Design of Secret Reconstruction With Optimal Communication Efficiency

Xingfu Yan, Changlu Lin, Rongxing Lu, *Senior Member, IEEE*, and Chunming Tang

***Abstract*— The efficiency of secret reconstruction, measured by either channel efficiency or communication efficiency, is always a challenging issue in designing secret sharing schemes and has received considerable attention in recent years. In this letter, aiming at this challenge, we introduce an ingenious strategy, called "jumping skill," and use it to build a new secret reconstruction scheme. Since only fewer shares are needed to recover the secret, the proposed secret reconstruction scheme is optimal in its communication efficiency. Extensive simulations are conducted, and the results indicate that the upper bound of the communication efficiency can be achieved in our proposal.**

***Index Terms*— Secret sharing, communication efficiency, linear code, access structure.**

I. Introduction

THE CONCEPT of (t, n) threshold secret sharing was introduced by Shamir [6] and Blakey [2] respectively in 1979. Due to its promising feature, secret sharing has been widely discussed in past decades. Among all discussions of secret sharing, the efficiency is always a challenging topic when the secret sharing technique is considered in many practical applications. Generally speaking, there are two measures for the efficiency of a secret sharing scheme, namely the *channel efficiency* and *communication efficiency*. The former captures the number of secure channels between the dealer and players in the secret distribution phase or among players in the secret reconstruction phase [5], while the latter focuses on the total information transmitted in the channels [1], [3], and [4]. We focus on discussing the communication efficiency in the phase of secret reconstruction.

In 2008, Wang and Wong [8] built an efficient secret sharing scheme by using polynomial evaluation over $GF(q)$, where $q > n + v$, and elaboratively evaluated the communication efficiency in secret reconstruction. In particular, their scheme requires each involved player to contribute his/her partial share instead of whole share, and the upper bound of communication efficiency in their scheme is obtained. While they claimed that the upper bound is optimal in one special case, they also left an open problem to optimize the communication efficiency in other cases. Concretely, they gave the upper bound of communication efficiency measured by communication rate as $(|A| - t + 1)/|A|$, where A is a set of participants who work together to reconstruct the secret. The communication rate is optimal if $|A| \geq t + v - 1$, where v is an integer. However, it is not optimal if $t \leq |A| < t + v - 1$. In 2012, Zhang *et al.* [9] proposed an efficient threshold changeable secret sharing scheme over $GF(q)$, where $q > n$. However, their scheme only focuses on the communication efficiency in the secret distribution phase. In 2016, Huang *et al.* [3] proposed a secret sharing scheme based on codes, which can achieve the minimum communication efficiency if $l = n$, where l is the number of participants who work together to recover the secret. They proved that the upper bound of communication efficiency can be touched universally for all possible values of $t \leq l \leq n$ by using random linear code constructions. In 2018, Bitar and Rouayheb [1] proposed a secret sharing scheme with the help of Staircase codes. Their construction can achieve the optimal communication efficiency for all possible values of $t \leq l \leq n$. However, Staircase code requires dividing the secret and the shares into many symbols in some small finite field. Different from the above-mentioned, in our setting, we aim to design our scheme based on a simple polynomial over finite field, which would be much simpler than any existing coding strategy.

We will explore the open problem left in [8] and present a novel method to design a new secret reconstruction scheme to optimize communication efficiency in case of $t \leq |A| < t + v - 1$. Our key idea lies in that each participant in secret reconstruction phase chooses some components of the share in a discontinued way. We name it as "*jumping skill*", and it is quite different from the Wang-Wong's scheme in which each participant contributes the whole share or some continued components of the share in the secret reconstruction phase. Our new scheme is much more efficient than Wang-Wong's scheme under the condition of $t \leq |A| < t + v - 1$, because, with "*jumping skill*" strategy, the number of shares' components used for recovering secret is reduced hugely, which also implies the total number of shares needed is reduced. Superficially, we evaluate that the communication efficiency of our scheme is optimal from extensive simulation results. We find that the communication efficiency in our scheme is the same as Bitar-Rouayheb's scheme when $k = 0$ (we only use the polynomial over finite field without the tools of Staircase codes); and it is near Bitar-Rouayheb's case when $k \neq 0$ (see Section III-A for the parameter k). In addition, both our results and Bitar-Rouayheb's are better than Wang-Wong's work.

II. Preliminaries

A. Secret Sharing

Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a set of n players and D denote the dealer. Let $2^{\mathcal{P}}$ be the family of all subsets of $\mathcal{P}$.

