IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 7, 2019, accepted November 12, 2019, date of publication November 20, 2019, date of current version December 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2954672

A New Secure Encryption Scheme Based on Group Factorization Problem

YUE CONG[1], HAIBO HONG[2], JUN SHAO[2], SONG HAN[2], JIANHONG LIN[3], AND SHUAI ZHAO[2,4]

[1]Zhejiang Agricultural Business College, Shaoxing 312088, China
[2]School of Computer science and Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, China
[3]Zhejiang Ponshine Information Technology Company, Hangzhou 310000, China
[4]Computing Center, Zhejiang Gongshang University, Hangzhou 310018, China

Corresponding author: Haibo Hong (honghaibo1985@163.com).

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61602408, Grant 61972050, Grant 61972352, and Grant U1709217, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY19F020005, Grant LY18F020026, and Grant LZ18F020003, and in part by the Key Research and Development Program of Hangzhou under Grant 20182011A46.

ABSTRACT As special types of factorization of finite groups, logarithmic signatures and covers have been used as the main components of cryptographic keys for secret key cryptosystems such as *PGM* and public key cryptosystems like MST_1, MST_2, MST_3 and $eMST_3$. In particular, as a natural analogue of integer factorization problem (IFP), group factorization problem (GFP) and its hardness assumption over certain factorization basis, referred as logarithmic signature, play a core role in the security arguments for the family of *MST* cryptosystems. Security is not the unique goal of designing a cryptosystem. Instead, efficiency is also a major issue. In this paper, we design a new secure encryption scheme based on group factorization problem (GFP). Furthermore, we present the security analysis and demonstrate the performance of our scheme. Comparing with $eMST_3$, our scheme is simplified with more efficiency.

INDEX TERMS Encryption scheme, group factorization problem, logarithmic signatures, random covers.

I. INTRODUCTION

Nowadays, the security of many public key cryptosystems is based on the hardness assumptions of certain problems over finite abelian algebraic structures such as cyclic groups and finite fields. Two well-known hard problems are the integer factorization problem (IFP) and discrete logarithm problem (DLP) [14], [18], [20], [39]. However, Shor's and other quantum algorithms [22], [37], [41], [42] can solve the IFP and DLP in polynomial time. For instance, Grover's algorithm [22] can improve brute-force attacks by significantly reducing search spaces for private keys. In other words, these hardness assumptions would be broken if quantum computers become practical [31], [34], [35]. Note that the theoretical foundations for many current public cryptographic primitives lie in the intractability of mathematical problems closer to number theory than group theory. Number theory deals mostly with abelian groups. It is well known that non-commutative algebraic structures can increase the hardness of some mathematical problems significantly [7], [9], [36]. Therefore, it is meaningful to design secure and efficient cryptosystems based on non-abelian algebraic structures.

It is always remained an attractive aspect for researchers to study the underlying intractable assumptions of mathematical problems for cryptographic primitives. Regarding the non-commutative cryptography, the related work started from 1980's, when the difficult problems in group theory were incorporated into cryptographic domain. In 1984, Wagner and Magyarik [50] devised a public key cryptosystem on the basis of undecidable word problem in groups and semigroups. After that, Birget *et al.* [8] pointed out that Wagner's method is not based on the word problem but on a simpler assumption. Furthermore, they designed a new public key cryptosystem based on the word problem in finite generated groups. In 1999, Anshel *et al.* [1] put forward a key exchange protocol based on the intractability of the solving equation problem in non-abelian groups. At the same time, they claimed that the braid group can be used as a platform in public key cryptosystems. Subsequently, Dehornoy [15], [26] systematically developed the braid group cryptography on the basis of conjugacy search problem (CSP). In 2002, Grigoriev and Ponomarenko [21] proposed the first homomorphic

The associate editor coordinating the review of this manuscript and approving it for publication was Tony Thomas.

encryption scheme based on non-abelian groups. The corresponding intractable assumption is the membership problem (MP) in the integer matrix group. Hereafter, Eick [17], Shpilrain and Ushakov [46] and Baumslag *et al.* [6] et al. raised several public key cryptosystems on the basis of polycyclic groups and linear groups. In 2006, Cao *et al.* [12] recommended an innovative perspective for designing public key cryptosystems based on non-commutative rings. Since 2009, Habeeb *et al.* [23], [27]–[29] brought forward a series of key exchange protocols and public key encryption schemes based on group ring matrices, corresponding intractable assumptions are reported to be DLP and factorization problem (FP) in group ring matrices, respectively. Afterwards, Eftekhari [16], [33], [36], [40] gave an efficient quantum algorithm in polynomial complexity on the DLP in group ring matrices. Recently, algebraic eraser (AE) has also become a typical representative of non-commutative cryptography because of its potential to resist against known quantum attacks [2]–[5].

At the same time, group factorization problem (GFP) has gradually become a typical intractable assumption in group theory [13], [30], [32], [43], [48]. A type of cryptosystems based on GFP has achieved rapid development in recent thirty years. From 1986 to 2010, Lempken *et al.* [30], [32], [43], [48] have made great achievements on devising cryptosystems based on logarithmic signatures and covers in non-abelian groups. Especially in 2009, Lempken *et al.* [30] put forward a practical platform—Suzuki 2-group [25] and put *MST* cryptosystems into practice. In 2013, Svaba *et al.* [44] analyzed the LS in finite abelian groups in detail, and devised an efficient factorization algorithm with respect to (fused) transversal logarithmic signatures. In 2017, Hong *et al.* [24] made some progress towards searching the minimal length key for *MST* cryptosystems and presented a theoretical proof for MLS conjecture. In the same year, Reichl [38] specifically discussed GFP in finite abelian groups, and proposed an efficient algorithm for factorizing logarithmic signatures. In 2018, van Trung [47] put forward a general method of constructing strong aperiodic logarithmic signatures for abelian p-groups, and promoted the practical application of *MST* cryptosystems. So far, *MST* cryptosystems are not known to be susceptible to quantum algorithm attacks, which makes them viable to be candidates for post-quantum public-key cryptography.

A. OUR MOTIVATIONS AND CONTRIBUTIONS

Our main motivation is to design a new secure encryption scheme based on random covers and logarithmic signatures. Comparing with known schemes, our scheme has higher efficiency.

