paper, I have included discussion on possible attacks of cheaters and bounds of detect ability and identify ability of my proposed scheme under these attacks.



The rest of this paper is organized as follows. In the next section, I provide some preliminaries. Detection and identification of cheaters I describe attacks of cheaters. I analyze my scheme under three attacks and calculate bounds of detect ability and identify ability of my proposed scheme.

A ***(k,** n)* threshold scheme have the following characteristics:

(1) The secret is divided into ***n*** shadows.
(2) Any ***k*** or more shadows can be used to reconstruct the secret.
(3) Any ***k*** - 1 or less shadows reveal no knowledge about the secret.

Shamir [l] introduced an elegant and efficient ***(k,** n)*

II. PRELIMINARIES

In this section, I introduce some basic preliminaries.

2.1 Shamir’s Secret sharing scheme

Shamir's secret sharing scheme [Sha79] is a threshold scheme based on polynomial interpolation. To allow any m out of n people to construct a given secret, an (m-1)-degree polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 \ldots\ldots\ldots\ldots\ldots\ldots + a_{m-1} x^{m-1}$$

over the finite field $GF(q)$ is constructed such that the coefficient a_0 is the secret and all other coefficients are random elements in the field; the field is known to all participants. Each of the n shares is a pair (x_i, y_i) of numbers satisfying

$f(x_i) = y_i$ and $x_i \neq 0$. Given any m shares, the polynomial is uniquely determined and hence the secret a_0 can be computed. However, given m-1 or feIr shares, the secret can be any element in the field. Therefore, Shamir's scheme is a perfect secret sharing scheme

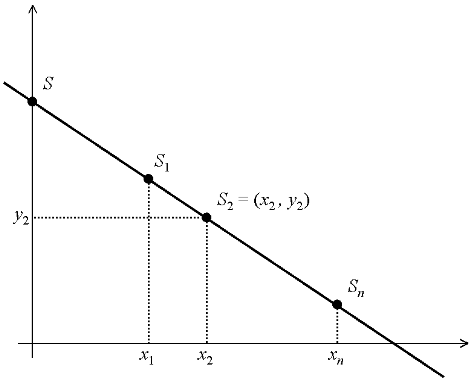


Fig. Shamir’s secret sharing scheme

A special case where m = 2 (that is, two shares are required for retrieval of the secret) is given in Figure. The polynomial is a line and the secret is the point where the line intersects with the y-axis. Namely, this point is the point $(0,f(0)) = (0, a_0)$. Each share is a point on the line. Any two points determine the line and hence the secret. With just a single point, the line can be any line that passes the point, and hence the secret can be any point on the y-axis

C denotes number of fake shares and j($n \geq j \geq t$) denotes number of participants .J=$\{i_1\ldots\ldots i_j\}$ algorithms:

1. *Share generation algorithm* the dealer D first picks a polynomial $f(x)$ of degree $t-1$ randomly:

$f(x) = a0+a1x+\ldots\ldots\ldots\ldots\ldots+a_{t-1}x^{t-1}$, in which the secret $s = a0$ and all coefficients $a0, a1,\ldots\ldots, a_{t-1}$ are in a finite field F, and D computes:

$s_1 = f(1), s_2 = f(2), \ldots, s_n = f(n).$

Then, the algorithm outputs a list of n shares $(s1, s2\ldots., sn)$ and distributes each share s_i to corresponding shareholder Pi secretly.

2. *Secret reconstruction algorithm* this algorithm takes any t shares $(s_{i1}, \ldots, s_{it})$ where $\{i_1, \ldots, i_t\} \subset \{1, 2, \ldots, n\}$ as inputs, and outputs the secret s.

Above scheme satisfies the basic requirements of secret sharing scheme as follows: (1) With knowledge of any t or more than t shares, it can reconstruct the secret s easily; (2) With knowledge of feIr than t shares, it cannot get *any* information about the secret s. Shamir’s scheme is *information-theoretically secure* since the scheme satisfies these two requirements without making any computational assumption.

