










Encryption Scheme Based on the Generalized Suzuki 2-groups and Homomorphic Encryption

Gennady Khalimov¹ , Yevgen Kotukh² , Sang-Yoon Chang³ ,
Yaroslav Balytskyi³ , Maksym Kolisnyk¹ , Svitlana Khalimova¹ ,
and Oleksandr Marukhnenko¹ 

¹ Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

² Sumy State University, Sumy, Ukraine

³ University of Colorado Colorado Springs, Colorado Springs, CO, USA

Abstract. This article describes a new implementation of MST-based encryption for generalized Suzuki 2-groups. The well-known MST cryptosystem based on Suzuki groups is built on a logarithmic signature at the center of the group, resulting in a large array of logarithmic signatures. An encryption scheme based on multiparameter non-commutative groups is proposed. The multiparameter generalized 2 - Suzuki group was chosen as one of the group constructions. In this case, a logarithmic signature is established for the entire group. The main difference from the known one is the use of homomorphic encryption to construct coverings of logarithmic signatures for all group parameters. This design improves a secrecy of the cryptosystem is ensured at the level of a brute-force attack.

Keywords: MST cryptosystem · Logarithmic signature · Random cover · Generalized Suzuki 2-groups

1 Introduction

Recent advances in quantum computing for solving complex problems formulate new trends for building secure public-key cryptosystems. The main directions in this area are the solution of the problem of finding the conjugate element in the theory of non-commutative groups and the word problem in groups and semigroups. The word complexity problem was proposed by Wagner and Magyarik [1] and implemented in several cryptosystems. One of the best known and most studied is a cryptosystem based on factorization in finite groups of permutations, called the logarithmic signature [2]. In 2009, Lempken et al. described an MST3 public-key cryptosystem based on a logarithmic signature and a Suzuki 2-group [2]. In 2008 Magliveras et al. [4] presented a comprehensive analysis of the MST3 cryptosystem identifying limitations for the logarithmic signature and stated that the transitive logarithmic signature is not suitable for the MST3 cryptosystem. In 2010, Swaba et al. [5] analyzed all known attacks on MST cryptography and built a more secure eMST3 cryptosystem by adding a secret homomorphic coverage. In 2018, T. van Trung [7] proposed a general method for constructing strong

aperiodic logarithmic signatures for Abelian p-groups, which is a further contribution to the practical application of MST cryptosystems.

The construction of MST cryptosystems based on multiparameter non-commutative groups was proposed in [7–9]. MST cryptosystems based on multi-parameter groups allow optimizing the costs of cryptosystem parameters and secrecy.

Generalized Suzuki 2-groups are multivariable and have the highest group order compared to other multivariable groups. The first implementation of the cryptosystem on the generalized Suzuki 2-group is presented in [8] and does not provide protection against brute force attacks with sequential brute force key recovery. Analysis of MST cryptosystems by group shows their vulnerability to highlighted text attacks. The design feature of all known MST implementations is the presence of known texts and, as a consequence, the possibility of such cryptanalysis. A secure encryption scheme is proposed based on the generic Suzuki 2-group with homomorphic encryption.

2 Proposal

The generalizations of Suzuki 2-groups is defined over a finite field, $F_q, q = 2^n, n > 0$ for a positive integer l and $a_1, a_2, \dots, a_l \in F$ for some automorphism θ of F as [10]:

$$A_l(n, \theta) = \{S(a_1, a_2, \dots, a_l) | a_i \in F_q\}$$

Each element of $A_l(n, \theta)$ can be expressed uniquely and it follows that $|A_l(n, \theta)| = 2^{nl}$ and $A_l(n, \theta)$ define a group of order 2^{nl} . If $l = 2$, this group is isomorphic to a Suzuki 2-group $A(n, \theta)$.

Group operation is defined as a product:

$$\begin{aligned} S(a_1, a_2, \dots, a_l)S(b_1, b_2, \dots, b_l) &= S(a_1 + b_1, a_2 + (a_1\theta)b_1 \\ &+ b_2, a_3 + (a_2\theta)b_1 + (a_1\theta^2)b_2 + b_3, \\ &\dots, a_l + (a_{l-1}\theta)b_1 + \dots + (a_1\theta^{l-1})b_{l-1} + b_l). \end{aligned}$$

with the Identity element being $S(0_1, 0, \dots, 0)$.

The inverse element is given by:

$$\begin{aligned} S(a_1, a_2, a_3, \dots, a_l)^{-1} &= S(a_1, a_2 + a_1\theta a_1, a_3 + a_2\theta a_1 \\ &+ a_1\theta^2(a_2 + a_1\theta a_1), \dots, a_l + a_{l-1}\theta a_1 + \dots). \end{aligned}$$

The group G is nonabelian group and has nontrivial center:

$$Z(G) = \{S(0, 0, \dots, c) | c \in F_q\}.$$

Assume that θ is the Frobenius automorphism of $F, \theta : x \rightarrow x^2$. For the fixed finite field, the group $A_l(n, \theta)$ order is greater than the classical Suzuki 2 - group.

In the new implementation of the cryptosystem, we have changed the encryption algorithm and suggest using homomorphic encryption for random covers. In this case, the complexity of the key recovery attack will be determined by exhaustive search over the entire group.

2.1 Description of the Scheme

Our proposal is to create a logarithmic signature for the whole generalized Suzuki 2-group and homomorphic encryption of random covers in the logarithmic signature.

Let's take a look at the basic steps of encryption.

Key Generation.

We fix a large group $A_l(n, \theta) = \{S(a_1, a_2, \dots, a_l) | a_i \in F_q\}$, $q = 2^n$.

Let's build a tame logarithmic signatures $\beta_k = [B_{1(k)}, \dots, B_{s(k)}] = (b_{ij})_k = S(0, \dots, 0, b_{ij(k)}, 0, \dots, 0)$ of type: $(r_{1(k)}, \dots, r_{s(k)})$, $i = \overline{0}, s(k), j = \overline{1}, r_{i(k)}, b_{ij(k)} \in F_q$, $k = \overline{1, l}$.

Let's set a random cover:

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, \dots, a_{ij(k)}^{(l)})$$

of the same type as β_k , where $a_{ij} \in A_l(n, \theta)$, $a_{ij(k)}^{(v)} \in F_q \setminus \{0\}$, $i = \overline{1, s}, j = \overline{1, r_{i(k)}}$, $k = \overline{1, l}$.

Select the random covers:

$w_{(k)} = [W_{1(k)}, \dots, W_{s(k)}] = (w_{ij})_{(k)} = S(w_{ij(k)}^{(1)}, w_{ij(k)}^{(2)}, \dots, w_{ij(k)}^{(l)})$ of the same types as $\beta_{(k)}$, where $w_{ij} \in A_l(n, \theta)$, $w_{ij(k)} \in F_q \setminus \{0\}$, $i = \overline{0}, s(k), j = \overline{1, r_{i(k)}}$, $k = \overline{1, l}$.

Let's generate random $t_{0(k)}, \dots, t_{s(k)} \in A_l(n, \theta) \setminus Z$, $t_{i(k)} = S(t_{i1(k)}, \dots, t_{il(k)})$, $t_{ij(k)} \in F^\times$, $i = \overline{0}, s(k)$, $k = \overline{1, l}$. Choose

$$\begin{aligned} \tau_{0(k)}, \dots, \tau_{s(k)} &\in A_l(n, \theta) \setminus Z, \tau_{i(k)} \\ &= S(\tau_{i1(k)}, \dots, \tau_{il(k)}), \tau_{ij(k)} \in F^\times, i = \overline{0}, s(k), k = \overline{1, l}. \end{aligned}$$

Let's take $t_{s(k-1)} = t_{0(k)}$, $\tau_{s(k-1)} = \tau_{0(k)}$, $k = \overline{1, l}$.

