Arabian Journal for Science and Engineering (2020) 45:2395–2406
https://doi.org/10.1007/s13369-019-03992-7

RESEARCH ARTICLE - SPECIAL ISSUE - INTELLIGENT COMPUTING AND INTERDISCIPLINARY APPLICATIONS

A Hybrid-Based Verifiable Secret Sharing Scheme Using Chinese Remainder Theorem

Om Prakash Verma[1] · Nitin Jain[2] · S. K. Pal[3]

Received: 12 December 2018 / Accepted: 19 June 2019 / Published online: 25 July 2019

Abstract
It is not always in the best interests to rely on an individual to have control of entire sensitive information. This has led to the need for secret sharing schemes, which divide secret (key) among many participants or shareholders. To avoid any cheating by any of the shareholders, the need for verifiable secret sharing (VSS) has emerged. In this context, a hybrid approach for VSS scheme is suggested in this paper. The proposed algorithm shares multiple secrets among shareholders, where shareholders are also divided/classified into different levels. Hence, it includes multiple as well as multilevel secret sharing. Secrets can be recovered at intra- or inter-level, where shareholders of higher level can contribute their shares to lower levels. To reduce the complexity, the one-way hash function is used instead of the hard number-theoretic problems. The proposed scheme stands against the dishonest dealer and shareholders. To rule out a typical dishonest strategy of leaking secret information in the valid shares, the concept of dealer leakage resilience is used by reducing the dealer's powers of selecting random values on his own. The execution is also done using cryptographic libraries. Finally, it is demonstrated that the scheme satisfies the security requirements of VSS.

Keywords Verifiable secret sharing schemes · Hash functions · Dealer leakage resilience · Secret recovery · Chinese remainder theorem · Dishonest participants

1 Introduction

The concept of secret sharing (SS) schemes was coined by Shamir [1] and Blakley [2] in 1979. Since then, it has attracted the interest of several researchers. SS has been found valuable in several applications such as witness encryption [3], secure communication [4], and access control [5]. In SS schemes, there are two significant role players, one is the dealer and another is the group of shareholders (participants). The dealer splits the secret into n parts and distributes these shares among n shareholders. These shareholders when combining their shares can recover the secret. The scheme is referred to as a thresholding scheme if the secret can be recovered by combining t out of n ($t \leq n$) shares. However, less than t parts must not reveal any information about the secret. There are some drawbacks in the SS schemes presented in [1, 2] which may act as a constraint for practical usage:

- Fake shares may be distributed by the malicious dealer, and in turn, secret reconstruction is not possible.
- A deceitful shareholder may submit a fake/invalid share, which leads to incorrect share reconstruction, and the true secret would only be known to the deceitful shareholder.
- Need of mutually trusted dealer for the generation and distribution of shares.
- There is a requirement of the private channel for share distribution.

An advancement of SS schemes, known as verifiable secret sharing (VSS) schemes, came into the picture to handle the dishonesty of shareholders mainly or dealer. The dealer may be biased in the distribution of shares or the reconstruction of the secret.

✉ Nitin Jain
garg.nitin007@gmail.com

[1] Department of ECE, Delhi Technological University, Delhi, India

[2] Department of Information Technology, Delhi Technological University, Delhi, India

[3] Directorate of Information Technology & Cyber Security, DRDO, Delhi, India

In traditional SS schemes, it is assumed that the shareholders and the dealer are honest and reliable enough. Though in practical scenarios, the dealer does not trust the players completely, and consequently, it is reasonable to expect that players may not trust the dealer as well. To make SS verifiable, some auxiliary information is to be added that helps the shareholders to verify their respective shares. The shares are that shareholders do not accept the shares if they find them inconsistent or invalid. With the help of VSS schemes, it is possible for the shareholders to verify their shares without having access to the secret and even without revealing their shares. Other flavours of SS schemes include multiple [6], multilevel [7], weighted [8], and protected SS (PSS) schemes [9].

2 Related Work

In multiple SS schemes, there are multiple (say p) secrets instead of a single secret as in traditional SS schemes. To share p secrets, one approach is to run p instances of the simple scheme. However, this seems to be a very naïve way and not a desirable solution due to high computational complexity. So a scheme is desirable if single run [6] can share all p secrets. Recent work in this direction is done by Amroudi et al. [10], where authors obviate the need of a secure channel by encrypting the shares with the NTRU cryptosystem which is a lattice-based and reasonably fast approach. A multivariate polynomial's coefficient is used to share the multi-secret with the verification of shares performed by using the hash function. Another work in this league is a scheme by Meng et al. [11] that uses cellular automata and the hash function for verifiability. Trust management without the dealer is achieved with the help of linear computations with the simultaneous use of parallel computation for efficiency. Another multiple SS scheme is proposed by Tentu et al. [12], where multiple secrets are distributed using discrete logarithm and quadratic residue problem. This scheme is used for the level-ordered access structure. Cheng et al. [13] proposed a verifiable multi-secret sharing based upon the Lagrange polynomial and the public key cryptosystem. They used a linear feedback shift register (LFSR)-based cryptosystem to enhance the efficiency of the scheme. The scheme provides reasonably good security with added efficiency. In recent past, Giri et al. [14] proposed a multi-scheme whose assumption is based upon the geometry in the finite field. The scheme is claimed to be secured as the shares which are shared with the participant, are not the actual values but the shadow values. Liu et al. [15] proposed a multi-secret scheme which proved the failure of asynchronous reconstruction of share given by the Harn and Hsu [16]. They also proved that by getting the reconstruction of any of the secret, rest of the secrets could be obtained illegitimately. They improved the abnormality of the scheme by taking the common pairwise key for a pair of shareholders.

In multilevel or hierarchical SS schemes [7], participants are divided into m different levels and a threshold is associated with each level. For secret recovery, a participant from the targeted level or higher level can contribute in the secret reconstruction. Zhong et al. [17] extended the idea of giving a shadow number to images. Shadow image as a share stops the cheating in the shareholder before the actual image is recovered. They extended the idea of a weighted scheme by giving the higher priority to the shareholder at a higher level; i.e. capabilities of shareholders at different levels are different.

In weighted SS schemes [8], a weight with a positive value is assigned to each participant. Secret reconstruction is possible only when the sum of weights of the authorised subset is equal to or greater than the threshold. In previously described schemes [1–7], each shareholder has unity weight. However, in this, different shareholders may be assigned different weights. The concept of such schemes can be applied directly when there is a need to give more rights to higher rank officials.

In SS schemes, traditionally, to avoid the chances of recovery of a secret by non-shareholders, secure pairwise channels are established among the shareholders via means of a shared key, which are used to exchange the shares. To reduce this computational inefficiency, Harn et al. [9] coined PSS scheme. In this, in addition to the secret reconstruction, the shared key is also established with the help of shares possessed by the shareholders in a pairwise manner. Though this scheme is computationally less efficient than the Shamir's SS scheme, it can be used even if the adversary has unlimited computational power.

