

Research Article

A Digital Signature Scheme Based on MST_3 Cryptosystems

Haibo Hong, Jing Li, Licheng Wang, Yixian Yang, and Xinxin Niu

*Information Security Center, State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing 100876, China*

Correspondence should be addressed to Licheng Wang; wanglc@bupt.edu.cn

Received 5 December 2013; Revised 13 March 2014; Accepted 14 March 2014; Published 20 May 2014

Academic Editor: Wang Xing-yuan

Copyright © 2014 Haibo Hong et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As special types of factorization of finite groups, logarithmic signature and cover 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 , and MST_3 . Recently, Svaba et. al proposed a revised MST_3 encryption scheme with greater security. Meanwhile, they put forward an idea of constructing signature schemes on the basis of logarithmic signatures and random covers. In this paper, we firstly design a secure digital signature scheme based on logarithmic signatures and random covers. In order to complete the task, we devise a new encryption scheme based on MST_3 cryptosystems.

1. Introduction

With the interdisciplinary development of information science, physical science, and biological science, a lot of new technology appeared in the field of cryptography and has made new progress. The new branches of cryptography mainly consist of quantum cryptography, chaotic cryptography, DNA cryptography, and so forth. The security of quantum cryptography is based on the Heisenberg uncertainty principle. Quantum cryptography is the only one that can realize unconditional security at present [1–4]. Matthews [5] firstly applied chaos theory in cryptography and proposed a chaotic stream cipher scheme based on revised logistic map. From then on, chaotic cryptography has attracted wide attention [6, 7]. Most of the researches in chaotic cryptography focus on secret key cryptography. With the recent constructions due to Wang et al. [8–14], chaos-based public key cryptographic protocols come to us. DNA cryptography, which utilizes DNA computing, is a new branch of cryptography in recent years [15, 16]. Using the high storage density and high parallelism of DNA molecular, DNA cryptography can realize the encryption, authentication, signature, and so forth [17].

Meanwhile, cryptographers look forward to applying new intractable mathematical problems in classical cryptography. Currently, most public cryptographic primitives are based on

the perceived intractability of certain mathematical problems in very large finite abelian groups [18]. Prominent hard problems consist of the problem of factoring large integers, the discrete logarithm problem over a finite field F_q or an elliptic curve, and so forth. However, due to quantum algorithms for factoring integer and solving the discrete logarithm problem, most known public-key cryptosystems will be insecure when quantum computers become practical. Therefore, it is an imminent work to design effective cryptographic schemes which can resist quantum attacks. Actually, since the 1980s, several experts have been trying to design new cryptography schemes based on difficult problems in group theory. In 1985, Wagner and Magyarik [19] proposed an approach to designing public-key cryptosystems based on groups and semigroups with undecidable word problem. In 2000, Ko et al. [20] developed the theory of braid-based cryptography based on the hardness of the conjugator search problem (CSP) in braid groups. In 2004, Eick and Kahrobaei [21] proposed a new cryptosystem based on polycyclic groups. In 2005, Shpilrain and Ushakov [22] suggested that Thompson's group may be a good platform for constructing public-key cryptosystems. Recently, Kahrobaei et al. [23] proposed a public key exchange on the basis of matrices over group rings. Meanwhile, an active branch of noncommutative cryptography based on the hardness of group factorization problem has achieved great success during the last two decades. In 1986,

Magliveras [24] proposed a symmetric cryptosystem PGM based on a special type of factorization of finite groups named logarithmic signatures for finite permutation groups. Then, the algebraic properties of logarithmic signatures and cryptosystem PGM were specifically discussed in [25, 26]. In 2002, Magliveras et al. [27] put forward two public key cryptosystems MST_1 and MST_2 . In 2009, Lempken et al. [18] designed a new public key cryptosystem MST_3 on the basis of random covers and logarithmic signatures for nonabelian finite groups. Meanwhile, there are some interesting papers studying attacks on MST_1 , MST_2 , and MST_3 [28–33]. In 2010, Svaba and van Trung [34] constructed an $eMST_3$ cryptosystem by adding a homomorphism as a component of secret key. However, until now, there is no paper on constructing digital signature schemes on the basis of MST cryptosystem. Hence, Svaba and van Trung put forward an open problem on constructing digital signature schemes based on random covers and logarithmic signatures.

Our main contribution is to devise a digital signature scheme based on random covers and logarithmic signatures. In this process, we also construct a secure and more efficient encryption scheme based on MST_3 cryptosystems.

The rest of contents are organized as follows. Necessary preliminaries are given in Section 2. In Section 3, we specifically describe a new encryption scheme and give corresponding security analysis. In Section 4, we propose a digital signature scheme based on random covers and logarithmic signatures; The related comparisons and illustrations are presented in Section 5.

2. Preliminaries

2.1. Cover and Logarithmic Signature. Let G be a finite abstract group and let $X = [x_1, x_2, \dots, x_r]$ and $Y = [y_1, y_2, \dots, y_s]$ be two elements in $G^{[Z]}$. Then

$$X \otimes Y = [x_1 y_1, \dots, x_1 y_s, x_2 y_1, \dots, x_2 y_s, \dots, x_r y_1, \dots, x_r y_s]. \quad (1)$$

If $X = [x_1, \dots, x_r] \in G^{[Z]}$, \overline{X} denotes the element $\sum_{i=1}^r x_i$ in the group ring $\mathbb{Z}G$.

Definition 1 (cover and logarithmic signature [18, 27]). Suppose that $\alpha = [A_1, A_2, \dots, A_s]$ is a sequence of $A_i \in G^{[Z]}$, such that $\sum_{i=1}^s |A_i|$ is bounded by a polynomial in $\log |G|$. Let

$$\overline{A_1} \cdot \overline{A_2} \cdots \overline{A_s} = \sum_{g \in G} a_g g, \quad a_g \in \mathbb{Z}. \quad (2)$$

Let S be a subset of G . Then α is

- (i) a *cover* for G (or S) if $a_g > 0$ for all $g \in G$ ($g \in S$),
- (ii) a *logarithmic signature* for G (or S) if $a_g = 1$ for every $g \in G$ ($g \in S$).

The sequences A_i are called the *blocks*; the vector (r_1, \dots, r_s) with $r_i = |A_i|$ is the *type* of α and the *length* of α is defined to be $l(\alpha) = \sum_{i=1}^s r_i$.

