I.J. Mathematical Sciences and Computing, **2016, 2, 1-13**
Published Online April 2016 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijmsc.2016.02.01

Available online at ***http://www.mecs-press.net/ijmsc***

A Novel Verifiable Secret Sharing with Detection and Identification of Cheaters' Group

Qassim Al Mahmoud

Faculty of Mathematics and Computer Science, the University of Bucharest, Romania

Abstract

Shamir's (t, n)-SS scheme is very simple to generate and distribute the shares for a secret among n participants by using such polynomial. We assume the dealer a mutually trust parity when he distributes the shares to participants securely. In addition when the participants pooling their shares in the secret reconstruction phase a honest participants can always reconstruct the real secret by Pooling areal shares. The property of verifiability enables participants to verify that their shares are consistent. Tompa and Woll suggested an important cheating scenario in Shamir's secret reconstruction. They found a solution to remove a single cheater with small probability, unfortunately, their scheme is based on computational assumptions. In addition each participants will receive a huge number of shares. In this paper we will construct scheme to be information-theoretically secure verifiable secret sharing which does not contain a single cheater. On the other hand we will eliminate these problems in Tompa and Woll scheme. Our proposed scheme is not only to detect and identify a cheater, but to prevent him from recovering the secret when the honest participants cannot.

Index Terms: Secret sharing, verifiable secret sharing, honest participants, dishonest participants, single cheater, cheaters' group.

1. Introduction

Secret sharing schemes introduced by both Blakley [1] and Shamir [2] independently in 1979 as a solution for safeguarding cryptographic keys and have been studied extensively in the literatures. In basic secret sharing scheme, a secret S is divided into n shares and shared among a set of n shareholders by a mutually trusted dealer in such a way that any t or more than t shares will be able to reconstruct this secret; but fewer than t shares cannot know any information about s. Such a scheme is called a (t, n) secret sharing, denoted as (t, n)-SS.

* Corresponding author. Tel.:
E-mail address:

Shamir's (t, n)-SS scheme is very simple to generate and distribute the shares for a secret among n participants by using such polynomial. We assume the dealer a mutually trust parity when he distributes the shares to participants securely, in addition when the participants pooling their shares in the secret reconstruction phase, honest participants can always reconstruct the real secret by Pooling areal share(s).

In 1985, Chor et al. [3] extended the original secret sharing and presented a notion of verifiable secret sharing (VSS). The property of verifiability enables participants to verify that their shares are consistent. According to the security property, VSSs can be classified into two types: the computationally security [4] and the unconditionally security [5, 6]. Feldman's VSS [4] is based on the hardness of solving the discrete logarithm, Nikova's VSS [5] and Pedersen's VSS [6] are unconditionally security. There are VSS schemes based on some computational assumptions. For example, Feldman's VSS scheme [4] is based on the discrete logarithm assumption. Later, Pedersen [6] (Pedersen, 1992) used a commitment scheme to remove the assumption in Feldman's VSS scheme to propose a VSS scheme which is information-theoretically secure, However, in Pedersen's VSS scheme the dealer can succeed in distributing incorrect shares if the dealer can find the commitment value and then solve the discrete logarithm problem.

In this paper we will examine the scenario that was found by Tompa and Woll [7], they suggested that in Shamir's secret reconstruct algorithm a dishonest participant (i.e. cheater) decided to pool a fake share in order to get the real secret, thus, the other honest participants get a wrong one. Shamir's scheme does not prevent any malicious behavior of dishonest participants during secret reconstruction. Cheater detection and identification are very important to a fair reconstruction of a secret. Our proposed scheme is not only to detect and identify a cheater, but to prevent him from recovering the secret when the honest participants cannot.

There are many research papers study to investigate the problem of cheater detection and identification for secret sharing schemes. Some of these papers [8, 9, 10, and 11] consider that the dealer needs to generate and distribute additional information, such as using check vectors and certificate vectors for each participants. Some of other papers [12, 13] proposed their schemes based on an error-correcting code in which fake shares can be detected as error codes and corrected based on coding technique. For example, McEliece and Sarwate [13] suggested constructing a secret sharing scheme based on Reed-Solomons code. Their scheme can guarantee that the secret is a real secret by honest participants. There are some papers [14, 15, 16] propose secret sharing schemes based on computational assumptions. Since these schemes are conditionally secure, the ability to detect and identify cheaters are much stronger than those schemes that are unconditionally secure. For example such that scheme based on RSA [15].