Another class of VSS schemes is known as publically VSS (PVSS) scheme [18, 19]. Such VSS schemes possess a unique property that anyone can verify that distributed shares are valid or not, i.e. maliciousness of the shareholders can be handled by this type of scheme. Shareholders receive a valid share but do not submit a valid one during reconstruction. A remarkable PVSS scheme was presented by Behnad et al. [20], where members of the participant can be proven by themselves, avoiding illegal member's participation.

With the proliferation of big data and cloud computing technology and its associated requirement, homomorphic secret sharing schemes were proposed in the recent past. Though the concept of cryptographic homomorphism is ancient, it has been touched by various researchers from time to time. Li et al. in 2018 discussed the various cryptographic primitives which can be used for privacy preservation requirement of various online applications [21]. A scheme by Rajabi et al. [22], whose security is based upon the approximate shortest polynomial problem, exploits homomorphic as well as collision resistance property by taking appropriate Knapsack function. The verification of shares can also

be done using public channels. Another variant of VSS is asynchronous verifiable SS (AVSS) scheme, where fault tolerance in multiparty computation can be handled. Basu et al. [23] proposed an optimistic AVSS scheme, where the payoff cost of failure possesses linearity, i.e. proportional to the number of failures. A different approach which adds nonmalleability to SS scheme was proposed by Goyal et al. [24]. With this scheme, if the shares are tempered, then either the original secret can be recovered, or the recovered secret is unrelated to the original secret.

By getting motivation from these requirements, our work proposes a hybrid-based VSS scheme using Chinese remainder theorem (CRT) that is based on hash functions [7, 25, 26]. The proposed scheme also stands against the dishonest dealer and shareholders. To rule out a typical dishonest strategy of leaking secret information in the valid shares, the concept of dealer leakage resilience is used by reducing the dealer's powers of selecting random values on his own. In the results and analysis section, it is confirmed that the scheme adheres to the security requirement of VSS.

The rest of the paper is organised as follows: In Sect. 3, the preliminary background and applications of SS schemes are explained. Section 4 explains the proposed work. Next, Sect. 5 demonstrates the experimental results and also explains how the proposed scheme can be used for Defence application also. Further, Sect. 6 analyses the scheme against various security parameters, where the comparison is also made with the existing schemes. Finally, Sect. 7 concludes the paper.

3 Preliminary Background and Applications of SS Schemes

3.1 Background of SS Schemes

Simple SS schemes are not of much interest in practical scenarios. A threshold value plays an important role. Very first idea in this league is a scheme due to Adi Shamir [1] in 1979. In every SS scheme, there are two phases, one is share generation and another is secret reconstruction. Shamir's scheme is based on Lagrange's polynomial interpolation which satisfies the basic requirements of SS schemes. Shareholders can unlock the secret if t (out of n) or more shares are known. Shamir's scheme is divided into two algorithms, namely share generation and share reconstruction.

3.1.1 Share Generation

In this, the dealer selects a polynomial $f(x)$ (given by (1)) of degree $t-1$ whose coefficients are randomly chosen from a finite field by the dealer,

$$f(x) = a_0 + a_1 * x + a_2 x^2 + \cdots a_{t-1} x^{t-1} \tag{1}$$

Dealer computes a set of n shares $\{f(1), f(2), \ldots, f(n)\}$ and distributes them among the participants through the private channels.

3.1.2 Secret Reconstruction

The secret reconstruction is not done until t parties are involved. For example, as a minimum two points are required to construct the equation of a line, three points are required for formulating a quadratic equation and similarly, t shares are combined to reconstruct equation of degree $t-1$. According to Shamir's scheme, the polynomial reconstruction is done using the Lagrange's polynomial interpolation, i.e.

$$f(x) = \sum_{i=1}^{t} f(i) \prod_{j=1, j\neq i}^{t} (x-j)\big/(i-j) \tag{2}$$

Another landmark work in this direction was presented by Blakey [2] in the same year where the scheme was based on hyperplane geometry. It can be summarised that as the secret is a specific point in space, each share corresponds to hyperplane and the number of planes intersecting (if more significant than the threshold) reveals the secret.

The notion of verifiability in SS schemes was first presented by Chor et al. [27], where verification of received share is done without any information about the secret. VSS schemes can be interactive and non-interactive [28], where non-interactive schemes are more efficient in comparison with the interactive ones. Initially, interactive schemes were presented in which the dealer and players communicate with each other to check the validity of the shares. This sometimes increases the overhead of the dealer as he has to communicate with N players. Later, non-interactive schemes were introduced which reduced the dealer's overhead (communication). Max Mignotte [29] came with his seminal work in 1983 that was based on CRT and used a particular sequence of integers rather than using an interpolation polynomial for secret construction. Another popular construction is due to Feldman [30] which is verifiable and non-interactive one based on Shamir's scheme. The security is based on discrete logarithm problem (DLP) which is assumed to be computationally secure. To make the scheme unconditionally secure, Pedersen [31] used a commitment to function in his scheme.

On the other hand, if the dealer can get commitment values and break DLP, he can distribute fake shares. In 2008, Kaya et al. [32] proposed another VSS scheme based on CRT and proved its security. They also proposed a joint random secret sharing (JRSS) and proactive SS scheme protocol. In 2010, Harn and Lin [33] defined (n, t, n) the SS scheme based on Pedersen's schemes and presented the notion of strong

VSS and t consistency. They also presented a robust (n, t, n) scheme based on Benaloh [34] scheme. Subsequently, in 2012 to 2014 Meng et al. [35] and Mahmoud [36, 37] proposed different VSS schemes. In the direction of PVSS, different schemes [18–20, 38–45] have been proposed from time to time with different capabilities.

3.2 Applications

There are various applications [3–5, 46] of SS schemes ranging from traditional to contemporary. SS schemes can be used for hierarchal organisations to share a single secret. The proposed scheme (Sect. 4) can be used to share multiple secrets in a multilevel environment with fulfilling the necessary security requirements. Other applications of SS are as follows:

Securing Cryptographic Keys play an essential role in any cryptosystem. In such cases, the key is split into different parts. Each part is termed as a share of the key, and these shares are distributed to all the participants who pool their shares for key construction.

Electronic Voting also called as E-Voting uses electronic systems for casting and counting votes. To avoid plausible dishonesty, SS schemes can be adopted in the E-Voting system. Each vote can be treated as a secret, and shares of the vote are distributed among the authorities who are counting the votes. Now only t authority can access the vote, and it cannot be manipulated by any $t-1$ authorities. SS schemes add security and reliability to the E-Voting system. Another possible application of the electronic system is *E-Auction.* In this system, participants put an offer for the items and allocation is done based on their offered prices.

