IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 8, 2020, accepted October 24, 2020, date of publication November 2, 2020, date of current version November 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3035278

Non-Interactive Dealer-Free Dynamic Threshold Secret Sharing Based on Standard Shamir's SS for 5G Networks

CHINGFANG HSU[1], LEIN HARN[2], ZHE XIA[3], AND MAOYUAN ZHANG[1]

[1]School of Computer Science, Central China Normal University, Wuhan 430079, China
[2]Department of Computer Science Electrical Engineering, University of Missouri–Kansas City, Kansas City, MO 64110, USA
[3]Department of Computer Science, Wuhan University of Technology, Wuhan 430071, China

Corresponding author: Chingfang Hsu (cherryjingfang@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772224 and Grant 61872152, in part by the Fundamental Research Funds for the Central Universities under Grant CCNU19TS019, and in part by the Research Planning Project of the National Language Committee under Grant YB135-40.

ABSTRACT Wireless group communications and mobile computing have demonstrated its potential capacity in the next generation of mobile communication networks and wireless systems (5G), where devices have the particularity of being heterogeneous and so have different capabilities in terms of storage, computing, communication and energy. Conventional protocols are not suitable for 5G networks since this environment needs more flexible and simple protocols for secure group communications. Hence, how to realize the dynamical security is a big challenge for 5G networks. In data security management, the longer the system runs, the greater the attacker's capabilities become. A threshold changeable secret sharing scheme (TCSS) in which shares of a (t, n) SS generated by the dealer initially can be used to reconstruct the secret but having a larger threshold j, (i.e., $t < j \leq n$), is a secure way to protect the secret for a longer period of time. A straightforward approach to design a non-interactive dealer-free TCSS is to let the dealer follow Shamir's SS to generate multiple shares for different thresholds, i, for $i = t, t+1, \cdots, n$. Using this approach, each shareholder needs to store $n - t + 1$ shares. In this article, we propose a non-interactive dealer-free TCSS in which each shareholder only needs to store $\left\lceil \frac{n-1}{t} \right\rceil$ shares. Our proposed TCSS can support standard Shamir's (t, n) SS. Our technique can thus be applied to existing Shamir schemes even if they were set up without consideration to future threshold increases. It is unconditionally secure and simpler than most of the existing schemes.

INDEX TERMS Dealer-free, Lagrange interpolation, non-interactive, Shamir's secret sharing scheme, threshold changeable secret sharing scheme.

I. INTRODUCTION

The number of devices towards 5G networks connected to Internet is constantly increasing since its appearance. The emerging technology for 5G networks gives rise to revolutionary applications, such as, automated driving, vehicle platooning, extended sensors, vehicle joint coordinate calculation and remote driving, etc. Hence, group-oriented applications exhibit its potential capacity in the next generation of wireless communications. The devices for 5G networks are heterogeneous and may have different capabilities in terms of storage, computation, communication and energy. Typically, many of these devices have small physical size and are limited in memory, computing abilities and energy supply. One of the main challenges faced by the IoT towards 5G is how to make the communications secure among these heterogeneous devices. The conventional protocols are not suitable for 5G, because this environment need more flexible and simple protocols for secure group communications. Hence, how to realize the dynamically secure is a big challenge for 5G networks.

Data security has been considered one of the main foundations for the continued growth of Internet of Things connectivity and an important issue to be treated in the development of 5G networks. Secret sharing (SS) schemes are ideal for storing information that is highly sensitive and

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran Tariq.

highly important. Examples include encryption keys, missile launch codes, and numbered bank accounts. Each of these pieces of information must be kept highly confidential, as their exposure could be disastrous, however, it is also critical that they should not be lost. Traditional methods for encryption are ill-suited for simultaneously achieving high levels of confidentiality and reliability. This is because when storing the encryption key, one must choose between keeping a single copy of the key in one location for maximum secrecy or keeping multiple copies of the key in different locations for greater reliability. Increasing reliability of the key by storing multiple copies lowers confidentiality by creating additional attack vectors; there are more opportunities for a copy to fall into the wrong hands. Secret sharing schemes address this problem and allow arbitrarily high levels of confidentiality and reliability to be achieved. Secret sharing schemes are important in 5G networks environments [18]–[21], where a key can be distributed over many servers by a threshold secret sharing mechanism. The key is then reconstructed when needed. Secret sharing has also been suggested for 5G networks where the links are liable to be tapped by sending the data in shares which makes the task of the eavesdropper harder. The security in such environments can be made greater by continuous changing of the way the shares are constructed. Therefore, how to efficiently realize dynamic threshold secret sharing is a very valuable problem for 5G networks.