Our proposed scheme is being protected from a single cheater. We will see in secret reconstruction phase the scheme does not contain a single dishonest participant (cheater) who pools a fake share to deceive the other participants in order to get the real secret and the honest participants get a wrong one. Typically, the proposed scheme will start when a dealer applies the same secret generation algorithm as in Shamir's scheme to generate the shares of a certain secret S, then he distributes shares for participants securely. Also the dealer broadcast the commitments values as in Pedersen's verifiable secret sharing scheme to enable the participants to verify the shares are consistent. So far our scheme is nothing more than Pedersen's secret sharing scheme. The difference in our scheme that is when the participants received their shares from dealer, each participants act as dealer, then they divide their shares into two sub shares, where the second sub share kept as a secret. Moreover, Shamir's secret generation algorithm and Pedersen's verification shares are applied to the first sub share, and then each participant distributes the new shares securely, also each participant broadcasts sub commitments values for each other.

Note that in our scheme the number of shares for each participant are (n+1) shares, one share got from the dealer and (n) shares got from each other. In secret reconstruction algorithm any t participant in authorized set will be split into two subsets. Each subset contains at least two or more than two participants; the participants in each subset separately, will release the second sub shares. Then they apply shares verification as in Pedersen's VSS for the shares of first sub shares to insure that they are honest participants. So far both subsets do not contain cheaters, thus all participants in both subsets apply together t times of secret reconstruction algorithm as in Shamir's SS to reconstruct the first sub shares for each participant. Each subset separately, collaborates in

order to find the shares of secret. Again they apply Pedersen's verification to insure that all shares are consistent. Our scheme is based on both Shamir's and Pedersen's secret sharing schemes to eliminate a single cheater that found by Tompa and Woll scenario [7].

This paper is organized as follow: section 2 will be the previous study, which is divided to Shamir's scheme, Pedersen's VSS, and Tompa and Woll scheme, in section 3, it will be explanation to our scheme, in Section 4 it will discuss the security analysis for our scheme, and then finally the conclusion will be in section 5.

2. Previous Study

In this section we have to mention, in general, the two important threshold schemes in secret sharing: the first part in this section talks about Shamir's secret sharing scheme, and the second part will be about Pedersen's VSS. The third part we will focus about cheating scenario that is found by Tompa and Woll scheme [7], in addition their solution scheme for that scenario.

2.1. Shamir's scheme [2]

In 1979, Shamir has introduced the threshold secret sharing as a solution for safeguarding cryptographic keys. His scheme has generated the thinking of how to share a secret with multi participants, and it has been used until now as the root for wide research papers in computer security. Thus, we should give an overview of his important scheme on which our scheme depends.

In Shamir's $(t,n)-$ scheme based on Lagrange interpolating polynomial, there are n participants, $P=\{P_1,P_2,...,P_n\}$ and a dealer D. The scheme consists of two algorithms:

1- Generation Shares Algorithm:

Dealer D does the following:

- Picks a polynomial $f(x)$ of degree (t-1) randomly $f(x)=a_0+a_1x+...+a_{t-1}x^{t-1}$, in which the secret $S=a_0$ and all coefficients $a_0,a_1,...a_{t-1}$ are in a finite field $F_p=GF(P)$
- Computes: $s_1=f(1),s_2=f(2),...,s_n=f(n)$
- Outputs a list of n shares $(s_1,s_2,...s_n)$, and distributes each share to corresponding participants privately.

2- Secret Reconstruction Algorithm:

With any t shares, we can reconstruct the secret S as t participants work together and then, pooling their shares, then apply Lagrange's interpolation to find the coefficients in polynomial used $f(x)$, and then the secret is $f(0)=S$

We note that the above scheme satisfies the basic requirements of the secret sharing scheme as follows:

- With knowledge of any t or more than t shares, it can reconstruct the secret S.
- With knowledge of any fewer than t shares, it cannot reconstruct secret S.

Shamir's scheme is information-theoretically secure since the scheme satisfies these two requirements without making any computational assumption. For more information on this scheme, readers can refer to the original paper [2].

In Shamir's (t, n) SS, a dealer is a third trusted party who generates and distributes shares to n participants by using such polynomial, t participants and (more) can reconstruct the secret S, and less than t know nothing about S.

2.2. Pedersen's VSS Scheme

In Feldman's VSS scheme [4] is that the committed values are publicly known and the privacy of secret s depends on the difficulty of solving the discrete logarithm problem. In other words, Feldman's scheme is computationally secure. In 1992 Pedersen [6] proposed a non-interactive and information-theoretically secure VSS scheme based on Feldman's VSS scheme.

