Journal of Information Security and Applications 51 (2020) 102430

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A verifiable secret sharing scheme with combiner verification and cheater identification

Shyamalendu Kandar[a,*], Bibhas Chandra Dhara[b]

[a] Department of Information Technology, Indian Institute of Engineering Science and Technology, Shibpur,Howrah 711103, India
[b] Department of Information Technology, Jadavpur University, Salt Lake Campus, Kolkata 700098, India

ARTICLE INFO

Article history:

Keywords:
Secret sharing
Verifiable secret sharing
Cheater identification
Combiner verification

ABSTRACT

In threshold secret sharing (SS) scheme, widely known as (k, n) threshold secret sharing, a secret S is divided into n shares and distributed to participants by a dealer in such a way that S can successfully be retrieved by a combiner from k or more shares collected from participants, but fewer than k shares will get no information about the secret. Verifiable secret sharing (VSS) scheme adds verifiable feature to secret sharing mechanism to check whether the retrieved information is the original secret or not. It helps to avoid mishap before using the secret. VSS may also helps to identify the participant submitting wrong information. Cheating detection and cheater identification are two well known terms in verifiable secret sharing. The former finds whether the right secret is retrieved and the later detects the participant(s), who has/have submitted wrong share. In the current work we have proposed a verifiable secret sharing scheme with cheater identification facility. The scheme also facilitates combiner verification by the participants to check whether share submission request is coming from a valid combiner or not. Security analysis of the proposed scheme have proved its immunity against different types of attacks.

1. Introduction

Secret sharing emerged as a research wing of in the field of information security to protect sensitive information like cryptographic keys from misuse by wrong hands. The journey of secret sharing started after the individual proposals in the field by Shamir [1] and Blakley [2] in 1979. Lagrange polynomial interpolation is the base of Shamir's proposal [1] whereas the Blakley method [2] is established on the concept of hyperplane geometry. In 1983 Asmuth et. al. proposed another secret sharing scheme based on Chinese remainder theorem (CRT). All the proposals are threshold secret sharing scheme widely known as (k, n) threshold secret sharing. In threshold secret sharing, an authorized person, known as dealer divides a secret S into n shares and shares are distributed to n authenticated participants. After this, dealer has no role to play. The secret can only be reconstructed by an authenticated person known as combiner or by grouping sufficient number of authenticated participants. If sufficient number of shares, let k, $(k \leq n)$ are gathered then an only the secret can be reconstructed. In Shamir's secret sharing, gathering shares from any subset of $(k-1)$ or less participants retrieve no information about the secret.

The proposed work is based on Shamir's secret sharing, and for further mentioning of the term 'secret sharing' is interpreted as Shamir's scheme if specifically not mentioned.

In secret sharing scheme, there are three actors namely dealer, participants and combiner. Dealer is authorized to share a secret and distribute the shares to the participants. It is assumed that dealer does not store the secret and the shares. Participants hold the shares distributed by a dealer and finally combiner is given right to choose threshold (or more) number of participants and collect shares from them. Combiner may be one of the participants or another entity having the role of reconstruction of the secret from the collected shares. In Shamir's scheme it is assumed that all the three actors are trusted. It means dealer provides right shares to the participants, share submission request comes from trusted combiner and participants do not submit any wrong information to the combiner. But these may not hold always, thus leaving a great security concern in secret sharing. Verifiable secret sharing (VSS) deals with the security issues and tries to provide solutions for those. VSS mainly performs cheating detection and/or cheater identification. In cheating detection, if a participant submits wrong information it can only be identified after reconstruction of the secret, but the wicked participant is generally left beyond traceable. There is again a high chance of inclusion of that wicked participant

* Corresponding author.
E-mail address: shyamalenduk@it.iiests.ac.in (S. Kandar).

https://doi.org/10.1016/j.jisa.2019.102430
2214-2126/

in the subset of k when combiner opting for next trial. But usefulness of identifying the constructed information as the true secret or not, can not be neglected. In cheater identification method, a wicked participant can be identified by a combiner before secret reconstruction process, thus saves time for the combiner.

VSS is of two types i) Interactive and ii) Non-interactive. In interactive VSS, participants exchange messages among themselves or with the dealer. On the other hand, in non-interactive VSS no exchange of message is required.

Depending on the activity, VSS can be divided into two groups, a) Authentication of the dealer b) Cheating detection and/or cheater identification. In the first type, each participant can authenticate its share coming from a single dealer (mainly generated from a same polynomial) and for the later one the combiner (may be one of the participants or a trusted actor) can verify the authenticity of the reconstructed secret and/or can detect a participant submitting a wrong share.

In this article we have presented a verifiable secret sharing scheme which can identify the cheater (participant submitting fake information), if persists in the secret sharing process. In the proposed scheme we have also introduced the facility of combiner verification by the participants, as the share submission requests may come from an adversary and in a remote system where no one is known to the other, the chance is highly possible.