Let's define an additional group operation:

$$\begin{aligned} S(a_1, a_2, \dots, a_l) \circ^{(k)} S(b_1, b_2, \dots, b_l) = \\ S(a_1 + b_1, a_2 + b_2, \dots, a_k + b_k, a_{k+1} + a_k^2 b_1 + \dots + a_1^{2^k} b_k \\ + b_{k+1}, \dots, a_l + a_{l-1}^2 b_1 + \dots + a_1^{2^{l-1}} b_{l-1} + b_l). \end{aligned}$$

The inverse element $S^{-(k)}$ for the group operation $\circ^{(k)}$ is

$$S^{-(k)}(a_1, a_2, \dots, a_l) = S(a_1, a_2, \dots, a_k, \alpha_{k+1}, \dots, \alpha_l)$$

where

$$\begin{aligned} \alpha_{k+1} &= a_{k+1} + a_k^2 a_1 + \dots + a_2^{2^{k-1}} a_{k-1} + a_1^{2^k} a_k, \\ \alpha_{k+2} &= a_{k+2} + a_{k+1}^2 a_1 + \dots + a_3^{2^{k-1}} a_{k-1} + a_2^{2^k} a_k + a_1^{2^{k+1}} \alpha_{k+1}, \\ &\dots \\ \alpha_l &= a_l + a_{l-1}^2 a_1 + \dots + a_{l-k}^{2^k} a_k + a_{l-k-1}^{2^{k+1}} \alpha_{k+1} + \dots + a_l^{2^{l-1}} \alpha_{l-1} \end{aligned}$$

The application of additional group operation $\circ^{(k)}$ leads to homomorphic representation of group elements $S(a_1, a_2, \dots, a_l) \xrightarrow{\circ^{(k)}} S(a_1, a_2, \dots, a_k, \alpha_{k+1}, \dots, \alpha_l) = S^{(k)}$.

We apply inverse homomorphic transformation for the inverse and direct elements $S_1^{-(k)}$, $S_2^{(k)}$ of the group for the calculation in group with left inverse element $S_1^{-(n)\circ}$.

$S_3 = S_1^{-(k)\circ} \cdot S_2^{(k)\circ}$ For $S_1^{-(k)}$ we have:

$S^{-(k)\circ} = S^\circ(a_1, a_2, \dots, a_k, \alpha_{k+1}, \dots, \alpha_l) = S(\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_l)$, where

$$\alpha_1 = a_1, \alpha_2 = a_2 + a_1^2 a_1, \dots, \alpha_k = a_k + a_{k-1}^2 a_1 + \dots, a_l^{2^{k-1}} a_{k-1}.$$

and for $S_2^{(k)}$ respectively to $S_3 = S_1^{-(k)\circ} \cdot S_2^{(k)\circ}$ we get

$$S^{(k)\circ} = S^\circ(b_1, b_2, \dots, b_k, \beta_{k+1}, \dots, \beta_l) = S(\beta_1, \dots, \beta_k, \beta_{k+1}, \dots, \beta_l)$$

$$\beta_1 = b_1, \beta_2 = b_2 + a_1^2(b_1 + a_1), \dots$$

$$\beta_k = b_k + a_{k-1}^2(b_1 + a_1) + \dots, a_l^{2^{k-1}}(b_{k-1} + a_{k-1}).$$

Homomorphic transformations for $S^{-(k)\circ}$, $S^{(k)\circ}$ are needed to for not breaking the group operation when calculating the elements of the group $A_l(n, \theta)$.

Let $f(e)$ be a homomorphic cryptographic transformation with respect to addition $f(a + b) = f(a) + f(b)$, $e, a, b \in F_q$ and the corresponding inverse transformation $\hat{f}(e) = e$. We calculate the covering of the logarithmic signatures:

$$h_{(k)} = [h_{1(k)}, \dots, h_{s(k)}] = t_{(i-1)(k)}^{-(k)} \circ^{(k)} (w_{ij})_{(k)} \circ^{(k)} (b_{ij})_{(k)} \circ^{(k)} t_{i(k)}$$

and coverings of the homomorphic cryptographic transformation:

$$g_{(k)} = [g_{1(k)}, \dots, g_{s(k)}] = \tau_{(i-1)(k)}^{-(k)} \circ^{(k)} f(w_{ij})_{(k)} \circ^{(k)} \tau_{i(k)}, \text{ where}$$

$$f(w_{(k)}) = f(w_{ij})_{(k)} = S(f(w_{ij(k)_1}), f(w_{ij(k)_2}), \dots, f(w_{ij(k)_l})),$$

$$i = \overline{1, s(k)}, j = \overline{1, r_i(k)}, k = \overline{1, l}.$$

An output public key is (a_k, h_k, g_k) , and a private key $[f, \beta(k), (t_{0(k)}, \dots, t_{s(k)}), (\tau_{0(k)}, \dots, \tau_{s(k)})]$, $k = \overline{1, l}$ respectively.

Encryption

Let the message to be $x = S(x_1, \dots, x_l)$ and the public key (a_k, h_k, g_k) , $k = \overline{1, l}$ respectively. Choose a random $R = (R_1, \dots, R_l)$, $R_1, \dots, R_l \in \mathbb{Z}_{|F_q|}$.

Compute the ciphertext y_1, y_2, y_3 as:

$$\begin{aligned} y_1 &= \alpha(R) \cdot x = \alpha_1(R_1) \cdot \alpha_2(R_2) \dots \alpha_l(R_l) \cdot x \\ &= S\left(\sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} a_{ij(k)}^{(1)} + x_1, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} a_{ij(k)}^{(2)} + x_2 + *, \right. \\ &\quad \left. \dots, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} a_{ij(k)}^{(l)} + x_l + *, \right) \end{aligned}$$

$$\begin{aligned}
y_2 &= h(R) = h_1(R_1) \circ^{(1)} \\
&\left(h_2(R_2) \circ^{(2)} \dots \left(h_{l-1}(R_{l-1}) \circ^{(l-2)} \left(h_{l-1}(R_{l-1}) \circ^{(l-1)} h_l(R_l) \right) \right) \right) \\
&= S \left(\sum_{k=1}^l \sum_{i=1, j=R_{i(k)}}^{s(k)} w_{ij(k)}^{(1)} + \sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}, \sum_{k=1}^l \sum_{i=1, j=R_{i(k)}}^{s(k)} w_{ij(k)}^{(2)} \right. \\
&\quad \left. + \sum_{i=1, j=R_{i(2)}}^{s(2)} \beta_{ij(2)} + *, \dots, \sum_{k=1}^l \sum_{i=1, j=R_{i(k)}}^{s(k)} w_{ij(k)}^{(l)} + \sum_{i=1, j=R_{i(l)}}^{s(l)} \beta_{ij(l)} + * \right)
\end{aligned}$$

Here, the (*) components are determined by cross-calculations in the group operation of the product of $t_{0(k)}, \dots, t_{s(k)}$ and the product of $w_{(k)}(R_k) + \beta_{(k)}(R_k)$.

$$\begin{aligned}
y_3 &= g(R) = g_1(R_1) \circ^{(1)} \\
&\left(g_2(R_2) \circ^{(2)} \dots \left(g_{l-1}(R_{l-1}) \circ^{(l-2)} \left(g_{l-1}(R_{l-1}) \circ^{(l-1)} g_l(R_l) \right) \right) \right) \\
&= S \left(\sum_{k=1}^l \sum_{i=1, j=R_{i(k)}}^{s(k)} f(w_{ij(k)}^{(1)}) +, \sum_{k=1}^l \sum_{i=1, j=R_{i(k)}}^{s(k)} f(w_{ij(k)}^{(2)}) + *, \dots, \right. \\
&\quad \left. \sum_{k=1}^l \sum_{i=1, j=R_{i(k)}}^{s(k)} f(w_{ij(k)}^{(l)}) + * \right)
\end{aligned}$$

Here, the (*) components are determined by cross-calculations in the group operation of the product of $\tau_{0(k)}, \dots, \tau_{s(k)}$ and the product of $f(w_{(k)}(R_k))$.