The remaining paper is organized as follows: In Section 2, we review the related results in *MST* cryptosystems; In Section 3, we specifically presents our proposal along with its security analysis; The performance and illustrations are introduced in Section 4.

II. PRELIMINARIES

A. COVER, LOGARITHMIC SIGNATURE AND GROUP FACTORIZATION PROBLEM

Definition 1 (Cover and Logarithmic Signature [30], [48]): Let $\mathbb{G}$ be a finite group, $\mathbb{A} \subseteq \mathbb{G}$. Let $\alpha = [A_1, \cdots, A_k]$ be the ordered sequence of subsets A_i in $\mathbb{G}$ such that $A_i = [a_{i1}, \cdots, a_{ir_i}]$ with $a_{ij} \in \mathbb{G}$ $(1 \leq j \leq r_i)$. Then, α is called a **cover** for $\mathbb{G}$ (or $\mathbb{A}$) if each $g \in \mathbb{G}$ (or $\mathbb{A}$) can be represented as a product

$$g = a_{1j_1} \cdots a_{kj_k} \tag{1}$$

with $a_{ij_i} \in A_i$ $(1 \leq i \leq k)$. If each $g \in \mathbb{G}$(or $\mathbb{A}$) can be expressed in an unique way, then α is said to be a **logarithmic signature** for $\mathbb{G}$ (or $\mathbb{A}$).

The sequences A_i are called the **blocks**, the vector $(r_1, \cdots, r_k)$ with $r_i = |A_i|$ is the **type** of α, the **length** of α is defined to be $l(\alpha) = \sum_{i=1}^{k} r_i$. If the factorization aforementioned (1) can be achieved in polynomial with $\lceil \log_2 |\mathbb{G}| \rceil$, then α is called **tame** (**factorizable**).

Definition 2 (Cover (Logarithmic Signature) Mappings [30], [48]): Let $\alpha = [A_1, A_2, \cdots, A_k]$ be a cover (logarithmic signature) for $\mathbb{G}$ of type $(r_1, r_2, \cdots, r_k)$ with $A_i = [a_{i,1}, a_{i,2}, \cdots, a_{i,r_i}]$, let j_i be integers, $1 \leq j_i \leq r_i$, and let $m = \prod_{i=1}^{k} r_i$. Let $m_1 = 1$ and $m_i = \prod_{j=1}^{i-1} r_j$ for $i = 2, \cdots, k$. Consider the maps λ_α and θ_α defined by

$$\begin{aligned} \lambda_\alpha : \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_k} &\to \mathbb{Z}_m \\ (j_1, j_2, \cdots, j_k) &\mapsto \sum_{i=1}^{k} j_i m_i. \end{aligned} \tag{2}$$

and

$$\begin{aligned} \theta_\alpha : \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_k} &\to \mathbb{G} \\ (j_1, j_2, \cdots, j_k) &\mapsto a_{1j_1} \cdot a_{2j_2} \cdots a_{kj_k} \end{aligned} \tag{3}$$

Note that λ_α is a bijection, and both λ_α and λ_α^{-1} are efficiently computable. Define the surjective (bijection) map

$$\tilde{\alpha} : \mathbb{Z}_m \to \mathbb{G} x \mapsto \theta_\alpha(\lambda_\alpha^{-1}(x)) = a_{1j_1} \cdot a_{2j_2} \cdots a_{kj_k} \tag{4}$$

Cryptographic Hypothesis 1 (Group Factorization Problem [43], [49]): Let $\alpha = [A_1, A_2, \cdots, A_k]$ be a cover (logarithmic signature) for $\mathbb{G}$ of type $(r_1, r_2, \cdots, r_k)$ with $A_i = [a_{i,1}, a_{i,2}, \cdots, a_{i,r_i}]$, then the map $\tilde{\alpha} : \mathbb{Z}_m \to \mathbb{G}$ induced by α with $m = \prod_{i=1}^{k} r_i$ is a one-way function.

Remark 1: As described as Cryptographic Hypothesis 1, the complexity of solving the GFP depends on m. According to [43], when $\mathbb{G}$ is a cyclic group, the GFP with respect to α amounts to solving the discrete logarithm problem (DLP) in $\mathbb{G}$. In view of the fact that non-commutative algebraic structures can increase the hardness of some mathematical problems significantly, the complexity of GFP in non-abelian groups such as the Suzuki 2-group is much more intractable. In fact, let $|\mathbb{G}| = \prod_{j=1}^{k} p_j^{b_j}$ be the prime power decomposition of $|\mathbb{G}|$, we have that $l(\alpha) \geq \sum_{j=1}^{k} b_j p_j$. When $l(\alpha) = \sum_{j=1}^{k} b_j p_j$, it follows that $m = \prod_{i=1}^{k} r_i = \prod_{j=1}^{k} p_j^{b_j}$ is exponential based on non-abelian generators p_j for $1 \leq j \leq k$. In other words, it is in general an intractable problem to find a factorization $g = a_{1j_1} \cdot a_{2j_2} \cdots a_{kj_k}$ for the given group $\mathbb{G}$ and an element $g \in \mathbb{G}$.

B. MST_3 CRYPTOSYSTEMS AND THE SUZUKI 2-GROUP

In 2002, Lempken *et al.* [30] devised an encryption scheme named MST_3 by using logarithmic signatures and random covers. In this scheme, the secret key are a tame logarithmic signature and several random numbers, the public key are a random cover and its sandwich transform. Subsequently, Blackburn *et al.* [10] specifically analysed MST_3 cryptosystem and put forward effective attacks based on this scheme. Furthermore, in order to overcome known attacks, Svaba and Van Trung [43] proposed an enhanced version named $eMST_3$ cryptosystem. In order to improve the security of this scheme, the authors took advantage of a secret homomorphism to protect the secret logarithmic signature. Meanwhile, they utilized random numbers to realize probabilistic encryption.