The rest of the paper is organized as follows. A literature survey of state-of-the-art schemes are presented in Section 2. Some basic definitions related to the proposed scheme as preliminaries are discussed in Section 3. The proposed method is illustrated in Section 4. Section 5 discusses the performance of the proposed method against different security agreements. Finally conclusion is drawn in Section 6

2. Literature survey

The term 'Verifiable secret sharing (VSS)' has been used by Chor et. al. [3] where verifications are made by simultaneous broadcast network. Tompa and Woll [4] have shown that a dishonest participant can reconstruct the secret from the shares collected from another $(k-1)$ participants by simple trick. It just uses another polynomial $h(x)$ such that $h(0) = a$ and $h(i_j) = 0$ for $j = 1$ to k except m, its own ID and the secret is revealed as $S = S' - a$, where S' is the reconstructed value using Lagrange interpolation polynomial. Feldman [5] have proposed a verifiable secret sharing based on commitment property. It verifies whether all the shares are generated from same polynomial or not. This is known as dealer verification. Combiner performs the authenticity checking of the shares submitted by the participants from the commitments, and if any participant submits a wrong share (cheat) the secret reconstruction process is halted by declaring that cheating has occur. But the scheme requires a number of information to be made public and there is a chance of information disclosure from which secret may be guessed. Pedersen scheme [6] is a well known non interactive verifiable secret sharing which can identify cheater. The method have used two entry commitment property. But here the combiner is considered trusted, which may not hold always. Harn et. al. [7] have proposed a 'strong' verifiable secret sharing scheme where each participant can also act as a dealer and size of each share is same as the size of secret. Zhang et. al [8] have employed bilinear pairing-based ElGamal cryptosystem to define a novel VSS proposal. In [9] authors have presented two non-interactive VSS proposals using monotone Boolean circuit. In Wang et. at. [10] VSS proposal each participant can play the role of dealer and secret is considered as a random element generated by all the participants from a bilinear group. A recent VSS proposal [11] have used symmetric bivariate polynomial to identify the cheater from the group of users participating in the secret reconstruction group, or from the group of rest of the users. The verifiable secret sharing techniques discussed in the above section are based on Shamir's method [1].

Chinese remainder theorem (CRT) is the backbone of Asmuth et. al. [12] secret sharing method. Harn et al. [13] have included a verifiability feature to the existing Asmuth scheme and have proved it to be perfectly secure. In [14] a CRT based verifiable secret sharing is proposed for long lived secret using statistically hiding commitment property. Verifiable secret sharing schemes in [15], [16],have also used Asmuth scheme [12] in defining the proposals.

Blakley's [2] proposal on secret sharing is based on hyperplane geometry and not widely used as less than threshold number of shares leaks information about secret. [17,18] are some of the proposals which have defined VSS proposals based on hyperplane geometry.

In publicly verifiable secret sharing (PVSS) everybody, not only the actors (participants and combiner) are able to verify whether the shares are correctly distributed or not. One such publicly verifiable secret sharing proposed by Stadler et. al. [19] have used ElGamal's public key system to address their scheme. Fujisaki et. al. [20] have presented practical and provably secure publicly verifiable secret sharing scheme which is $O(|M|)$ times more efficient than Stadler et. al. [19] scheme where $|M|$ is the size of the secret. An improved version of PVSS and its application to electronic voting technique is presented in [21]. Some recent proposals on PVSS are available in [22,23].

In multi secret sharing (MSS) more than one secret are shared in a single secret sharing process and retrieval of one secret does not disclose the secrecy of other secrets. A number of multi secret sharing proposals [24–27] are available in literature. Verifiability is also a security concern in multi secret sharing scheme. Shao et. al. [28] have presented a verifiable multi secret sharing scheme (VMSS) based on YCH method [25]. The requirement of secure channel between dealer and participants is marked as a disadvantage of the Shao et. al. [28] scheme. A discrete logarithm and RSA cryptosystem based VMSS over YCH scheme [25] is presented in [29]. Here the necessity of a secure channel is removed as the participants can choose their own shadows. Hu et. al. [30] have used linear feedback shift register(LFSR) based public key cryptosystem to verify the authenticity of data and have implemented a cheating resistance mechanism. Another efficient LFSR based VMSS scheme is noticed in [31]. A hash function based cheater identification method is available in [32]. Here the combiner can detect the authenticity of information received from some participant by computing hash function. Hash function is a cryptographic primitive which is easy to compute but hard to find inverse. Some notable recent works on verifiable multi secret sharing scheme are available in [32–35].

Image secret sharing is getting its ways with the increased applications and transmissions of image in diverse fields like military, medical application, security (fingerpring, face or iris recognition), industry (product monitoring), remote sensing and overall sharing photographs in social media. A number of image secret sharing proposals are available in literature [36–40]. Verifiability can be added to image secret sharing like secret sharing of information. Some pioneer works in verifiable image secret sharing are available in [41–43].

There are a number of applications like e-voting technique [44], e-auction [45,46], secret image sharing [43,47], audio sharing [48] etc. which are heavily dependent on verifiable secret sharing.

Most of the methods mentioned in the literature have focused on verification of the dealer [5,49] (whether dealer is trusted or shares are computed from same polynomial or not) by the participants and cheating detection and/or cheater identification [11,30,32]. But there is a high change of reconstruction of

secret if 'k' participants conspire and gather their shares leaving the remaining participants in dark. Appointing a combiner give relief to all the participants from this threat. But in real situation of remote environment where no one is known to the other, a combiner may also be untrustworthy. It may also happen that an adversary, masquerading as combiner is asking the participants to submit their shares, leaving the concern of getting the secret in some wrong hand. The cheating by the participants (by submitting wrong information) is still valid.