More generally, if $\alpha = [A_1, A_2, \dots, A_s]$ is a logarithmic signature (cover) for G , then each element $g \in G$ can be

expressed uniquely (at least one way) as a product of the form [18]

$$g = a_1 \cdot a_2 \cdots a_s, \quad (3)$$

for $a_i \in A_i$. α is called *tame* (factorizable) if the factorization above can be achieved in polynomial in the width w of G .

Definition 2 (cover (logarithmic signature) mappings [35]). Let $\alpha = [A_1, A_2, \dots, A_s]$ be a cover (logarithmic signature) of type (r_1, r_2, \dots, r_s) for G with $A_i = [a_{i,1}, a_{i,2}, \dots, a_{i,r_i}]$, where $m = \prod_{i=1}^s r_i$. Let $m_1 = 1$ and $m_i = \prod_{j=1}^{i-1} r_j$ for $i = 2, \dots, s$. Let τ denote the canonical bijection

$$\tau : \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_s} \longrightarrow \mathbb{Z}_m \quad (4)$$

$$\tau(j_1, j_2, \dots, j_s) = \sum_{i=1}^s j_i \cdot m_i.$$

Then the surjective (bijection) mapping $\alpha' : \mathbb{Z}_m \rightarrow G$ induced by α is

$$\alpha'(x) = a_{1j_1} \cdot a_{2j_2} \cdots a_{sj_s}, \quad (5)$$

where $(j_1, j_2, \dots, j_s) = \tau^{-1}(x)$.

2.2. MST_3 Cryptosystems and Suzuki 2-Groups. In [18], Lempken et al. utilized logarithmic signatures and random covers to construct a generic MST_3 encryption scheme. In this scheme, the public key consists of a tame logarithmic signature as well as some random numbers, and the secret key is composed of a random cover and a sandwich transformation of the cover [27]. The intractability assumptions of this scheme are group factorization problem on nonabelian groups.

Furthermore, motivated by attacks in [31], Svaba and van Trung devised an enhanced version of the generic scheme [34] named $eMST_3$ cryptosystems. In this scheme, they introduced a secret homomorphism to mask the secret logarithmic signature with a transformation of a random cover. Meanwhile, they proposed a new setup with random encryption.

Until now, the only instantiation of MST_3 cryptosystems is a Suzuki 2-group of order q^2 with $q = 2^m$ ($m \geq 3$) [18, 34]. From [34], the Suzuki 2-group of order q^2 can be denoted by $A(m, \theta)$, where θ is an automorphism of \mathbb{F}_q with an odd order. Moreover, the group $A(m, \theta)$ can be represented by a matrix group G and

$$G = \{S(a, b) \mid a, b \in \mathbb{F}_q\}, \quad (6)$$

where

$$S(a, b) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\theta \\ 0 & 0 & 1 \end{pmatrix} \quad (7)$$

is a 3×3 matrix over \mathbb{F}_q . Hence, G is of order q^2 and the center $\mathcal{Z}(G) = \{S(0, b) \mid b \in \mathbb{F}_q\}$. Besides, to store the group

elements conveniently, $S(a, b)$ can be denoted by (a, b, a^θ) , so the product of two elements in group G is

$$\begin{aligned} S(a_1, b_1) S(a_2, b_2) &= S(a_1, b_1, a_1^\theta) S(a_2, b_2, a_2^\theta) \\ &= (a_1 + a_2, b_1 + b_2 + a_1 a_2^\theta, a_1^\theta + a_2^\theta), \end{aligned} \quad (8)$$

and the computation of the product just requires a single multiplication and four additions in \mathbb{F}_q .

Furthermore, the inverse of an element in group G is

$$S(a, b, a^\theta)^{-1} = S(a, a^\theta \cdot a + b, a^\theta) = S(a, a^{\theta+1} + b, a^\theta), \quad (9)$$

and it also requires a single multiplication and one addition in \mathbb{F}_q . If $g = S(x, y) \in G$ and $x, y \in \mathbb{F}_q$, then x and y can be denoted by g_a and g_b , respectively. Hence, $g = S(g_a, g_b)$, where g_a and g_b are the corresponding projections of g along the first and second coordinates.

3. Building Block: A New MST_3 Encryption Scheme

Through comparison and analysis, we find that it is rather difficult to devise signature schemes based on the two MST_3 encryption schemes [18, 34]. Therefore, in order to complete the task, we design a new encryption scheme based on logarithmic signatures and random covers. In our scheme, the original secret key f becomes a component of public key, and the encryption process is also simplified. Meanwhile, compared with original schemes, our scheme has a bit improvement in efficiency.

3.1. Description of the Scheme

Key Generation

Input: a large group $G = A(m, \theta)$, $q = 2^m$.

Output: a public key $[\alpha, \gamma, f]$ with corresponding private key $[\beta, (t_0, \dots, t_s)]$.

(1) Choose a tame logarithmic signature $\beta = [B_1, B_2, \dots, B_s] = (b_{ij}) = (S(0, b_{(ij)-b}))$ of type (r_1, r_2, \dots, r_s) for \mathcal{Z} , where $b_{ij} \in G$ and $b_{(ij)-b} \in \mathbb{F}_q$.

(2) Select a random cover $\alpha = [A_1, A_2, \dots, A_s] = (a_{ij}) = (S(a_{(ij)-a}, a_{(ij)-b}))$ of the same type as β for a certain subset J of G such that $A_1, \dots, A_s \subseteq G \setminus \mathcal{Z}$, where $a_{ij} \in G$, $a_{(ij)-a} \in \mathbb{F}_q \setminus \{0\}$, and $a_{(ij)-b} \in \mathbb{F}_q$.

(3) Choose $t_0, t_1, \dots, t_s \in G \setminus \mathcal{Z}$.

(4) Construct a homomorphism $f: G \rightarrow \mathcal{Z}$ defined by $f(S(a, b)) = S(0, a)$.

(5) Compute $\gamma := (h_{ij}) = (S(h_{(ij)-a}, h_{(ij)-b}))$, where $h_{ij} = t_{i-1}^{-1} \cdot f(a_{ij}) \cdot b_{ij} \cdot t_i$.

(6) Output public key $[\alpha, \gamma, f]$ and private key $[\beta, (t_0, \dots, t_s)]$.

Encryption

Input: a message $x \in \mathcal{Z}$ and the public key $[\alpha, \gamma, f]$.

Output: a ciphertext (y_1, y_2) of the message m .