Let p and q be two large primes numbers such that q| (p−1), and g, h $\in Z_p$ are two elements of order q. There are n participants $P=\{P_1,P_2,..,P_n\}$ and a dealer D who will divide a secret $s \in Z_p$ we describe Pedersen's scheme below.

1- Generation Shares Algorithm:

Dealer D does as follows:

- Picks a polynomial $f(x)=a_0+a_1x+...+a_{t-1}x^{t-1}$ of degree at most $(t-1)$ randomly, in which the secret $S=a_0=f(0)$ and all coefficients $a_0,...,a_{t-1}$ are in Z_p
- Picks $b_0,...,b_{t-1} \in Z_p$ at random. Let $k(x)=b_0+b_1x+...+b_{t-1}x^{t-1}$.
- Computes shares (s_i,t_i) for i = 1, . . . , n and each coefficient's commitment of added sum of polynomials of f (x) and k(x) as follows: $(s_i,t_i)=(f(i),(k(i))$
- Computes $c_j=g^{a_j}h^{b_j} \bmod p$ for j = 0, 1. . . t −1.
- Outputs a list of n shares (s_i,t_i) and distributes each share to corresponding participants P_i privately. D also broadcasts c_j

2- Share verification:

Each participant P_i, who has received the share (s_i,t_i) and all broadcasted information, can verify that share defines a secret by testing:

$$g^{s_i}h^{t_i} \bmod p=\prod_{j=0}^{t-1}c^{i^j}{}_j \pmod p \quad (1)$$

3- Secret Reconstruction Algorithm:

It is same as Shamir's scheme.

In Pedersen's scheme, the value g^{a_0} is not made publicly known, that is, the secret S is embedded in the commitment $c_0 = g^{a_0+ub_0}$, where $u = \log_g h$. Thus, no information directly about the secret S even if an attacker with unlimited computing power can solve $u = \log_g h$, the attacker still gets no information about the secret s.

2.3. Tompa and Woll scheme [7]

Tompa and Woll [7] suggested an important a cheating scenario. They supposed t participants $P = \{P_1, P_2, .., P_t\}$ decided to pool their corresponding shares $s_i = \{s_1, s_2, .., s_t\}$, in secret reconstructing algorithm and one of them decided to cheat (i.e. pool a fake share). The dishonest participant say P_1 does as follow: find polynomial $g(x)$ of degree at most (t-1), such that $g(0) = -1$, and $g(s_2) = g(s_3) = ... = g(s_t) = 0$, he gives the share $s_1 + g(1)$ instead of the share s_1, having a shares $\{s_1 + g(1), s_2, .., s_t\}$ the Interpolates a polynomial reconstruct the polynomial of degree (t-1) $f(x) + g(x)$ and the free coefficient will be $f(0) + g(0) = s - 1$, then the honest participant will get wrong secret S and the p_1 get the correct secret.

We note that the scenario above successfully completed if and only if the scheme has only one cheater, but if there exist separately more than one cheater without any collaboration to cheat, then the scenario fails.

Our scheme is suggested in this paper to eliminate a single cheater in Shamir's SS that was found by Tompa and Woll scenario [7].

Tompa and Woll have suggested a solution to their scenario in same their paper [8] to detect the cheater, such that each participant will receive (k) of different shares for a secret S. And only one of these (k) shares is the share of real secret and the rest (k-1) shares are shares of dummy public values (i.e. the real secret is embedded in the dummy values, the participants do not know in which round of secret reconstruction phases will get the real secret). In secret reconstruction algorithm the participants need (k) round at most until find the real secret which is a different from the dummy values. A cheater can succeed to pool fake share to deceive the other honest participant with small probability (1/k), and then he gets a real secret exclusively. Tompa and Woll scheme is conditionally security (i.e. based on computational assumptions), this mean it is not secure against a single cheater (i.e. if that cheater succeeds to deceive the other participants with small probability). We note that the security of their scheme depend on the number of shares (k). In addition to make that probability small each participant should receive a huge number of shares, thus their scheme is impracticable in secret sharing scheme applications.

Next section is shown us our scheme is unconditionally security (i.e. information-theoretically secure), and the participants need to receive n of different shares (n is a number of all participants in (k, n)-threshold secret sharing scheme). Our scheme is suggested to remove the computational assumptions in Tompa and Woll [7].