A number of secret sharing proposals [50–52] have employed a trusted combiner to reconstruct the secret. Some verifiable secret sharing proposals have adopted a combiner [32,33,53,54] to perform cheating detection and/or cheater identification but in all of the cases the combiner is considered to be trusted.

In the current article we have proposed a verifiable secret sharing method where a participant can identify whether the combiner from which shares submission requests are coming, is valid or not. A combiner can also detect whether any cheating occur while receiving shares from the participants. One important advancement of the proposed scheme is that, participant do not get the exact share and ID. Thus it is impossible to retrieve the secret by 'k' participants, accumulating their shares beyond the knowledge of the combiner. The security analysis of the proposed method against different security threats proves its resistance against those threats.

3. Preliminaries

The proposed VSS scheme is based on Shamir's secret sharing method [1]. Here, share generation and secret reconstruction are based on polynomial interpolation as addressed in Shamir's secret sharing scheme [1]. To define the verifiability, in the proposed method, one way hash function is used.

3.1. Shamir's secret sharing scheme

In this secret sharing scheme, to share the secret S into k shares, a $(k-1)$ degree polynomial $f \in F_p$ for a prime number p is choosen. Shares are computed as $y_i = f(x_i))$ for $x_i \neq 0$ and the pairs (x_i, y_i) is sent to $participant_i$. Here, secret is $S = f(0)$. In this context, we need at least k shares (x_i, y_i) to recover f and hence to find the secret $S = f(0)$ also. The polynomial is defined as

$$f(x) = a_{k-1}.x^{k-1} + a_{k-2}.x^{k-2} + \ldots + a_1 x + a_0 \ (mod\ p) \tag{1}$$

where each $a_i \in F_p, 0 \leq i \leq k-1,\ a_{k-1} \neq 0$ and the secret is $f(0) = a_0$. To make the secret sharing as (k, n) threshold sharing, n shares are computed for distinct and randomly selected n points $\{x_i : 1 \leq i \leq n \ and \ x_i(\neq 0) \ \in F_p\}$ and distributed to n participants.

The recovery of the secret in this scheme is straightforward. When, any k pairs of (x_i, y_i) are available then by Lagrange interpolation technique, over the field F_p, the polynomial f can be determined uniquely as

$$f(x) = \sum_{i=1}^{k} y_i \prod_{1 \leq j \leq k, j \neq i} \frac{x_j - x}{x_j - x_i} \quad (mod\ p) \tag{2}$$

Since, the secret is $f(0)$ the secret can be computed as

$$S = f(0) = \sum_{i=1}^{k} y_i \prod_{1 \leq j \leq k, j \neq i} \frac{x_j}{x_j - x_i} \quad (mod\ p) \tag{3}$$

3.2. One way hash function

One way hash function is an important tool in cryptography and used widely in various encryption processes. Hash functions are useful because they are deterministic in nature. One way hash functions are collision-resistant. It is hard to find two distinct values that maps to same hashed value. Hash function obey Avalanche effect, i.e. a small change (may be a single bit) to the input value results a huge change in the output. 'Easy to compute but hard to find inverse' property of one way hash function has made it an important tool for cryptographic primitive mainly in public key cryptography. Some examples of hash functions are MD4, MD5, SHA, SHA256.

Table 1
Notation used throughout the paper.

Notation	Description
n	Number of participant
k	Value of the threshold
$h(.)$	One way hash function
$\|\|$	Concatenation Operation
CID	Identification number of the combiner
pwd	Password of the combiner
r	Random number chosen by combiner
ID_i	Identification of the ith participant
$SHARE_i$	Share generated by the dealer for ith participant
SW_i	Shadow share for ith participant
SID_i	Shadow ID sent to $participant_i$

4. Proposed method

In the proposed method dealer is given the authority compute the shares from a secret and distribute to the selected participants. Here, dealer is considered as trusted entity. The combiner is given the authority to collect the shares from the participants and reconstruct the secret. Combiner is known to dealer but do not trustworthy. Role of the dealer is to share the secret and sent those to the authorized participants. In the proposed method the participants only hold the shadow shares, not the original and each participant can verify the authenticity of the combiner. Combiner can also verify the participants. The organization hierarchy of a bank can be taken as an example for this case. The CEO is treated as a dealer and the branch manager is the combiner. Some officers working under branch manager are the participants. To gain the access of the secret information (may be code of vault) branch manager has to accumulate information from the officers. If the branch manager is changed, the CEO has to generate some information without resharing the secret and the participants have to modify their belonging information by new information sent by CEO.

The notations used throughout the presentation are summarized in Table 1.

4.1. Proposed

Proposed method consists of three phases, namely i) Registration ii) Share generation and distribution and iii) Secret reconstruction and verification

In Registration phase, a secure communication is made between dealer and combiner. Combiner sends a key (PSK) and a verifier code (V) to the dealer through a secure channel. Here, PSK and V are generated from combiner ID (CID), password (pwd) and a random number r.