(1) Choose a random $R \in \mathbb{Z}_{|\mathcal{Z}|}$.

(2) Compute

$$\begin{aligned} y_1 &= \alpha'(R) \cdot m, \\ y_2 &= \gamma'(R) \\ &= t_0^{-1} \cdot f(\alpha'(R)) \cdot \beta'(R) \cdot t_s. \end{aligned} \quad (10)$$

(3) Output (y_1, y_2) .

Decryption

Input: a ciphertext pair (y_1, y_2) and the private key $[\beta, t_0, \dots, t_s]$.

Output: the message $m \in \mathcal{Z}$ corresponding to ciphertext (y_1, y_2) .

(1) Compute $R = \beta'^{-1}(y_2 t_s^{-1} f(y_1)^{-1} t_0)$.

(2) Compute $m = \alpha'(R)^{-1} \cdot y_1$.

(3) Output m .

Correctness

For $m \in \mathcal{Z}$ and $R \in \mathbb{Z}_{|\mathcal{Z}|}$, we have

$$\begin{aligned} y_1 &= \alpha'(R) \cdot m, \\ y_2 &= \gamma'(R) \\ &= b_{1j_1} t_0^{-1} f(a_{1j_1}) t_1 \cdots b_{sj_s} t_{s-1}^{-1} f(a_{sj_s}) t_s \\ &= b_{1j_1} b_{2j_2} \cdots b_{sj_s} t_0^{-1} f(a_{1j_1} a_{2j_2} \cdots a_{sj_s}) t_s \\ &= \beta'(R) \cdot t_0^{-1} \cdot f(\alpha'(R)) \cdot t_s \\ &= \beta'(R) \cdot t_0^{-1} \cdot f(\alpha'(R) \cdot m) \cdot t_s \\ &= \beta'(R) \cdot t_0^{-1} \cdot f(y_1) \cdot t_s \\ &\implies \beta'(R) = y_2 \cdot t_s^{-1} \cdot f(y_1)^{-1} \cdot t_0; \end{aligned} \quad (11)$$

then using β'^{-1} we can recover the random number R by

$$\beta'^{-1}(\beta'(R)) = \beta'^{-1}(y_2 t_s^{-1} f(y_1)^{-1} t_0) = R. \quad (12)$$

Consequently, using y_1 we can recover message m by

$$m = \alpha'(R)^{-1} \cdot y_1. \quad (13)$$

3.2. Security Analysis

3.2.1. Attack on Private Key. (a) In general, the adversary tries to obtain β and (t_0, t_s) from the equation

$$\beta'(R) = \gamma_2 \cdot t_s^{-1} \cdot f(y_1)^{-1} \cdot t_0, \quad (14)$$

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

The adversary mainly attempts to compute enough values $\beta'(R_i)$ in order to construct β using the corresponding conclusion in [27]. If β is of type (r_1, r_2, \dots, r_s) , then one can construct a logarithmic signature equivalent to β by using n selected values $\beta'(R_i)$, where $n = 1 - s + \sum_{k=1}^s r_k$. Let $\{R_1, R_2, \dots, R_n\}$ be a collection of random numbers chosen by the adversary. Then

$$\begin{aligned} \beta'(R_i) &= y_{i2} t_s^{-1} f(y_{i1})^{-1} t_0 \\ &= f(y_{i1})^{-1} y_{i2} t_s^{-1} t_0, \quad i = 1, \dots, n, \end{aligned} \quad (15)$$

where $y_{i1} = \alpha'(R_i) \cdot m$, $y_{i2} = \gamma'(R_i)$, and $f(y_{i1})^{-1} \in \mathcal{X}$. Note that in the equation above, $f(y_{i1})^{-1}$ and y_{i2} are known and $\beta'(R_i) \in \mathcal{X}$; then we have

$$\begin{aligned} f(y_{i1})^{-1} y_{i2} t_s^{-1} t_0 &\in \mathcal{X} \\ \implies t_0 &\in t_s y_{i2}^{-1} f(y_{i1}) \mathcal{X}. \end{aligned} \quad (16)$$

Since $t_s \in G \setminus \mathcal{X}$, there are $q^2 - q$ possibilities for t_s . If t_s is chosen, from $t_0 \in t_s y_{i2}^{-1} f(y_{i1}) \mathcal{X}$, there are q possibilities for t_0 . Hence, there are $q(q^2 - q)$ suitable pairs (t_0, t_s) . Besides, for each solution pair (t_0, t_s) , there are q equivalent solutions $(t_0 z, t_s z)$ with $z \in \mathcal{X}$. Consequently, there are $q^2 - q$ different solutions, so the success probability of the attacker is $1/q(q - 1)$.

(b) In this attack, an adversary mainly wants to utilize equivalent secret key $[\beta^*, (t_0^*, \dots, t_s^*)]$ to replace the real secret key $[\beta, (t_0, \dots, t_s)]$. From [34], we can see that the adversary only needs to let $t_i^* = t_i z_i$ ($1 \leq i \leq s$) and $b_{ij}^* = b_{ij} c_{ij}$ ($1 \leq i \leq s, 1 \leq j \leq r_i$) for $z_i, c_{ij} \in \mathcal{X}$. So for the first block of γ , we have

$$h_{1j} = b_{1j} t_0^{*-1} z_0 f(a_{1j}) t_1. \quad (17)$$

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

$$\begin{aligned} h_{11} &= b_{11}^* c_{11} t_0^{*-1} z_0 f(a_{11}) t_1 \\ &= b_{11}^* t_0^{*-1} f(a_{11}) (t_1 c_{11} z_0) \implies t_1^* = t_1 c_{11} z_0, \\ h_{1j} &= b_{1j} t_0^{*-1} z_0 f(a_{1j}) (t_1^* c_{11} z_0) \quad j = 2, \dots, r_1, \\ b_{1j}^* &= b_{1j} c_{1j} = h_{1j} t_1^{*-1} f(a_{1j})^{-1} t_0^* \implies c_{1j} = c_{11} = b_{11}, \\ h_{21} &= b_{21}^* c_{21} t_1^{*-1} c_{11} z_0 f(a_{21}) t_2 \implies t_2^* = t_2 c_{21} c_{11} z_0, \\ h_{2j} &= b_{2j} t_1^{*-1} c_{11} z_0 f(a_{2j}) t_2^* c_{21} c_{11} z_0 \quad j = 2, \dots, r_2, \\ b_{2j}^* &= b_{2j} c_{2j} = h_{2j} t_2^{*-1} f(a_{2j})^{-1} t_1^* \implies c_{2j} = c_{21} = b_{21} \\ &\vdots \end{aligned} \quad (18)$$