3. A Novel Verifiable Secret Sharing with Detection and Identification of Cheaters' Group

In this section we will show how we can share a certain secret S securely, such that in secret reconstruction phase when the participants agree to recover a secret. Thus our scheme will not contain any single cheater. Our scheme is based on both Shamir's and Pedersen's schemes.

Let p and q be two large primes numbers such that q| (p−1), and g, h $\in Z_p$ are two elements of order q. There are n participants $P = \{P_1, P_2, .., P_n\}$ and a dealer D who will divide a secret $S \in Z_p$ we describe our scheme below.

1- Generation Shares Algorithm:

The dealer does the same as Shamir's scheme and Pedersen's scheme to generate and distribute the shares of secret S.

After the all participants received the shares s_i from dealer, each participant p_i does as follows:

- Applies Pedersen's scheme to verify the dealer is an honest.
- Divides a share S_i of the secret S in two sub shares $s_i = s_{i,0} + s_{i,1}$
- Keeps $s_{i,1}$ secret.
- Picks a sub polynomial $f_i(x) = s_{i,0} + s_{i,1}x + ... + s_{i,t-1}x^{t-1}$ of degree at most $(t-1)$ randomly, in which the sub share $s_{i,0} = f_i(0)$ is a secret, and all coefficients $s_{i,0}, ..., s_{i,t-1}$ are in Z_p (see table1)
- Picks $b_{i,0}, ..., b_{i,t-1} \in Z_p$ at random. Let $k_i(x) = b_{i,0} + b_{i,1}x + ... + b_{i,t-1}x^{t-1}$
- Computes shares $(d_{i,j}, t_{i,j})$ of sub share $S_{i,0}$ for $i, j = 1, .., n$ and $i \neq j$, each coefficient's commitment of added sum of polynomials of $f_i(x)$ and $k_i(x)$ as follows: $(d_{i,j}, t_{i,j}) = (f_i(j), (k_i(j))$ (see table 1, 2).
- Keeps $f_i(0) = s_{i,0} = d_{i,0} \quad \forall i = j$ secret
- Computes sub commitments $c_{i,j} = g^{s_{i,j}} h^{b_{i,j}} \bmod p$ for j = 0. . . t −1, $\forall i$
- Outputs a list of n shares $(d_{i,j}, t_{i,j})$, and distributes to corresponding participants P_i privately. D also broadcasts $C_{i,j}$.

Table 1. Shares $d_{i,j}$ of the Sub Shares $s_{i,0}$ $\forall i = 1 \quad to \quad$ n , $\forall j = 0 \quad to \quad$ n

P_1	$s_{1,0}$	$d_{1,2}$	$d_{1,3}$	.		.	.	$d_{1,n}$
P_2	$d_{2,1}$	$s_{2,0}$	$d_{2,3}$	.	.	.	.	$d_{2,n}$
P_3	$d_{3,1}$	$d_{3,2}$	$s_{3,0}$	.	.	.	.	$d_{3,n}$
P_4	$d_{4,1}$	$d_{4,2}$	$d_{4,3}$	$s_{4,0}$	.	.	.	$d_{4,n}$
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	$s_{i,0}$	.	.
.	.	.	.	.	.	.	.	
P_n	$d_{n,1}$	$d_{n,2}$	.	.	.	.	.	$s_{n,0}$

Table 2. The Commitments $t_{i,j}$ $\forall i = 1 \; to \; \mathrm{n}$, $\forall j = 0 \quad to \quad \mathrm{n}$

P_1	$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	.		.	.	$t_{1,n}$
P_2	$t_{2,0}$	$t_{2,1}$	$t_{2,2}$	.	.	.	.	$t_{2,n}$
P_3	$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	.	.	.	.	$t_{3,n}$
P_4	$t_{4,0}$	$t_{4,1}$	$t_{4,2}$	.	.	.	.	$t_{4,n}$
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	
P_n	$t_{n,0}$	$t_{n,1}$	$t_{n,2}$	.	.	.	.	$t_{n,0}$

2- Shares verification:

Share verification S_i of secret is the same as Pedersen's scheme.