So far, the only platform of MST cryptosystems is the Suzuki 2-group of order q^2 with $q = 2^{\kappa}(\kappa \geq 3)$ [30], [43]. Also, the Suzuki 2-group of order q^2 can be denoted by $A(\kappa, \theta)$, where θ is an automorphism of $\mathbb{F}_q$ with an odd order. Moreover, the group $A(\kappa, \theta)$ can be represented by a matrix group $\mathbb{G} = \{S(a, b) | a, b \in \mathbb{F}_q\}$, where

$$S(a, b) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^{\theta} \\ 0 & 0 & 1 \end{pmatrix} \tag{5}$$

is a 3×3 matrix over $\mathbb{F}_q$. Therefore, $\mathbb{G}$ is of order q^2 and the center $\mathcal{Z}(\mathbb{G}) = \{S(0, b) | b \in \mathbb{F}_q\}$. In order to store the group elements conveniently, $S(a, b)$ can be denoted by (a, b, a^{θ}), then the product of two elements in group $\mathbb{G}$ is

$$\begin{aligned} S(a_1, b_1)S(a_2, b_2) &= S(a_1, b_1, a_1^{\theta})S(a_2, b_2, a_2^{\theta}) \\ &= (a_1 + a_2, b_1 + b_2 + a_1 a_2^{\theta}, a_1^{\theta} + a_2^{\theta}) \end{aligned} \tag{6}$$

In addition, the inverse of an element in group $\mathbb{G}$ can be expressed as

$$S(a, b, a^{\theta})^{-1} = S(a, a^{\theta} \cdot a + b, a^{\theta}) = S(a, a^{\theta+1} + b, a^{\theta}) \tag{7}$$

and it also requires one multiplication and one addition in $\mathbb{F}_q$. If $g = S(a, b) \in \mathbb{G}$, $a, b \in \mathbb{F}_q$, then a and b can be denoted by $g_{\cdot x}$ and $g_{\cdot y}$, respectively. Thus, we have that $g = S(g_{\cdot x}, g_{\cdot y})$. For clarity, we would like to introduce the notations used in this paper (See Table 1).

III. MAIN RESULTS

Compared with $eMST_3$, a few changes have taken place in public key γ, the ciphertext pairs of our proposal are independent of each other, and the encryption process is also simplified.

TABLE 1. Notations used in this paper.

$\mathbb{F}_q$	the finite field defined on q, where $q = 2^{\kappa}(\kappa \geq 3)$
θ	an automorphism of $\mathbb{F}_q$ with an odd order
$A(\kappa, \theta)$	the Suzuki 2-group of order q^2
$\mathcal{Z}$	the center of $A(\kappa, \theta)$
$\underset{s}{\approx}$	two sample spaces are statistically indistinguishable

A. FULL SCHEME

1) `KeyGen`(κ): Let κ be the system security parameter, $\mathbb{G} = A(\kappa, \theta)$ be the Suzuki 2-group with order q^2, and the message space $\mathcal{Z} = \{S(0, b) | b \in \mathbb{F}_q\}$ be the center of $\mathbb{G}$, where $q = 2^{\kappa}(\kappa \geq 3)$. Then it outputs the public key $[\alpha, \gamma]$ and the corresponding private key $[\beta, (t_0, \cdots, t_k), f]$.
   - Choose a tame logarithmic signature $\beta = [B_1, B_2, \cdots, B_k] = (b_{ij}) = (S(0, b_{(ij)\cdot y}))$ of type $(r_1, r_2, \cdots, r_k)$ for $\mathcal{Z}$, where $b_{ij} \in \mathcal{Z}$ and $b_{(ij)\cdot y} \in \mathbb{F}_q$;
   - Select a random cover $\alpha = [A_1, A_2, \cdots, A_k] = (a_{ij}) = (S(a_{(ij)\cdot x}, a_{(ij)\cdot y}))$ of the same type as β for a subset A of $\mathbb{G}$ such that $A_1, \cdots, A_k \subseteq \mathbb{G} \backslash \mathcal{Z}$, where $a_{ij} \in \mathbb{G} \backslash \mathcal{Z}$, $a_{(ij)\cdot x} \in \mathbb{F}_q \backslash \{0\}$ and $a_{(ij)\cdot y} \in \mathbb{F}_q$;
   - Choose $t_0, t_1 \cdots, t_k \in \mathbb{G} \backslash \mathcal{Z}$;
   - Construct a secret homomorphism $f : \mathbb{G} \rightarrow \mathcal{Z}$;
   - Compute $\gamma := (h_{ij}) = (S(h_{(ij)\cdot x}, h_{(ij)\cdot y}))$, where $h_{ij} = t_{i-1}^{-1} \cdot f(a_{ij}) \cdot b_{ij} \cdot t_i$;
   - Output public key pk $= [\alpha, \gamma]$ and private key sk $= [\beta, (t_0, \cdots, t_k), f]$.
2) `Enc`(pk, m): For a message $m \in \mathcal{Z}$, the ciphertext is a pair (y_1, y_2) which is produced as follows:
   - Select a random number $R \in \mathbb{Z}_{|\mathcal{Z}|}$;
   - Compute

$$\begin{aligned} y_1 &= \tilde{\alpha}(R) \cdot m \\ y_2 &= \tilde{\gamma}(R) \\ &= t_0^{-1} \cdot f(\tilde{\alpha}(R)) \cdot \tilde{\beta}(R) \cdot t_k; \end{aligned} \tag{8}$$

   - Output (y_1, y_2).
3) `Dec`(sk, C): For the ciphertext pair $(y_1, y_2) \in \mathbb{G} \times \mathbb{G}$, the user utilizes private key $[\beta, (t_0, \cdots, t_k), f]$ to calculate a plaintext $m' \in \mathcal{Z}$ as follows:
   - Compute $R' = \tilde{\beta}^{-1}(y_2 t_k^{-1} f(y_1)^{-1} t_0)$;
   - Compute $m' = \tilde{\alpha}(R')^{-1} \cdot y_1$;
   - Output m'.

Theorem 1 (Correctness): The aforementioned encryption scheme is consistent.