Manuscript received February 1, 2018; revised March 26, 2018 and May 7, 2018; accepted May 17, 2018. Date of publication May 30, 2018; date of current version August 10, 2018. The work of X. Yan and C. Lin was supported in part by National Natural Science Foundation of China (Nos. 61572132 and U1705264). The work of R. Lu was supported in part by Natural Sciences and Engineering Research (NSERC) Discovery Grants (no. Rgpin 04009), NBIF Start-Up Grant (Rif 2017-012). The work of C. Tang was supported in part by National Natural Science Foundation of China (No. 61772147), Guangdong Province Natural Science Foundation of major basic research and Cultivation project (No. 2015A030308016). The associate editor coordinating the review of this paper and approving it for publication was H. Le-Minh. *(Corresponding author: Changlu Lin.)*

X. Yan and C. Lin are with the College of Mathematic and Informatics, Fujian Normal University, Fuzhou 350117, China (e-mail: xfyan78@163.com; cllin@fjnu.edu.cn).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada (e-mail: rxlu@ieee.org).

C. Tang is with the School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China (e-mail: ctang@gzhu.edu.cn).

Digital Object Identifier 10.1109/LCOMM.2018.2842042

Let S be the set of all possible secrets and S_i be the set of all possible shares for each player P_i. An *authorised set* is defined as a subset of players who are legal to recover the secret. The collection of all of authorised sets is called *access structure* denoted as Γ.

Definition 1 (Secret Sharing Scheme): A secret sharing scheme, which realizes an access structure, has both secret distribution phase and secret reconstruction phase, where distribution algorithm $\mathbf{Dis}$ *and reconstruction algorithm* $\mathbf{Rec}$ *are used to distribute the secret and recover the secret, respectively.*

- ***Secret distribution phase.*** *D divides a secret s into n shares, that is, $\mathbf{Dis}(s) = (s_1, s_2, \ldots, s_n)$, and sends the share s_i to the player P_i privately.*
- ***Secret reconstruction phase.*** *Players in $A \in \Gamma$ collect their shares to recover the secret in the way of $\mathbf{Rec}(s_A) = s$.*

In addition, it also necessarily satisfies two requirements, namely, 1) secret is recovered by the set in Γ correctly; 2) no information about the secret is obtained by the participants in subset $B \notin \Gamma$.

If the number of participants in each authorised subset of all n players is t or more than t, and the number of participants in subset $B \notin \Gamma$ is $t-1$ or less than $t-1$, we call t is the threshold value. For instance, Shamir's secret scheme [6] is usually considered a (t, n) threshold secret sharing scheme.

B. Communication Efficiency of Secret Sharing

We then give the definition of communication rate which measures the communication efficiency.

Definition 2 (Communication Rate): Let Π be a secret sharing scheme for an access structure Γ, the communication rate for $A \in \Gamma$ is defined as $\rho = H(S)/\sum_{P_i \in A} H(S_i)$.

The symbol $H(S)$ indicates the 'uncertainty' of the secret $s \in S$ and can be seen as the 'size' of secret. Similarly, the value of $H(S_i)$ can represents the 'size' of share $s_i \in S_i$ given to P_i. Note that, this quantity $H(S)$ is actually defined as *entropy* [7].

Wang and Wong [8] provided the upper bound of the communication rate for a threshold secret sharing scheme with the following lemma.

Lemma 1 [8]: Let Π be a (t, n)-threshold secret sharing scheme, for any $A \subseteq \mathcal{P}$ and $A \in \Gamma$, we have $\rho \leq \dfrac{|A| - t + 1}{|A|}$.

Wang and Wong claimed that the communication rate of secret reconstruction for A is $\rho = v/[v + t - 1]$ from Lemma 1 when $l \geq t + v - 1$ and it is the upper bound, while the communication rate of A is $\rho = v/[(v - l + t)l]$ when $l < t + v - 1$, which is far less than the upper bound.

III. Our Secret Reconstruction Scheme

A. Description of Our Secret Reconstruction Scheme

Recall that each involved player needs to present the whole share or the continued components in the last part of each share to recover the secret in Wang-Wong's scheme [8]. Different from Wang-Wong's scheme, each player will select components of share in a discontinued way to rebuild the secret in our scheme. We call it as "*jumping skill*", since this selection way means that someone jumps from one point to another. Specifically, we assume that the share of each player consists of several components such as $(a_1, a_2, \ldots, a_9)$, as shown in Fig. 1. The chosen components of share are $a_4, \ldots, a_9$ in Wong-Wang's scheme [8], while they are a_4, a_7, a_9 in our proposed scheme.