Output: a ciphertext (y_1, y_2, y_3) of the message x .

Decryption *Input:* a ciphertext (y_1, y_2, y_3) and a private key $[f, \beta_{(k)}, t_{i(k)}, \tau_{i(k)}]$, $i = \overline{0, s(k)}, k = \overline{1, l}$.

To decrypt a message x , we need to restore random numbers $R = (R_1, R_2, \dots, R_l)$. Compute

$$\begin{aligned}
D^{(1)}(R) &= D^{(1)}(R_1, R_2, \dots, R_l) = t_{0(1)} \circ^{(1)} y_2 \circ^{(l)} t_{s(l)}^{-l)} \\
&= S \left(\sum_{i=1, j=R_{i(1)}}^{s(1)} w_{ij(1)}^{(1)} + \beta_1(R_1), *, \dots, * \right), \\
G^{(1)}(R) &= G^{(1)}(R_1, R_2, \dots, R_l) = \tau_{0(1)} \circ^{(1)} y_3 \circ^{(l)} \tau_{s(l)}^{-l)} \\
&= S \left(\sum_{i=1, j=R_{i(1)}}^{s(1)} f(w_{ij(1)}^{(1)}), *, \dots, * \right),
\end{aligned}$$

$$D^{(1)}(R)' = D^{(1)}(R) \circ^{(1)} \hat{f}(G^{(1)}(R))^{-l)} = S \left(\sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}, *, * \right) \text{ Restore } R_1 \text{ with}$$

$$\beta_{(1)}(R_1) = \sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)} \text{ using } \beta_{(1)}(R_1)^{-1}, \text{ because } \beta_1 \text{ is simple.}$$

For the further calculation, it is necessary to remove the component $h_1(R_1)$ from y_2 and $g_1(R_1)$ from y_3 . Compute

$$y_2^{(1)} = h_1(R_1)^{-(1)\circ} \cdot y_2^\circ, y_3^{(1)} = g_1(R_1)^{-(1)\circ} \cdot y_3^\circ, D(R)^{(2)} = t_{0(2)} \circ^{(2)} y_2^{(1)} \circ^{(l)} t_{s(l)}^{-(l)},$$

$$G(R)^{(2)} = \tau_{0(2)} \circ^{(2)} y_3^{(1)} \circ^{(l)} \tau_{s(l)}^{-(l)},$$

$$D^{(2)}(R)' = D^{(2)}(R) \circ^{(2)} \hat{f}(G^{(2)}(R))^{-(2)} = S(0, \sum_{i=1, j=R_i(2)}^{s(2)} \beta_{ij(2), *}, *).$$

and restore R_2 with $\beta_{(2)}(R_2) = \sum_{i=1, j=R_i(2)}^{s(2)} \beta_{ij(2)}$ using $\beta_{(2)}(R_2)^{-1}$, because β_2 is simple. We continue the calculations iteratively until the last value R_l is restored. We have the following recurrent relations for $n = \bar{1}, l - 1$:

$$y_2^{(n)} = h_n(R_n)^{-(n)\circ} \cdot y_2^{(n-1)\circ}, y_3^{(n)} = g_n(R_n)^{-(n)\circ} \cdot y_3^{(n-1)\circ},$$

$$D^{(n+1)}(R) = t_{0(n+1)} \circ^{(n+1)} y_2^{(n)} \circ^{(l)} t_{s(l)}^{-(l)}, G^{(n+1)}(R) = \tau_{0(n+1)} \circ^{(n+1)} y_3^{(n)} \circ^{(l)} \tau_{s(l)}^{-(l)},$$

$$D^{(n+1)}(R)' = D^{(n+1)}(R) \circ^{(n+1)} \hat{f}(G^{(n+1)}(R))^{-(n+1)} =$$

$$S(0, 0, \dots, 0, \sum_{i=1, j=R_i(n+1)}^{s(n+1)} \beta_{ij(n+1)}, *)$$

$$\text{Restore } R_{n+1} \text{ with } \beta_{(n+1)}(R_{n+1}) = \sum_{i=1, j=R_i(n+1)}^{s(n+1)} \beta_{ij(n+1)} \text{ using } \beta_{(n+1)}(R_{n+1})^{-1}.$$

Recovery of the message $x = a(R_1, R_2, \dots, R_l)^{-1} \cdot y_1$.

Example

We will show the correctness of the obtained expressions in the following simple example.

Let's fix the four-parameter generalized Suzuki group $G = A_4(n, \theta)$ over the finite field $F_q, q = 2^5, g(x) = x^5 + x^3 + 1$. Assume that θ is the Frobenius automorphism of $F_q, \theta : \alpha \rightarrow \alpha^2$. Group operation is defined as:

$$S(a_1, a_2, a_3, a_4)S(b_1, b_2, b_3, b_4) = S(a_1 + b_1, a_2 + a_1^2 b_1 + b_2,$$

$$a_3 + a_2^2 b_1 + a_1^4 b_2 + b_3, a_4 + a_3^2 b_1 + a_2^4 b_2 + a_1^8 b_3 + b_4).$$

The inverse element is determined as:

$$S(a_1, a_2, a_3, a_4)^{-1} = S(a_1, a_2 + a_1^3, a_3 + a_2^2 a_1 + a_1^4 a_2', a_4 + a_3^2 a_1 + a_2^4 a_2' + a_1^8 a_3')$$

$$\text{where } a_2' = a_2 + a_1^3, a_3' = a_3 + a_2^2 a_1 + a_1^4 a_2'.$$

Let's consider the basic steps of our calculations.

Generation of public and private keys

First stage is to generate a tame logarithmic signature with the dimension of corresponding selected type $(r_{1(k)}, \dots, r_{s(k)})$ and finite field F_q . The construction of arrays of logarithmic signatures is presented in [11]. For our example, we use the construction of simple logarithmic signatures without analyzing the details of their secrecy. Let's $\beta_{(k)}$

for $k = \overline{1, 3}$ have the types of $(2^2, 2^3)$, $(2, 2^2, 2^2)$, $(2^2, 2, 2^2)$, $(2^2, 2^2, 2)$. They are represented as strings and elements of the group over the field F_q in the table provided below (Table 1).