In share generation and distribution phase, dealer selects distinct ID (ID_i) for each of the n participants. Dealer generates shares $SHARE_i$ from 'S' using Shamir's scheme [1]. Then shadow shares SW_i are generated from $SHARE_i$ using PSK and instead of $SHARE_i$, SW_i along with some additional information is sent to the ith participant. Shadow share SW_i is sent to $participant_i$ along with some verifier codes through any channel.

In secret reconstruction and verification phase, combiner chooses k or more participants and ask them to submit their

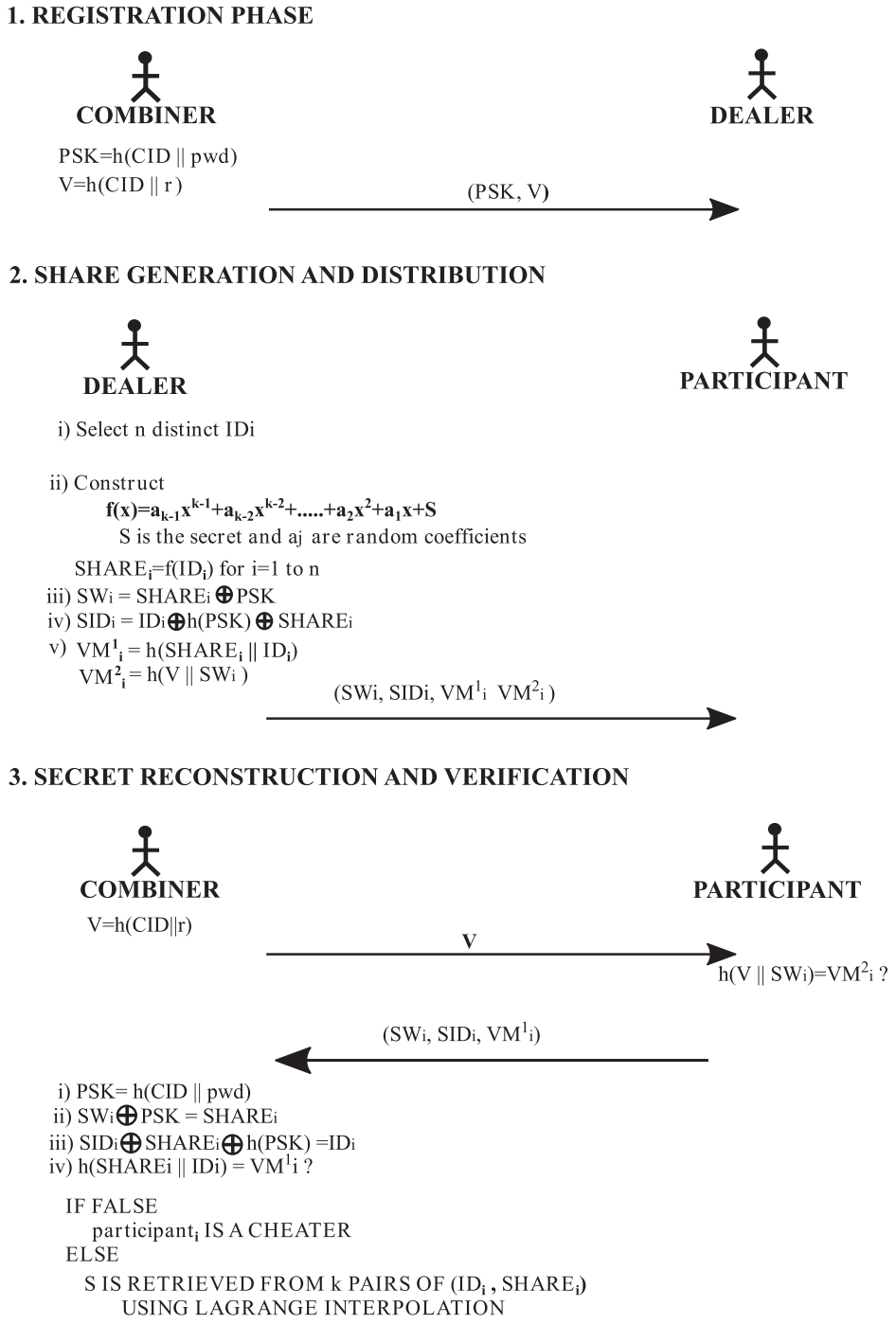

Fig. 1. Diagrammatic sequence of the proposed method.

information by sending them a message. Each participant do some operation with the message and compare it with a verifier code under its possession. If a match found, participant submits its part to the combiner. Combiner checks the authenticity of the submitted information, and if found authentic it computes the ID_i and $SHARE_i$ from the received data. The secret S is retrieved using Lagrange interpolation. The proposed method is described as follows and the block diagram of the proposed method is presented in Fig. 1.