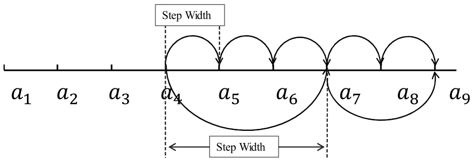

Fig. 1. An example for "jumping skill".

We claim that the one jump from a_i to a_j is named *step* and the *step width* of the window is defined as $j - i$. Clearly, there are 5 steps in Wang-Wong's scheme and all step widths are 1, while there are only two steps (from a_4 to a_7 and from a_7 to a_9) in our scheme and the step widths are $3 = 7 - 4$ (from a_4 to a_7) and $2 = 9 - 7$ (from a_7 to a_9) respectively. The details of our secret reconstruction scheme is described as follows.

Assume that $S = GF(q)^v$ is the set of secret for some integer v and prime power $q > n + v$. Let $x_1, x_2, \ldots, x_n \in GF(q)\backslash\{1, 2, \ldots, v\}$ be public distinct values and $s = (r_1, r_2, \ldots, r_v) \in GF(q)^v$ be a secret and t is the threshold value. We note that the distribution phase in our scheme is the same as that in Wang-Wong's secret sharing scheme.

1) Secret Distribution Phase: The dealer D chooses randomly a set of polynomials $(f_1(x), f_2(x), \ldots, f_v(x))$ over $GF(q)$ with the degree $t + i - 2$, for $i = 1, 2, \ldots, v$, such that,

$$\begin{aligned} &f_1(1) = r_1;\\ &f_2(1) = r_1, f_2(2) = r_2;\\ &f_3(1) = r_1, f_3(2) = r_2, f_3(3) = r_3;\\ &\quad\vdots\\ &f_v(1) = r_1, f_v(2) = r_2, f_v(3) = r_3, \ldots, f_v(v) = r_v. \end{aligned}$$

Finally, the dealer sends $s_j = (f_1(x_j), f_2(x_j), \ldots, f_v(x_j)) \in GF(q)^v$ as the share to player P_j privately for $j = 1, 2, \ldots, n$.

2) Secret Reconstruction Phase: Assume the players in A where $|A| = l$ and $t \leq l < t + v - 1$ work together to recover the secret s, and $l > v$. Without loss of generality, let $A = \{P_1, P_2, \ldots, P_l\}$. There are two choices according to the values of k, where $v \equiv k \pmod{l - t + 1}$.

- When $k = 0$, it implies v is the multiple of $l - t + 1$ and the last step width is $l - t + 1$, each participant P_j in A, for $j = 1, 2, \ldots, l$, affords some special components of their shares as follows, $(f_{l-t+1}(x_j), f_{2(l-t+1)}(x_j), f_{3(l-t+1)}(x_j), \ldots, f_v(x_j))$. All participants recover the polynomial $f_{l-t+1}(x)$, $f_{2(l-t+1)}(x)$, and so on, until $f_v(x)$. The secret is computed easily via $f_v(i)$ for $i = 1, 2, \ldots, v$.
- When $k \neq 0$, in other words, the last step width is k. Any $t + k - 1$ participants from A, there is no harm in assuming $P_1, P_2, \ldots, P_{t+k-1}$,

contribute their partial components, $(f_{l-t+1}(x_j), f_{2(l-t+1)}(x_j), f_{3(l-t+1)}(x_j), \dots, f_{v-k}(x_j), f_v(x_j))$, for $j = 1, 2, \dots, t+k-1$. The rest of $l-(t+k-1)$ participants provide the following components, $(f_{l-t+1}(x_j), f_{2(l-t+1)}(x_j), f_{3(l-t+1)}(x_j), \dots, f_{v-k}(x_j))$, for $j = t+k-1, \dots, l$. All participants recover the polynomial $f_{l-t+1}(x)$, $f_{2(l-t+1)}(x)$, and so on, until $f_{v-k}(x)$ and $f_v(x)$. The secret is computed easily via $f_v(i)$ for $i = 1, 2, \dots, v$.

It is noted that in Wang-Wong's reconstruction scheme, there are $v-l+t$ polynomials to be recovered, while our scheme only recovers $v/(l-t+1)$ polynomials when $k=0$, or $[(v-k)/(l-t+1)]+1$ polynomials when $k \neq 0$. This indicates that the number of polynomial recovered in the secret reconstruction phase is fewer than that of Wang-Wong's scheme. Since the computation complexity of recovering each interpolation polynomial f_i is $O({m_i}^2)$ where m_i is the degree of each polynomial f_i, we conclude that complexity of recovering f_v in both schemes are in the same scale.