In general speaking, there are two types of security in most cryptographic schemes, either information-theoretic secure or computationally secure. If a scheme is computationally secure, the security of the scheme is based on some mathematical assumptions. For example, the security of RSA scheme is based on the assumption that factoring a composite number into two large primes is a mathematical hard problem. The security of most practical cryptographic schemes belongs to this type. The other type of security is information-theoretic secure. If a scheme is information-theoretic secure, there is no mathematical assumption made to achieve its security. In other words, since information-theoretic security (also called ***unconditionally security***) does not depend on any computational assumption, schemes with information-theoretic security are more attractive than most schemes with computational security. In the following theorem, we prove that our proposed threshold changeable secret sharing scheme (TCSS) is information-theoretic secure.

Design principles for dynamic threshold secret sharing in 5G networks include security and implementation principles. For security principles, it is well known that unconditional security is more secure than computational security. For implementation principles, consider that currently Shamir's (t, n) threshold SS is the most widely used as a general cryptographic tool in many security applications since it is unconditional security and very simple, just polynomial-based. In order to realize compatibility and low cost based on existing Shamir's scheme, dynamic threshold secret sharing in 5G networks should be simple and easy to implement. They should use basic constructions of the standard Shamir's SS. Hence the previous TCSS scheme based on non-standard Shamir's (t, n)-threshold scheme cannot be applied to increase the threshold of existing standard Shamir (t, n)-threshold schemes which were not originally designed for threshold changeability and in which each shareholder has only a single share of one Shamir (t, n)-threshold scheme.

In a (t, n) threshold SS, the threshold value, represents the capability of a SS to protect the secret against both inside and outside attacks. In general, the larger the threshold value is, the bigger number of attackers can be tolerated by the scheme. In 1979, Shamir [1] and Blakley [2] proposed two (t, n) SSs separately. Shamir's scheme is based on a univariate polynomial with degree $t - 1$ and Blakley's scheme is based on the geometry.

In data security management, the longer the system runs, the greater the attacker's capabilities become. In 1999, Martin *et al.* [3] extended a threshold SS to the ***threshold changeable secret sharing*** (TCSS). A TCSS in which shares of a (t, n) SS generated by the dealer initially can be used to reconstruct the secret but having a larger threshold l, (i.e., $t < l \leq n$), is a secure way to protect the secret for a longer period of time. In this article, we propose a non-interactive dealer-free TCSS based on Shamir's (t, n) SS. In our proposed TCSS, shareholders can use their original shares obtained from the dealer initially to reconstruct the secret but having a larger threshold without interacting with the dealer or other shareholders. That is, there is no information exchange from the dealer to shareholders or among shareholders. Our proposed TCSS is a simple modification of Shamir's SSs. The security of our proposed schemes is unconditionally secure.

The rest of this article is organized as follows. In the next section, we review related works. We give some preliminaries in Section III. In Section IV, we introduce model of our proposed scheme. We propose a TCSS based on standard Shamir's (t, n) SS in Section V, and security analysis is given in Section VI. We conclude in Section VII.

II. RELATED WORKS

Using original shares of a (t, n) SS to reconstruct the secret but with a larger threshold, (i.e., $t < l \leq n$), is a secure way to protect the secret for a longer period of time. This is because the longer the system runs, the greater the attacker's capabilities become. The threshold of original Shamir's (t, n) SS is a fixed value. A TCSS in which shares of a (t, n) SS generated by the dealer initially can be used to reconstruct the secret but having a larger threshold l is a robust SS.

One simple way to design a TCSS is to let the dealer to prepare the threshold changeability while generating shares for shareholders during set up [3]–[7]. For example, instead of providing only one share per shareholder using standard Shamir's SS, the dealer needs to prepare multiple shares per shareholder or publish some public values during set

up. Later, in the secret reconstruction, shareholders can use their shares to compute and release values based on these additional information. The trade-offs of this approach is that each shareholder does not need to have any interaction with the dealer or with other shareholders (i.e., there is no secure channel needed), but shareholders need more storage space to store their shares or to access some public information. In addition, since the changeability of threshold needs to be predicated in advance, this approach is only feasible for some applications when the changeability of threshold is predicable.