1. **Registration:**
   In this phase combiner uses its ID (CID) and password (pwd) computes PSK and V as
   $PSK = h(CID||pwd)$
   $V = h(CID||r)$, where r is a random number.
   and sends (PSK, V) to the dealer through a secure channel.
2. **Share Generation and distribution:**
   (i) Dealer selects n participants and chooses ID_i $(ID_i \neq ID_j)$ for $participant_i$.
   (ii) Use the Shamir's secret sharing scheme and generate shares $(ID_i, SHARE_i)$, where $SHARE_i = f(ID_i)$, for $i = 1$ *to* n and f is the sharing polynomial.
   (iii) Dealer calculates
   Shadow share $SW_i = SHARE_i \oplus PSK$,
   Shadow ID, $SID_i = ID_i \oplus h(PSK) \oplus h(SW_i || SHARE_i)$ and two verifier messages as

$VM_i^1 = h(SID_i \,||SHARE_i \,||\, ID_i)$
$VM_i^2 = h(SID_i) \oplus V$
and (SW_i, SID_i, VM_i^1, VM_i^2) are sent to $participant_i$ through any channel. Hash function 'h' is made public.

3. **Secret Reconstruction and Verification:**
   (i) Secret reconstruction is initialized by combiner by selecting k or more participants. Combiner asks $participant_i$, to submit SW_i, SID_i and VM_i^1 by sending him a message $V = h(CID||r)$.
   (ii) $participant_i$ checks
   If $h(SID_i) \oplus V = VM_i^2$?
   If 'Yes', it sends (SW_i, SID_i and VM_i^1) to the combiner.
   (iii) Upon receiving the values, combiner computes
   $h(CID||pwd) = PSK$ from its own ID and password.
   $SW_i \oplus PSK = SHARE_i$
   $SID_i \oplus h(SW_i \,||\, SHARE_i) \oplus h(PSK) = ID_i$
   (iv) It checks if $h(SID_i \,||SHARE_i \,||\, ID_i) = VM_i^1$? If 'Yes', $participant_i$ has submitted the right share. Else $participant_i$ is a cheater.
   (v) If right shares are submitted, then combiner retrieves S from k set of (ID_i, $SHARE_i$) using Lagrange interpolation.

5. Security analysis and comparison

In this section, we analyze the security to prove the robustness of the proposed scheme against kind of threats. Here, we have discussed six security threats and found that proposed scheme is robust against the threads. This section also contains a comparison of the proposed scheme with some existing verifiable schemes to prove its superiority. We have taken into account Liu. et. al scheme [11] and Adhikari et. al. scheme [55] as comparable scheme.

5.1. Security analysis of the proposed scheme

In this subsection we have analyzed the proposed scheme against seven different security attacks by presenting seven theorems and have shown that the scheme can resist all of these. The theorems are discussed as follows.

Theorem 1. *Any subgroup of participants with k members cannot retrieve the secret.*

Proof. To retrieve a secret in (k, n) secret sharing, k ($k < n$) or more set of (ID_i, $SHARE_i$) are required. In the proposed scheme, each participant possess a shadow share SW_i and shadow ID SID_i. SW_i and SID_i are generated using $SHARE_i \oplus PSK$ and $ID_i \oplus h(PSK) \oplus h(SW_i \,||\, SHARE_i)$ respectively. Both SW_i and SID_i need PSK to retrieve ID_i and $SHARE_i$ respectively. PSK is a combiner entity computed from its CID and pwd. Thus, ID_i and $SHARE_i$ can't be retrieved by any participant. Therefore, k participants will fail to retrieve the secret by accumulating information to their possession. □

Theorem 2. *Any adversary can not retrieve the secret by performing 'Man-in-the-middle attack'.*

Proof. An adversary ($\mathcal{A}$) may fetch the request message V sent by a valid combiner and impersonate as a legal combiner by retransmitting this message to k participants. $participant_i$ checks VM_i^2 and if found authentic, (SW_i, SID_i, VM_i^1) are sent to $\mathcal{A}$. But $\mathcal{A}$ can not retrieve ID_i and $SHARE_i$ from SID_i and SW_i both of these need PSK, which is only available to combiner. Thus SID_i and SW_i are of no use to $\mathcal{A}$ and it fails to retrieve the secret. □

Theorem 3. *Any adversary will fail to retrieve the secret by corrupting k participants.*

Proof. An adversary ($\mathcal{A}$) may take the opportunity of a prolong lifetime of some secret. It may collect (SW_i, SID_i) pair from k corrupted participants. But due to the non availability of PSK the retrieved information are of no use to $\mathcal{A}$ and it fails to retrieve the secret. □

Theorem 4. *Proposed scheme can successfully identify the cheater.*

Proof. Valid combiner requires at least k pairs of (ID_i, $SHARE_i$) to retrieve the secret and $participant_i$ is supposed to submit (SW_i, SID_i, VM_i^1) to the combiner. Let $participant_j$ submits SW_j' in place of SW_j. □

$SW_j \oplus PSK$ generates $SHARE_j'$ other than $SHARE_j$.

In computation, $SID_j \oplus h(SW_j \,||\, SHARE_j') \oplus h(PSK)$ will return let ID_j', different from ID_j.

$h(SID_j||SHARE_j||ID_j)$ will generate $VM_j^{1'}$ which will not match with VM_j^1 and $participant_j$ will be marked as 'cheater'.

It is very hard for $participant_j$ to change SW_j and SID_j so that it match with VM_j^1.