B. Main Results

We here prove our proposed scheme satisfies the correctness of secret sharing scheme claimed in Definition 1. Note that the privacy is obvious because our scheme is constructed based on Shamir's threshold secret sharing scheme via the polynomial over the finite field.

Theorem 1: Let Π *denote the proposed scheme above, the participants in the authorized set* A $(|A| = l, t \leq l < t+v-1)$ *can work together to recover the secret* $s = (r_1, r_2, \dots, r_v)$ *correctly.*

Proof: There are two cases to reconstruct the secret considering $k=0$ and $k \neq 0$. Actually, their processes of reconstruction are same. Thus, we prove the correctness when $k \neq 0$ only as follows. Let $A = \{P_1, P_2, \dots, P_l\}$, and P_j provides $(f_{l-t+1}(x_j), f_{2(l-t+1)}(x_j), f_{3(l-t+1)}(x_j), \dots, f_{v-k}(x_j))$ for $j = 1, \dots, l$. There are l values $f_{l-t+1}(x_1), f_{l-t+1}(x_2), \dots, f_{l-t+1}(x_l)$, then the polynomial $f_{l-t+1}(x)$ is reconstructed because the degree of $f_{l-t+1}(x)$ is $l-1$. The values, $f_{l-t+1}(1), f_{l-t+1}(2), \dots, f_{l-t+1}(l-t+1)$, are computed by the polynomial $f_{l-t+1}(x)$, and they are used to recover the second polynomial $f_{2(l-t+1)}(x)$ with the help of the components of share $f_{2(l-t+1)}(x_1), f_{2(l-t+1)}(x_2), \dots, f_{2(l-t+1)}(x_l)$. The polynomials $f_{j(l-t+1)}(x)$ for $j = 3, 4, \dots, (v-k)/(l-t+1)$ are recovered in the same way. Finally, the last polynomial $f_v(x)$ is reconstructed by any $t+k-1$ components of the set $\{f_v(x_1), \dots, f_v(x_l)\}$ together with the known $v-k$ values $f_v(1), f_v(2), \dots, f_v(v-k)$ via computing from $f_{v-k}(x)$. In a nutshell, all secrets $(r_1, \dots, r_v)$ are computed as $r_i = f_v(i)$. ■

From Theorem 1, we know that the recovery of secret is guaranteed even if we reduce the number of shares that are used for reconstructing the secret. From Definition 2, the information rate is represented via the size of secret and share. Intuitively, the information rate is also represented by the number of the components since there are several components in each secret or share in our scheme. When we calculate the information rate in the secret reconstruction, the size of secret is a fixed parameter. However, the size of all shares is variable as it is determined by the number of components contributed by all participants.

Lemma 2: Let w *be the number of steps, if* w *is fixed, the total number of components of shares involved in secret reconstruction required is invariant and irrelevant to the step width of each step.*

Proof: Assume that the participants in the authorized set $A = \{P_1, P_2, \dots, P_l\} \in \Gamma$ reconstruct the secret via recovering the polynomial $f_v(x)$, and they compute the polynomial $f_v(x)$ with two methods and w steps as follows, *Method 1*:

$$f_{a_1}(x) \xrightarrow{\text{step1}} \dots \xrightarrow{\text{step}(w-1)} f_{a_w}(x) \xrightarrow{\text{step}w} f_v(x)$$

and *Method 2*:

$$f_{b_1}(x) \xrightarrow{\text{step1}} \dots \xrightarrow{\text{step}(w-1)} f_{b_w}(x) \xrightarrow{\text{step}w} f_v(x).$$