Similarly, SS can be used for *Threshold Schemes for Multiple Servers as well.* Shares are spread across multiple servers, and even $t-1$ shares do not give any information. The scheme works even if one or two servers meet any failure and the secret can still be recovered.

Distributed Signatures is a mathematical way to authenticate a message. It is generally a hash code of the message, encrypted with a secret key. Sender puts his signature to authenticate the message. If there are multiple co-signers, each of them signs the message one by one according to the priority. However, this is not an efficient way because any co-signer can repudiate. The SS schemes can be adopted in such a scenario. Signing key acts as secret which is shared among all the co-signers. Each share is given to each co-signer, and no one is having complete control over the secret. Minimum t co-signers need to pool their shares for signing key construction. Thus, the scheme is secure and repudiation is not possible.

In the next section, a hybrid-based VSS scheme is proposed and in the subsequent sections, the results are analysed and compared with the existing VSS schemes.

4 Proposed Algorithm

The proposed scheme works for multiple secrets in the multilevel structured environment (hierarchal organisation). In this, the shareholders are divided into z levels $(L_1, L_2, \ldots, L_Z)$ with L_1 and L_Z as the highest and lowest levels, respectively. Each ith level is assumed to have N_i shareholders. For example, if $N_3 = 4$ it implies that there are 4 shareholders at level 3. There is a dealer D who wants to share k secrets $(M_0, M_1, \ldots, M_{k-1})$ among the shareholders, and let t be the threshold of the protocol. Whole protocol is divided into 2 phases: share generation and secret reconstruction. The essential conditions necessary for successful secret reconstruction are:

- The secret can be reconstructed if there are t or more valid shares available.
- The secret cannot be reconstructed if the number of shares is less than t.

Each shareholder keeps $k+t$ values as their shares which are used to reconstruct k secrets. The whole algorithm is explained as below:

4.1 Share Generation

Assume there are k secrets and all are from Z_{p}^* where p is a big prime.

Case 1 Intra-Level Secret Sharing

- D forms a polynomial $f(x)$ of a degree $(t+k-1)$ from Z_{p}^*, i.e.

$$f(x) = \sum_{i=0}^{t+k-1} ai * x^i \bmod p \tag{3}$$

  where $a_0 = M_0, a_1 = M_1, \ldots, a_{k-1} = M_{k-1}$ and $a_k, a_{k+1}, \ldots, a_{k+t-1}$ are the private values given by the shareholders to the dealer through a private channel.
- D selects an integer I_0. For each level, a sequence of pairwise co-prime positive integers is selected and made public. Integers at each level equal to the number of shareholders at that level, i.e. $\left(I_1^i, I_2^i, \ldots, I_{N_i}^i\right)$ with $\left(I_1^i < I_2^i < \cdots < I_{N_i}^i\right)$ where $i = 1, 2, \ldots, z$ and greatest common divisor (GCD) of I_0 with every other selected integer should be 1.

- D creates $t + k$ shares of the polynomial, and for each share $f(r)$, dealer forms $f(r) + \delta^i_{x,N_i} * I_0$, where δ^i_{x,N_i} is a random value selected by the dealer for share number x of shareholder N_i at ith level with x varying from 1 to $t + k$. In N_i, N is the number of shareholders at ith level. The value δ^i_{x,N_i} is different for each level and each share. $\left(f(r) + \delta^i_{x,N_i} * I_0\right)$ should lie between

$$\left(I^i_{N_{i-t+2}} * I^i_{N_{i-t+3}} * \cdots * I^i_{N_i}\right) < \left(f(r) + \delta^i_{x,N_i} * I_0\right) < \left(I^i_1 * I^i_2 \cdots I^i_t\right) \quad (4)$$

This is the threshold range for every level, and secrets should lie in this range; otherwise, the algorithm would be inconsistent, i.e. reconstruction can be possible by combing less than t shares. The value to be shared is S^i_{x,N_i}: (S^i_{x,N_i} corresponds to share a number x of the shareholder N_i at ith level with x varying from 1 to $t + k$).

$$S^i_{x,N_i} = \left(f(r) + \delta^i_{x,N_i} * I_0\right) \bmod I^i_{N_i} \quad (5)$$

- Before distributing S^i_{x,N_i}, D computes its hash values and these values are made public so that everyone can access it. Shareholders accept the share if and only if its hash value matches with the previous hash value published by the dealer otherwise discard it. This mechanism checks the dishonesty of the dealer and makes the scheme verifiable. Thus, the dealer is not able to distribute invalid shares.
- The dealer distributes shares S^i_{x,N_i}. Similarly, $t+k$ polynomial values are shared among all the shareholders at each level.

Case 2 Inter-Level Secret Sharing
For inter-level SS, D, needs to select another parameter $I^i_{N_{i,j}}$, where the shareholder N_i contributes his share to jth level for secret reconstruction with.

$$I^j_t < I^i_{N_{i.j}} < I^j_{N_{j-t+2}} \quad (6)$$

Then, the dealer computes $\Delta S^i_{x,N_{i,j}}$

$$\Delta S^i_{x,N_{i,j}} = f(r) + \delta^i_{x,N_i} * I_0 - S^i_{x,N_i} \quad (7)$$

with a share of the shareholder in inter-level sharing as $S^i_{x,N_i} + \Delta S^i_{x,N_{i,j}}$.

4.2 Secret Reconstruction

A system of equations is formed based on the distributed shares. Dealer D accepts shares only if the share is valid, which is verified using the hash value published by the D before. An equation which is formed which is given as:

Case 1 Intra-Level Secret Sharing

$$\delta^i_{x,N_i} * I_0 \bmod I^i_{N_i} \quad (8)$$

Case 2 Inter-Level Secret Sharing

$$S^i_{x,N_i} + \Delta S^i_{x,N_{i,j}} \bmod I^i_{N_i,N_j} \quad (9)$$

Using CRT, a unique solution for $X = f(r) + \delta x, i * I_0$, $f(r)$ can be reconstructed by

$$f(r) = x \bmod I_0 \quad (10)$$

After getting all the polynomial shares by CRT, the following equation is used to reconstruct the polynomial

$$f(x) = \sum_{i=1}^{t} f(i) \prod_{j=1, j\neq i}^{t} (x-j)/(i-j) \bmod p = a_0 + a_1 \cdot x^1 + \cdots a_{k+t-1} \cdot x^{k+t-1} \quad (11)$$

Thus, the authorised set of shareholders reconstructs the k secrets.

The proposed scheme is demonstrated in Fig. 1 which shows 3 levels with 3 shareholders at each level.