Theorem 5. *Proposed scheme provides the flexibility of quit of an existing combiner and appointing a new combiner.*

Proof. Let combiner Cmb_i quits and this is informed to the dealer. Dealer asks Cmb_i to submit its PSK_i and V_i. Dealer appoints a new combiner Cmb_j and also asks him to submit his PSK_j and V_j. It is to be noted that the communication between dealer and existing and new combiner are performed through secure channel. □

Upon receiving the information, dealer computes
$M_1 = PSK_i \oplus PSK_j$
$M_2 = h(PSK_i) \oplus h(PSK_j)$
$M_3 = V_i \oplus V_j$
Dealer sends M_1, M_2 and M_3 to each of the participants and each of them updates its part as (SW_i', SID_i', $VM_i'^2$) where
$SW_i' = SW_i \oplus M_1$
$(SHARE_i \oplus PSK_i \oplus PSK_i \oplus PSK_j = SHARE_i \oplus PSK_j)$
$SID_i' = SID_i \oplus M_2$
$(ID_i \oplus h(PSK_i) \oplus h(SW_i \,||\, SHARE_i) \oplus h(PSK_i) \oplus h(PSK_j)$
$= ID_i \oplus h(PSK_j) \oplus h(SW_i \,||\, SHARE_i))$
$VM_i'^2 = VM_i^2 \oplus M_3$
$(h(SID_i) \oplus V_i \oplus V_i \oplus V_j = h(SID_i) \oplus V_j)$
Here each participant can update its information without knowing about the secret and the dealer is given relief from storing the secret.

Theorem 6. *Proposed scheme provides the flexibility to a combiner to change his/her password pwd and/or random number r.*

Proof. If a combiner wants to update its password from pwd_i to pwd_j and/or random number r_i to r_j, it informs the dealer with its old and new PSK and V. Dealer executes Theorem 5 with updated M_1, M_2 and M_3. $participant_i$ also updates its information accordingly. □

Theorem 7. *Proposed scheme is resistant to insider attack at dealer side.*

Proof. In insider attack, someone let $\mathcal{A}$ who is given authorization to maintain computers and networks related to the dealer, misuses its power and steals critical information. In the proposed scheme, dealer is not storing any information related to secret. It does not maintain the information of PSK, V, SID_i or SW_i in any secret sharing process. Thus $\mathcal{A}$ will get no fruitful information from which secret can be retrieved. □

Table 2
Comparison of the proposed scheme with the existing.

Schemes	Cheating detection	Cheater identification	Cheater identification capability	Combiner verification
Adhikary et. al. Scheme	✓	✓	$\frac{k-1}{3}$	$\times^{\psi}$
Liu et. al. Scheme	✓	✓	$\frac{n-k+1}{2}$	$\times^{\psi}$
Proposed Technique	✓	✓	k	✓

ψ: No role of combiner. Participants group to retrieve the secret

5.2. Comparison with some existing schemes

In verifiable secret sharing scheme an illicit participant may submit a false information as share and it leads to the generation of a wrong information is of no use in place of the correct secret. Cheating detection technique can only check whether the retrieved information is the right secret or not. If it is not the right one, in next reconstruction attempt some of the existing participants are excluded and new participants are included. Till it left the doors open of the inclusion of some illicit participant. Cheater identification mechanism provides the relief by checking the authenticity of the submitted information before reconstruction of the secret. In most of the existing VSS proposals on cheater identification, the participants are divided into two groups- trusted and untrusted. The trusted participants play the role to identify cheater from the untrusted set of participants. Thus there exists a threshold value of the number of illicit participants to be detected by the VSS scheme. In this paper, this threshold value is mentioned as cheater identification capability. It is generally observed that the number of trusted participants wins over the number of untrusted participants.

In this subsection proposed scheme is compared with two existing verifiable secret sharing schemes in terms of cheater identification and most number of cheater it can identify (capability). First a brief discussion of the existing schemes are given below and then the proposed method is compared with them.

Adhikari et. al. scheme[55] have proposed a (k, n) threshold verifiable secret sharing scheme against rushing cheaters. Rushing cheaters are those who submit forged shares in reconstruction process after share submission of honest participants. This scheme allows multiple rounds of interaction with shareholders in the reconstruction process.

Liu et. al. scheme[11] have used bivariate polynomial to define a verifiable (k, n) secret sharing scheme. The scheme consists of two algorithms. The first one can identify the cheater by the m $(m \geq k)$ users participating in the secret reconstruction process and the second one can identify the cheater from the collaboration of rest non-involved $(n - m)$ users.

The comparison of the proposed scheme with the existing methods are presented in Table 2.

In the comparable schemes there is no existence of combiner. Here participants form a group to retrieve the secret. To find the existence of some illicit participant, the honest participants have to play their role. Thus, there exist a threshold of number of cheaters to be detectable in these schemes. Whereas in our scheme the existence of k out of k cheaters can be detected. To prevent k participants from the retrieval of the secret beyond the knowledge of the rest, both the techniques assumes that the number of cheaters must be less than k. But the proposed scheme acts well if there exist k out of k cheaters. Hence the proposed scheme is superior than the comparable schemes.

In some verifiable secret sharing schemes [32,33,54] there exist a trusted combiner. But in the process of secret sharing the combiner may be a remote actor like the participants, thus there is a high chance of a fake combiner asking the participants to submit their shares. But in the proposed scheme each participant can check the authenticity of a combiner using verifier message VM_2^i, which removes the threat of the existence of a fake combiner. As proofed in Theorems 2, and 3 an adversary pretending as combiner by performing 'man in the middle attack' or by corrupting k participants also fails to retrieve the secret. This provides a strong base of the acceptability of the proposed scheme.