Proof 1: For a valid ciphertext pair $(y_1, y_2) \in \mathbb{G} \times \mathbb{G}$, it follows that

$$\begin{aligned} y_1 &= \tilde{\alpha}(R) \cdot m \\ y_2 &= \tilde{\gamma}(R) \\ &= b_{1j_i} t_0^{-1} f(a_{1j_1}) t_1 \cdots b_{kj_k} t_{k-1}^{-1} f(a_{kj_k}) t_k \\ &= b_{1j_i} b_{2j_2} \cdots b_{kj_k} t_0^{-1} f(a_{1j_1} a_{2j_3} \cdots a_{kj_k}) t_k \end{aligned}$$

$$
\begin{aligned}
&= \tilde{\beta}(R)\cdot t_0^{-1}\cdot f(\tilde{\alpha}(R))\cdot t_k\\
&= \tilde{\beta}(R)\cdot t_0^{-1}\cdot f(\tilde{\alpha}(R)\cdot m)\cdot t_k\\
&= \tilde{\beta}(R)\cdot t_0^{-1}\cdot f(y_1)\cdot t_k\\
&\Rightarrow \tilde{\beta}(R) = y_2\cdot t_k^{-1}\cdot f(y_1)^{-1}\cdot t_0, \qquad (9)
\end{aligned}
$$

then using $\tilde{\beta}^{-1}$, we can recover the random number R by

$$\tilde{\beta}^{-1}(\tilde{\beta}(R)) = \tilde{\beta}^{-1}(y_2 t_k^{-1} f(y_1)^{-1} t_0) = R = R'. \qquad (10)$$

Consequently, using y_1 we can recover message m by

$$m' = \tilde{\alpha}(R')^{-1}\cdot y_1 = \tilde{\alpha}(R)^{-1}\cdot y_1 = m. \qquad (11)$$

B. SECURITY ANALYSIS

Now, we proceed to prove the security of the aforementioned construction. By using the classic techniques in [11], [19], our proposal can be easily proved to be IND-CCA2 secure in the standard model. Then, we briefly introduce the proof of our idea.

Theorem 2: The aforementioned proposal is indistinguishable against adaptively chosen ciphertext attacks (IND-CCA2) in standard model assuming that the GFP is intractable in $\mathbb{G}$.

Proof 2: If there exists an adversary $\mathcal{A}$, who can break the CCA security of the proposal, then the challenger $\mathcal{B}$ can solve the GFP in $\mathbb{G}$. The general ideas are presented as follows.

Setup $\mathcal{B}$ sets the public values α and γ, then sends them to $\mathcal{A}$. Clearly, $\mathcal{A}$ has no ideas about the corresponding private key $[\beta, (t_0, \cdots, t_k), f]$.

Phase 1 $\mathcal{B}$ builds the following decryption oracle.

- Decryption Oracle $\mathcal{O}_{dec}$: $\mathcal{A}$ sends a ciphertext $C = (y_1, y_2) \in \mathbb{G}\times\mathbb{G}$ to this oracle, $\mathcal{B}$ firstly computes $R = \tilde{\beta}^{-1}(y_2 t_k^{-1} f(y_1)^{-1} t_0)$ and searches whether R exists in Table T_{dec}. If it exists, $\mathcal{B}$ sends $m = \tilde{\alpha}(R)^{-1}\cdot y_1$ to $\mathcal{A}$; otherwise, $\mathcal{B}$ sends $\perp$ to $\mathcal{A}$.

Challenge $\mathcal{A}$ sends the challenger $\mathcal{B}$ two messages $m_0, m_1 \in \mathcal{Z}$ with the same matrix form. $\mathcal{B}$ computes the challenge ciphertext $C^* = (y_1^*, y_2^*)$ as follows:

- Choose a random R^* from $\mathbb{Z}_{|\mathcal{Z}|}$, and compute $y_2^* = \tilde{\gamma}(R^*)$.
- Compute $y_1^* = \tilde{\alpha}(R^*)\cdot m_\delta$, where δ is a random number from $\{0, 1\}$.

At last, $\mathcal{B}$ sends C^* to $\mathcal{A}$ as the challenge ciphertext.

Phase 2 It is almost the same as Phase 1, except that $\mathcal{A}$ can not directly send C^* to the decryption oracle $\mathcal{O}_{dec}$.

Guess $\mathcal{A}$ outputs the guess b' on b. $\mathcal{B}$ randomly chooses R' from Table T_{dec}, and sets R^* as R'. If $\mathcal{A}$ can output a correct guess, then R' is the correct R^* with probability $1/q_{dec}$ at least, where q_{dec} denotes the maximum number of queries to the decryption oracle $\mathcal{O}_{dec}$ by $\mathcal{A}$.

In analogy with the construction of FullIdent in [11], since q_{dec} is polynomially bounded, so $\mathcal{B}$ breaks the GFP with non-negligible probability $1/q_{dec}$. Specifically, suppose that $\mathcal{A}$'s advantage in guessing $b' = b$ is ϵ which is non-negligible, then $\mathcal{B}$'s advantage in breaking the GFP is about ϵ/q_{dec} which is also non-negligible. According to the classic conclusion in [11], [19], we have that: if no polynomially bounded adversary has a non-negligible advantage in breaking our scheme, the proposal is indistinguishable against adaptively chosen ciphertext attacks (IND-CCA2).

Remark 2: Apparently, one-wayness of our scheme depends on Cryptographic Hypothesis 1. Thence, we obtain corresponding security level in analogy with the method in [11], [19]. Here, we omit the proof of Theorem 2 and attempt to pave an unique path to verify the security of our scheme by using a heuristic method of analyzing the complexity of known attacks.

1) ATTACK ON SECRET KEY

a. In order to obtain the private key β and (t_0, t_k, f), the adversary attempt to extract useful information from the equation

$$\tilde{\beta}(R) = y_2\cdot t_k^{-1}\cdot f(y_1)^{-1}\cdot t_0 \qquad (12)$$

where $R\in\mathbb{Z}_{|\mathcal{Z}|}, y_1 = \tilde{\alpha}(R)\cdot m, y_2 = \tilde{\gamma}(R), f(y_1)^{-1}\in\mathcal{Z}$.