Table 1. Logarithmic signature generation

$$\beta_k = [B_{1(k)}, B_{2(k)}, B_{3(k)}, B_{4(k)}] = (b_{ij})_{(k)}, (b_{ij})_{(k)} \in A_{l=4}(n, \theta)$$

$B_{1(1)}$		$B_{1(2)}$		$B_{1(3)}$		$B_{1(4)}$	
00000	0, 0, 0, 0	00000	0, 0, 0, 0	00000	0, 0, 0, 0	00000	0, 0, 0, 0
10000	$\alpha^0, 0, 0, 0$	10000	$0, \alpha^0, 0, 0$	10000	$0, 0, \alpha^0, 0$	10000	$0, 0, 0, \alpha^0$
01000	$\alpha^1, 0, 0, 0$	01000	$0, \alpha^1, 0, 0$	$B_{2(3)}$		01000	$0, 0, 0, \alpha^1$
11000	$\alpha^{14}, 0, 0, 0$	11000	$0, \alpha^{14}, 0, 0$	00000	0, 0, 0, 0	11000	$0, 0, 0, \alpha^{14}$
$B_{2(1)}$		$B_{2(2)}$		11000	$0, 0, \alpha^{14}, 0$	$B_{2(4)}$	
01000	$\alpha^1, 0, 0, 0$	11000	$0, \alpha^{14}, 0, 0$	10100	$0, 0, \alpha^{28}, 0$	00000	$0, 0, 0, 0$
10100	$\alpha^{28}, 0, 0, 0$	11100	$0, \alpha^{22}, 0, 0$	01100	$0, 0, \alpha^{15}, 0$	00100	$0, 0, 0, \alpha^2$
11010	$\alpha^{26}, 0, 0, 0$	10010	$0, \alpha^5, 0, 0$	$B_{3(3)}$		$B_{3(4)}$	
00110	$\alpha^{16}, 0, 0, 0$	00110	$0, \alpha^{16}, 0, 0$	01000	$0, 0, \alpha^1, 0$	01000	$0, 0, 0, \alpha^1$
10001	$\alpha^{25}, 0, 0, 0$	$B_{3(2)}$		10010	$0, 0, \alpha^5, 0$	00110	$0, 0, 0, \alpha^{16}$
11101	$\alpha^{21}, 0, 0, 0$	10000	$0, \alpha^0, 0, 0$	01101	$0, 0, \alpha^{27}, 0$	00001	$0, 0, 0, \alpha^4$
10011	$\alpha^{18}, 0, 0, 0$	10011	$0, \alpha^{18}, 0, 0$	10111	$0, 0, \alpha^9, 0$	11011	$0, 0, 0, \alpha^{19}$
11111	$\alpha^{20}, 0, 0, 0$						

Construct random covers α_k , for the same type as $\beta_{(k)}$

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, a_{ij(k)}^{(3)}, a_{ij(k)}^{(4)})$$

where $a_{ij} \in A_{l=4}(n, \theta)$, $a_{ij(k)}^{(v)} \in F_q \setminus \{0\}$, $i = \overline{1, s}, j = \overline{1, r_{i(k)}}, k = \overline{1, 4}$.
 In the field representation α_k has the following form (Table 2)

Table 2. Random covers construction

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, a_{ij(k)}^{(3)}, a_{ij(k)}^{(4)})$$

$k = 1$	$k = 2$	$k = 3$	$k = 4$
$A_{1(1)}$	$A_{1(2)}$	$A_{1(3)}$	$A_{1(4)}$
$\alpha^6, \alpha^{11}, \alpha^{17}, \alpha^{27}$	$\alpha^{17}, \alpha^5, \alpha^{26}, \alpha^{28}$	$\alpha^0, \alpha^2, \alpha^{14}, \alpha^{20}$	$\alpha^{20}, \alpha^{14}, \alpha^{30}, \alpha^{13}$
$\alpha^{11}, \alpha^5, \alpha^7, \alpha^5$	$\alpha^{20}, \alpha^{14}, \alpha^{19}, \alpha^{24}$	$\alpha^{17}, \alpha^{27}, \alpha^{16}, \alpha^{10}$	$\alpha^4, \alpha^2, \alpha^{13}, \alpha^{17}$
$\alpha^{21}, \alpha^{18}, 0, \alpha^{16}$	$\alpha^{30}, \alpha^{21}, \alpha^6, \alpha^3$	$A_{2(3)}$	$\alpha^{19}, \alpha^{13}, \alpha^{26}, \alpha^{22}$

(continued)

Table 2. (continued)

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, a_{ij(k)}^{(3)}, a_{ij(k)}^{(4)})$$

$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^5, \alpha^{29}, \alpha^{12}, \alpha^{16}$	$\alpha^6, \alpha^9, \alpha^{13}, \alpha^{22}$	$\alpha^{28}, \alpha^{29}, 0, \alpha^{25}$	$\alpha^6, \alpha^{28}, \alpha^{12}, \alpha^4$
A₂(1)	A₂(2)	$\alpha^{10}, \alpha^{12}, \alpha^{22}, \alpha^{30}$	A₂(4)
$\alpha^4, \alpha^7, \alpha^4, \alpha^2$	$\alpha^{30}, \alpha^{14}, \alpha^{27}, \alpha^{30}$	$\alpha^{13}, \alpha^{23}, \alpha^{19}, \alpha^{19}$	$\alpha^{18}, \alpha^1, \alpha^1, \alpha^{24}$
$\alpha^{12}, \alpha^{11}, \alpha^3, \alpha^1$	$\alpha^1, \alpha^{18}, 0, \alpha^{13}$	$\alpha^0, \alpha^{10}, \alpha^1, \alpha^{20}$	$\alpha^{26}, \alpha^{28}, \alpha^{15}, \alpha^0$
$\alpha^{18}, \alpha^{15}, \alpha^{14}, \alpha^{30}$	$\alpha^1, \alpha^{18}, \alpha^{28}, \alpha^{30}$	A₃(3)	A₃(4)
$\alpha^3, \alpha^{19}, \alpha^{26}, \alpha^2$	$\alpha^{25}, \alpha^5, \alpha^0, \alpha^{13}$	$\alpha^{11}, \alpha^{27}, \alpha^{29}, \alpha^{18}$	$\alpha^{16}, \alpha^{17}, \alpha^{29}, \alpha^{17}$
$\alpha^{11}, \alpha^{18}, \alpha^{21}, \alpha^{28}$	A₃(2)	$\alpha^5, \alpha^1, \alpha^{12}, \alpha^{22}$	$\alpha^{18}, \alpha^0, \alpha^1, \alpha^{15}$
$\alpha^{16}, \alpha^{18}, \alpha^{10}, \alpha^{24}$	$\alpha^3, \alpha^{29}, \alpha^{25}, 0$	$\alpha^{30}, \alpha^{18}, \alpha^6, \alpha^{11}$	$\alpha^4, \alpha^9, \alpha^{23}, \alpha^{19}$
$\alpha^{17}, \alpha^{16}, 0, \alpha^{27}$	$\alpha^{25}, \alpha^{19}, \alpha^{23}, \alpha^2$	$0, 0, \alpha^{17}, \alpha^{23}$	$\alpha^{19}, \alpha^{20}, \alpha^{30}, \alpha^{10}$
$\alpha^{25}, \alpha^{17}, \alpha^8, \alpha^{12}$			

Choose random $A_l(n, \theta)$ $t_{0(k)}, t_{1(k)}, \dots, t_{s(k)} \in A_l(n, \theta), s(k), k = \overline{1, 4}$ and $t_{2(1)} = t_{0(2)}, t_{3(2)} = t_{0(3)}, t_{3(3)} = t_{0(4)}$ (Table 3)

Table 3. Random t vectors

$$t_{0(k)}, t_{1(k)}, \dots, t_{s(k)} \in A_{l=4}(n, \theta), s(k), k = \overline{1, 4}$$

$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^1, \alpha^5, \alpha^{17}, \alpha^{16}$ $\alpha^{25}, \alpha^{17}, \alpha^{23}, \alpha^{27}$ $\alpha^{13}, \alpha^0, \alpha^{28}, \alpha^{10}$	$\alpha^{13}, \alpha^0, \alpha^{28}, \alpha^{10}$ $\alpha^{30}, \alpha^2, \alpha^{17}, \alpha^2$ $\alpha^6, \alpha^7, \alpha^{30}, \alpha^{18}$ $\alpha^9, \alpha^4, \alpha^9, \alpha^{20}$	$\alpha^9, \alpha^4, \alpha^9, \alpha^{20}$ $\alpha^{14}, \alpha^{28}, \alpha^{17}, \alpha^{22}$ $\alpha^{26}, \alpha^5, \alpha^{16}, \alpha^{30}$ $\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^6$	$\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^6$ $\alpha^{22}, \alpha^{30}, \alpha^{22}, \alpha^{16}$ $\alpha^{24}, \alpha^{29}, \alpha^{15}, \alpha^{30}$ $\alpha^3, 0, \alpha^{14}, \alpha^9$