We first compute the polynomial $f_{c_1}(x)$ where $c_1 \in \{a_1, b_1\}$, and then compute $f_{c_2}(x)$, and so on, until the final polynomial $f_v(x)$. Concretely, the polynomial $f_{a_1}(x)$ with degree $t+a_1-2$ is reconstructed by $t+a_1-1$ components located in the a_1-th position of shares provided by participants in A. The polynomial $f_{a_2}(x)$ with degree $t+a_2-2$ is computed by any $t+a_2-a_1-1$ components from $\{f_{a_2}(x_1), f_{a_2}(x_2), \dots, f_{a_2}(x_l)\}$ located in the a_2-th position of shares and a_1 values $f_{a_2}(1) = f_{a_1}(1), f_{a_2}(2) = f_{a_1}(2), \dots, f_{a_2}(a_1) = f_{a_1}(a_1)$ calculated via $f_{a_1}(x)$. Similarly, we can reconstruct the polynomial $f_{a_w}(x)$. Finally, the polynomial $f_v(x)$ is computed with the help of any $t+v-a_w-1$ components from $\{f_v(x_1), \dots, f_v(x_l)\}$ located in the v-th position of shares and the a_w values $f_v(1) = f_{a_w}(1), f_v(2) = f_{a_w}(2), \dots, f_v(a_w) = f_{a_w}(a_w)$ calculated via $f_{a_w}(x)$. Therefore, the total of components involved in the secret reconstruction in method 1 is $tw+v-w = (t+a_1-1)+(t+a_2-a_1-1)+\cdots+(t+v-a_w-1)$. It is also trivial to compute the total of components involved in the secret reconstruction in method 2 as $tw+v-w = (t+b_1-1)+(t+b_2-b_1-1)+\cdots+(t+v-b_w-1)$, and the resultant value is identical to that in method 1. As a result, we have proved this lemma. ■

Lemma 3: Assume that $l = |A|$ *where* $A \in \Gamma$ *and* l *is predefined, and the number of steps* w *is variant, then the information rate in our secret reconstruction is*

$$\rho = \begin{cases} \dfrac{v}{(w+1)l}, & \textit{where} \dfrac{v}{l-t+1} - 1 \leq w, \ \textit{if } k=0; \\ \dfrac{v}{wl+t+k-1}, & \textit{where} \dfrac{v-k}{l-t+1} \leq w, \ \textit{if } k \neq 0. \end{cases} \tag{1}$$

Here, $w \leq v-1, v \equiv k \pmod{l-t+1}$. *Furthermore, the function of* ρ *is decreasing when* w *is increasing.*

Proof: From Lemma 2, we know that the total number of components of shares involved in our scheme is determined by the number of steps w. Given the value l which is the number of participants working together to recover the secret, the total number of components of shares involved is a function only related to w. If $k=0$, l participants provide some components of their shares, $(f_{l-t+1}(x_j), f_{2(l-t+1)}(x_j), f_{3(l-t+1)}(x_j), \dots, f_v(x_j))$, for $j = 1, \dots, l$, to recover $f_v(x)$ with w steps. Then, there are $w+1$ groups $\{f_i(l-t+1)(x_j), f_v(x_j)\}$ for $i = 1, 2, \dots, w$. The total number of components of shares involved is $(w+1)l$. Actually, the information rate is $\rho = v/[(w+1)l]$. If $k \neq 0$, l participants recover $f_v(x)$ with w steps by contributing the some components of their shares, $(f_{l-t+1}(x_j), f_{2(l-t+1)}(x_j), f_{3(l-t+1)}(x_j), \ldots, f_{v-k}(x_j))$ and any $t+k-1$ components from $\{f_v(x_j)\}$, for $j = 1, \ldots, l$. Then, there are w groups $\{f_{i(l-t+1)}(x_j)\}$ and 1 group $\{f_v(x_{j_m})\}$ for $m = 1, \ldots, t+k-1$. Actually, the information rate is $\rho = v/(wl+t+k-1)$. So, we get the Eq.(1), which is a decreasing function obviously. ■

Theorem 2: The information rate ρ in our secret reconstruction is optimal.

Proof: Assume that there are l participants involved in scheme. If the step width is $l-t+2$ and the first jump is from $f_{l-t+1}(x)$ to $f_{2(l-t+1)+1}(x)$, then we need $l-t+1$ known values from $f_{2(l-t+1)+1}(x)$ and $l+1$ extra values from different participants to recover the polynomial $f_{2(l-t+1)+1}(x)$ of degree $2l-t+1$. However, it is contradictory to the fact that l participants can only produce l extra values. As a result, we conclude that the maximal step width is $l-t+1$ except the last step. The maximal step width implies that the number of steps w is minimal. From Lemmas 2 and 3, we know that the communication rate ρ in our reconstruction scheme is maximum when the number of steps is minimal, because ρ is a decreasing function. As a result, our scheme is optimal in communication efficiency. ■

Wang and Wong [8] claimed that the communication rate of A is $\rho = v/[(v-l+t)l]$ if $l < t+v-1$. The communication rate in our proposed secret reconstruction scheme is higher than in Wang-Wong's scheme. The communication efficiency in our scheme is the same as that in Bitar-Rouayheb's scheme if $k = 0$ even though our scheme is based on polynomial and does not split each component into smaller symbols; and it is near Bitar-Rouayheb's case if $k \neq 0$. We note that the parameter q of $GF(q)$ is greater than $n+v$ in both Wang-Wong's scheme and our scheme, while q is greater than n in Bitar-Rouayheb's scheme.