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

$$\begin{aligned} \gamma'(R) &= \beta'(R) t_0^{-1} f(\alpha'(R)) t_s \\ &= \beta'(R) t_0^{*-1} z_0^{-1} f(\alpha'(R)) t_s^* z_0 \prod_{k=1}^s c_k \\ &= \left(\beta'(R) \prod_{k=1}^s c_k \right) t_0^{*-1} f(\alpha'(R)) t_s^*. \end{aligned} \quad (19)$$

Let $\beta'(R) = b_{1x_1} b_{2x_2} \dots b_{sx_s}$, $\beta^* := (b_{ij}^*)$, and $b_{ij}^* = b_{ij} c_i$ for $c_i \in \mathcal{X}$; then

$$\begin{aligned} \beta^*(R) &= b_{1x_1}^* b_{2x_2}^* \dots b_{sx_s}^* \\ &= b_{1x_1} c_1 b_{2x_2} c_2 \dots b_{sx_s} c_s \\ &= \beta'(R) \prod_{k=1}^s c_k. \end{aligned} \quad (20)$$

Since β^* is tame, so the adversary can use forgery secret key $[\beta^*, (t_0^*, \dots, t_s^*)]$ to recover the random number R . Meanwhile, from conclusions in [31], as there are $q = |G/\mathcal{X}|$ possible choices for t_0 in $t_0 \mathcal{X}$, the complexity for this attack is $\mathcal{O}(q)$. Since the center \mathcal{Z} of Suzuki 2-group has a large order q , so the attack is computationally infeasible.

3.2.2. Attack on Ciphertext

OW (onewayness). In the stage of encryption, from the equation $y_1 = \alpha'(R) \cdot x$, we can get that $x = \alpha'(R)^{-1} \cdot y_1$. Hence, if the adversary wants to recover message x , he either directly seeks the random number R or recovers R from $\gamma'(R)$. However, since q is large enough and γ' is a one-way map, so the attack is computationally infeasible.

IND (indistinguishability). Although we cannot give a formal proof on the indistinguishability of the scheme, we would like to analyse it in a heuristic manner. Suppose that (y_1^*, y_2^*) is the ciphertext of m_0 or m_1 , where $y_1^* = \alpha'(R) \cdot m_\delta$, $y_2^* = \gamma'(R)$, $\delta = 0$ or 1 , m_0 , and m_1 are randomly selected by the adversary. Then we can analyse the following two cases:

$$\begin{aligned} y_1 &= \alpha'(R) \cdot m_0 & y_2 &= \gamma'(R), \\ y_1' &= \alpha'(R') \cdot m_1 & y_2' &= \gamma'(R'). \end{aligned} \quad (21)$$

Since R and R' are randomly selected, and they admit the same distribution, thus, R and R' are statistically indistinguishable for the adversary. It can be denoted by $R \approx_s R'$. Meanwhile, since α' and β' are both one-way maps, so we can get that $\alpha'(R) \approx_s \alpha'(R')$ and $\gamma'(R) \approx_s \gamma'(R')$. Besides, since $m_0 \approx_s m_1$, so $\alpha'(R) \cdot m_0 \approx_s \alpha'(R') \cdot m_1$. Consequently, we can get that $(y_1, y_2) \approx_s (y_1', y_2')$.

4. A Digital Signature Scheme Based on the New MST_3 Cryptosystem

In this section, we utilize the encryption scheme above to construct a digital signature scheme based on random covers and logarithmic signatures.

4.1. Description of the Scheme

Key Generation

Input: a large group $G = A(m, \theta)$ and $q = 2^m$.

Output: a public key $[\alpha, \gamma, f, H]$ with corresponding private key $[\beta, (t_0, \dots, t_s)]$.

(1) Choose a tame logarithmic signature $\beta = [B_1, B_2, \dots, B_s] := (b_{ij}) = (S(0, b_{(ij).b}))$ of type (r_1, r_2, \dots, r_s) for \mathcal{Z} , where $b_{ij} \in G$ and $b_{(ij).b} \in \mathbb{F}_q$.

(2) Select a random cover $\alpha = [A_1, A_2, \dots, A_s] := (a_{ij}) = (S(a_{(ij).a}, a_{(ij).b}))$ of the same type as β for a certain subset J of G such that $A_1, \dots, A_s \subseteq G \setminus \mathcal{Z}$, where $a_{ij} \in G$, $a_{(ij).a} \in \mathbb{F}_q \setminus \{0\}$, and $a_{(ij).b} \in \mathbb{F}_q$.

(3) Choose $t_0, t_1, \dots, t_s \in G \setminus \mathcal{Z}$.

(4) Construct a homomorphisms $f: G \rightarrow \mathcal{Z}$ defined by $f(S(a, b)) = S(0, a)$.

(5) Compute $\gamma := (h_{ij}) = (S(h_{(ij).a}, h_{(ij).b}))$, where $h_{ij} = t_{i-1}^{-1} \cdot f(a_{ij}) \cdot b_{ij} \cdot t_i$.

(6) Define a hash function $H: G \times G \rightarrow G$.

(7) Output public key $[\alpha, \gamma, f, H]$ and private key $[\beta, (t_0, \dots, t_s)]$.

Signature

Input: a message $m \in G$ and private key $[\beta, (t_0, \dots, t_s)]$.

Output: signature $\sigma = (S_1, S_2)$.

(1) Randomly select $z \in \mathcal{Z}$ and compute a random element $r = t_0^{-1} z t_s \in G$. Let $c_2 = r$, $c_1 = H(m, r)$.

(2) Compute $S_1 = \beta'^{-1}(f(c_1))^{-1} \cdot t_0 \cdot c_2 \cdot t_s^{-1}$ and $S_2 = \alpha'(S_1)^{-1} \cdot c_1$.

(3) Output $\sigma = (S_1, S_2)$.

Verification

Input: the message $m \in G$, signature $\sigma = (S_1, S_2)$, and public key $[\alpha, \gamma, f, H]$.

Output: 0 or 1.

(1) Compute $A = \alpha'(S_1) \cdot S_2$ and $B = H(m, \gamma'(S_1) \cdot f(S_2))$.

(2) If $A = B$, output 1; otherwise output 0.