The inverse elements $t_{0(k)}^{-(k)}, t_{1(k)}^{-(k)}, \dots, t_{s(k)}^{-(k)}$ of the group $A_4(n, \theta)$ were computed with reference below (Table 4):

Table 4. Computing of inverse elements $t_{0(k)}^{-(k)}, t_{1(k)}^{-(k)}, \dots, t_{s(k)}^{-(k)}$

$$\tau_{0(k)}^{-(k)}, \tau_{1(k)}^{-(k)}, \dots, \tau_{s(k)}^{-(k)}$$

$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^1, \alpha^0, \alpha^{22}, \alpha^{21}$ $\alpha^{25}, \alpha^7, \alpha^3, \alpha^{15}$ $\alpha^{13}, \alpha^{19}, \alpha^7, \alpha^{24}$	$\alpha^{13}, \alpha^0, \alpha^7, \alpha^{24}$ $\alpha^{30}, \alpha^2, \alpha^{15}, \alpha^{21}$ $\alpha^6, \alpha^7, \alpha^{28}, \alpha^{24}$ $\alpha^9, \alpha^4, \alpha^8, \alpha^{25}$	$\alpha^9, \alpha^4, \alpha^9, \alpha^{25}$ $\alpha^{14}, \alpha^{28}, \alpha^{17}, \alpha^{21}$ $\alpha^{26}, \alpha^5, \alpha^{16}, \alpha^{13}$ $\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^{30}$	$\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^6$ $\alpha^{22}, \alpha^{30}, \alpha^{22}, \alpha^{16}$ $\alpha^{24}, \alpha^{29}, \alpha^{15}, \alpha^{30}$ $\alpha^3, 0, \alpha^{14}, \alpha^9$

Similarly, we choose random $\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)} \in A_l(n, \theta)$, $s(k) = \overline{1, 4}$ and $t_{2(1)} = t_{0(2)}, t_{3(2)} = t_{0(3)}, t_{3(3)} = t_{0(4)}$:
and the inverse elements $\tau_{0(k)}^{-(-k)}, \tau_{1(k)}^{-(-k)}, \dots, \tau_{s(k)}^{-(-k)}$ (Table 5):

Table 5. Computing of random τ vectors $\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)} \in A(P_\infty) \setminus Z$

$\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)} \in A(P_\infty) \setminus Z, s(k) = \overline{1, 4}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^4, \alpha^{22}, \alpha^7, \alpha^{12}$	$\alpha^{29}, \alpha^{21}, \alpha^{30}, \alpha^{13}$	$\alpha^2, \alpha^{17}, \alpha^{22}, \alpha^2$	$\alpha^{20}, 0, \alpha^3, \alpha^0$
$\alpha^8, 0, \alpha^{13}, \alpha^{16}$	$\alpha^{24}, \alpha^{20}, \alpha^{17}, \alpha^{25}$	$0, \alpha^{22}, \alpha^{16}, \alpha^{24}$	$\alpha^{21}, \alpha^{16}, \alpha^{12}, \alpha^{16}$
$\alpha^{29}, \alpha^{21}, \alpha^{30}, \alpha^{13}$	$\alpha^4, \alpha^7, \alpha^{16}, \alpha^{30}$	$\alpha^6, \alpha^{21}, \alpha^{25}, \alpha^{18}$	$\alpha^{16}, \alpha^{28}, \alpha^{19}, \alpha^{16}$
	$\alpha^2, \alpha^{17}, \alpha^{22}, \alpha^2$	$\alpha^{20}, 0, \alpha^3, \alpha^0$	$\alpha^{28}, \alpha^{17}, \alpha^{26}, \alpha^4$

Table 6. Computing of inverse elements $\tau_{0(k)}^{-(-k)}, \tau_{1(k)}^{-(-k)}, \dots, \tau_{s(k)}^{-(-k)}$

$\tau_{0(k)}^{-(-k)}, \tau_{1(k)}^{-(-k)}, \dots, \tau_{s(k)}^{-(-k)}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^4, \alpha^{18}, \alpha^9, \alpha^0$	$\alpha^{29}, \alpha^{21}, \alpha^2, \alpha^5$	$\alpha^2, \alpha^{17}, \alpha^{22}, \alpha^{11}$	$\alpha^{20}, 0, \alpha^3, \alpha^0$
$\alpha^8, \alpha^{24}, \alpha^2, \alpha^{30}$	$\alpha^{24}, \alpha^{20}, \alpha^{22}, \alpha^{29}$	$0, \alpha^{22}, \alpha^{16}, \alpha^2$	$\alpha^{21}, \alpha^{16}, \alpha^{12}, \alpha^{16}$
$\alpha^{29}, \alpha^{15}, \alpha^2, \alpha^5$	$\alpha^4, \alpha^7, \alpha^{12}, \alpha^{28}$	$\alpha^6, \alpha^{21}, \alpha^{25}, \alpha^3$	$\alpha^{16}, \alpha^{28}, \alpha^{19}, \alpha^{16}$
	$\alpha^2, \alpha^{17}, \alpha^{24}, \alpha^{11}$	$\alpha^{20}, 0, \alpha^3, \alpha^{22}$	$\alpha^{28}, \alpha^{17}, \alpha^{26}, \alpha^4$

Construct random covers w_k , for the same type as $\beta(k)$

$w(k) = [W_{1(k)}, \dots, W_{s(k)}] = (w_{ij})_{(k)} = S(w_{ij(k)}^{(1)}, w_{ij(k)}^{(2)}, \dots, w_{ij(k)}^{(l)})$, where $w_{ij} \in A_{l=4}(n, \theta)$, $w_{ij(k)}^{(v)} \in F_q$, $i = \overline{0, s(k)}, j = \overline{1, r_i(k)}, k = \overline{1, 4}$ (Table 6 and 7).

Table 7. Construct random covers w_k

$w(k) = [W_{1(k)}, \dots, W_{s(k)}] = (w_{ij})_{(k)} = S(w_{ij(k)}^{(1)}, \dots, w_{ij(k)}^{(4)})$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$W_{1(1)}$	$W_{1(2)}$	$W_{1(3)}$	$W_{1(4)}$
$\alpha^{20}, \alpha^{20}, \alpha^{12}, \alpha^4$	$\alpha^9, \alpha^{28}, \alpha^{27}, \alpha^2$	$\alpha^3, \alpha^2, \alpha^{10}, 0$	$\alpha^{30}, \alpha^{14}, \alpha^1, \alpha^{28}$
$\alpha^7, \alpha^9, \alpha^{17}, \alpha^{20}$	$\alpha^{16}, \alpha^{13}, \alpha^6, \alpha^{21}$	$\alpha^5, \alpha^{10}, \alpha^{19}, \alpha^{16}$	$\alpha^6, \alpha^{28}, \alpha^{30}, \alpha^{20}$
$\alpha^{25}, \alpha^6, \alpha^{23}, \alpha^{27}$	$\alpha^{25}, 0, \alpha^4, \alpha^{27}$	$W_{2(3)}$	$\alpha^{13}, \alpha^{19}, \alpha^{26}, \alpha^{11}$
$\alpha^3, \alpha^0, \alpha^{23}, \alpha^{29}$	$\alpha^1, \alpha^0, \alpha^{17}, \alpha^{17}$	$\alpha^{12}, \alpha^{20}, \alpha^{14}, \alpha^3$	$\alpha^{16}, \alpha^{27}, \alpha^9, \alpha^{21}$