Specifically, the adversary takes advantage of enough values $\tilde{\beta}(R_i)$ to construct β by using the corresponding conclusion in [48]. If β is of type $(r_1, r_2, \cdots, r_k)$, then one can construct a logarithmic signature equivalent to β by using n selected values $\tilde{\beta}(R_i)$, where $n = 1 - k + \sum_{k=1}^{k} r_k$. Let $\{R_1, R_2, \cdots, R_n\}$ be a series of random numbers chosen by the adversary. Then

$$
\begin{aligned}
\tilde{\beta}(R_i) &= y_{i2} t_k^{-1} f(y_{i1})^{-1} t_0\\
&= f(y_{i1})^{-1} y_{i2} t_k^{-1} t_0\\
&\Rightarrow \tilde{\beta}(R_i) f(y_{i1}) = y_{i2} t_k^{-1} t_0, \quad i = 1, 2, \cdots, n \qquad (13)
\end{aligned}
$$

where $y_{i1} = \tilde{\alpha}(R_i)\cdot m$ and $y_{i2} = \tilde{\gamma}(R_i)$. Notice that y_{i2} is known, $f(y_{i1})$ and $\tilde{\beta}(R_i)\in\mathcal{Z}$, it follows that

$$
\begin{aligned}
&y_{i2} t_k^{-1} t_0 \in \mathcal{Z}\\
&\Rightarrow t_0 \in t_k y_{i2}^{-1}\mathcal{Z}. \qquad (14)
\end{aligned}
$$

Since $t_k \in \mathbb{G}\setminus\mathcal{Z}$, there are $q^2 - q$ possibilities for t_k. If t_k is chosen, there are q possibilities for t_0 owning to $t_0 \in t_k y_{i2}^{-1}\mathcal{Z}$. Hence, there are $q(q^2-q)$ suitable pairs (t_0, t_k). Besides, for each solution pair (t_0, t_k), there are q equivalent solutions $(t_0 z, t_k z)$ with $z\in\mathcal{Z}$. Furthermore, since $f(y_{i1})$ is unknown, there are q possible choices for $f(y_{i1})$ on the left side of equation (13). Consequently, there are $q(q^2-q)$ different solutions, it follows that the complexity of this attack is $\mathcal{O}(q(q^2-q))$.

b. In this attack, the adversary intents to take advantage of equivalent private key $[\beta^*, (t_0^*, \cdots, t_k^*), f]$ to replace the original private key $[\beta, (t_0, \cdots, t_k), f]$. From [43], the adversary may let $t_i^* = t_i z_i (1\le i\le k)$ and $b_{ij}^* = b_{ij} c_{ij} (1\le i\le k, 1\le j\le r_i)$ for $z_i, c_{ij}\in\mathcal{Z}$. so for the first block of γ, it follows that:

$$h_{1j} = b_{1j} t_0^{*-1} z_0 f(a_{1j}) t_1 \qquad (15)$$

Let $b_{i1}^* = id$, then $c_{i1} = b_{i1}$, we have

$$\begin{aligned}
h_{11} &= b_{11}^* c_{11} t_0^{*-1} z_0 f(a_{11}) t_1 \\
&= b_{11}^* t_0^{*-1} f(a_{11})(t_1 c_{11} z_0) \Rightarrow t_1^* = t_1 c_{11} z_0 \\
h_{1j} &= b_{1j} t_0^{*-1} z_0 f(a_{1j})(t_1^* c_{11} z_0) \quad j = 2, \cdots, r_1 \\
b_{1j}^* &= b_{1j} c_{1j} = h_{1j} t_1^{*-1} f(a_{1j})^{-1} t_0^* \Rightarrow c_{1j} = c_{11} = b_{11} \qquad (16) \\
h_{21} &= b_{21}^* c_{21} t_1^{*-1} c_{11} z_0 f(a_{21}) t_2 \Rightarrow t_2^* = t_2 c_{21} c_{11} z_0 \\
h_{2j} &= b_{2j} t_1^{*-1} c_{11} z_0 f(a_{2j}) t_2^* c_{21} c_{11} z_0 \quad j = 2, \cdots, r_2 \\
b_{2j}^* &= b_{2j} c_{2j} = h_{2j} t_2^{*-1} f(a_{2j})^{-1} t_1^* \Rightarrow c_{2j} = c_{21} = b_{21} \\
&\vdots \qquad (17)
\end{aligned}$$

We can get that $c_{ij} = c_{i1} = b_{i1}$ for all $i = 1, \cdots, k$. If we denote $c_{ij} = c_i$, then $t_i^* = t_i z_0 \prod_{k=1}^{i} c_k$.

$$\begin{aligned}
\tilde{\gamma}(R) &= \tilde{\beta}(R) t_0^{-1} f(\tilde{\alpha}(R)) t_k \\
&= \tilde{\beta}(R) t_0^{*-1} z_0^{-1} f(\tilde{\alpha}(R)) t_k^* z_0 \prod_{s=1}^{k} c_s \\
&= (\tilde{\beta}(R) \prod_{s=1}^{k} c_s) t_0^{*-1} f(\tilde{\alpha}(R)) t_k^* \\
&= (\tilde{\beta}(R) \prod_{s=1}^{k} c_s) t_0 f(\tilde{\alpha}(R)) t_k \qquad (18)
\end{aligned}$$

Let $\tilde{\beta}(R) = b_{1x_1} b_{2x_2} \cdots b_{kx_k}$, $\beta^* := (b_{ij}^*)$ and $b_{ij}^* = b_{ij} c_i$ for $c_i \in \mathcal{Z}$, then

$$\begin{aligned}
\tilde{\beta}^*(R) &= b_{1x_1}^* b_{2x_2}^* \cdots b_{kx_k}^* \\
&= b_{1x_1} c_1 b_{2x_2} c_2 \cdots b_{kx_k} c_k \\
&= \tilde{\beta}(R) \prod_{s=1}^{k} c_s. \qquad (19)
\end{aligned}$$

Since β^* is tame, the adversary can take advantage of forged private key $[\beta^*, (t_0^*, \cdots, t_k^*), f]$ to recover the random number R. Then, there are $q = |\mathbb{G}|/|\mathcal{Z}|$ possible choices for t_0 in $t_0\mathcal{Z}$ and q possible choices for $f(\tilde{\alpha}(R))$, so the complexity for this attack is $\mathcal{O}(q^2)$ and it's computationally infeasible.