5 Results and Discussion

5.1 Experimental Results

The above proposed scheme described in Sect. 4 is implemented in C/C++ using GMP (GNU Multiple Precision) and NTL (Number Theory Library) libraries and tested on 3-GHz third-generation system. GMP is a free library which is multi-precision and can used for various types of operations on signed integers, floating point numbers, and rational numbers. The richness of function, friendly interface, and freely availability makes it so popular and useful. The limit of precision just depends upon machine not on the library. The application includes cryptography and its application, security over the internet, algebraic number theory, and many more. For better insight, implementation results are presented for small numbers and the algorithm is tested for large numbers as well. For demonstration, shareholders are divided into 3 levels ($z = 3$), namely L_1, L_2, and L_3 with 3, 4, and 7 as the number of shareholders at respective levels, i.e. $N_1 = 3$, $N_2 = 4$, $N_3 = 7$. The threshold (t) and the prime (p) being considered are 3 and 563, respectively. Number of secrets

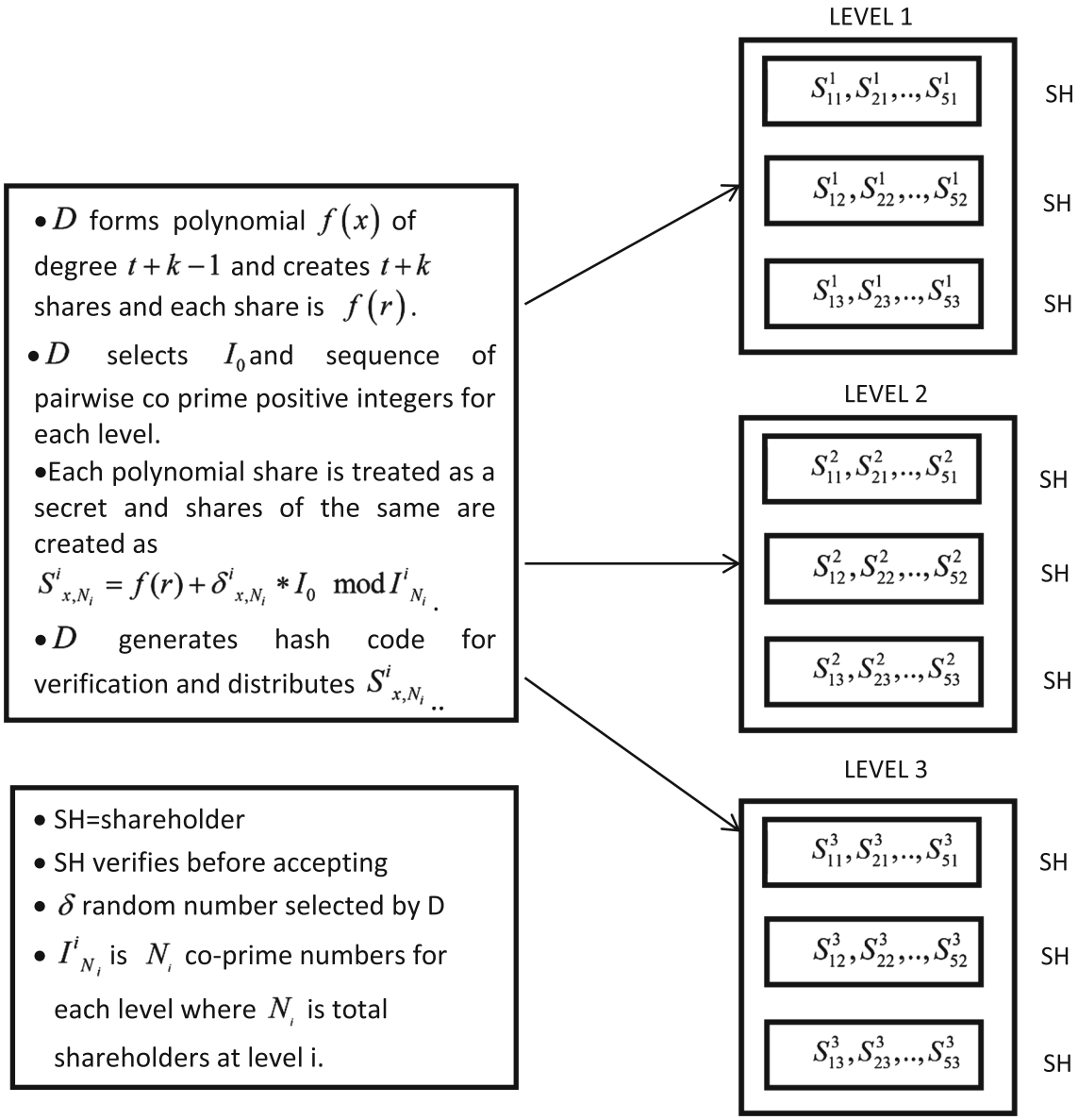

Fig. 1 Proposed algorithm

to be shared is 2 ($k = 2$), where $K_0 = 3$ and $K_1 = 2$ and the coefficient values provided by an authorised set of players are 2, 1, 0 (authorised set used for secret reconstruction comprises 3 players).

(1) Dealer forms the polynomial of a degree $t + k - 1$ using the above values, i.e.

$$f(x) = 3 + 2 * x + 2 * x^2 + 1 * x^3 + 0 * x^4 \quad (12)$$

(2) Dealer selects $I_0 = 863$ and the sequence of pairwise co-prime integers selected for each level are

- For level 1: $I_1 = 137$, $I_2 = 139$, $I_3 = 250$, and threshold range for this level is (34750, 4760750)
- For level 2: $I_1 = 293$, $I_2 = 307$, $I_3 = 313$, $I_4 = 319$, and threshold range for this level is (99847, 28154663)
- For level 3: $I_1 = 229$, $I_2 = 233$, $I_3 = 239$, $I_4 = 241$, $I_5 = 277$, $I_6 = 281$, $I_7 = 283$, and threshold range for this level is (79523, 12752323)

(3) Dealer creates $t + k$ shares: $f(1) = 8$, $f(2) = 23$, $f(3) = 54$, $f(4) = 107$, $f(5) = 188$, and selects $\delta_{x,i}$ as a value for each level which is shown in Table 1.

Therefore, all 5 shares of a 1st shareholder are:

$8 + 550 * 863 \bmod 137 = 90$

$23 + 558 * 863 \bmod 137 = 22$

$54 + 510 * 863 \bmod 137 = 3$

Table 1 $\delta_{x,i}$ values selected by the dealer

Levels	$\delta_{1,i}$	$\delta_{2,i}$	$\delta_{3,i}$	$\delta_{4,i}$	$\delta_{5,i}$
Level 1	550	558	510	620	456
Level 2	9864	8824	8999	9345	9500
Level 3	10,946	10,567	11,001	10,765	10,899

$$107 + 620 * 863 \bmod 137 = 45$$
$$188 + 456 * 863 \bmod 137 = 115 \quad (13)$$

Similarly, shares of other shareholders are calculated which are shown in Table 2.