Each participant P_i, who has received the share $(d_{i,j}, t_{i,j})$ and all broadcasted information $C_{i,j}$, can verify that shares define a secret $S_{i,0}$ by testing:

$$g^{s_{i,j}} h^{t_{i,j}} \bmod p = \prod_{k=0}^{t-1} c^{j^k}{}_{i,k} (\mathrm{mod}\ p) \tag{2}$$

Next step will tell us the scheme still has no cheater because last step of shares verification satisfied that no participant can cheat. In the other hand the participants in each subset work together separately to insure that the participants release the real shares $d_{i,j}$ of sub shares $s_{i,0}$. In addition no participant can still reconstruct the secret S, and then each participant who belongs to the same subset cannot cheat each other.

3- Secret Reconstruction Algorithm:

Suppose t of participants $P_t = \{P_1, ... P_t\}$ decided to reconstruct the secret S, they do the following:

- Splitting themselves into two disjoint subsets randomly, say A and B subsets, where $P_t = \{A \cup B\}$, and $A \cap B = \phi$, where $A = \{P_1, ... P_k\}$, and $B = \{P_{k+1}, ... P_t\}$.
- The participants who belong to the same subset work together, then pooling the second sub shares $s_{i,1}$ for each other.
- All participants in the both subsets work together in order to reconstruct a first sub shares $s_{i,0}$ by pooling their shares $d_{i,j}$ as in Shamir's scheme to find the shares of secret $s_i = s_{i,1} + s_{i,0}$.

- The participants who belong to the same subset again work together separately, then apply Pedersen's verification scheme to insure that all participants pooling the real two sub shares of s_i by test:

$$g^{s_i} h^{t_i} \bmod p = \prod_{j=0}^{t-1} c^{j^k}{}_j \pmod p \tag{3}$$

Note that in the last step the participants who belong to the same subset cannot cheat each other because they still know nothing about the other shares in another sub set.

- After that both subsets insure that all participants pooling their real shares. Then both subsets send permission for each other to tell there is no single cheater detected inside each one. Finally, they pool the shares and again apply the same as Shamir's scheme to reconstruct the secret S.

Our scheme guarantees that both subsets do not contain a single cheater, but does not guarantee that one of both subsets as whole to be cheaters' group (i.e. we defined the subset which the participants collaborate and then decided to cheat), because in the last step of secret reconstruction the participants who belong to the same subset they can work together to cheat the other participants who belong to another subset as follow: they collaborate to decide pool one of fake share. On the other hand they can successfully activate the scenario that is suggested by Tompa and Woll [7]. In section of security analysis we will give more details about this problem.

Next we illustrate our scheme in a simple example.

Example: Let $p_i = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$ be the number of participants who want to play this scheme and the threshold is $t = 4$.

1- Shares generation algorithm:

Dealer generates and distributes the shares for secret S= 5 same as in Shamir's secret generation algorithm by chosen $f(x) = 5 + 2x + 3x^2 + x^3$, then the shares are $s_i = \{11, 29, 65, 129, 215, 341, 509\}$, (see table1) Each participant p_i received the shares s_i from the dealer does the following:

- Uses Pedersen's scheme to verify the dealer is honest.
- Divides the shares into two sub shares $s_i = s_{i,0} + s_{i,1}$

$$s_1 = 7 + 4,\ s_2 = 12 + 17,\ s_3 = 18 + 47,\ s_4 = 42 + 87,$$
$$s_5 = 15 + 200,\ s_6 = 90 + 251,\ \text{and } s_7 = 63 + 446$$

- Picks sub polynomials of degree ($t - 1 = 3$), and then generates shares $d_{i,j}$ for each sub shares $\{s_{1,0} = 7, s_{2,0} = 12, s_{3,0} = 8, s_{4,0} = 42, s_{5,0} = 15, s_{6,0} = 90, s_{7,0} = 63\}$ as in Shamir's scheme, $\forall i, j = 1 \quad to \quad 7$ (see table2).
- Picks $b_{i,0}, ..., b_{3,t-1} \in Z_p$ random, and let $k_i(x) = b_{i,0} + b_{i,1}x + b_{i,2}x^2 + b_{i,3}x^3$, then find $t_{i,j} = k_i(j)$, as in Pedersen's shares verification (see table 5).
- Distributes $(d_{i,j}, t_{i,j})$ $\forall i \neq j$, and make $f_i(0) = s_{i,0} = d_{i,0}$ $\forall i = j$ secret (see tables 4)