One alternative approach of TCSSs [7]–[9] requires shareholders to work together to refresh their shares in order to change the threshold. The trade-off of this approach is that original shares can be used to generate new shares; but shareholders need to interact with each other in order to refresh their shares (i.e., secure channels among shareholders are needed). Furthermore, verifiable SS (VSS) [10], [11] is needed to verify the validity of their new shares after the refreshing process.

Steinfeld *et al.* proposed a Lattice-based TCSS [12], [13] to support standard Shamir's share generation algorithm and a Lattice-based TCSS [14] to support standard Chinese Remainder Theorem (CRT) share generation algorithm. Their schemes do not require any secure channels and is called ***TCSSs without dealer***. The basic idea of their schemes to increase the threshold is to let each shareholder to introduce an appropriate amount of random noise to his/her share obtained from the dealer initially. Thus, each new share will contain only partial information of his/her share obtained from the dealer initially. Lattice-based reduction techniques are used to construct an "*error-correction*" algorithm to recover the secret. The TCSS proposed by Steinfeld *et al.* [12], [13] cannot use standard Shamir's secret reconstruction algorithm to recover the secret. In 2012, Zhang *et al.* [6] proposed a non-interactive dealer-free TCSS which is based on a computationally secure SS [15]. The security of their TCSS is computationally secure and their scheme does not need any secure channel. A dealer-free TCSS is proposed by Nojoumian and Stinson [9] which needs interactions among shareholders in the secret reconstruction. A collusion attack resistance TCSS is proposed by Zhang and He [8] which uses a partial broadcast channel (PBC) in both share distribution phase and secret reconstruction to replace secure channels. However, interactions among shareholders are needed in the secret reconstruction. A threshold changeable secret sharing scheme based on the Chinese Remainder Theorem is proposed by Jia *et al.* [16] which is computationally secure. The TCSS proposed by Meng *et al.* [17] which is based on a bivariate polynomial, cannot use standard Shamir's secret reconstruction algorithm to recover the secret.

In this article, we propose a non-interactive dealer-free TCSS based on Shamir's (t, n) SS. There is a straightforward approach to design a non-interactive dealer-free TCSS. During registration, the dealer can follow Shamir's SS to generate multiple shares for different thresholds, for $i = t, t+1, \cdots, n$. Using this approach, each shareholder needs to store $n-t+1$ shares. Later, in secret reconstruction, shareholders can present their shares corresponding to the proper threshold. But using this straightforward approach, the large number of shares kept by each shareholder becomes the main problem. To overcome this problem, the main advantage using our proposed TCSS is that each shareholder only needs to store $\left\lceil \frac{n-1}{t} \right\rceil$ shares. The main contributions of this article are summarized in the following.

- A non-interactive dealer-free (t, n) TCSS is proposed.
- The proposed TCSS can support standard Shamir's SS including both share generation and secret reconstruction, which is simpler than most of the existing schemes.
- The proposed TCSSs is unconditionally secure.

III. PRELIMINARIES

In this section we introduce some fundamental backgrounds. In a secret sharing scheme, a secret s is divided into n shares by a mutually trusted dealer and the secret is shared among a set of n shareholders in such a way that any authorized subset of shareholders can reconstruct the secret but any unauthorized subset of shareholders cannot determine the secret. If any unauthorized subset of shareholders cannot obtain any information of the secret, the scheme is called perfect. The set of authorized subsets of shareholders is called access structure and the set of unauthorized subsets of shareholders is called prohibited structure.

Formally, let $P = \{1, \cdots, n\}$ be a set of shareholders. According to Shannon's entropy function, [22] stated that a secret sharing scheme with respect to access structure, Γ, satisfies the following:

1) Correctness. Any authorized subset of shareholders can compute s. Namely, for any $\in \Gamma$, it has $H(S \mid A) = 0$.
2) Security. Any unauthorized subset of shareholders cannot recover. Namely, for any $A \notin \Gamma$, it is $0 < H(S \mid A) \leq H(S)$. In the case that $(S \mid A) = H(S)$, shareholders in A obtain no information on s. This is the case we are interested in and the security of this scheme is perfect.