Case 1 Intra-Level Secret Sharing

While recovering the secret from level 2, 3 out of 4 shareholders need to contribute their shares. Say, first 3 are taking part in the protocol. Following the system of equations needs to be solved using CRT:

$$X = 111 \bmod 293$$
$$X = 144 \bmod 307$$
$$X = 292 \bmod 313 \quad (14)$$

This gives $X = 8$. In the same way, equations can be formed with other shares of the shareholders and results can be obtained accordingly.

Case 2 Inter-Level Secret Sharing

Considering secret reconstruction done at level 3, a 1st shareholder of each level is contributing their shares for reconstruction. Dealer selects two values (because 2 out of 3 shares belong to other levels) between 241 and 277 which are co-prime to one another. Say the values are 253 and 263; following system of equations is formed for secret recovery:

$$X = 90 + 55 \bmod 253$$
$$X = 111 + 124 \bmod 263$$
$$X = 156 \bmod 229 \quad (15)$$

Solving these equations using CRT, we get $X = 8$ and similarly other shares are obtained. Further, these values are used in Lagrange's interpolation to reconstruct the polynomial

$$f(x) = 3 + 2 * x + 2 * x^2 + 1 * x^3 + 0 * x^4 \quad (16)$$

Moreover, the secrets are recovered.

5.2 Application of the Proposed Scheme

The proposed scheme can be advantageous to share multiple secrets in a multilevel environment (for organisations having hierarchal structures). Considering an example of Indian Army, suppose a Colonel is having some secrets (secret keys/passwords) and he is on leave or some special mission for some days. Practically, it is not advisable to hand over the secrets to a single officer (superior or subordinate). So, he would make shares of the secrets and hand it over to officers of various ranks. He may give some shares (these shares include shares formed by splitting multiple secrets to be circulated) to higher rank officers (Lieutenant Colonel or Brigadier) and others to peers or subordinates (Major, Captain and Lieutenant). Now, if an emergency arises for secret reconstruction at Captain level, then, the officer only at a peer or higher rank can contribute in share reconstruction. The secret is reconstructed, provided the threshold condition is satisfied. This algorithm can be used in the case when a higher rank officer (say Colonel) does not want entities or members at lower levels (Major, Captain, and Lieutenant) to recover secrets on their own without any member of lower levels. For this, he can set the threshold value more than the number of entities present at that (lower) level or another alternative is to provide more shares to entities at a higher level and less number of shares to entities at lower levels.

6 Security Analysis and Comparison

The proposed work is analysed in this section, and a comparison with some existing schemes is also performed.

6.1 Security Analysis

Traceability Algorithm is said to be traceable when it is possible to find out whether any participant during the reconstruction phase has submitted any invalid or fake share or not.

Proof Let $f(i)$ be the original valid share and $f'(i)$ is the fake or invalid share. If any participant sends $f'(i)$ to the dealer instead of $f(i)$, then the dealer does not accept the share because

$$H(f(i)) \neq H\left(f'(i)\right) \quad (17)$$

Here, H is one-way hash function and it is complicated to find 2 values that result in the same hash value. Thus, the algorithm is traceable.

Robustness Scheme is said to be robust if all the secrets can be recovered by pooling t or more shares. Use of Lagrange Interpolation has made the scheme more robust. Any t honest players can unlock the shared secret.

Table 2 Shares of shareholders

Shareholders	1st share	2nd share	3rd share	4th share	5th share
1st shareholder of level 1	90	22	3	45	115
2nd shareholder of level 1	112	81	110	17	68
3rd shareholder of level 1	158	77	184	167	216
1st shareholder of level 2	111	65	226	17	255
2nd shareholder of level 2	144	0	12	259	253
3rd shareholder of level 2	292	158	35	84	279
4th shareholder of level 2	125	286	136	203	69
1st shareholder of level 3	156	106	35	1	79
2nd shareholder of level 3	120	190	99	126	48
3rd shareholder of level 3	170	60	120	133	180
4th shareholder of level 3	170	145	204	234	36
5th shareholder of level 3	152	227	19	276	213
6th shareholder of level 3	29	51	51	161	112
7th shareholder of level 3	149	235	116	261	237

Confidentiality Scheme holds confidentiality if even $t-1$ players are not able to reveal the secret. Assume $t-1$ participants are available for secret recovery and product of their moduli is X'. These $t-1$ shareholders use CRT to recover a secret. Suppose they obtained a value S'. The relation between the original secret and the recovered secret is

$$S = S' + \delta * X' \tag{18}$$

Here, S is the original secret. Predicting the correct value of δ to reach the original secret is very difficult. Thus, even with $t-1$ shares, the scheme does not leak any information about the secret.

Consistency Algorithm holds consistency if any set of valid shares of the secret reveals the same secret. Here in the proposed algorithm, consistency is achieved due to Lagrange's interpolation and whether the share is valid or not is verified through one-way hash function.

Dealer Leakage Resilient (DLR) Dealer is said to be dishonest if he subliminally leaks the information in the valid shares. This dishonest strategy allows the dealer to preserve consistency in the system and helps the attacker to unlock secret before reconstruction phase from the leaked information. The system exhibits DLR-VSS property if the attacker does not gain information about the secret before the reconstruction phase.

Proof The DLR-VSS property is achieved by taking the power of randomness from the dealer. The dealer does not have the capability of employing randomness in the system. By this, the dealer will no longer be able to hide information because no value is selected by his own choice.

Salted Hashing can be used in place of simple hashing. In salted hashing, a random number, referred as salt, is added to the share before using one-way hash functions. Salted hashing ensures that no two similar secrets yield similar hash codes. However, the only dealer can verify shares submitted by shareholders. It is assumed that the dealer is honest and he is not distributing invalid shares. When we randomise the hashes, rainbow tables, lookup tables, and reverse lookup tables are no more an effective tool. For the pre-computation of rainbow or lookup table, salt needs to be known in advance and this is not possible.

Another possible method to use salted hashing and still verification is possible from both ends, i.e. shareholders can verify shares before accepting it from dealer and dealer also can verify share before accepting it from shareholders before reconstruction phase. This can be achieved by treating salt (or random number) as one of the secrets. The constant term of the polynomial will be the salt, and degree of the polynomial is $t+k$.