Tables 3. Sub Polynomials with Shares of Sub Shares by Users p_i, $\forall i, j = 1 \quad to \quad 7$

p_i	$f_i(x)$	$f_i(j) = d_{i,j}$
p_1	$f_1(x) = 7 + 4x + 3x^2 + 2x^3$	$f_1(j) = d_{1,j}$
p_2	$f_2(x) = 12 + x + 2x^2 + 7x^3$	$f_2(j) = d_{2,j}$
p_3	$f_3(x) = 18 + 3x + x^2 + 5x^3$	$f_3(j) = d_{3,j}$
p_4	$f_4(x) = 42 + 4x + 5x^2 + 3x^3$	$f_4(j) = d_{4,j}$
p_5	$f_5(x) = 15 + 7x + 7x^2 + 2x^3$	$f_5(j) = d_{5,j}$
p_6	$f_6(x) = 90 + 12x + 9x^2 + x^3$	$f_6(j) = d_{6,j}$
p_7	$f_7(x) = 63 + 4x + 9x^2 + 2x^3$	$f_7(j) = d_{7,j}$

Table 4. Shares $d_{i,j}$ of the first Parts of Shares $s_{i,0}$ $\forall i, j = 1 \quad to \quad 7$, $i \neq j$, and $f_i(0) = s_{i,0} = d_{i,0}$ $\forall i = j$

P_1	$s_{1,0}$ =7	$d_{1,2}$ =43	$d_{1,3}$ =100	$d_{1,4}$ =199	$d_{1,5}$ =352	$d_{1,6}$ =571	$d_{1,7}$ =868
P_2	$d_{2,1}$ =22	$s_{2,0}$ =12	$d_{2,3}$ =222	$d_{2,4}$ =496	$d_{2,5}$ =942	$d_{2,6}$ =1602	$d_{2,7}$ =2518
P_3	$d_{3,1}$ =27	$d_{3,2}$ =66	$s_{3,0}$ =18	$d_{3,4}$ =366	$d_{3,5}$ =683	$d_{3,6}$ =1152	$d_{3,7}$ =1803
P_4	$d_{4,1}$ =54	$d_{4,2}$ =94	$d_{4,3}$ =180	$s_{4,0}$ =42	$d_{4,5}$ =562	$d_{4,6}$ =894	$d_{4,7}$ =1344
P_5	$d_{5,1}$ =31	$d_{5,2}$ =73	$d_{5,3}$ =153	$d_{5,4}$ =283	$s_{5,0}$ =15	$d_{5,6}$ =741	$d_{5,7}$ =1093
P_6	$d_{6,1}$ =112	$d_{6,2}$ =158	$d_{6,3}$ =234	$d_{6,4}$ =316	$d_{6,5}$ =500	$s_{6,0}$ =90	$d_{6,7}$ =958
P_7	$d_{7,1}$ =78	$d_{7,2}$ =123	$d_{7,3}$ =210	$d_{7,4}$ =351	$d_{7,5}$ =558	$d_{7,6}$ =843	$s_{7,0}$ =63

2- Shares verification and secret reconstruction:

Let us suppose t =4 participants say $\{p_1, p_2, p_3\}$, and p_4 want to reconstruct secret S they doing the following steps:

- Splitting themselves into two disjoint subsets randomly, $A = \{p_1, p_2\}$ and $B = \{p_3, p_4\}$, then each subset works separate to pool their second part sub shares of secret S $\{s_{1,1} = 4, s_{2,1} = 17\}, \{s_{3,1} = 47, s_{4,1} = 87\}$ for each other.
- The participants who belong to the same subset work together, then pooling the second sub share $\{s_{1,0}, s_{2,0}, s_{3,0}, s_{4,0}\}$ for each other of secret S by pooling their sub shares $\{d_{i,j}\}$, $\forall i \neq j$ of first part

of secret shares, then by applying Shamir's secret reconstruction algorithm, such that $\{d_{1,2}, d_{1,3}, d_{1,4}\}$ to find $s_{1,0}$ and $\{d_{2,1}, d_{2,3}, d_{2,4}\}$ to find $s_{2,0}$, and so on $s_{3,0}$, and $s_{4,0}$. These values take from table1, and then $\{s_{1,0} = 7, s_{2,0} = 12, s_{3,0} = 8, s_{4,0} = 42\}$

- The participants in group $A = \{p_1, d_2\}$ calculates together their shares $\{s_1 = s_{1,0} + s_{1,1} = 7 + 4 = 11, s_2 = s_{2,0} + s_{2,1} = 17 + 12 = 29\}$, also the participants in $B = \{p_3, d_4\}$ do the same to find $\{s_3 = s_{3,0} + s_{3,1} = 18 + 47 = 65, s_4 = s_{4,0} + s_{4,1} = 42 + 87 = 129\}$.
- Each subset works together and used Pedersen's verification algorithm to verify that no participant inside subset pools a fake second parts sub shares $s_{i,1}$, and then insure that shares are correct shares of secret S by test:

$$g^{s_i} h^{t_i} \bmod p = \prod_{j=0}^{t-1} c^{j^k}{}_j \pmod p \tag{4}$$

- Then both subsets send permission for each other to tell there is no single cheater detected inside each one.
- Finally, they pool the shares and again apply the same as Shamir's scheme to reconstruct the secret S is 5.