A perfect secret sharing scheme is ideal if the shares of shareholders are taken from the same domain as the secret (as proved in [3], this is the minimal size of the shares).

Secret sharing scheme based on polynomials. In Shamir's (t, n) SS [10] based on a linear polynomial, the dealer selects a polynomial, $f(x)$, with degree $t-1$ and $f(0) = s$ where s is the secret. The dealer generates shares, $f(x_i), i = 1, 2, \cdots, n$, for shareholders, where x_i is the public information associated with each shareholder, U_i. Each share, (x_i), is an integer in $GF(p)$. Shamir's SS satisfies both security requirements of a (t, n) SS. That are, 1) with t or more than t shares can recover the secret, and 2) with fewer than t shares cannot obtain any information of the secret. Shamir's SS is unconditionally secure.

IV. MODEL OF OUR SCHEME

In our proposed TCSS, dealer is responsible to register shareholders and generates shares for shareholders initially. The registration process is the same as Shamir's (t, n) SS. In Shamir's scheme, dealer selects a polynomial with $t-1$ degree and uses it to generate one share for each shareholder. But, in our TCSS, dealer selects r different polynomial with $t-1$ degree each and uses them to generate r shares for each shareholder. The secret reconstruction of our TCSS is the same as Shamir's SS which is based on the Lagrange interpolation polynomial.

We want to point out that since in Shamir's SS the dealer uses a polynomial with $t-1$ degree to generate shares, knowing only t shares can recover the secret. Thus, the threshold of Shamir's SS is fixed. However, in our proposed TCSS, each shareholder has r shares corresponding to r different polynomials with $t-1$ degree each. Since each shareholder reveals a linear combination of these r shares in the secret reconstruction for a different threshold value, say l for example, we will show that the secret can only be recovered if there are l or more than l shareholders participated in the process.

There are two types of attacks, inside and outside attacks, considered in our scheme.

1) INSIDE ATTACK

The inside attackers are colluded shareholders who own valid shares and try to recover the secret by themselves. Just like most threshold SSs, our proposed scheme needs to prevent up to $t-1$ colluded shareholders working together to recover the secret. So, in our TCSS, the threshold with respect to inside attack is the fixed value,.

2) OUTSIDE ATTACK

The outside attack is performed by someone who is not a shareholder but tries to recover the secret. In a TCSS, we assume that the capability of outside attacker is increased as time runs. Thus, the threshold of a SS may increase from its original value, to any value, l, where $t < l \leq n$. In other words, in a TCSS, the threshold with respect to outside attack is not a fixed value. The threshold, is $t \leq l \leq n$.

V. TCSS SCHEME

In our TCSS, dealer selects r different polynomial with $t-1$ degree each. Then, dealer follows Shamir's SS to use these polynomials to generate r shares for each shareholder. The secret reconstruction of our TCSS is the same as Shamir's SS which is based on the Lagrange interpolation polynomial. Each released value of shareholder is a linear combination of r shares. Therefore, knowing this released value, attacker cannot recover each individual share. We will also show that the secret can only be recovered after receiving released values from all shareholders participated in the secret reconstruction.

A. PROPOSED SCHEME

1) SHARE GENERATION

For n participants $\{U_1, U_2, \cdots, U_n, \}$ and a prime number p, the original threshold in Shamir's SS is t. The dealer selects r (i.e., $= \left\lceil \frac{n-1}{t} \right\rceil$. We will explain this condition in Theorem 2) different polynomials, $h_i(x), i = 1, 2, \cdots, r$, with $t-1$ degree each, where the total dimension of the linear subspace spanned by these r polynomials are rt, and then, the dealer uses them to generate r shares, $h_i(x_j), i = 1, 2, \cdots, r$, for each shareholder, U_j, $j = 1, 2, \cdots, n$, whose public information is $x_j \notin [1, r]$. Shares, $h_i(x_j), i = 1, 2, \cdots, r$, are sent to shareholder, U_j, secretly. Furthermore, for the secret, the dealer publishes, a_i, $i = 1, 2, \cdots, r$, such that $\sum_{i=1}^{r} a_i h_i\,(i)\ mod\ p = s$, where s is the secret.