(continued)

Table 7. (continued)

$$w^{(k)} = [W_{1(k)}, \dots, W_{s(k)}] = (w_{ij}^{(k)}) = S(w_{ij(k)}^{(1)}, \dots, w_{ij(k)}^{(4)})$$

$W_{2(1)}$	$W_{2(2)}$	$\alpha^{23}, \alpha^{12}, \alpha^5, \alpha^{27}$	$W_{2(4)}$
$\alpha^7, \alpha^{21}, \alpha^6, \alpha^{21}$	$\alpha^{21}, \alpha^{14}, \alpha^{14}, \alpha^0$	$\alpha^2, \alpha^3, \alpha^{24}, \alpha^{16}$	$\alpha^2, \alpha^{21}, \alpha^8, \alpha^{29}$
$\alpha^{18}, \alpha^{21}, \alpha^{22}, \alpha^6$	$\alpha^{19}, \alpha^{29}, \alpha^{19}, \alpha^{13}$	$\alpha^{12}, \alpha^5, \alpha^{21}, \alpha^{14}$	$\alpha^4, \alpha^2, \alpha^1, \alpha^{23}$
$\alpha^{18}, \alpha^{19}, \alpha^{12}, \alpha^{15}$	$\alpha^{25}, \alpha^{26}, \alpha^{12}, \alpha^{17}$	$W_{3(3)}$	$W_{3(4)}$
$\alpha^{16}, \alpha^{12}, \alpha^{14}, \alpha^6$	$\alpha^{10}, \alpha^{19}, \alpha^{23}, \alpha^4$	$\alpha^{14}, \alpha^6, \alpha^0, \alpha^{17}$	$0, \alpha^0, \alpha^{25}, \alpha^3$
$\alpha^{23}, \alpha^4, \alpha^1, \alpha^{30}$	$W_{3(2)}$	$\alpha^{17}, \alpha^{13}, \alpha^7, \alpha^4$	$\alpha^3, \alpha^{19}, \alpha^{17}, \alpha^{24}$
$\alpha^5, \alpha^{26}, \alpha^6, \alpha^{19}$	$\alpha^{28}, \alpha^0, \alpha^{13}, \alpha^{17}$	$\alpha^{25}, \alpha^{24}, \alpha^{27}, \alpha^8$	$\alpha^{28}, \alpha^{28}, \alpha^{14}, \alpha^{26}$
$\alpha^{22}, \alpha^{17}, \alpha^{13}, \alpha^{21}$	$\alpha^{14}, \alpha^0, \alpha^3, \alpha^3$	$\alpha^{13}, 0, \alpha^{21}, \alpha^7$	$\alpha^{24}, \alpha^{18}, \alpha^{27}, \alpha^{13}$
$\alpha^{28}, \alpha^{27}, \alpha^9, \alpha^{24}$			

The next step is to calculate the arrays h_k . Within the condition of the example, we obtain:

$$h_{(k)} = [h_{1(k)}, \dots, h_{s(k)}] = t_{(i-1)(k)}^{- (k)} \circ^{(k)} (w_{ij})_{(k)} \circ^{(k)} (b_{ij})_{(k)} \circ^{(k)} t_{i(k)}$$

$$i = \overline{1, s(k)}, j = \overline{1, r_i(k)}, k = \overline{1, 4}.$$

Let's a homomorphic cryptographic transformation for a field element $e \Rightarrow \rho_i e$ where ρ_i is a secret parameter. The transformation is chosen to be the simplest. You can also use more complex homomorphic transformations with respect to the addition operation. We define homomorphic cryptographic transformation for a group element S as

$$f(S(e_1, e_2, e_3, e_4)) = S(\rho_1 e_1, \rho_2 e_2, \rho_3 e_3, \rho_4 e_4),$$

and let's $\rho = (\rho_1, \rho_2, \rho_3, \rho_4) = (\alpha^4, \alpha^5, \alpha^6, \alpha^7)$.

Let's a homomorphic cryptographic transformation for a field element $e \Rightarrow \rho_i e$ where ρ_i is a secret parameter. The transformation is chosen to be the simplest (Table 8).

You can also use more complex homomorphic transformations with respect to the addition operation. We define homomorphic cryptographic transformation for a group element S as

$$f(S(e_1, e_2, e_3, e_4)) = S(\rho_1 e_1, \rho_2 e_2, \rho_3 e_3, \rho_4 e_4),$$

and let's $\rho = (\rho_1, \rho_2, \rho_3, \rho_4) = (\alpha^4, \alpha^5, \alpha^6, \alpha^7)$.

Next, we compute the arrays g_k via the homomorphic transformation

$$g_{(k)} = [g_{1(k)}, \dots, g_{s(k)}] = \tau_{(i-1)(k)}^{- (k)} \circ^{(k)} f(w_{ij})_{(k)} \circ^{(k)} \tau_{i(k)}$$

$i = \overline{1, s(k)}, j = \overline{1, r_i(k)}, k = \overline{1, 4}$. See the Table 9 for the results.

An output public key (a_k, h_k, g_k) , and a private key $[f, \beta_{(k)}, (t_{0(k)}, \dots, t_{s(k)}), (\tau_{0(k)}, \dots, \tau_{s(k)})], k = \overline{1, 4}$.

Table 8. Construct arrays h_k

$h_k = S(h_{ij(k)}^{(1)}, h_{ij(k)}^{(2)}, h_{ij(k)}^{(3)}, h_{ij(k)}^{(4)})$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$h_{1(1)}$	$h_{1(2)}$	$h_{1(3)}$	$h_{1(4)}$
$\alpha^{16}, \alpha^{20}, \alpha^{22}, \alpha^{30}$	$\alpha^{24}, 0, \alpha^{16}, 0$	$\alpha^{27}, \alpha^{25}, \alpha^{27}, \alpha^{30}$	$\alpha^7, \alpha^{25}, \alpha^9, \alpha^{19}$
$\alpha^{20}, \alpha^7, \alpha^{21}, \alpha^{15}$	$\alpha^7, \alpha^{25}, \alpha^{21}, \alpha^3$	$\alpha^{21}, \alpha^{15}, \alpha^{20}, \alpha^{14}$	$\alpha^{26}, \alpha^{21}, \alpha^{26}, 0$
$0, \alpha^{27}, \alpha^{26}, \alpha^{13}$	$\alpha^4, \alpha^{22}, 0, \alpha^{21}$	$h_{2(3)}$	$\alpha^{16}, \alpha^5, \alpha^{30}, \alpha^{10}$
$\alpha^{17}, \alpha^{16}, \alpha^{28}, \alpha^{26}$	$\alpha^{14}, \alpha^{22}, \alpha^3, \alpha^5$	$\alpha^{27}, \alpha^{10}, \alpha^{21}, \alpha^{23}$	$\alpha^{13}, \alpha^2, \alpha^1, \alpha^{29}$
$h_{2(1)}$	$h_{2(2)}$	$\alpha^{15}, \alpha^6, \alpha^{12}, \alpha^9$	$h_{2(4)}$
$\alpha^{26}, 0, \alpha^{29}, \alpha^{11}$	$\alpha^{25}, \alpha^5, \alpha^3, \alpha^{26}$	$\alpha^{16}, \alpha^2, \alpha^7, \alpha^{17}$	$\alpha^{20}, \alpha^5, \alpha^{19}, \alpha^6$
$\alpha^{17}, \alpha^7, \alpha^{26}, \alpha^{29}$	$\alpha^9, \alpha^2, \alpha^{12}, \alpha^{14}$	$\alpha^{27}, \alpha^{28}, \alpha^{28}, \alpha^{11}$	$\alpha^{26}, \alpha^8, \alpha^{14}, \alpha^6$
$\alpha^{27}, \alpha^{11}, \alpha^{28}, \alpha^{16}$	$\alpha^{21}, \alpha^{26}, \alpha^{25}, \alpha^{21}$	$h_{3(3)}$	$h_{3(4)}$
$\alpha^2, \alpha^3, \alpha^{11}, \alpha^4$	$\alpha^{13}, \alpha^{12}, \alpha^{22}, \alpha^7$	$\alpha^{27}, \alpha^9, \alpha^{21}, \alpha^{15}$	$\alpha^{30}, \alpha^{26}, \alpha^{30}, \alpha^{14}$
$\alpha^{19}, \alpha^{16}, \alpha^{25}, \alpha^5$	$h_{3(2)}$	$\alpha^7, \alpha^8, \alpha^4, \alpha^4$	$\alpha^{24}, \alpha^{25}, \alpha^9, \alpha^{18}$
$\alpha^8, \alpha^8, \alpha^{19}, \alpha^{19}$	$\alpha^{29}, \alpha^9, \alpha^1, \alpha^{12}$	$\alpha^2, \alpha^{10}, \alpha^{30}, \alpha^{24}$	$\alpha^{25}, \alpha^{11}, \alpha^{15}, \alpha^6$
$\alpha^8, \alpha^{10}, \alpha^1, \alpha^{30}$	$\alpha^{16}, \alpha^{28}, \alpha^1, \alpha^3$	$0, \alpha^{11}, \alpha^{12}, \alpha^{21}$	$\alpha^3, \alpha^{10}, \alpha^{10}, \alpha^{22}$
$\alpha^{12}, \alpha^{27}, \alpha^0, \alpha^{21}$			