4. Security Analysis

In this section we will show how our scheme is protected from single cheater. In addition we will analyze the security of scheme in three malicious behaviors of dishonest participants:

1. In the state that a single participant; $p_m \in \{p_1, p_2, ..., p_t\}$ released the second sub share $s_{m,1}$ of share. Our scheme prevents him from releasing a fake share for other participants who belong to the same subset.

We know the sub shares $s_{i,1}, \forall i \ 1 \text{ to } t$ tell nothing about the share s_i and the secret S. if p_m is a single participant who try to active the scenario in section (2.3). When all participants p_i successfully completed the reconstruction algorithm of first sub shares $s_{i,0}$, $\forall i \ 1 \text{ to } t$, the participants who are belong to same subset calculate together the shares $s_i = s_{i,0} + s_{i,1}$, and then they apply Pedersen's verification shares to insure that s_i are the real shares of the secret S (i.e. the participants who belong to the same subset where p_m, they can insure that s_m is a real share of secret S).

In this stage the participants who belong to the same subset still know nothing about the shares of participants who belong to another subset, thus the participants insure that both subsets do not contain a single cheater. This implies that our scheme is protected from this type of dishonest behavior and guarantees that there is no single cheater.

2. In the state that a single participant; $p_m \in \{p_1, p_2, ..., p_t\}$ released the share $d_{i,j}$ of sub share $s_{m,0}$ .Our scheme prevents him to releasing a fake share for all participants in both subsets.

In reconstruction algorithm of first sub shares $s_{i,0}$, suppose p_m tries to pool a fake share instead to his share $d_{m,0}$. In the end of this algorithm the participants still know nothing about all shares of the secret S even if he know the shares s_i of participants who belong to the same subset. Thus he cannot get a real secret because he needs to know t shares of secret, then he should pool a real sub share $d_{m,0}$. In addition the other participants in his subset will apply Pedersen's verification algorithm, and then they can detect him as cheater. So far that algorithm tells only the shares of the secret for the participant who belong to the same subset (i.e. the participants who do not belong to the same subset know nothing about the shares in that subset), p_m knows only the shares of participants in his subset. On the other hand p_m know nothing about the shares of participant in the other subset. Then he cannot deceive all participants in this scheme. This implies our scheme is protected from this type of behavior and guarantees that there is no single cheater.

3. In the state that the participants who belong to the same subset, and decided to collaborate as cheaters' group, our scheme enable them to act as one cheater in order to deceive the others participants in the other subset.

Unfortunately, our scheme fails in this type of cheating because those participants can collaborate to pool one fake share of the secret to deceive the other participants in the other subset.

The final step of secret reconstruction algorithm tells us that all participants in both subsets will pool their shares in order to reconstruct the secret S, the cheaters' group can successfully activate the scenario that was discussed in section (2.3), and then they get the real secret and the other participants in honest subset get a wrong one. The suggested solution to this problem is to use the idea of one way hash function and arithmetic coding that found by T.C. Wu and T. S. Wu [17], but the different is that we need to apply only hash function in the second sub shares $s_{i,1}$; otherwise our scheme will be classified into two types:

1. First type is unconditionally security scheme according to outside adversary (i.e. adversary who does not possess any share); this kind of adversary cannot get the shares s_i of secret even if he succeeds to attack a public hash function, and then find sub shares $s_{i,1}$.
2. Second type is conditionally security scheme with satisfy the condition that; in secret reconstruction algorithm, the inside adversary (i.e. cheater who is one of participants in scheme), can convince the other participants who belong to his subset to work with him as cheaters' group.

Remark: second type tells us that our scheme cannot prevent the cheaters' group from recovering the secret when the honest subset cannot. Moreover, hash function helps our scheme to detect and idintify the cheaters' group.