2) SECRET RECONSTRUCTION FOR CHAGEABLE THRESHOLD

Shares generated initially can be used to reconstruct the secret with different threshold, for $l \in [t, n]$. In the following discussion, let us assume that the threshold is $\in [t, n]$, and shareholders, $\{U_{w_1}, U_{w_2}, \cdots, U_{w_l}, \}$, are participating in the secret reconstruction.

Step1. Each shareholder, U_{w_v}, accesses the public information, a_i, $i = 1, 2, \cdots, r$, and uses his/her shares, $h_i(x_{w_v}), i = 1, 2, \cdots, r$, to compute and release the value, $c_v = \sum_{i=1}^{r} a_i h_i \left(x_{w_v}\right) \prod_{j=1, j\neq v}^{l} \frac{i - x_{w_j}}{x_{w_v} - x_{w_j}} mod\ p$.

Step 2. After having all values, c_v, $v = 1, 2, \cdots, l$, the secret can be computed as $s = \sum_{v=1}^{l} c_v mod\ p$.

B. EXAMPLE

1) SHARE GENERATION

For $n = 5$ participants $\{U_1, U_2, \cdots, U_5, \}$ and $p = 100$, support that the original threshold in Shamir's SS is $t = 2$. The dealer selects $r = 2$ (i.e., $r = \left\lceil \frac{n-1}{t} \right\rceil$) different polynomials, $h_1\,(x) = x + 1$ and $h_2\,(x) = 2x + 1$, with $t-1 = 1$ degree each and uses them to generate $r = 2$ shares, $h_i(x_j), i = 1, 2$, for each shareholder, U_j, $j = 1, 2, 3, 4, 5$, whose public information is $x_j \notin [1, 2]$. We can assume that $x_1 = 3, x_2 = 4, x_3 = 5, x_4 = 6, x_5 = 7$. Shares, $h_1\,(x_1) = 4, h_2\,(x_1) = 7$, are sent to shareholder, U_1 secretly. Share, $h_1\,(x_2) = 5, h_2\,(x_2) = 9$, are sent to shareholder, U_2 secretly. Share, $h_1\,(x_3) = 6, h_2\,(x_3) = 11$, are sent to shareholder, U_3 secretly. Share, $h_1\,(x_4) = 7, h_2\,(x_4) = 13$, are sent to shareholder, U_4 secretly. Share, $h_1\,(x_5) = 8, h_2\,(x_5) = 15$, are sent to shareholder, U_5 secretly. Furthermore, for the secret, assume that the dealer publishes, $a_1 = 1 and a_2 = 2$, such that $\sum_{i=1}^{2} a_i h_i\,(i)\ \boldsymbol{mod}\ p = s = 12$, where s is the secret.

2) SECRET RECONSTRUCTION FOR CHANGEABLE THRESHOLD

Shares generated initially can be used to reconstruct the secret with different threshold, l for $l \in [t, n]$. In the following discussion, let us assume that the threshold is $= 3 \in [t, n]$,

and shareholders, $\{U_1, U_2, U_3\}$, are participating in the secret reconstruction.

Step1. Each shareholder in $\{U_1, U_2, U_3\}$ accesses the public information, $a_i, i = 1, 2$, and uses his/her shares, $h_1(x_1) = 4, h_2(x_1) = 7, h_1(x_2) = 5, h_2(x_2) = 9, h_1(x_3) = 6, h_2(x_3) = 11$, to compute and release the value, $c_1 = 66, c_2 = 6, c_3 = 40$.

Step 2. After having all values, $\boldsymbol{c_v}, \boldsymbol{v = 1, 2, 3}$, the secret can be computed as $\boldsymbol{s = \sum_{v=1}^{3} c_v \, mod \, 100 = 12}$.

VI. SECURITY ANALYSIS

We first use the following theorem to prove the correctness of our TCSS.

Theorem 1: The secret can be reconstructed in Step 2 of secret reconstruction as $= \sum_{v=1}^{l} c_v mod\, p$.