2.1 Secrets majority

If the shares $s_1, \ldots, s_m$ are *inconsistent*, it is easy to see that secrets s_i for $i = 1, \ldots, u$ reconstructed by combinations of t out of m shares are not identical. Then, I can divide the set $U = \{s_1, \ldots, s_u\}$ containing all reconstructed secrets into several mutually disjoint subsets Ui, for $i = 1, \ldots, v$. Each subset contains same secret. These subsets satisfy following conditions.

$U = U_1 \cup \ldots\ldots \cup Uv$, where $U_i = \{s^{i1}, \ldots, s^{iwi}\}$ and $s^{wi} = s^{i1} = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots = s^{iwi}$;

$U_k \cap U_l = \emptyset$ for $1 \le k, \ l \le v$ and $k \ne l$.

For all subsets U_i for $i = 1, \dots\dots.., v$ as defined previously, set $w_i = |U_i|$ and $w_z = \max_i \{w_i\}$, then the secret s^{wz} is said to be the majority of secrets.

III. **ALGORITHMS**

My aim to describe approach to detect and identify cheaters. Then, I propose my scheme which is based on Shamir's *(t, n)*-SS scheme. One unique feature of my proposed scheme is that I use the same share for secret reconstruction to detect and identify cheaters. My scheme is an extension of Shamir's *(t, n)*-SS scheme.

Method for detecting cheaters In Shamir's *(t, n)*-SS scheme, a $t - 1$ degree interpolating polynomial can be uniquely reconstructed based on t shares. Thus, if there are more than t shares and there is no faked share, a consistent polynomial should be reconstructed for all combinations of t shares. Cheater detection is determined by detecting inconsistent polynomials (or secrets) among all reconstructed secrets. HoIver, cheaters can collaborate to determine their faked shares to fool honest shareholders to believe that a faked secret is a real secret. In Sec. 5, I will discuss bounds of detect ability of my proposed detecting scheme under three attacks as presented in next section.

Method for identifying cheaters When cheaters have been detected, there are inconsistent reconstructed polynomials (or secrets) for all combinations of t shares. Among all reconstructed secrets, if the legitimate secret is the majority of secrets as I have defined in Def. 2, I can use the *majority voting mechanism* to identify each faked share. I need to investigate conditions that the legitimate secret is the majority of secrets. In addition, I will discuss bounds of identify ability of my proposed identifying scheme under three attacks as presented in next section.

I use c to denote the number of faked shares and $j \ (n \ge j \ge t)$ to denote the number of participants in a secret reconstruction. There are $j - c$ legitimate shares in a secret reconstruction.

```
Algorithm 1 (Cheater detection)
Input: $t, n, J, si1, \dots, si\,j$
1. Compute an interpolated polynomial $f(x)$ of $j$ points $(i_i, si_1), \dots, (i_j, si_j)$. Set the degree of $f(x)$ to be $d$.
2. If $d = t - 1$, then $s = f(0)$, and
Output: There is no cheater and Secret is $s$ ; otherwise
Output: There are cheaters.
```

```
Algorithm 2 (Cheater identification)
Input: $t, n, s, J, T, si_1, \dots, si_j$
1. For all $Ti \in \tau$, compute $si = F(Ti)$ where $i = 1, \dots, u$.
2. Divide $U = \{s^1, \dots, s^u\}$ into $v$ subsets $Ui$ such that
   $U = U1 \cup \dots\dots.. \cup Uv$ where
   $U_k \cap U_l = \emptyset$ for $1 \le k, l \le v$ and $k \ne l$, and
   $U_i = \{s^{i1}, \dots.., s^{iwi}\}$ where $s^{wi} = s^{i1} = \dots\dots\dots\dots. = s^{iwi}$ .
3. Set $wz = \max_i \{w_i\}$, and set $s = s^{wz}$ .
4. Pick $Tk \in T$ such that $s = F(Tk) = FTk(s_{ik1} \dots s_{ikt})$,
    and set $R = J - \{i_{k1}, \dots, i_{kt}\}$.
5. Pick $i_r \in R$ orderly and remove it from $R$, and
    compute $s^r = F(s_{ir}, s_{ik2}, \dots\dots\dots.., s_{ikt})$.
6. If $s^r = s$, then put $i_r$ into $H$; otherwise put $i_r$ into $C$.
7. Return Step 5 until $R = \emptyset$.
Output: The cheater set is $C$.
```

Remark 2 The computational complexity of algorithm 1 is $O(1)$ and the complexity of algorithm 2 is $O(j\,!)$, where $j \le n$. I want to point out that n is the total number of shares in a secret sharing scheme and n is independent with the security of secret sharing scheme.
Here, I discuss about three attacks of cheaters that are against my proposed detection and the identification scheme.