2) ATTACK ON CIPHERTEXT

a: ONE-WAYNESS OF CIPHERTEXTS

As we all known that one-wayness is the basic requirement for public-key cryptography. Therefore, we should consider one-wayness of ciphertexts in our proposal. In the encryption phase, we can get that $m = \tilde{\alpha}(R)^{-1} \cdot y_1$ from $y_1 = \tilde{\alpha}(R) \cdot m$. Thence, if the adversary wants to obtain the original message m, he(she) either guesses the random number R, or recovers the random number R from the cover mapping $y_2 = \tilde{\gamma}(R)$. However, since q is large enough and $\tilde{\gamma}$ is a one-way function from Cryptographic Hypothesis 1, so it is computationally infeasible for the adversary to recover R from $\tilde{\gamma}$.

b: INDISTINGUISHABILITY OF CIPHERTEXTS

The adversary $\mathcal{A}$ sends the challenger $\mathcal{B}$ two messages $m_0, m_1 \in \mathcal{Z}$ with the same matrix form. $\mathcal{B}$ computes the challenge ciphertext $C^* = (y_1^*, y_2^*)$ as follows:

- Choose a random R^* from $\mathbb{Z}_{|\mathcal{Z}|}$, and compute $y_2^* = \tilde{\gamma}(R^*)$.
- Compute $y_1^* = \tilde{\alpha}(R^*) \cdot m_\delta$, where δ is a random number from $\{0, 1\}$.

If $\mathcal{A}$ can not output the correct b, then challenge ciphertext C^* is statistical indistinguishable.

In this case, we can analyse the following two cases:

$$\begin{aligned}
y_1^* &= \tilde{\alpha}(R^*) \cdot m_0 \\
y_2^* &= \tilde{\gamma}(R^*) \qquad (20)
\end{aligned}$$

and

$$\begin{aligned}
y_1' &= \tilde{\alpha}(R') \cdot m_1 \\
y_2' &= \tilde{\gamma}(R'). \qquad (21)
\end{aligned}$$

Since R^* and R' admit the same probability distribution, it follows that R^* and R' are statistical indistinguishable for the adversary. It can be denoted by $R^* \underset{s}{\approx} R'$. Meanwhile, since $\tilde{\alpha}$ and $\tilde{\beta}$ are both one-way maps, so we can get that $\tilde{\alpha}(R^*) \underset{s}{\approx} \tilde{\alpha}(R')$ and $\tilde{\gamma}(R^*) \underset{s}{\approx} \tilde{\gamma}(R')$. Besides, since $m_0 \underset{s}{\approx} m_1$, so $\tilde{\alpha}(R^*) \cdot m_0 \underset{s}{\approx} \tilde{\alpha}(R') \cdot m_1$. Consequently, we can get that $(y_1^*, y_2^*) \underset{s}{\approx} (y_1', y_2')$.

IV. DISCUSSION

In this section, we focus on analyzing the efficiency and related security parameters of our proposed scheme. Here, we investigate the number of basic operations for one encryption/decryption. The basic operation is composed of addition (Add), multiplication (Mult), exponentiation with θ (Exp(θ)), generation of m-bit random R (PRG), and factorization of $\beta'(R) \in \mathcal{Z}$ for β using the Algorithms 9-11 (Factor) in [43]. Then, the time of an Add operation is denoted as T_{Add}, the time of a Mult operation is denoted as T_{Mult}, the time of an Exp(θ) is denoted as T_{Exp}, the time of a PRG is denoted as T_{PRG} and the time of a Factor is denoted as T_{Factor}.

Table 2 demonstrates the number of basic operations required for $eMST_3$ scheme and our proposed scheme. Table 3 reveals the number of basic operations required in the key generation phase (including public keys and private keys). In addition, we utilize the NTL library [45], measure on a machine with macOS, 1.8 GHz Intel Core i5 processor, 4G RAM and 1600 MHz DDR3, and implement our scheme in C++. We obtain average time of every operation in one encryption/decryption using the method of repeated computing one thousand times, and the experimental results reveal that $T_{Add} = 0.019ms$, $T_{Mult} = 0.26ms$, $T_{Exp} = 3.556ms$, $T_{PRG} = 1.8ms$ and $T_{Factor} = 2.74ms$.

Upon receiving the computational overheads of T_{Add}, T_{Mult}, T_{Exp}, T_{PRG} and T_{Factor}, on the one hand, we vary k from $\{8, 16, 24, 32, 40, 48, 56, 64, 72, 80\}$ and depict the variation of computational overheads of $eMST_3$ and our

TABLE 2. The computational overheads of one encryption/decryption.

		$\mathbb{F}_{2^\kappa}$ Add	$\mathbb{F}_{2^\kappa}$ Mult	$\mathbb{F}_{2^m}$ Exp(θ)	$\mathbb{F}_{2^\kappa}$ PRG	Factor
Encryption[1]	$eMST_3$ scheme [43]	8k-6	2k-2	-	1	-
	Our scheme	8k-7	2k-2	-	1	-
Decryption[2]	$eMST_3$ scheme	4k+15	k+5	1	-	1
	Our scheme	4k+10	k+3	-	-	1

[1] In the encryption, our scheme reduces one multiplication of the element in center $\mathcal{Z}$. Therefore, comparing with $eMST_3$, the number of ($\mathbb{F}_{2^\kappa}$ Add) reduces one.

[2] In the decryption, our scheme reduces one inverse operation, one multiplication operation, and one $\mathbb{F}_{2^\kappa}$ Exp(θ) operation, so it reduces five ($\mathbb{F}_{2^\kappa}$ Add) and two ($\mathbb{F}_{2^\kappa}$ Mult).

TABLE 3. The computational overheads in the key generation phase.

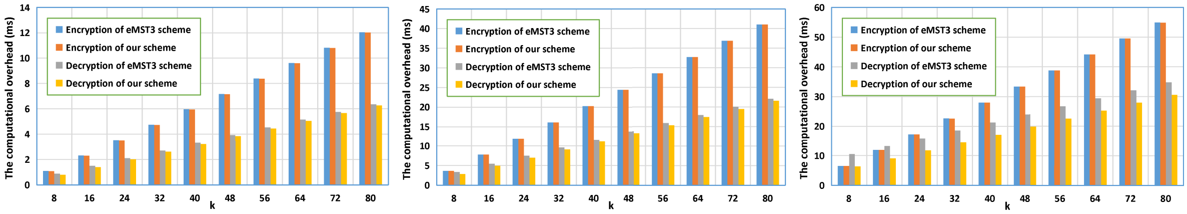
	private key β	private key $[t_0, \cdots, t_s, f]$	public key α	public key γ
$\mathbb{F}_{2^\kappa}$ Add	T [3]	-	T	9T+k
$\mathbb{F}_{2^\kappa}$ Mult	-	k+1 [4]	T-k	2T+k
$\mathbb{F}_{2^\kappa}$ PRG	$\sum_{l=1}^{v} r_l^*$ [5]	2(k+1)	2T-k	-