Proof: If all l shareholders participated in the secret reconstruction in Step 1 and act honestly to compute and release their values, $c_v, v = 1, 2, \cdots, l$, then we have

$$\begin{aligned}
&\sum_{v=1}^{l} c_v \, mod \, p \\
&= \sum_{v=1}^{l} \left(\sum_{i=1}^{r} a_i h_i(x_{w_v}) \prod_{j=1, j\neq v}^{l} \frac{i - x_{w_j}}{x_{w_v} - x_{w_j}} \right) mod \; p \\
&= \sum_{i=1}^{r} a_i \left(\sum_{v=1}^{l} h_i(x_{w_v}) \prod_{j=1, j\neq v}^{l} \frac{i - x_{w_j}}{x_{w_v} - x_{w_j}} \right) mod \; p \\
&= \sum_{i=1}^{r} a_i h_i(i) = s.
\end{aligned}$$

There are two types of security in most cryptographic schemes, either information-theoretic secure or computationally secure. If a scheme is computationally secure, the security of the scheme is based on some mathematical assumptions. If a scheme is information-theoretic secure, there is no mathematical assumption made to achieve its security. Since information-theoretic security (also called ***unconditionally security***) does not depend on any computational assumption, schemes with information-theoretic security are more attractive than most schemes with computational security. In the following theorem, we prove that our proposed TCSS is information-theoretic secure.

Theorem 2: The proposed TCSS scheme is unconditionally secure.

Proof: Unconditional security implies that no assumptions are made about the computing power and resources available to an adversary. We can see that there is not any computational assumption in our scheme. It is a univariate-polynomial-based TCSS scheme, which is the same as Shamir's SS. Hence, our TCSS scheme is unconditionally secure.

In the following discussion, we analyze the security to show that our TCSS can prevent attacks as presented in Section IV.

Inside attack:

Theorem 3: The TCSS can resist up to $t-1$ *inside attackers working together to recover the secret.*

Proof: In our proposed TCSS, shares are generated by r different polynomials, $h_i(x), i = 1, 2, \cdots, r$, with $t-1$ degree each. Thus, to recover each polynomial needs at least t original shares of each polynomial. This security is the same as Shamir's SS with threshold. The threshold with respect to inside attack is t.

Outside attack:

We use the following theorem to prove the security.

Theorem 4: The TCSS can resist outside attack as presented in Section IV.

Proof: To prove the security of our TCSS (i.e., secure for any threshold, $l \in [t, n]$), we need only to show that it is secure under the worst scenario. In a TCSS, we assume that the capability of outside attacker is increase as time runs. The worst scenario is when the threshold of a TCSS is its maximal value, n, in which it requires to have n shareholders participated in the secret reconstruction. In other words, we assume that outside attacker has already known $n-1$ released values, c_r, in Step 1.

First, in Step 1 of secret reconstruction, since each released value, $c_v = \sum_{i=1}^{r} a_i h_i(x_{w_v}) \prod_{j=1, j\neq v}^{l} \frac{j - x_{w_j}}{x_{w_v} - x_{w_j}} mod\, p$, is a linear combination of shares, $h_i(x_{w_v}), i = 1, 2, \cdots, r$, it is impossible for the attacker to recover each individual share, $h_i(x_{w_v})$. Furthermore, since each released value, $c_v = \sum_{i=1}^{r} a_i h_i(x_{w_v}) \prod_{j=1, j\neq v}^{l} \frac{j - x_{w_j}}{x_{w_v} - x_{w_j}} mod\, p$, is a function of additive sum of polynomials, $h_i(x), i = 1, 2, \cdots, r$, consisting of rt coefficients, the attacker can therefore establish $n-1$ equations from these $n-1$ released values. If the number of unknown coefficients of polynomials, $h_i(x), i = 1, 2, \cdots, r$, is larger than the number of equations available to the attacker (i.e., $rt > n-1$), the attacker cannot recover these polynomials and the secret. Thus, the condition, $r = \left\lceil \frac{n-1}{t} \right\rceil$ specified in the share generation can provide security of this TCSS.