5. Conclusions

In this paper we have examined the scenario of cheating that is discussed in Tompa and Woll scheme [8], and we have constructed our scheme to eliminate a single cheater in Shamir SS that found by them. Our

scheme extends Shamir's SS and is based on Pedersen's verifiable SS to insure that dealer is an honest parity. We have seen our suggested scheme is not only detecting and identifying the cheaters, moreover it prevents him from recovering the secret when the honest participants cannot. In security analysis we studied three types of states for cheaters, two types about the state of a single cheater, and the third type was talking about cheaters' group. We proposed a solution to cheaters' group by using a public one way hash function based on scheme that is suggested by T.C. Wu and T. S. Wu. Finally we classified our scheme into two types; first type is unconditionally security scheme according to outside adversary, and Second type is conditionally security scheme according to inside adversary.

References

[1] G.R. Blakley, Safeguarding cryptographic keys, Proceedings of the AFIPS'79 National Computer Conference, vol. 48, AFIPS Press, 1979, pp. 313–317.

[2] Shamir, How to share a secret, Communications of the ACM 22 (11) (1979) 612–613.

[3] B. Chor, S. Goldwasser, S. Micali, B. Awerbuch, Verifiable secret sharing and achieving simultaneity in the presence of faults, Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, 21–23 October, Oregon, Portland, IEEE Computer Society, 1985, pp. 383–395.

[4] Feldman, P., 1987. A practical scheme for non-interactive verifiable secret sharing. In: Proceedings of the 28th IEEE Symposium on Foundations of Computer Science, 27–29 October. IEEE Computer Society, Los Angeles, California, pp. 427–437.

[5] Nikov, V., Nikova, S., 2005. On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Schemes, Cryptology e-print archive 2003/210.

[6] Pedersen, T.P., 1992. Non-interactive and information-theoretic secure verifiable secret sharing. In: Advances in Cryptology-CRYPTO'91, LNCS, vol. 576. Springer- Verlag, Berlin, pp. 129–140.

[7] Tompa M., Woll H.: How to share a secret with cheaters. J. Cryptol. **1**(3), 133–138 (1989).

[8] Araki T.: Efficient (k, n) threshold secret sharing schemes secure against cheating from n − 1 cheaters.In: Proceedings of ACISP'07, LNCS, vol. 4586, pp. 13–142. Springer-Verlag (2007).

[9] 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).

[10] 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).

[11] Rabin T., Ben-Or M.: Verifiable secret sharing and multiparty protocols with honest majority. In: Proceedings of the 21st Annual ACM Symposium on the Theory of Computing, pp. 73–85 (1989).

[12] Bhndo C., De Santis A., Gargano L., Vaccaro U.: Secret sharing schemes with veto capabilities. In: Proceedings of the First French-Israeli Workshop on Algebraic Coding, LNCS, vol. 781, pp. 82–89. Springer-Verlag (1993).

[13] McEliece R.J., Sarwate D.V.: On sharing secrets and Reed-Solomon codes. Comm. ACM 24, 583–584(1981).

[14] Charnes C., Pieprzyk J., Safavi-Naini R.: Conditionally secure secret sharing scheme with disenrolment capability. In: Proceedings of CCS'94, pp. 89–95. ACM (1994).

[15] Lin H.Y., Harn L.: A generalized secret sharing scheme with cheater detection. In: Proceedings of Asiacrypt'91, LNCS, vol. 739, pp. 149–158. Springer-Verlag (1991).

[16] Tartary C., Wang H.: Dynamic threshold and cheater resistance for shamir secret sharing scheme. In:Proceedings of Inscrypt'06, LNCS, vol. 4318, pp. 103–117. Springer-Verlag (2006).

[17] T.-C. Wu and T.-S. Wu, Cheating detection and cheater identification in secret sharing schemes, IEE Transactions on Computers and Digital Techniques 142 (1995), 367-369.

Authors' Profiles

Qassim Al Mahmoud received his B.S. degree in Mathematics and Computer Science from University of Baghdad in Iraq, 2002. He received his M.S. degree in Information Technology from University of Arab Academic for accounting and Information Technology in Jordan, 2007. He received a Ph.D. degree in the Information Security, Faculty of Mathematics and Computer Science, University of Bucharest, Romania. Now he is Assistance Professor of computer science at King Khalid University.

How to cite this paper: Qassim Al Mahmoud,"A Novel Verifiable Secret Sharing with Detection and Identification of Cheaters' Group", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.2, No.2, pp.1-13, 2016.DOI: 10.5815/ijmsc.2016.02.01