Table 9. Construct arrays g_k

$g_k = S(g_{ij(k)}^{(1)}, g_{ij(k)}^{(2)}, g_{ij(k)}^{(3)}, g_{ij(k)}^{(4)})$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$g_{1(1)}$	$g_{1(2)}$	$g_{1(3)}$	$g_{1(4)}$
$\alpha^{27}, \alpha^{21}, \alpha^{17}, \alpha^{13}$	$\alpha^{14}, \alpha^{16}, \alpha^7, \alpha^{18}$	$\alpha^5, \alpha^6, \alpha^{22}, \alpha^{30}$	$0, \alpha^{21}, \alpha^{19}, \alpha^9$
$\alpha^{28}, \alpha^{18}, \alpha^2, \alpha^1$	$\alpha^5, \alpha^{25}, \alpha^{18}, 0$	$\alpha^{18}, \alpha^{18}, \alpha^8, \alpha^7$	$\alpha^{19}, \alpha^3, \alpha^{20}, \alpha^{19}$
$0, \alpha^{17}, \alpha^1, \alpha^{13}$	$\alpha^{24}, \alpha^3, \alpha^1, \alpha^{13}$	$g_{2(3)}$	$\alpha^4, \alpha^4, \alpha^{30}, \alpha^{30}$
$\alpha^{22}, \alpha^9, \alpha^{29}, \alpha^{26}$	$\alpha^{20}, \alpha^0, 0, \alpha^{23}$	$\alpha^{12}, \alpha^0, \alpha^1, \alpha^0$	$\alpha^{21}, \alpha^{23}, \alpha^4, \alpha^3$
$g_{2(1)}$	$g_{2(2)}$	$\alpha^2, \alpha^3, \alpha^6, 0$	$g_{2(4)}$
$\alpha^{20}, \alpha^{29}, \alpha^{17}, \alpha^{13}$	$\alpha^9, \alpha^5, \alpha^{25}, \alpha^{30}$	$0, \alpha^{29}, \alpha^5, \alpha^{11}$	$\alpha^5, \alpha^1, \alpha^{15}, \alpha^5$
$\alpha^{21}, \alpha^0, \alpha^{25}, \alpha^{28}$	$\alpha^1, \alpha^8, \alpha^7, \alpha^{17}$	$\alpha^{12}, \alpha^{14}, \alpha^{26}, \alpha^{23}$	$\alpha^0, \alpha^2, \alpha^3, \alpha^{30}$
$\alpha^{21}, \alpha^{27}, \alpha^{21}, \alpha^{21}$	$\alpha^{15}, \alpha^{10}, \alpha^{13}, \alpha^9$	$g_{3(3)}$	$g_{3(4)}$
$\alpha^{11}, \alpha^{30}, \alpha^{22}, \alpha^5$	$\alpha^{11}, \alpha^{23}, \alpha^{29}, \alpha^{18}$	$\alpha^{30}, \alpha^{17}, \alpha^{26}, \alpha^2$	$\alpha^5, \alpha^{30}, \alpha^{25}, \alpha^{11}$
$\alpha^{15}, \alpha^{24}, \alpha^{17}, \alpha^{24}$	$g_{3(2)}$	$\alpha^8, \alpha^{23}, \alpha^{16}, \alpha^9$	$\alpha^2, \alpha^0, \alpha^{12}, \alpha^9$
$\alpha^7, \alpha^{30}, \alpha^{20}, \alpha^{24}$	$\alpha^{27}, \alpha^{24}, \alpha^6, \alpha^9$	$\alpha^{22}, \alpha^9, \alpha^9, \alpha^{10}$	$\alpha^{26}, \alpha^{18}, \alpha^{11}, \alpha^{17}$
$\alpha^{19}, \alpha^{19}, \alpha^3, \alpha^2$	$\alpha^7, \alpha^{24}, \alpha^{25}, \alpha^{26}$	$\alpha^{13}, \alpha^{21}, \alpha^{11}, \alpha^{26}$	$\alpha^{16}, \alpha^{10}, \alpha^{30}, \alpha^{14}$
$\alpha^6, \alpha^{10}, \alpha^{17}, \alpha^{17}$			

Encryption

Input: a message $m \in A_l(n, \theta)$, $m = S(m_1, m_2, m_3, m_4)$, $m_i \in F_q$ and the public key $[f_k, (a_k, h_k, g_k)]$, $k = \overline{1, 4}$.

Let $m = (\alpha^1, \alpha^2, \alpha^3, \alpha^4) = S(\alpha^1, \alpha^2, \alpha^3, \alpha^4)$.

Choose a random $R = (R_1, R_2, R_3, R_4) = (10, 20, 30, 14)$.

We obtain the following R_i expansions for given types of $(r_{1(k)}, \dots, r_{s(k)})$, $k = \overline{1, 4}$

$$R_1 = (R_{1(1)}, R_{2(1)}) = (2, 2) = 10,$$

$$R_2 = (R_{1(2)}, R_{2(2)}, R_{3(2)}) = (0, 1, 1) = 20,$$

$$R_3 = (R_{1(3)}, R_{2(3)}, R_{3(3)}) = (0, 3, 3) = 30.$$

$$R_4 = (R_{1(4)}, R_{2(4)}, R_{3(4)}) = (2, 1, 1) = 14$$

Compute the cipher text:

$$y_1 = a'(R) \cdot m = a'_1(R_1) \cdot a'_2(R_2) \cdot a'_3(R_3) \cdot a'_4(R_4) \cdot m = S(\alpha^7, \alpha^6, \alpha^{22}, \alpha^{11})$$

where:

$$a'_1(R_1) = a_1(10) = a_{1(1)}(2)a_{2(1)}(2) = S(\alpha^{23}, \alpha^{13}, \alpha^{20}, \alpha^{20}),$$

$$a'_2(R_2) = a_2(20) = a_{1(2)}(0)a_{2(2)}(1)a_{3(2)}(1) = S(\alpha^{26}, \alpha^3, \alpha^5, \alpha^{29}),$$

$$a'_3(R_3) = a_3(30) = a_{1(3)}(0)a_{2(3)}(3)a_{3(3)}(3) = S(0, \alpha^{27}, \alpha^8, \alpha^4),$$

$$a'_4(R_4) = a_4(14) = a_{1(4)}(2)a_{2(4)}(1)a_{3(4)}(1) = S(\alpha^5, \alpha^{12}, \alpha^{21}, \alpha^{16}).$$