[3] $T = \sum_{i=1}^{k} r_i, r_i = \prod_{j=1}^{v_i} r_{i_j}^* \cdot u_i$ for $1 \leq i \leq k$ and $\sum_{i=1}^{k} v_i = w$, where

$$u_i = \begin{cases} 0 & if \quad v_i = 1 \\ 1 & if \quad v_i > 1. \end{cases}$$

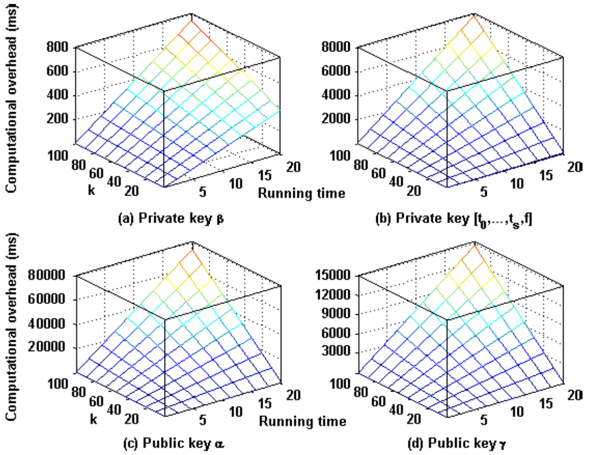
[4] For $a \in \mathbb{F}_q$, $\theta : a \to a^2$ is a Frobenius automorphism. Thus, θ can be denoted by one multiplication operation.

[5] w denotes the number of blocks before fusion.



(a) Add operation (b) Mult operation (c) Total

FIGURE 1. The computational overhead comparison between *eMST*$_3$ and our scheme for one encryption/decryption.



(a) Private key β (b) Private key [t$_0$,...,t$_s$,f] (c) Public key α (d) Public key γ

FIGURE 2. The computational overhead comparison between our private and public keys in the key generation phase.

scheme for one encryption/decryption in term of k, which is presented in Figure 1. As shown in Table 2 and Figure 1, comparing with $eMST_3$ scheme, our proposed scheme has a lower computational overhead for one encryption/decryption in terms of Add operation, Mult operation and total.

On the other hand, we vary k from $\{20, 40, 60, 80, 100\}$, running time from $\{5, 10, 15, 20\}$ and depict the computational overheads of our private and public keys for the key generation phase in Figure 2. As described in Table 3 and Figure 2, it is obvious that the computational overhead of generate public key α is the highest of all the others, that of generate private key β is the lowest, that of generate private key $[t_0, \ldots, t_s, f]$ is lower than that of generate public key γ. In addition, the generation of public keys needs a higher computational overhead in the key generation phase comparing with that of private keys.

V. CONCLUSION

In this paper, we put forward a new secure encryption schemes on the basis of random cover and logarithmic signature. The intractability assumption of our scheme is group factorization problem (GFP) on a type of Suzuki 2-group. Comparing with $eMST_3$ scheme, our scheme has higher efficiency. Also, our method is universal and can realize basic encryptions on files and images.

REFERENCES

[1] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography," *Math. Res. Lett.*, vol. 6, pp. 287–292, 1999.

[2] I. Anshel, M. Anshel, D. Goldfeld, and S. Lemieux, "Key agreement, the Algebraic EraserTM, and lightweight cryptography," *Contemp. Math.*, vol. 418, pp. 1–34, Jan. 2007.

[3] I. Anshel, D. Atkins, D. Goldfeld, and P. E. Gunnells, "Hickory hash (TM): Implementing an instance of an algebraic eraser (TM) hash function on an MSP430 Microcontroller," *IACR Cryptol. ePrint Arch.*, vol. 2016, p. 1052, Nov. 2016.

[4] D. Atkins and P. Gunnells, "Algebraic Eraser: A lightweight, efficient asymmetric key agreement protocol for use in no-power, low-power, and IoT devices," in *Proc. NIST Lightweight Cryptogr. Workshop*, vol. 20, 2015.

[5] I. Anshel, D. Atkins, D. Goldfeld, and P. E. Gunnells, "WalnutDSA (TM): A quantum resistant group theoretic digital signature algorithm," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 58, 2017.

[6] G. Baumslag, B. Fine, and X. Xu, "Cryptosystems using linear groups," *Applicable Algebra Eng. Commun. Comput.*, vol. 17, nos. 3–4, pp. 205–217, 2006.

[7] D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds., *Post-Quantum Cryptography*. Springer, 2009.

[8] J. Birget, S. S. Magliveras, and M. Sramka, "On public-key Cryptosystems based on combinatorial group theory," *Tatra Mt. Math. Publ.*, vol. 33, pp. 137–148, Jan. 2006.

[9] M. Bläser, "Noncommutativity makes determinants hard," *Inf. Comput.*, vol. 243, pp. 133–144, Aug. 2015.

[10] S. R. Blackburn, C. Cid, and C. Mullan, "Cryptanalysis of the MST$_3$ public key cryptosystem," *J. Math. Cryptol.*, vol. 3, no. 4, p. 321, 2009.

[11] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2001, pp. 213–229.

[12] Z. Cao, X. Dong, and L. Wang, "New public key cryptosystems using polynomials over non-commutative rings," *IACR Cryptol. ePrint Arch.*, vol. 2007, p. 9, Jan. 2007.

[13] A. Caranti and F. D. Volta, "The round functions of cryptosystem PGM generate the symmetric group," *Des. Codes Cryptogr.*, vol. 38, no. 1, pp. 147–155, 2006.

[14] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[15] P. Dehornoy, "Braid-based cryptography," *Contemp. Math.*, vol. 360, pp. 5–33, 2004.

[16] M. Eftekhari, "Cryptanalysis of some protocols using matrices over group rings," in *Proc. Int. Conf. Cryptol. Africa*. Cham, Switzerland: Springer, 2017, pp. 223–229.

[17] B. Eick and D. Kahrobaei, "Polycyclic groups: A new platform for cryptology?" 2004, *arXiv:math/0411077*. [Online]. Available: https://arxiv.org/abs/math/0411077

[18] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[19] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1999, pp. 537–554.