6. Conclusion

A verifiable secret sharing scheme is presented in this paper. In this scheme each participant is assigned a shadow share which removes the threat of reconstruction of the secret conspiring by grouping threshold number of participants from the remaining. Being a remote actor, a combiner is also verified to each participant before submitting information to it and this filters out the chance of an adversary acting as a combiner. Proposed method also provides cheater identification technique and facilitates the combiner and dealer to update its (combiner's) password and appoint new combiner respectively. It also provides immunity against different security threats. In the presented technique the dealer is assumed to be trusted to the participants. Verification of the dealer to the participants and verification of combiner by the dealer may be implemented in some future research.

References

[1] Shamir A. How to share a secret. Commun ACM 1979;22(11):612–13.
[2] Blakley GR, et al. Safeguarding cryptographic keys. In: Proceedings of the national computer conference, 48; 1979. p. 313–17.
[3] Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. In: Foundations of computer science, 1985., 26th annual symposium on. IEEE; 1985. p. 383–95.
[4] Tompa M, Woll H. How to share a secret with cheaters. J Cryptol 1989;1(3):133–8.
[5] Feldman P. A practical scheme for non-interactive verifiable secret sharing. In: Foundations of computer science, 1987., 28th annual symposium on. IEEE; 1987. p. 427–38.
[6] Pedersen TP. Non-interactive and information-theoretic secure verifiable secret sharing. In: Annual international cryptology conference. Springer; 1991. p. 129–40.
[7] Harn L, Lin C. Strong (n, t, n) verifiable secret sharing scheme. Inf Sci 2010;180(16):3059–64.
[8] Zhang J, Zhang F. Information-theoretical secure verifiable secret sharing with vector space access structures over bilinear groups and its applications. Future Gen Comput Syst 2015;52:109–15.
[9] Bai G, Damgård I, Orlandi C, Xia Y. Non-interactive verifiable secret sharing for monotone circuits. In: International conference on cryptology in Africa. Springer; 2016. p. 225–44.
[10] Wang N, Fu J, Zeng J. Verifiable secret sharing scheme without dealer based on vector space access structures over bilinear groups. Electronics Lett 2017.
[11] Liu Y, Yang C, Wang Y, Zhu L, Ji W. Cheating identifiable secret sharing scheme using symmetric bivariate polynomial. Inf Sci 2018;453:21–9.
[12] Asmuth C, Bloom J. A modular approach to key safeguarding. IEEE TransInfTheory 1983;29(2):208–10.
[13] Harn L, Fuyou M, Chang C-C. Verifiable secret sharing based on the chinese remainder theorem. Security Commun Netw 2014;7(6):950–7.
[14] Ersoy O, Pedersen TB, Kaya K, Selçuk AA, Anarim E. A crt-based verifiable secret sharing scheme secure against unbounded adversaries. Security Commun Netw 2016;9(17):4416–27.
[15] Iftene S. Secret sharing schemes with applications in security protocols.. Sci Ann Cuza Univ 2006;16:63–96.
[16] Kaya K, Selçuk AA. A verifiable secret sharing scheme based on the chinese remainder theorem. In: International conference on cryptology in India. Springer; 2008. p. 414–25.
[17] Yang X, Xia Z, Xiao M. Verifiable secret sharing and distributed key generation based on hyperplane geometry. In: Dependable computing and internet of things (DCIT), 2015 2nd international symposium on. IEEE; 2015. p. 142–5.