IV. Comparison of Efficiency

The simulation results indicate that our scheme is the upper bound when the step width is maximum for any $t \leq l < t+v-1$. Let $t = 51$, $v = 50$, and $l = 52, 53, \ldots, 99$, we give the diagram to compare the information rate of our secret reconstruction with that of Wang-Wong's scheme in Figures 2 and 3, under the following three cases: 1) the step width $k_1 = l-t+1$, 2) the step width $k_2 = l-t-2$, and 3) the step width $k_3 = 1$ (this is for Wang-Wong's scheme).

As shown in Fig. 2, it is clear that both lines of the number of steps in our scheme are below the line in Wang-Wong's scheme, that is, the number of steps in our scheme is less than in Wang-Wong's scheme. From Lemma 3, the corresponding communication rates ρ in our scheme are higher than that in Wang-Wong's scheme, so the lines of communication rate in our scheme is above the line of Wang-Wong's scheme in Fig. 3. We further know that the number of steps decrease slowly in Wang-Wong's scheme, while in our scheme it is rapid. Similarly, the communication rate ρ in Wang-Wong' scheme grows very slowly until the number of participants involved is close to 100, while the ρ in our scheme increases rapidly even if there are fewer participants. Besides, from both lines on the top and on the bottom in Figures 2 and 3 respectively, we know that for the same l, if the step width is bigger, the w is smaller. This implies that the communication rate ρ is larger as well since there are fewer components. Therefore, from Fig. 3, we can see our scheme outperforms Wang-Wong's scheme.

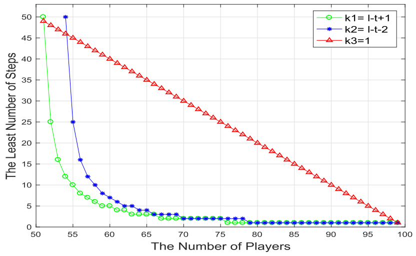

Fig. 2. Minimum steps number for each l.

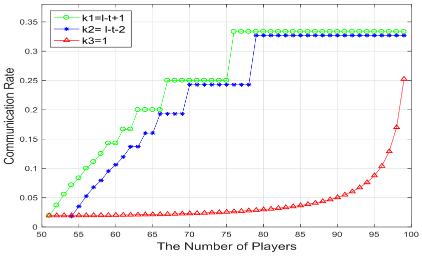

Fig. 3. The communication rate for each l.

V. Conclusion

We have studied the communication efficiency problems on the secret reconstruction phase. Specifically, we proposed a new strategy, called as "jumping skill", and used it to build a communication efficient secret reconstruction scheme. We found a kind of relationship between the number of participants who work together to recover the secret and the count of steps, and also showed that for different number of participants, the number of components of shares is only related to the step width if it is fixed. Finally, we proved that the communication efficiency of our proposed scheme is optimal bound.

References

[1] R. Bitar and S. E. Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," *IEEE Trans. Inf. Theory*, vol. 64, no. 2, pp. 933–934, Feb. 2018.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Amer. Fed. Inf. Process. Soc. (AFIPS)*, 1979, pp. 313–317.

[3] W. T. Huang *et al.*, "Communication efficient secret sharing," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7195–7206, Dec. 2016.

[4] K. M. Martin *et al.*, "Bounds and techniques for efficient redistribution of secret shares to new access structures," *Comput. J.*, vol. 42, no. 8, pp. 638–649, 1999.

[5] R. Safavi-Naini and H. Wang, "Secret sharing schemes with partial broadcast channels," *Des., Codes Cryptogr.*, vol. 41, no. 1, pp. 5–22, 2006.

[6] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[7] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. London, U.K.: Chapman & Hall, 2005.

[8] H. X. Wang and D. S. Wong, "On secret reconstruction in secret sharing schemes," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 473–480, Jan. 2008.

[9] Z. F. Zhang *et al.*, "Threshold changeable secret sharing schemes revisited," *Theor. Comput. Sci.*, vol. 418, pp. 106–115, Feb. 2012.