Knowledge of Number of Shares If t and k are not publicly known values, then, it is desirable that adversary must not get any information about some secrets (in case of multi-secret schemes) just by looking at the number of shares of each shareholder. This property is achieved by distributing $t+k$ shares instead of k shares, and t and k are kept a secret, so adversary is not able to access these values. Table 3 shows the comparison of the schemes [7, 25, 26, 47–50] by security assumptions. The acronyms R, C, V, and T stand for robustness, confidentiality, consistency, and traceability, respectively.

Table 3 shows that the proposed approach satisfies all the properties (R, C, V, and T) of VSS schemes. Therefore, it is confirmed that the scheme is verifiable.

In Table 4, the proposed algorithm is compared with other schemes [7, 25, 26, 47–50] by communication cost over secure and insecure channels. Communication cost over

Table 3 Comparisons through security property

Scheme No.	Robustness (R)	Confidentiality (C)	Consistency (V)	Traceability (T)
[7]	Yes	Yes	No	Yes
[47]	Yes	Yes	No	Yes
[48]	Yes	Yes	No	Yes
[25]	Yes	Yes	Yes	Yes
[49]	Yes	Yes	No	Yes
[26]	Yes	Yes	No	Yes
[50]	Yes	Yes	Yes	Yes
Proposed	Yes	Yes	Yes	Yes

Table 4 Comparison through communication cost

Scheme	Distribution cost over secure channels	Reconstruction cost over secure channels	Communication cost over insecure channels	Security assumption
[7]	$1024\,(n_1 + n_2 + \cdots n_z)$	$1024 * t$	$1024\,(n_1 + n_2 + \cdots n_z)$	Unconditionally secure
[47]	–	$160\,t$ or $160\,k$	$1184n + 160n + 1024t$ or $1184n + 160n + 1024k$	DLP
[48]	$1184\,n$	$160\,t$ or $160\,k$	$1024n + 160n$	RSA and DLP
[25]	$320\,n$	$160\,t$ or $160\,k$	$C * n$	Hashing
[49]	–	$160\,t$ or $160\,k$	$1184n + 1184n + 160n$ or $1184n + 1184n + 160k$	RSA and DLP
[26]	$160\,n$	$160\,k * t$	$160 * n * k + C * n * k$	Hashing
[50]	$320\,n$	$2048t$	$2048\,(n + 1) + 2048n$	DLP
Proposed	$160 * (t + k) * (n_1 + n_2 + \cdots n_z)$	$160\,k * t$	$(160 + C) * (n_1 + n_2 + \cdots n_z)$	Hashing

secure channels is analysed separately for both share distribution and share reconstruction. Here, n, t, and C, respectively, denote the number of shareholders, threshold, and any constant number. Communication cost over a secure and insecure channel is calculated using p (1024 bits), q(1024 bits), and $N = p * q$ (1184 bits). In addition to communication cost, security assumption of different schemes is also analysed.

In [7], variables n_1, n_2, and n_3 used are some shareholders at different levels, where z is the total number of levels. This scheme is multilevel secret sharing and uses Chinese remainder theorem. Consider there are z levels. Here, dealer publishes sequences of co-prime numbers equal to the number of shareholders for each level which are of 1024 bits each. This adds to the communication cost of 1024 $(n_1 + n_2 + \cdots n_z)$ bits over insecure channels. Dealer computes shares for n shareholder and distributes them which are of 1024 bit each which makes the communication cost over the secure channel to $1024 * n$ bits. Then, t shareholders collaborate to reconstruct the secret. Thus, the communication cost for reconstruction is $1024 * t$ bits.

In [47], each participant selects his secret shadow of 1184 bits and sends it to the dealer through secure channel which makes the communication cost over the secure channel to $1184\,n$ bits. There are two possible cases, first is when $t > k$, in this case, dealer forms polynomial of degree $(t - 1)$. He creates shares of the polynomial of 160 bits each and publishes them $(160 * n)$. Dealer computes t values of 1024 bits that are used in verification phase and publishes them $(1024 * t)$. t shares of 160 bit each are pooled to recover the secret which makes cost of reconstruction as $160 * t$. Second case arises, when $t < k$. This time dealer forms polynomial of degree $(k - 1)$. He creates shares of the polynomial of 160 bits each and publishes them $(160 * n)$. Dealer computes t value of 1024 bits that are used in verification phase and publishes them $(1024 * t)$. k shares of 160 bit each are pooled to recover the secret which makes cost of reconstruction to $160 * k$ in the second scenario.

In [48], which is multi-secret sharing scheme, where each participant selects his secret shadow of 1184 bits and sends it to the dealer through secure channel which makes the communication cost over the secure channel to $1184 * n$ bits. After some computation, dealer publishes a value of 1024 bits for each participant, which adds $1024 * n$ bits to the communication cost over insecure channels (public channel); then,

Table 5 Comparison through various parameters

Property	[7]	[25]	[50]	[26]	[51]	Proposed algorithm
Dealer publishes the share	No	No	Yes	Yes	No	No
Hash for verifiability	No	Yes	No	Yes	–	Yes
Modular exponentiation or DLP	No	No	Yes	No	No	No
Multi-use scheme	–	No	No	Yes	No	Yes
Can verify dealer's honesty	No	Yes	Yes	No	No	Yes
Can verify shareholder's honesty	No	Yes	Yes	Yes	No	Yes
Has unconditional security	Yes	No	No	No	Yes	No
Outside adversary does not know number of secrets	–	Yes	–	No	No	Yes
Secret revealing order	–	All at a time	All at a time	Any	Any	Any
Conspiracy attack resistance	Yes	Yes	Yes	Yes	Yes	Yes
SETUP attack resistance	No	No	Yes	No	No	Yes

dealer uses public channel to distribute shares of 160 bits for each shareholder $(160 * n)$. t or k shareholders submit their shares for secret reconstruction. Thus, the reconstruction cost becomes $160 * t$ if secrets are less than threshold and it is $160 * k$, if secrets are more than threshold.

In [25], there are k secrets to be shared. There are two cases. In the first case, $t > k$, in this dealer forms 2 polynomials of degree $(t - 1)$. One is used to generate shares of multiple secrets, and other is used for verification phase. Dealer computes n shares of 160 bits each, to each polynomial and send it via secure channel to each shareholder which makes the communication cost over secure channel to $(2n*160)$ bits. Then, he publishes (uses insecure channel) the one hash code for the two shares of constant length C which add $C * n$ communication cost over insecure channels. Now, in the reconstruction phase, combiner/dealer combines t out of n shares of 160 bit each of 1st polynomial to recover the secret, that adds communication cost of $160 * t$ 160*t over secure channel. In the second case, $t < k$, here dealer forms polynomials of degree $(k - 1)$. In this case, the communication cost for reconstruction of secrets is $160 * k$.