Correctness. For a given message $m \in G$,

$$\begin{aligned} \gamma'(S_1) &= t_0^{-1} \cdot f(\alpha'(S_1)) \cdot \beta'(S_1) \cdot t_s \\ \implies S_1 &= \beta'^{-1} \left(f(\alpha'(S_1))^{-1} \cdot t_0 \cdot \gamma'(S_1) \cdot t_s^{-1} \right). \end{aligned} \quad (22)$$

Meanwhile, $S_1 = \beta'^{-1}(f(c_1))^{-1} \cdot t_0 \cdot c_2 \cdot t_s^{-1}$ and $c_1 = \alpha'(S_1) \cdot S_2$.

Hence,

$$\begin{aligned} &f(\alpha'(S_1))^{-1} \cdot t_0 \cdot \gamma'(S_1) \cdot t_s^{-1} \\ &= f(c_1)^{-1} \cdot t_0 \cdot c_2 \cdot t_s^{-1} \\ &= f(\alpha'(S_1) \cdot S_2)^{-1} \cdot t_0 \cdot c_2 \cdot t_s^{-1} \\ &= f(\alpha'(S_1))^{-1} \cdot t_0 \cdot (f(S_2)^{-1} \cdot c_2) \cdot t_s^{-1} \\ &\implies \gamma'(S_1) = f(S_2)^{-1} \cdot c_2 \\ &\implies c_2 = \gamma'(S_1) \cdot f(S_2). \end{aligned} \quad (23)$$

Consequently, we have

$$\begin{aligned} H(m, c_2) &= c_1 \\ \implies H(m, \gamma'(S_1) \cdot f(S_2)) &= \alpha'(S_1) \cdot S_2. \end{aligned} \quad (24)$$

4.2. Security Analysis

4.2.1. Attack on Private Key. (a) Compared with the encryption scheme in Section 3, we add a secure hash function in the signature scheme. Hence, analysis of the security of the signature scheme is similar to that in the encryption scheme. In the signature scheme, the goal of the general attack is also to determine β and (t_0, t_s) from the equation

$$\beta'(R) = y_2 t_s^{-1} f(y_1)^{-1} t_0, \quad (25)$$

where $y_1 = \alpha'(R) \cdot x$, $y_2 = \gamma'(R)$, and $f(y_1)^{-1} \in \mathcal{Z}$. Let $\{R_1, R_2, \dots, R_n\}$ be a collection of random numbers chosen by the adversary. Then we have

$$\begin{aligned} \beta'(R_i) &= y_{i2} t_s^{-1} f(y_{i1})^{-1} t_0 \\ &= f(y_{i1})^{-1} y_{i2} t_s^{-1} t_0, \end{aligned} \quad (26)$$

where $y_{i1} = \alpha'(R_i) \cdot x$, $y_{i2} = \gamma'(R_i)$, and $f(y_{i1})^{-1} \in \mathcal{Z}$. Then

$$\begin{aligned} f(y_{i1})^{-1} y_{i2} t_s^{-1} t_0 &\in \mathcal{Z} \\ \implies t_0 &\in t_s y_{i2}^{-1} f(y_{i1}) \mathcal{Z}. \end{aligned} \quad (27)$$

As described in Section 3, there are $q^2 - q$ different solutions; the success probability of the adversary is $1/(q(q-1))$.

(b) In our signature scheme, we construct a ciphertext pair (c_1, c_2) then obtain the signature $\sigma = (S_1, S_2)$ by decrypting the pair (c_1, c_2) . Therefore, analysis of the equivalent key is similar to that in Section 3. In this attack, an adversary mainly wants to utilize equivalent secret key $[\beta^*, (t_0^*, \dots, t_s^*)]$

to replace the real secret key $[\beta, (t_0, \dots, t_s)]$. As described in Section 3, for a random number $R \in \mathbb{Z}_{|\mathcal{X}|}$,

$$\begin{aligned} \gamma'(R) &= \beta'(R) t_0^{-1} f(\alpha'(R)) t_s \\ &= \beta'(R) t_0^{*-1} z_0 f(\alpha'(R)) t_s^* \prod_{k=1}^s c_k \\ &= \left(\beta'(R) \prod_{k=1}^s c_k \right) t_0^{*-1} f(\alpha'(R)) t_s^*. \end{aligned} \quad (28)$$

Let $\beta'(R) = b_{1x_1} b_{2x_2} \cdots b_{sx_s}$ and $\beta^* := (b_{ij}^*), b_{ij}^* = b_{ij} c_i$; then

$$\begin{aligned} \beta^*(R) &= b_{1x_1}^* b_{2x_2}^* \cdots b_{sx_s}^* \\ &= b_{1x_1} c_1 b_{2x_2} c_2 \cdots b_{sx_s} c_s \\ &= \beta'(R) \prod_{k=1}^s c_k. \end{aligned} \quad (29)$$

Consequently, the complexity for this attack is $\mathcal{O}(q)$. While, due to the center \mathcal{Z} of Suzuki 2-group having a large order q , so the attack is computationally infeasible.

4.2.2. Unforgeability. Suppose that Eve attempts to forge a message-signature pair (m^*, S_1^*, S_2^*) such that

$$\alpha(S_1^*) \cdot S_2^* = H(m^*, \gamma'(S_1^*) \cdot f(S_2^*)). \quad (30)$$

Case 1. Eve chooses a random number $S_1^* \in \mathbb{Z}_{|\mathcal{X}|}$ and $S_2^* \in G$ then computes $\alpha(S_1^*) \cdot S_2^*$ and $\gamma'(S_1^*) \cdot f(S_2^*)$. If Eve can get a message m^* satisfying the above equation, then he can answer the preimage of hash function H , but it is infeasible since H is a secure cryptographic hash function.

Case 2. Eve randomly selects two elements $m^* \in G$ and $S_2^* \in G$ and computes $c_1^* = H(m^*, c_1^*)$. In order to obtain a valid S_1^* , Eve selects c_1^* and computes $y = H(m^*, c_1^* \cdot f(S_2^*)) \cdot (S_2^*)^{-1}$. Getting a right S_1^* such that $\alpha(S_1^*) \cdot S_2^* = H(m^*, \gamma'(S_1^*) \cdot f(S_2^*))$ is equivalent to solving the equations $c_1^* = \gamma'(S_1^*)$ and $y = \alpha'(S_1^*)$. Since α' and γ' are both one-way functions, so Eve cannot answer right S_1^* by considering the corresponding ciphertext (c_1^*, y) .