VII. COMPARISON

In this section, we compare our scheme with the latest two TCSS scheme and one TCSS scheme based on standard Shamir's SS. We briefly introduce these three schemes following. In 2020, Jia *et al.* [16] proposed a TCSS based on the Chinese Remainder Theorem (CRT). In this scheme, a different threshold can be activated at any time through the public broadcast channel. However, this scheme is computationally secure. Furthermore, the computational time using CRT takes much longer than polynomial-based computation. In 2020, Meng *et al.* [17] proposed two TCSS schemes, one is based on a bivariate polynomial and the other is based on the combination of bivariate and univariate polynomials. Their schemes use binding values in the secret reconstruction phase to achieve the threshold changeable property. Their scheme is unconditionally secure and is based on bivariate polynomials. In 2004, Steinfeld *et al.* [12] proposed a Lattice-based TCSS to support standard Shamir's secret generation algorithm. Their scheme does not need any secure channels and is called a TCSS without dealer. However, their scheme cannot

use standard Shamir's secret reconstruction to recover the secret.

	Jia's scheme [19]	Meng's scheme [20]	Steinfeld 's scheme [12.13]	Our scheme
Security	Computational security	Unconditional security	Computational security	Unconditional security
Implementation	Chinese Remainder Theorem-based	Bivariate polynomial-based	Lattice & Shamir's SS-based	Shamir 's SS-based

FIGURE 1. Comparison with previous TCSS schemes.

The comparison includes two aspects: security and implementation, which is shown in Figure 1. For security principles, it is well known that unconditional security is more secure than computational security. For implementation principles, consider that currently Shamir's (t, n) threshold SS is the most widely used as a general cryptographic tool in many security applications since it is unconditional security and very simple, just univariate-polynomial-based. To realize compatibility and low cost based on existing Shamir's scheme, dynamic threshold secret sharing in 5G networks should be simple and easy to implement. They should use basic constructions of the standard Shamir's SS. That is, TCSS for 5G networks can support standard Shamir's SS including both share generation and secret reconstruction.

The previous TCSS scheme based on non-standard Shamir's SS [19.20] cannot be applied to increase the threshold of existing standard Shamir (t, n)-threshold schemes which were not originally designed for threshold changeability.

The previous lattice-based TCSS scheme for standard Shamir's SS [12.13] is based on computational assumption, that is CVP problem, which is not conditionally secure and cannot use standard Shamir's secret reconstruction algorithm to recover the secret such that the computational cost is higher than standard Shamir's secret reconstruction. Our proposed TCSS is a simple modification of Shamir's SSs. This technique can thus be applied to existing Shamir schemes even if they were set up without consideration to future threshold increases. Furthermore, there is no information exchange from the dealer to shareholders or among shareholders and the security of our proposed schemes is unconditionally secure.

VIII. CONCLUSION

We propose a non-interactive dealer-free (t, n) SS with threshold changeability. Our proposed scheme is a simple modification of Shamir's (t, n) SS but each shareholder needs to keep $\left\lceil \frac{n-1}{t} \right\rceil$ shares. The scheme is unconditionally secure which can support standard share generation and secret reconstruction. Hence, this method can provide flexible and dynamical security for secure group communications in 5G networks.

DATA AVAILABILITY STATEMENT

The data used to support the findings of this study are included within the article.