Type 1 *attack* the cheaters of this type attack can be either honest shareholders who present their shares in error *accidentally* or dishonest shareholders who present their faked shares *without* any collaboration. Each faked share of this attack is just a random integer and is completely independent with other shares.

Type 2 *attack* the cheaters of this type attack are dishonest shareholders who modify their shares on purpose to fool honest shareholders. In this type attack, I assume that all shareholders release their shares *synchronously*. Thus, cheaters can only collaborate among themselves to figure out their faked shares before secret reconstruction; but cannot modify their shares after knowing honest shareholders' shares (i.e. I assume that all shares must be revealed simultaneously). Under this assumption, only when the number of cheaters is larger than or equal to the threshold value t, the cheaters can implement an attack successfully to fool honest shareholders.

Type 3 *attack* the cheaters of this type attack are dishonest shareholders who modify their shares on purpose to fool honest shareholders. In this type attack, I assume that all shareholders release their shares *asynchronously*. Since shareholders release their shares one at a time, the optimum choice for cheaters is to release their shares after all honest shareholders releasing their shares.

The cheaters can modify their shares accordingly. I consider the worst-case analysis to determine the bounds of detect ability and identify ability of my proposed scheme.

A. Cheater detection

The cheater problem is a serious obstacle for secret sharing schemes. A cheater is a qualified participant who possesses a true share, but releases a fake share or withholds a share during a reconstruction of the secret. If a cheater releases a fake share or withholds a share on secret reconstruction, then he/she can obtain the secret and exclude others. Thus, the cheater has an advantage over the other shareholders.

Schemes	**Shamir**	**Blakley**	**Tompa**	**Wall**	**Proposed**
Perfect sharing	Yes	No	No	No	Yes
Size of share	Same	Small	Larger	Larger	Same
Method used for SSS	Polynomial	Hyper plane	One way hash	One way hash	Polynomial
Reveal info	Yes	Yes	No	No	No
Cheater detection	No	No	Yes	Yes	Yes
Cheater identification	No	No	Yes	Yes	Yes

V. PROPOSED WORK

Cheater identification scheme is based on Lagrange interpolation**.** In the (*t*,*n*)-threshold scheme proposed in this chapter a secret is an integer number *S*.

Secret sharing schemes protect the secrecy and integrity of information by distributing the information over different locations. The (*t, n)* threshold secret sharing schemes Ire introduced by Shamir and Blakley independently in 1979 for protecting the cryptographic keys. Generation of shares and reconstruction of shares are challenging task in cheaters scenario. Cheaters identification is critical task on the time of share reconstruction. In this dissertation I proposed a roust secret share generation technique such technique based on cyclic point intersection of langrage's interpolation. In the process of share generation, construction and cheater identification, I proposed fmy steps. (i) Cyclic share generation (ii) share reconstruction and (iii) cheater identification. The proposed scheme used some notations are defined I assume that P is a participant set that contain n participant p1, p2, p3……………pn. Such that p= {p1,p2,p3,…………pn} and c1,c2 …cn are cyclic prefix of interpolation equation. Each member of P shares a secret K and hold a secret cyclic prefix Ci where 1≤i≤n.

5.1 Share generation phase

Assume that a dealer wants to share a secret K among the n members in P. First, the dealer specifies the threshold value t freely within the range 1 ≤ t ≤ n. then dealer select three point of prime in subsequent in cyclic x ,y, z .