Case 3. Eve randomly chooses one pair (m^*, S_1^*) and $r \in \mathcal{Z}$ then computes $S_2^* = \alpha'(S_1^*)^{-1} \cdot H(m^*, \gamma'(S_1^*) \cdot r)$. If $f(S_2^*) = r$, then Eve can forge one valid signature. Note that the probability of this case is $\Pr[f(S_2^*) = r] = 1/q$ for $|\mathcal{Z}| = q$. Since q is large enough, this attack is computationally infeasible.

5. Comparisons and Illustrations

5.1. Comparisons. In this subsection, we compare $eMST_3$ encryption scheme in [34] and our encryption scheme on number of basic operations. Then, we make further efforts to show the performance of our signature scheme. We

summarize the number of basic operations (addition (ADD), multiplication (MULT), exponentiation with θ ($\text{EXP}(\theta)$), etc.).

Table 1 shows the number of operations required for $eMST_3$ scheme and our scheme. The corresponding operations are namely addition (ADD), multiplication (MULT), exponentiation with θ ($\text{EXP}(\theta)$), generation of m -bit random R (PRNG) [36], and factorization of $\beta'(R) \in \mathcal{Z}$ with respect to a logarithmic signature β using the Algorithms 9, 10, and 11 (FACTOR) [34].

Table 2 presents the number of operations required for public key and secret key. The corresponding operations are, namely, addition (ADD) and multiplication (MULT) generation of m -bit random R (PRNG) [36].

For example, when $s = 26$, $v = 52$, the number of multiplication for secret key β is 1792 and the number of generation of m -bit random R is 760; when $s = 23$, $v = 44$, the number of multiplication for secret key β is 2688 and the number of generation of m -bit random R is 948; when $s = 20$, $v = 58$, the number of multiplication for secret key β is 4864 and the number of generation of m -bit random R is 712.

Table 3 indicates the performance of the signature scheme. Table 4 indicates parameter size in our schemes. Here, we mainly analyse the number of elements in Suzuki 2-group.

Remark 3. In the community of cryptography based on chaos theory, a lot of efforts were focused on secret key cryptography in early years [5–7]. Recently, Wang et al. [8–14] made progress on building public key agreement protocols by using chaos theory. The corresponding schemes also have high efficiency and strong security. Being different from quantum cryptography, chaotic cryptography, and DNA cryptography, MST_3 cryptosystem is a public key cryptosystem of classical cryptography. The hardness of our encryption scheme is based on a type of intractable mathematical problem called group factorization problem. Meanwhile, our encryption scheme and signature scheme are efficient in classical computer.

5.2. A Toy Example. In this subsection, we present a toy example of signing a random element $m \in \mathbb{F}_q$. In fact, our method is universal in the sense that it can be used to sign documents or realize authentication protocols based on images.

Key Generation

Input: a Suzuki 2-group $G = A(m, \theta)$ with $m = 8$, $q = 2^8$ and $s = 2$.

Output: public key $[\alpha, \gamma, f, H]$ and private key $[\beta, t_0, t_1, t_2]$.

In general, let a pair (a, b) denote an element of group G . For simplicity, we use a binary number of an element $b \in \mathbb{F}_q$ to present $(0, b) \in \mathcal{Z}$ and a binary numbers pair to present $(a, b) \in G$.

TABLE 1: Number of basic operations for one encryption/decryption.

		\mathbb{F}_{2^m} ADD	\mathbb{F}_{2^m} MULT	\mathbb{F}_{2^m} EXP(θ)	\mathbb{F}_{2^m} PRNG	Factor
Encryption ¹	$eMST_3$ scheme [34]	$8s - 6$	$2s - 2$	—	1	—
	Our scheme	$8s - 7$	$2s - 2$	—	1	—
Decryption ²	$eMST_3$ scheme	$4s + 15$	$s + 5$	1	—	1
	Our scheme	$4s + 10$	$s + 3$	—	—	1

¹ Compared with $eMST_3$ scheme, our scheme reduces a step of multiplication with the element of the center \mathcal{Z} in the stage of encryption. Thus, the number of (\mathbb{F}_{2^m} ADD) reduces once.

² In the stage of decryption, our scheme reduces a step of inverse operation, a step of multiplication operation, and a \mathbb{F}_{2^m} EXP(θ) operation, so the number of (\mathbb{F}_{2^m} ADD) reduces five times and (\mathbb{F}_{2^m} MULT) reduces twice.

TABLE 2: Number of basic operations for public key generation.

	Secret key β	Secret key $[t_0, \dots, t_s]$	Public key α	Public key γ
\mathbb{F}_{2^m} ADD	T^3	—	T	$9T + s$
\mathbb{F}_{2^m} MULT	—	$s + 1^4$	$T - s$	$2T + s$
\mathbb{F}_{2^m} PRNG	$\sum_{i=1}^v r_i^{*5}$	$2(s + 1)$	$2T - s$	—

³ $T = \sum_{i=1}^s r_i$, $r_i = \prod_{j=1}^{u_i} r_{ij}^* \cdot w_i$ for $1 \leq i \leq s$ and $\sum_{i=1}^s u_i = v$, where $w_i = \begin{cases} 0 & \text{if } u_i = 1 \\ 1 & \text{if } u_i > 1 \end{cases}$.

⁴ For $a \in \mathbb{F}_q$, $\theta : a \rightarrow a^2$ is a Frobenius automorphism. Hence, θ can be reduced to a multiplication.

⁵ v represents the number of blocks before fusion.

(i) For simplicity, we use a one-way function H as the hash function in our scheme. That is, $H: G \times G \rightarrow G$ is given by

$$H((a_1, b_1), (a_2, b_2)) = (a_1^{a_2}, b_1^{b_2}). \quad (31)$$

Actually, one can also use standard hash functions like SHA1 and so forth.

(ii) A factorizable logarithmic signature $\beta = [B_1, B_2] = (b_{i,j}) = (S(0, b_{(ij),2}))$ of type (r_1, \dots, r_s) for \mathcal{Z} .