In [49], it is also a multi-secret sharing scheme, where participants select their secret shadow of 1184 bits and send it to the dealer via insecure channel, which leads to cost of $1184 * n$. Dealer publishes n values of 1184 bits $(1184 * n)$, which are used for verification. Dealer computes shares of 160 bits for the shareholders which are also published which makes the communication cost over in secure channel to $160 * n$ bits. Then, t or k shares are collaborating to reconstruct secrets, which depend on the value of k. Thus, the communication cost in reconstruction phase will be $160 * t$ or $160 * k$ bits over secure channel.

In Scheme [26], it is multi-secret sharing scheme which uses hashing for verification. The dealer sends a private value of 160 bits each, to each shareholder via secure channel which makes the communication cost over secure channel to $160*n$ bits. He publishes k shares of 160 bit each $(160 * n * k)$ and their hash codes of constant length $(C * n * k)$ for each participant. Then, t shares of k secrets are combined for the reconstruction which makes cost of reconstruction to $160 * k * t$.

Here in [50], each of n shareholders sends 2 private values via a secure channel, which are of 160 bit each, to form 2 polynomials makes $2n * 160$ cost over secure channel. Then, dealer generates and publishes (insecure channel) commitment value, each of 1024 bits for the $2n$ values, which leads to $2n * 1024$ cost over insecure channel. Now, dealer forms 2 polynomials, each of degree $t - 1$. After this, dealer computes n shares to from each polynomial and publishes them. This adds $2n*1024$ bits to communication cost over insecure channel. In reconstruction phase, combiner/dealer combines t out of n shares of 1024 bits each to recover the secret that adds communication cost of $2t * 1024$ over secure channel.

In the proposed algorithm (multilevel and multiple secret SS scheme), z levels are considered with n_i shareholders for each level (i varying from 1 to z). Dealer forms a polynomial of degree $t + k$, and for each level, publishes a sequence of co-prime numbers which are equal to the number of shareholders at that level $((n_1 + n_2 + \cdots + n_z) * 160$ bit). Each shareholder sends a private value to the dealer through a secure channel which adds $(160 * n)$ bits to the communication cost. Dealer forms $t + k$ shares of this polynomial and creates shares of a polynomial using CRT, and these shares which are of 160 bits, are distributed via a secure channel to shareholders $(160 * (t + k) * (n_1 + n_2 + \cdots + n_z))$. He also publishes the hash code $(C * (n_1 + n_2 + \cdots + n_z))$ of all the shares for verification. In the reconstruction phase, $t*k$ shares are used, which makes reconstruction cost $160 * t * k$ bits.

Table 5 shows the comparison of our scheme with other schemes [7, 25, 26, 50, 51] concerning various parameters mentioned in the table. Some of the properties are explained below:

- The scheme is multi-use if shares of participants are different for different secrets.
- The algorithm can resist conspiracy attack if $t-1$ corrupt shareholders cannot unlock the secret. A conspiracy-resistant scheme ensures that the reconstruction of recovered secret does not give information about open secrets.
- Secretly Embedded Trapdoor with Universal Protection (SETUP) is a technique, where an attacker breaks the security of the system, secret information is leaked, but other parties of the protocol are not able to detect this malicious behaviour. All VSS schemes are not SETUP resilient.
- The scheme is unconditionally secure if its security does not depend on any mathematical construct. It is said to be secure even if the adversary has unbounded computational power.

7 Conclusion and Future Directions

SS is an important sphere of Information Security and is attracting a lot of research interest these days. The primary objective is to develop efficient schemes that are secured and can be deployed practically. In this context, a hybrid-based VSS scheme is proposed in this paper which can be used to share multiple secrets in a multilevel environment. A single run of the scheme can share multiple secrets at different levels. The proposed algorithm holds for all requirements of VSS (Table 5), and the scheme is computationally efficient too (Table 4). The scheme also exhibits the property of dealer leakage resilience which is achieved by restricting the dealer to employ randomness. Consequently, the dealer is not able to hide secret information in the share of the shareholders. So, the proposed scheme to work in an environment where dealers and/or shareholders are not honest and also when they are not mutually trusted. Some promising future work directions are to find a method in which each level or layer can have different thresholds instead of a global threshold and also to find a way to distribute one master share instead of multiple shares for multiple secrets.

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
2. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference, vol. 48, pp. 313–317, June 1979
3. Garg, S.; Gentry, C.; Halevi, S.; Wichs, D.: On the implausibility of differing-inputs obfuscation and extractable witness encryption with auxiliary input. Algorithmica **79**(4), 1353–1373 (2017)
4. Martínez-Peñas, U.: Communication efficient and strongly secure secret sharing schemes based on algebraic geometry codes. arXiv:1610.06082 (2016)
5. Peng, K.: Threshold distributed access control with public verification: a practical application of PVSS. Int. J. Inf. Secur. **11**(1), 23–31 (2012)
6. Binu, V.P.; Sreekumar, A.: Threshold multi secret sharing using elliptic curve and pairing. arXiv:1603.09524 (2016)
7. Harn, L.; Fuyou, M.: Multilevel threshold secret sharing based on the Chinese remainder theorem. Inf. Process. Lett. **114**(9), 504–509 (2014)
8. Iftene, S.; Boureanu, I.C.: Weighted threshold secret sharing based on the Chinese remainder theorem. Sci. Ann. Cuza Univ. **15**(EPFL-ARTICLE-174320), 161–172 (2005)
9. Amroudi, A.N.; Zaghain, A.; Sajadieh, M.: A verifiable (k, n, m)-threshold multi-secret sharing scheme based on NTRU cryptosystem. Wirel. Pers. Commun. **96**(1), 1393–1405 (2017)
10. Harn, L.; Hsu, C.F.; Xia, Z.; Zhou, J.: How to share secret efficiently over networks. Secur. Commun. Netw. **2017**(4), 1–6 (2017)
11. Li, M.; Yu, J.; Hao, R.: A cellular automata based verifiable multi-secret sharing scheme without a trusted dealer. Chin. J. Electron. **26**(2), 313–318 (2017)
12. Tentu, A.N.; Basit, A.; Bhavani, K., Venkaiah, V.C.: Multi-secret sharing scheme for level-ordered access structures. In: International Conference on Number-Theoretic Methods in Cryptology, pp. 267–278. Springer, Cham, September 2017
13. Hu, C.; Liao, X.; Cheng, X.: Verifiable multi-secret sharing based on LFSR sequences. Theoret. Comput. Sci. **445**, 52–62 (2012)
14. Duari, B.; Giri, D.: An ideal and perfect (t, n) Multi-secret sharing scheme based on finite geometry. In: Information Technology and Applied Mathematics, pp. 85–94. Springer, Singapore (2019)
15. Zhang, T.; Ke, X.; Liu, Y.: (t, n) multi-secret sharing scheme extended from Harn-Hsu's scheme. EURASIP J. Wirel. Commun. Netw. **2018**(1), 71 (2018)
16. Harn, L.; Hsu, C.F.: (t, n) multi-secret sharing scheme based on bivariate polynomial. Wirel. Pers. Commun. **95**(2), 1–10 (2017)
17. Liu, Y.N.; Zhong, Q.; Xie, M.; Chen, Z.B.: A novel multiple-level secret image sharing scheme. Multimed. Tools Appl. **77**(5), 6017–6031 (2018)
18. Dehkordi, M.H.; Ghasemi, R.: A lightweight public verifiable multi secret sharing scheme using short integer solution. Wirel. Pers. Commun. **91**(3), 1459–1469 (2016)
19. Mashhadi, S.: Secure publicly verifiable and proactive secret sharing schemes with general access structure. Inf. Sci. **378**, 99–108 (2017)
20. Behnad, A.; Eghlidos, T.: A new, publicly verifiable, secret sharing scheme. Sci. Iran. **15**(2), 246–251 (2008)
21. Li, R.; Xiao, Y.; Zhang, C.; Song, T.; Hu, C.: Cryptographic algorithms for privacy-preserving online applications. Math. Found. Comput. **1**(4), 311–330 (2018)
22. Rajabi, B.; Eslami, Z.: A verifiable threshold secret sharing scheme based on lattices. Inf. Sci. (2018). https://doi.org/10.1016/j.ins.2018.11.004
23. Basu, S.; Tomescu, A.; Reiter, M.; Malkhi, D.: Asynchronous verifiable secret-sharing protocols on a good day. arXiv:1807.03720 (2018)
24. Goyal, V.; Kumar, A.: Non-malleable secret sharing for general access structures. In: Annual International Cryptology Conference, pp. 501–530. Springer, Cham, August 2018
25. Shao, J.: Efficient verifiable multi-secret sharing scheme based on hash function. Inf. Sci. **278**, 104–109 (2014)
26. Das, A.; Adhikari, A.: An efficient multi-use multi-secret sharing scheme based on hash function. Appl. Math. Lett. **23**(9), 993–996 (2010)
27. Chor, B.; Goldwasser, S.; Micali, S.; Awerbuch, B.: Verifiable secret sharing and achieving simultaneity in the presence of faults. In: 26th Annual Symposium on Foundations of Computer Science, pp. 383–395. IEEE, October 1985