The dealer randomly generates n different polynomials fi's of degree t−1, such that

$$Fi(X) = a(i,0) + a(i,1)X + \cdots \dots \dots \dots \dots + a(i,t-1)Xt - 1$$

Now then the cyclic point of intersection put into each generated shares Xc, Yc and Zc
As
Consider two distinct points J and K such that J = (xcJ, ycJ) and K = (xcK, ycK)

Let L = J + K where L = (xcL, ycL), then
xcL = s2 - xcJ – xcK
yL = -yJ + s (xJ – xL)
s = (yJ – yK)/(xJ – xK), s is the slope of the line through J and K.

If K = -J i.e. K = (xJ, -yJ) then J + K = O. where O is the point at infinity.If K = J then J + K = 2J then point doubling equations are used.Then dealers send the all generated shares to participant.

5.2 The Secret Reconstruction Phase

Assume that the participants P1, P2. Pr of any qualified subset in P wants to Cooperate to reconstruct the shared secret K. They can perform the following steps To determine the shared secret K. In the reconstruction phase I apply cyclic addition point of interpolation.

Consider a point J such that J = (xcJ, ycJ), where yJ ≠ 0
Let L = 2J where L = (xcL, ycL), Then
xcL = s2 – 2xJ mod p
ycL = -ycJ + s(xcJ - xcL) modZc
s = (3xcJ 2 + a) / (2yJ) mod Zc, s is the tangent at point J and a is one of the parameters chosen with the elliptic curve. If yJ = 0 then 2J = 0, where 0 is the point at infinity.

5.3 Cheaters detection phase

In the cheater detection phase ,reconstructed shares find the point of intersection of cyclic in langrage's interpolation the difference value of cyclic prefix is 0 there is no cheater and the cyclic point generate a difference 1 then there is cheater.

VII.CONCLUSIONS

In this paper, I consider the cases when there are more than *t* shareholders participated in secret reconstruction. Since there are more than *t* shares for reconstructing the secret, the redundant shares of a *(t, n)* secret sharing scheme can be used to detect and identify cheaters.

I introduce the property of consistency and the notion of the majority of secrets to detect and identity cheaters. The bounds of detect ability and identify ability under three attacks are presented. I utilizes shares for secret reconstruction to detect and identify cheaters. My scheme is an extension of Shamir's secret sharing scheme.

REFERENCES

[1] W. Trappe and l .C. Washington, "Introduction to Cryptography with Coding Theory", Pearson International Edition (2006)
[2] C. C. Thien and J.C.Lin, "Secret image sharing," Computers & Graphics, vol. 26, no.1, 765-770, 2002.
[3] Blakley G.R., "Safeguarding cryptographic keys. In: Proceedings of AFIPS'79", vol. 48, pp. 313–317 (1979).
[4] Brickell E.F., Stinson D.R., " The detection of cheaters in threshold schemes. In: Proceedings of Crypto'88", LNCS, vol. 403, pp. 564–577. Springer-Verlag (1990).
[5] CarpentieriM., " A perfect threshold secret sharing scheme to Identify cheaters", Des. Codes Cryptogr. **5**(3), 183–187 (1995).
[6] CarpentieriM., De Santis A., Vaccaro U, " Size of shares And Probability of cheating in threshold", schemes. In: Proceedings of Eurocrypt'93, LNCS, vol. 765, pp. 118 125. Springer-Verlag (1994).
[7] Charnes C., Pieprzyk J., Safavi-Naini R., "Conditionally Secure secret sharing scheme with disenrollment Capability" In: Proceedings of CCS'94, pp. 89–95. ACM (1994).
[8] Kurosawa K., Obana S., Ogata W.: *t*-cheater identifiable *(k, n)* secret sharing schemes. In: Proceedings of Crypto'95, LNCS, vol. 963, pp. 410–423. Springer-Verlag (1995).
[9] Rabin T., Ben- Or M., "Verifiable secret sharing and multiparty protocols wth honest majority", In:Proceedings of the 21st Annual ACM Symposium on the Theory of Computing, pp. 73–85 (1989).
[10] Shamir A., " How to share a secret. Comm.", ACM **22**(11), 612–613 (1979). [11] Simmons G., "An introduction to shared secret schemes and their applications", Sandia Report SAND 88-2298 (1988).
[12] Tompa M., Woll H, " How to share a secret with cheaters", J. Cryptol. **1**(3), 133–138 (1989).