(1) We first construct canonical logarithmic signature $[B_1^*, B_2^*, B_3^*]$ of type $(4, 8, 8)$ in standard form:

$$\begin{aligned}
 B_1^* &= \{[0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0], [0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0], \\
 &\quad [1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0], [1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]\}, \\
 B_2^* &= \{[1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0], [0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0], \\
 &\quad [0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0], [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0], \\
 &\quad [0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0], [0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0], \\
 &\quad [1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0], [1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0]\}, \\
 B_3^* &= \{[1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0], [1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1], \\
 &\quad [0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0], [1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1], \\
 &\quad [0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0], [0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1], \\
 &\quad [1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0], [0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1]\}. \quad (32)
 \end{aligned}$$

(2) Fuse blocks B_1^*, B_3^* to construct the product $B_2 = (B_1^* \cdot B_3^*)$ and let $B_1 = B_2^*$. That is, B_1, B_2 is the logarithmic signature of type (r_1, r_2) ($r_1 = 8, r_2 = 32$)

$$\begin{aligned}
 B_1 &= \{[1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0], [0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0], \\
 &\quad [0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0], [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0], \\
 &\quad [0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0], [0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0], \\
 &\quad [1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0], [1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0]\}, \quad (33)
 \end{aligned}$$

$$\begin{aligned}
 B_2 &= \{[1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0], [1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1], \\
 &\quad [0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0], [1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1], \\
 &\quad [0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0], [0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1], \\
 &\quad [1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0], [0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1], \\
 &\quad [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0], [1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1], \\
 &\quad [0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0], [1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1], \\
 &\quad [0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0], [0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1], \\
 &\quad [1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0], [0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1], \\
 &\quad [0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0], [0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1], \\
 &\quad [1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0], [0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1], \\
 &\quad [1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0], [1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1], \\
 &\quad [0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0], [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1]\},
 \end{aligned}$$

TABLE 3: Number of basic operations for digital signature scheme.

	\mathbb{F}_{2^m} ADD	\mathbb{F}_{2^m} MULT	\mathbb{F}_{2^m} EXP(θ)	\mathbb{F}_{2^m} PRNG	Factor
Signature	$4s + 11$	$s + 3$	—	1	1
Verification	$8s - 7$	$2s - 2$	—	—	—

$$\begin{aligned}
& [0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0], [0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1], \\
& [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0], [0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1], \\
& [1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0], [1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1], \\
& [0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0], [1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1] \}.
\end{aligned} \tag{34}$$

(i) A random cover $\alpha = [A_1, A_2] = (a_{ij}) = (S(a_{(ij),1}, a_{(ij),2}))$ of the same type as β

$$\begin{aligned}
A_1 = \{ & ([0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1], [0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0]), \\
& ([0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0], [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0]), \\
& ([1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0], [1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0]), \\
& ([1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0], [0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0]), \\
& ([1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0], [1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0]), \\
& ([1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1], [0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0]), \\
& ([0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1], [1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1]), \\
& ([0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1], [1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1]) \}, \\
A_2 = \{ & ([0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1], [0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0]), \\
& ([0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0], [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0]), \\
& ([0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0], [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1]), \\
& ([1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0], [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1]), \\
& ([1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0]), \\
& ([1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1], [1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0]), \\
& ([0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1], [1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0]), \\
& ([0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1], [0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1]), \\
& ([0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1], [0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0]), \\
& ([0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0], [0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0]), \\
& ([1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1], [1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1]), \\
& ([0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1], [1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0]), \\
& ([0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1], [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1]) \}.
\end{aligned}$$

TABLE 4: Parameter size.

	Public key	Secret key	Encryption	Signature
Number of elements	$2T^6$	$T + s + 1$	2	2

⁶ T is the same as Table 2.

$$\begin{aligned}
& ([1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0], [1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1]), \\
& ([1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0], [1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0]), \\
& ([0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1], [0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0]), \\
& ([1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1], [0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0]), \\
& ([1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0], [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0]), \\
& ([0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1], [1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1]), \\
& ([0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0], [1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]), \\
& ([1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0], [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0]), \\
& ([0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0], [0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0]), \\
& ([1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1], [0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0]), \\
& ([1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1], [1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1]), \\
& ([0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0], [1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1]), \\
& ([1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0], [0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0]), \\
& ([1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0], [1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0]), \\
& ([0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1], [1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0]), \\
& ([0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0], [1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1]), \\
& ([1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1], [0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0]), \\
& ([0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1], [0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]), \\
& ([0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1], [0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1]) \}.
\end{aligned} \tag{35}$$

(ii) Select $t_0, t_1, t_2 \in G \setminus \mathcal{Z}$:

$$\begin{aligned}
t_0 &= ([1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0], [1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1]), \\
t_1 &= ([0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0], [0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1]), \\
t_2 &= ([1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1], [1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0]).
\end{aligned} \tag{36}$$

(iii) Construct a homomorphism $f: G \rightarrow \mathcal{Z}: f(a, b) = (0, a)$.

(iv) Compute $\gamma = (h_{i,j}), h_{i,j} = t_{i-1}^{-1} \cdot f(a_{i,j}) \cdot b_{i,j} \cdot t_i = [V_1, V_2]$, and $i = 0, 1, 2$:

$$V_1 = \{([1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0], [1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0], [0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0], [1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0], [1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0], [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0]),$$

$$([1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0], [1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0], [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0], [1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1])\},$$
(37)

$$V_2 = \{([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1]),$$

$$([1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1], [1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0])\}.$$
(38)

Signature

(i) Choose a message $M = ([1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1], [1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1])$.

(ii) Sample $z = ([0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0], [1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0]) \in \mathcal{Z}$ and compute $r = t_0^{-1} \cdot z \cdot t_2$

$$c_2 = r = ([0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1], [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1]),$$

$$c_1 = H(M, r)$$

$$= ([0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1], [0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0]).$$
(39)

(iii) Signature $\sigma = (S_1, S_2)$:

$$S_1 = 71 \ (\in \mathbb{Z}_q),$$

$$S_2 = ([0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1], [0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0]).$$
(40)

Verification

(i) Compute

$$Y_1 = \alpha' (S_1) \cdot S_2$$

$$= ([0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1], [0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0]).$$
(41)

(ii) Compute

$$\gamma' (S_1)$$

$$= ([0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1], [0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0]),$$

$$f(S_2)$$

$$= ([0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0], [0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1]),$$

$$Y_2 = \gamma' (S_1) \cdot f(S_2)$$

$$= ([0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1], [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1]).$$
(42)

Since $Y_1 - c_1 = [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]$ and $Y_2 - c_2 = [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]$, so we can get that $H(M, \gamma'(S_1) \cdot f(S_2)) = \alpha'(S_1) \cdot S_2$.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (NSFC) (nos. 61103198, 61121061, 61370194) and the NSFC A3 Foresight Program (no. 61161140320).