[18] Xia Z, Yang X, Xiao M, He D. Provably secure threshold paillier encryption based on hyperplane geometry. In: Australasian conference on information security and privacy. Springer; 2016. p. 73–86.
[19] Stadler M. Publicly verifiable secret sharing. In: International conference on the theory and applications of cryptographic techniques. Springer; 1996. p. 190–9.
[20] Fujisaki E, Okamoto T. A practical and provably secure scheme for publicly verifiable secret sharing and its applications. In: International conference on the theory and applications of cryptographic techniques. Springer; 1998. p. 32–46.
[21] Schoenmakers B. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In: Annual international cryptology conference. Springer; 1999. p. 148–64.
[22] Mashhadi S. Secure publicly verifiable and proactive secret sharing schemes with general access structure. InfSci 2017;378:99–108.
[23] Sarkar P, Nandi S, Chowdhury MU. Publicly verifiable secret sharing scheme in hierarchical settings using clsc over ibc. In: International conference on applications and techniques in cyber security and intelligence. Springer; 2017. p. 194–205.
[24] He J, Dawson E. Multisecret-sharing scheme based on one-way function. Electron Lett 1995;31(2):93–5.
[25] Yang C-C, Chang T-Y, Hwang M-S. A (t, n) multi-secret sharing scheme. Appl Math Comput 2004;151(2):483–90.
[26] Deshmukh M, Nain N, Ahmed M. Efficient and secure multi secret sharing schemes based on boolean xor and arithmetic modulo. Multimedia Tools Appl 2018;77(1):89–107.
[27] Kandar S, Dhara BC. A (t, n) multi-secret sharing scheme with updated secret shadows. In: Proceedings of the international conference on computing and communication systems. Springer; 2018. p. 621–9.
[28] Shao J, Cao Z. A new efficient (t, n) verifiable multi-secret sharing (vmss) based on ych scheme. Appl Math Comput 2005;168(1):135–40.
[29] Dehkordi MH, Mashhadi S. An efficient threshold verifiable multi-secret sharing. Comput Standards Interfaces 2008;30(3):187–90.
[30] Hu C, Liao X, Cheng X. Verifiable multi-secret sharing based on lfsr sequences. Theor Comput Sci 2012;445:52–62.
[31] Mashhadi S, Dehkordi MH. Two verifiable multi secret sharing schemes based on nonhomogeneous linear recursion and lfsr public-key cryptosystem. Inf Sci 2015;294:31–40.
[32] Shao J. Efficient verifiable multi-secret sharing scheme based on hash function. Inf Sci 2014;278:104–9.
[33] Dehkordi MH, Farzaneh Y. A new verifiable multi-secret sharing scheme realizing adversary structure. Wirel Pers Commun 2015;82(3):1749–58.
[34] Liu Y, Zhang F, Zhang J. Attacks to some verifiable multi-secret sharing schemes and two improved schemes. Inf Sci 2016;329:524–39.
[35] Li M, Yu J, Hao R. A cellular automata based verifiable multi-secret sharing scheme without a trusted dealer. Chin J Electron 2017;26(2):313–18.
[36] Thien C-C, Lin J-C. Secret image sharing. Comput Graph 2002;26(5):765–70.
[37] Wang D, Zhang L, Ma N, Li X. Two secret sharing schemes based on boolean operations. Pattern Recognit 2007;40(10):2776–85.
[38] Liu Y-X, Yang C-N, Wu C-M, Sun Q-D, Bi W. Threshold changeable secret image sharing scheme based on interpolation polynomial. Multimedia Tools Appl 2019:1–15.
[39] Liu Y, Yang C. Scalable secret image sharing scheme with essential shadows. Signal Process 2017;58:49–55.
[40] Liu Y, Yang C-N, Wu S, Chou Y. Progressive (k, n) secret image sharing schemes based on boolean operations and covering codes. Signal Process 2018;66:77–86.
[41] Zhao R, Zhao J, Dai F, Zhao F. A new image secret sharing scheme to identify cheaters. Comput Standards Interfaces 2009;31(1):252–7.
[42] Patil S, Deshmukh P. Verifiable image secret sharing in matrix projection using watermarking. In: 2014 International conference on circuits, systems, communication and information technology applications (CSCITA). IEEE; 2014. p. 225–9.
[43] Li X, Xiao D, Mou H, Zhang R. A verifiable secret image sharing scheme based on compressive sensing. Wuhan Univ J Natl Sci 2018;23(3):219–24.
[44] Nair D.G., Binu V., Kumar G.S.. An improved e-voting scheme using secret sharing based secure multi-party computation. arXiv:150207469 2015;.
[45] Nojoumian M, Stinson DR. Efficient sealed-bid auction protocols using verifiable secret sharing. In: International conference on information security practice and experience. Springer; 2014. p. 302–17.
[46] Larson M, Hu C, Li R, Li W, Cheng X. Secure auctions without an auctioneer via verifiable secret sharing. In: Proceedings of the 2015 workshop on privacy-aware mobile computing. ACM; 2015. p. 1–6.
[47] Gao H, Hu M, Gao T, Cheng R. Random grid and reversible watermarking-based on verifiable secret sharing for outsourcing images in cloud. Int J Digital CrimeForensics (IJDCF) 2018;10(1):24–39.
[48] Bharti SS, Gupta M, Agarwal S. A novel approach for verifiable (n, n) audio secret sharing scheme. Multimedia Tools Appl 2018:1–29.
[49] Rajabi B, Eslami Z. A verifiable threshold secret sharing scheme based on lattices. Inf Sci 2019;501:655–61.
[50] Das A, Adhikari A. An efficient multi-use multi-secret sharing scheme based on hash function. ApplMathLett 2010;23(9):993–6.
[51] Chattopadhyay AK, Nag A, Majumder K. Secure data outsourcing on cloud using secret sharing scheme.. IJ Netw Security 2017;19(6):912–21.
[52] Pilaram H, Eghlidos T. An efficient lattice based multi-stage secret sharing scheme. IEEE Trans Depend Secure Comput 2015;14(1):2–8.
[53] Patel N, Vyavahare PD, Panchal M. A novel verifiable multi-secret sharing scheme based on elliptic curve cryptography. In: The tenth int. conf. on emerging security information, systems and technologies (SECURWARE 2016), Nice, France; 2016. p. 230–4.
[54] Tadayon MH, Khanmohammadi H, Haghighi MS. Dynamic and verifiable multi-secret sharing scheme based on hermite interpolation and bilinear maps. IET Inf Security 2014;9(4):234–9.
[55] Adhikari A, Morozov K, Obana S, Roy PS, Sakurai K, Xu R. Efficient threshold secret sharing schemes secure against rushing cheaters. In: International conference on information theoretic security. Springer; 2016. p. 3–23.