REFERENCES

[1] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS Nat. Comput. Conf.*, vol. 48. Atlantic, NJ, USA: AFIPS Press, 1979, pp. 313–317.
[3] K. Martin, J. Pieprzyk, R. Safavi-Naini, and H. Wang, "Changing thresholds in the absence of secure channels," *J. Austral. Comput.*, vol. 31, pp. 34–43, 1999.
[4] T. Lou and C. Tartary, "Analysis and design of multiple threshold changeable secret sharing schemes," in *Proc. Int. Conf. Cryptol. Netw. Secur.* Berlin, Germany: Springer, 2008, pp. 196–213.
[5] A. Maeda, A. Miyaji, and M. Tada, "Efficient and unconditionally secure verifiable threshold changeable scheme," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Berlin, Germany: Springer, 2001, pp. 403–416.
[6] Z. Zhang, Y. M. Chee, S. Ling, M. Liu, and H. Wang, "Threshold changeable secret sharing revisited," *Theor. Comput. Sci.*, vol. 418, pp. 106–115, Feb. 2012.
[7] R. Shi and H. Zhong, "A secret sharing with the changeable threshold value," in *Proc. Int. Symp. Inf. Eng. Electron. Commerce*, 2009, pp. 238–246.
[8] X. Zhang and M. He, "Collusion attack resistance and practice-oriented threshold changeable secret sharing schemes," in *Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Apr. 2010, pp. 745–752.
[9] M. Nojoumian and D. R. R. Stinson, "On dealer-free dynamic threshold schemes," *Adv. Math. Commun.*, vol. 7, no. 1, pp. 39–56, 2013.
[10] L. Harn and C. Lin, "Strong verifiable secret sharing," *Inf. Sci.*, vol. 180, no. 16, pp. 3059–3064, 2010.
[11] K. Peng, "Efficient VSS free of computational assumption," *J. Parallel Distrib. Comput.*, vol. 71, no. 12, pp. 1592–1597, Dec. 2011, doi: 10.1016/j.jpdc.2011.07.009.
[12] R. Steinfeld, H. Wang, and J. Pieprzyk, "Lattice-based threshold-changeability for standard Shamir secret-sharing schemes," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2004, pp. 170–186.
[13] R. Steinfeld, J. Pieprzyk, and H. Wang, "Lattice-based threshold changeability for standard shamir secret-sharing schemes," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2542–2559, 2007.
[14] R. Steinfeld, H. Wang, and J. Pieprzyk, "Lattice-based threshold-changeability for standard CRT secret-sharing schemes," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 242–259, Nov. 2007.
[15] H. Krawczyk, "Secret sharing made short," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 773. Springer, 1993, pp. 136–146.
[16] X. Jia, D. Wang, D. Nie, X. Luo, and J. Z. Sun, "A new threshold changeable secret sharing scheme based on the Chinese remainder theorem," *Inf. Sci.*, vol. 473, pp. 13–30, Jan. 2019.
[17] K. Meng, F. Miao, W. Huang, and Y. Xiong, "Threshold changeable secret sharing with secure secret reconstruction," *Inf. Process. Lett.*, vol. 157, May 2020, Art. no. 105928.
[18] L. Harn and C.-F. Hsu, "A practical hybrid group key establishment for secure group communications," *Comput. J.*, vol. 60, pp. 1582–1589, Jan. 2017.
[19] L. Harn, Z. Xia, C. Hsu, and Y. Liu, "Secret sharing with secure secret reconstruction," *Inf. Sci.*, vol. 519, pp. 1–8, May 2020.

[20] C.-F. Hsu, L. Harn, Y. Mu, M. Zhang, and X. Zhu, "Computation-efficient key establishment in wireless group communications," *Wireless Netw.*, vol. 23, no. 1, pp. 289–297, Jan. 2017.
[21] L. Harn, C.-F. Hsu, and B. Li, "Centralized group key establishment protocol without a mutually trusted third party," *Mobile Netw. Appl.*, vol. 23, no. 5, pp. 1132–1140, Oct. 2018.
[22] A. Beimel, "Secure schemes for secret sharing and key distribution," Dept. Comput. Sci., Technion-Israel Inst. Technol., Haifa, Israel, Tech. Rep., 1996.

CHINGFANG HSU received the M.Eng. and Ph.D. degrees in information security from the Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2010, respectively. From September 2010 to March 2013, she was a Research Fellow with the Huazhong University of Science and Technology. She is currently an Assistant Professor with Central China Normal University, Wuhan. Her research interests include cryptography and network security, especially in secret sharing and its applications.

LEIN HARN received the B.S. degree in electrical engineering from National Taiwan University, in 1977, the M.S. degree in electrical engineering from the State University of New York, Stony Brook, in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota, in 1984. He is currently a Professor with the Department of Electrical and Computer Engineering, University of Missouri–Kansas City (UMKC). He is also investigating new ways of using secret sharing in various applications.

ZHE XIA received the M.Eng. and Ph.D. degrees in information security from the University of Surrey, U.K., in 2005 and 2009, respectively. From 2009 to 2013, he was a Research Fellow with the University of Surrey. He is currently an Assistant Professor with the Department of Computer Science, Wuhan University of Technology, Wuhan, China. His research interests include cryptography and network security, especially in secret sharing and its applications.

MAOYUAN ZHANG received the Ph.D. degree in computer science from the Huazhong University of Science and Technology, Wuhan, China, in 2005. From 2005 to 2007, he was a Research Fellow with the Huazhong University of Science and Technology. He is currently a Professor with Central China Normal University, Wuhan. His research interests include web information retrieval and mining, especially in natural language processing.