References

- [1] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, Bangalore, India, 1984.
- [2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, pp. 3121–3124, 1992.
- [3] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters*, vol. 68, no. 5, pp. 557–559, 1992.
- [4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 146–195, 2002.
- [5] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.
- [6] M. S. Baptista, "Cryptography with chaos," *Physics Letters A*, vol. 240, no. 1–2, pp. 50–54, 1998.
- [7] G. Alvarez, G. Pastor, F. Montoya, and M. Romera, "Chaotic cryptosystems," in *Proceedings of the IEEE International Carnahan Conference on Security Technology*, pp. 332–338, 1999.
- [8] X.-Y. Wang and Q. Yu, "Block encryption algorithm based on dynamic sequences of multiple chaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 2, pp. 574–581, 2009.
- [9] X. Wang and J. Zhao, "An improved key agreement protocol based on chaos," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 4052–4057, 2010.
- [10] Y. Niu and X. Wang, "An anonymous key agreement protocol based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 4, pp. 1986–1992, 2011.
- [11] L. Hongjun, W. Xingyuan, and K. Abdurahman, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.
- [12] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.
- [13] W. Xingyuan and L. Dapeng, "A secure key agreement protocol based on chaotic maps," *Chinese Physics B*, vol. 22, no. 11, Article ID 110503, 2013.
- [14] Y.-Q. Zhang and X.-Y. Wang, "Spatiotemporal chaos in mixed linear–nonlinear coupled logistic map lattice," *Physica A: Statistical Mechanics and Its Applications*, vol. 402, pp. 104–118, 2014.
- [15] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024, 1994.
- [16] D. Boneh, C. Dunworth, R. J. Lipton, and J. Sgall, "On the computational power of DNA," *Discrete Applied Mathematics*, vol. 71, no. 1–3, pp. 79–94, 1996.
- [17] G. Cui, L. Qin, Y. Wang, and X. Zhang, "An encryption scheme using DNA technology," in *Proceedings of the 3rd International Conference on Bio-Inspired Computing: Theories and Applications (BICTA '08)*, pp. 37–41, October 2008.
- [18] W. Lempken, T. van Trung, S. S. Magliveras, and W. Wei, "A public key cryptosystem based on non-abelian finite groups," *Journal of Cryptology*, vol. 22, no. 1, pp. 62–74, 2009.
- [19] N. R. Wagner and M. R. Magyarik, "A public-key cryptosystem based on the word problem," in *Advances in Cryptology*, vol. 196 of *Lecture Notes in Computer Science*, pp. 19–36, Springer, Berlin, Germany, 1985.
- [20] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, and C. Park, "New public-key cryptosystem using braid groups," in *Advances in cryptology—CRYPTO 2000*, vol. 1880 of *Lecture Notes in Computer Science*, pp. 166–183, Springer, Berlin, Germany, 2000.
- [21] B. Eick and D. Kahrobaei, "Polycyclic groups: a new platform for cryptology?" <http://arxiv.org/abs/math/0411077>.
- [22] V. Shpilrain and A. Ushakov, "Thompsons group and public key cryptography," in *Applied Cryptography and Network Security*, vol. 3531 of *Lecture Notes in Computer Science*, pp. 151–164, 2005.
- [23] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public key exchange using matrices over group rings," *Groups, Complexity, and Cryptology*, vol. 5, no. 1, pp. 97–115, 2013.
- [24] S. S. Magliveras, "A cryptosystem from logarithmic signatures of finite groups," in *Proceedings of the 29th Midwest Symposium on Circuits and Systems*, pp. 972–975, Elsevier Publishing, Amsterdam, The Netherlands, 1986.
- [25] S. S. Magliveras and N. D. Memon, "Algebraic properties of cryptosystem PGM," *Journal of Cryptology*, vol. 5, no. 3, pp. 167–183, 1992.
- [26] A. Caranti and F. Dalla Volta, "The round functions of cryptosystem PGM generate the symmetric group," *Designs, Codes and Cryptography*, vol. 38, no. 1, pp. 147–155, 2006.
- [27] S. S. Magliveras, D. R. Stinson, and T. van Trung, "New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups," *Journal of Cryptology*, vol. 15, no. 4, pp. 285–297, 2002.
- [28] M. I. González Vasco and R. Steinwandt, "Obstacles in two public key cryptosystems based on group factorizations," *Tatra Mountains Mathematical Publications*, vol. 25, pp. 23–37, 2002.
- [29] J.-M. Bohli, R. Steinwandt, M. I. González Vasco, and C. Martínez, "Weak keys in MST_1 ," *Designs, Codes and Cryptography*, vol. 37, no. 3, pp. 509–524, 2005.
- [30] M. I. González Vasco, C. Martínez, and R. Steinwandt, "Towards a uniform description of several group based cryptographic primitives," *Designs, Codes and Cryptography*, vol. 33, no. 3, pp. 215–226, 2004.
- [31] S. S. Magliveras, P. Svaba, T. van Trung, and P. Zajac, "On the security of a realization of cryptosystem MST_3 ," *Tatra Mountains Mathematical Publications*, vol. 41, pp. 65–78, 2008.

- [32] S. R. Blackburn, C. Cid, and C. Mullan, "Cryptanalysis of the MST_3 public key cryptosystem," *Journal of Mathematical Cryptology*, vol. 3, no. 4, pp. 321–338, 2009.
- [33] M. I. G. Vasco, A. L. P. del Pozo, and P. T. Duarte, "A note on the security of MST_3 ," *Designs, Codes and Cryptography*, vol. 55, no. 2-3, pp. 189–200, 2010.
- [34] P. Svaba and T. van Trung, "Public key cryptosystem MST_3 cryptanalysis and realization," *Journal of Mathematical Cryptology*, vol. 4, no. 3, pp. 271–315, 2010.
- [35] W. Lempken and T. van Trung, "On minimal logarithmic signatures of finite groups," *Experimental Mathematics*, vol. 14, no. 3, pp. 257–269, 2005.
- [36] P. Marquardt, P. Svaba, and T. van Trung, "Pseudorandom number generators based on random covers for finite groups," *Designs, Codes and Cryptography*, vol. 64, no. 1-2, pp. 209–220, 2012.