[20] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Appl. Math.*, vol. 156, no. 16, pp. 3113–3121, 2008.

[21] D. Grigoriev and I. Ponomarenko, "Homomorphic public-key cryptosystems and encrypting Boolean circuits," *Applicable Algebra Eng. Commun. Comput.*, vol. 17, nos. 3–4, pp. 239–255, 2006.

[22] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, no. 2, p. 325, 1997.

[23] M. Habeeb, D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public key exchange using semidirect product of (semi)groups," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Berlin, Germany: Springer, 2013, pp. 475–486.

[24] H. Hong, L. Wang, H. Ahmad, Y. Yang, and Z. Qu, "Minimum length key in MST cryptosystems," *Sci. China Inf. Sci.*, vol. 60, no. 5, 2017, Art. no. 052106.

[25] G. Higman, "Suzuki 2-group," *Illinois J. Math.*, vol. 7, no. 1, pp. 79–96, 1963.

[26] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J.-S. Kang, and C. Park, "New public-key cryptosystem using braid groups," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2000, pp. 166–183.

[27] D. Kahrobaei and M. Anshel, "Decision and search in non-abelian Cramer-Shoup public key cryptosystem," *Groups-Complex.-Cryptol.*, vol. 1, no. 2, pp. 217–225, 2009.

[28] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public key exchange using matrices over group rings," *Groups Complex. Cryptol.*, vol. 5, no. 1, pp. 97–115, 2013.

[29] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "A CCA secure cryptosystem using matrices over group rings," *Contemp. Math. Amer. Math. Soc*, vol. 633, pp. 73–80, Feb. 2015.

[30] W. Lempken, T. van Tran, S. S. Magliveras, and W. Wei, "A public key cryptosystem based on non-abelian finite groups," *J. Cryptol.*, vol. 22, no. 1, pp. 62–74, 2009.

[31] R. Li, U. Alvarez-Rodriguez, L. Lamata, and E. Solano, "Approximate quantum adders with genetic algorithms: An IBM quantum experience," *Quantum Meas. Quantum Metrol.*, vol. 4, no. 1, pp. 1–7, 2017.

[32] S. S. Magliveras, "A cryptosystem from logarithmic signatures of finite groups," in *Proc. 29th Midwest Symp. Circuits Syst.* Amsterdam, The Netherlands: Elsevier, 1986, pp. 972–975.

[33] C. Monico and M. D. Neusel, "Cryptanalysis of a system using matrices over group rings," *Groups Complex. Cryptol.*, vol. 7, no. 2, pp. 175–182, 2015.

[34] D. Moody, L. Feldman, and G. A. Witte, "Securing tomorrow's information through post-quantum cryptography," Tech. Rep. 2018.

[35] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Secur. Privacy*, vol. 16, no. 5, pp. 38–41, Sep./Oct. 2018.

[36] A. D. Myasnikov and A. Ushakov, "Quantum algorithm for discrete logarithm problem for matrices over finite group rings," *Groups Complex. Cryptol.*, vol. 6, no. 1, pp. 31–36, 2014.

[37] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," (2003). *arXiv:quant-ph/0301141*. [Online]. Available: https://arxiv.org/abs/quant-ph/0301141

[38] D. Reichl, "Tame logarithmic signatures of abelian groups," *J. Math. Cryptol.*, vol. 11, no. 4, pp. 205–214, 2017.

[39] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[40] V. Roman'kov, "Linear decomposition attack on public key exchange protocols using semidirect products of (semi)groups," 2015, *arXiv:1501.01152*. [Online]. Available: http://arxiv.org/pdf/1501.01152.pdf

[41] M. Rötteler, "Quantum algorithms: A survey of some recent results," *Informatik—Forschung und Entwicklung*, vol. 21, nos. 1–2, pp. 3–20, 2006.

[42] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, 1999.

[43] P. Svaba and T. van Trung, "Public key cryptosystem MST$_3$: Cryptanalysis and realization," *J. Math. Cryptol.*, vol. 4, no. 3, pp. 271–315, 2010.

[44] P. Svaba, T. van Trung, and P. Wolf, "Logarithmic signatures for abelian groups and their factorization," *Tatra Mountains Math. Publications*, vol. 57, no. 1, pp. 21–33, 2013.

[45] Shoup Victor. (2016). *Number Theory Library (NTL) For C++*. [Online]. Available: https://www.shoup.net/ntl/

[46] V. Shpilrain and A. Ushakov, "Thompson's group and public key cryptography," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Berlin, Germany: Springer, 2005, pp. 151–163.

[47] T. van Trung, "Construction of strongly aperiodic logarithmic signatures," *J. Math. Cryptol.*, vol. 12, no. 1, pp. 23–35, 2018.

[48] T. van Trung, "New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups," *J. Cryptol.*, vol. 15, no. 4, pp. 285–297, 2002.

[49] M. I. G. Vasco and R. Steinwandt, *Group Theoretic Cryptography*, Atlanta, GA, USA: Chapman Hall, 2015.

[50] N. R. Wagner and M. R. Magyarik, "A public-key cryptosystem based on the word problem," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1984, pp. 19–36.

YUE CONG is currently a Lecturer with the Zhejiang Agricultural Business College. Her current research interests include electronic commerce and the Internet of Things security.

HAIBO HONG received the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, China, in 2015. He is currently an Assistant Professor with the School of Computer Science and Information Engineering, Zhejiang Gongshang University, China. His current research interests include information security and cryptography.

JUN SHAO received the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2008. He was a Postdoctoral Fellow with the School of Information Sciences and Technology, Pennsylvania State University, State College, PA, USA, from 2008 to 2010. He is currently a Professor with the School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou, China. His current research interests include network security and applied cryptography.

SONG HAN is currently a Professor with Zhejiang Gongshang University. He is also with Zhejiang Ponshine Information Technology Company, Ltd., Hangzhou, China. His current research interests include network security and data privacy protection.

JIANHONG LIN is currently the Chief Technology Officer of Zhejiang Ponshine Information Technology Company, Ltd., Hangzhou, China.

SHUAI ZHAO is currently an Engineer with the Computing Center, Zhejiang Gongshang University. His current research interests include privacy-preserving data aggregation and network security.