28. Bai, G.; Damgård, I.; Orlandi, C.; Xia, Y.: Non-interactive verifiable secret sharing for monotone circuits. In: International Conference on Cryptology in Africa, pp. 225–244. Springer, Cham, April 2016
29. Mignotte, M.: How to share a secret. In: Workshop on Cryptography, pp. 371–375. Springer, Berlin, Heidelberg, March 1982
30. Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: 28th Annual Symposium on Foundations of Computer Science, pp. 427–438. IEEE, October 1987
31. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Annual International Cryptology Conference, pp. 129–140. Springer, Berlin, Heidelberg, August 1991
32. Kaya, K.; Selçuk, A.A.: A verifiable secret sharing scheme based on the Chinese remainder theorem. In: International Conference on Cryptology in India, pp. 414–425. Springer, Berlin, Heidelberg, December 2008
33. Harn, L.; Lin, C.: Strong (n, t, n) verifiable secret sharing scheme. Inf. Sci. **180**(16), 3059–3064 (2010)
34. Benaloh, J.C.: Secret sharing homomorphisms: keeping shares of a secret secret. In: Conference on the Theory and Application of Cryptographic Techniques, pp. 251–260. Springer, Berlin, Heidelberg, August 1986
35. Meng, X.; Li, Y.: A verifiable dynamic threshold key management scheme based on bilinear pairing without a trusted party in mobile ad hoc network. In: 2012 IEEE International Conference on Automation and Logistics (ICAL), pp. 315–320. IEEE, August 2012
36. Al Mahmoud, Q.: Polynomial differential-based strong (n, t, n)-verifiable secret sharing. IET Inf. Secur. **7**(4), 312–317 (2013)
37. Mahmoud, Q.A.: A novel verifiable secret sharing with detection and identification of cheaters. Int. J. Math. Sci. Comput. (IJMSC) **2**(2), 1–13 (2016)
38. Stadler, M.: Publicly verifiable secret sharing. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 190–199. Springer, Berlin, Heidelberg, May 1996
39. 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, pp. 32–46. Springer, Berlin, Heidelberg, May 1998
40. Boudot, F.; Traoré, J.: Efficient publicly verifiable secret sharing schemes with fast or delayed recovery. In: International Conference on Information and Communications Security, pp. 87–102. Springer, Berlin, Heidelberg, November 1999
41. Ruiz, A.; Villar, J.L.: Publicly verifiable secret sharing from Paillier's cryptosystem. WEWoRC **74**, 98–108 (2005)
42. Heidarvand, S.; Villar, J.L.: Public verifiability from pairings in secret sharing schemes. In: International Workshop on Selected Areas in Cryptography, pp. 294–308. Springer, Berlin, Heidelberg, August 2008
43. Jhanwar, M.P.: A practical (non-interactive) publicly verifiable secret sharing scheme. In: International Conference on Information Security Practice and Experience, pp. 273–287. Springer, Berlin, Heidelberg, May 2011
44. Wu, T.Y.; Tseng, Y.M.: A pairing-based publicly verifiable secret sharing scheme. J. Syst. Sci. Complex. **24**(1), 186–194 (2011)
45. Shil, A.B.; Blibech, K.; Robbana, R.; Neji, W.: A new PVSS scheme with a simple encryption function. arXiv:1307.8209 (2013)
46. Beimel, A.: Secret-sharing schemes: a survey. In: International Conference on Coding and Cryptology, pp. 11–46. Springer, Berlin, Heidelberg, May 2011
47. Shao, J.; Cao, Z.: A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme. Appl. Math. Comput. **168**(1), 135–140 (2005)
48. Dehkordi, M.H.; Mashhadi, S.: An efficient threshold verifiable multi-secret sharing. Comput. Standards Interfaces **30**(3), 187–190 (2008)
49. Zhao, J.; Zhang, J.; Zhao, R.: A practical verifiable multi-secret sharing scheme. Computer Stand. Interfaces **29**(1), 138–141 (2007)
50. Olimid, R.F.: Dealer-leakage resilient verifiable secret sharing. IACR Cryptol. ePrint Arch. **2014**, 735 (2014)
51. Harn, L.: Secure secret reconstruction and multi-secret sharing schemes with unconditional security. Secur. Commun. Netw. **7**(3), 567–573 (2014)