Calculate

$$y_2 = h_1(R_1) \circ^{(1)} \left(h_2(R_2) \circ^{(2)} \left(h_3(R_3) \circ^{(3)} h_4(R_4) \right) \right) = S(0, \alpha^8, \alpha^{16}, \alpha^{17})$$

The components $h'_k(R_k)$ are calculated similarly to $a'_k(R_k)$ components, but using the appropriate multiplication operation. Compute the component y_3 :

$$y_3 = g_1(R_1) \circ^{(1)} \left(g_2(R_2) \circ^{(2)} \left(g_3(R_3) \circ^{(3)} g_4(R_4) \right) \right) = S(\alpha^{16}, \alpha^{14}, \alpha^1, \alpha^4).$$

We obtained output $y_1 = (\alpha^7, \alpha^6, \alpha^{22}, \alpha^{11})$, $y_2 = (0, \alpha^8, \alpha^{16}, \alpha^{17})$, $y_3 = (\alpha^{16}, \alpha^{14}, \alpha^1, \alpha^4)$.

Decryption

Input: a ciphertext (y_1, y_2, y_3) and private key $[f, \beta_{(k)}, t_{i(k)}, \tau_{i(k)}]$, $i = \overline{0, s(k)}$, $k = \overline{1, 4}$.

Output: the message $m \in A(P_\infty)$ corresponding to ciphertext (y_1, y_2, y_3) .

To decrypt a message m , we need to restore random numbers $R = (R_1, R_2, R_3)$.

Compute

$$D^{(1)}(R) = t_{0(1)} \circ^{(1)} y_2 \circ^{(4)} t_{s(4)}^{-4} = S(\alpha^{29}, \alpha^8, \alpha^{24}, \alpha^{28}),$$

$$G^{(1)}(R) = \tau_{0(1)} \circ^{(1)} y_3 \circ^{(4)} \tau_{s(4)}^{-4} = S(\alpha^{18}, \alpha^5, \alpha^7, \alpha^{30}),$$

$$D^{(1)}(R)' = D^{(1)}(R) \circ^{(1)} \hat{f}(G^{(1)}(R))^{-1} = S(\alpha^5, \alpha^{22}, \alpha^{21}, \alpha^0).$$

Restore R_1 with $\beta_{(1)}(R_1) = \sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}$ using $\beta_{(1)}(R_1)^{-1}$, because β_1 is simple.

We get $\beta_1(R_1) = \alpha^5 = (10010)$. Perform inverse calculations $\beta_{(1)}(R_1)^{-1}$.

$$10|010 R_1 = (*, 2)$$

$$11|010 \text{ row 1 from } B_{4(1)}$$

$$10|010 - 11|010 = 01|000 R_1 = (2, 2)$$

$$\text{We get } \beta_1(R_1)^{-1} = (2, 2) = 10$$

For further calculation, it is necessary to remove the component $h'_1(R_1)$ from y_2 and $g'_1(R_1)$ from y_3 .

Compute

$$y_2^{(1)} = h_1(R_1)^{-1} \circ y_2^\circ = S(\alpha^{26}, \alpha^{16}, \alpha^{17}, \alpha^{19}),$$

$$y_3^{(1)} = g_1(R_1)^{-1} \circ y_3^\circ = S(\alpha^{19}, \alpha^{18}, \alpha^{12}, \alpha^{19}),$$

$$D^{(2)}(R) = t_{0(2)} \circ^{(2)} y_2^{(1)} \circ^{(4)} t_{s(4)}^{-4} = S(\alpha^{26}, \alpha^{18}, \alpha^{16}, \alpha^2),$$

$$G^{(2)}(R) = \tau_{0(2)} \circ^{(2)} y_3^{(1)} \circ^{(4)} \tau_{s(4)}^{-4} = S(\alpha^{30}, \alpha^{27}, \alpha^0, \alpha^{11}),$$

$$D^{(2)}(R)' = D^{(2)}(R) \circ^{(2)} \hat{f}(G^{(2)}(R))^{-2} = S(0, \alpha^{12}, \alpha^4, \alpha^{30})$$

and restore R_2 with $\beta_{(2)}(R_2) = \sum_{i=1, j=R_{i(2)}}^{s(2)} \beta_{ij(2)}$ using $\beta_{(2)}(R_2)^{-1}$, because β_2 is

simple. We get $\beta_2(R_2) = \alpha^{12} = (01111)$. Restore R_2 with $\beta_2(R_2)$. We use the same calculations as in the example for $\beta_2(R_2)^{-1}$, and we get:

$$01111 R_2 = (*, *, 1)$$

$$10|011 \text{ row 1 from } B_{3(2)}$$

$$01111 - 10|011 = 11|10|0 R_2 = (*, 1, 1)$$

$$11|10|0 \text{ row 0 from } B_{3(2)}$$

$$11|10|0 - 11|10|0 = 00|00|0 R_2 = (0, 1, 1)$$

$$\text{We get } \beta_2(R_2)^{-1} = (0, 1, 1) = 20.$$

Remove the component $h'_2(R_2)$ from $y_2^{(1)}$ and $g'_2(R_2)$ from $y_3^{(1)}$. We get

$$y_2^{(2)} = h_3(R_3)^{-2} \circ y_2^{(1)\circ} = S(\alpha^{19}, \alpha^{18}, \alpha^{22}, \alpha^{15}),$$

$$y_3^{(2)} = g_3(R_3)^{-(2)\circ} \cdot y_3^{(1)\circ} = S(\alpha^{21}, \alpha^{10}, \alpha^0, \alpha^{19}),$$

$$D^{(3)}(R) = t_{0(3)} \circ^{(3)} y_2^{(2)} \circ^{(4)} t_{s(4)}^{-{(4)}} = S(\alpha^{23}, \alpha^5, \alpha^{18}, \alpha^{21}),$$

$$G^{(3)}(R) = \tau_{0(3)} \circ^{(3)} y_3^{(2)} \circ^{(4)} \tau_{s(4)}^{-{(4)}} = S(\alpha^{21}, \alpha^{10}, \alpha^7, \alpha^{13}),$$

$$D^{(3)}(R)' = D^{(3)}(R) \circ^{(3)} \hat{f}(G^{(3)}(R))^{-{(3)}} = S(0, 0, \alpha^{19}, \alpha^6)$$

We get $\beta_3(R_3) = \alpha^{19} = (11011)$.

Perform inverse calculations $\beta_3(R_3)^{-1}$.

$$111011 R_3 = (*, *, 3)$$

$$110111 \text{ row 3 from } B_{3(3)}$$

$$111011 - 110111 = 011100 R_3 = *, 3, 3)$$

$$011100 \text{ row 3 from } B_{2(3)}$$

$$011100 - 011100 = 0100100 R_3 = (0, 3, 3)$$

$$\text{We get } \beta_3(R_3)^{-1} = (0, 3, 3) = 30.$$

Remove the component $h'_3(R_3)$ from $y_2^{(2)}$ and $g'_3(R_3)$ from $y_3^{(2)}$.

As a result, we get:

$$y_2^{(3)} = h_3(R_3)^{-(3)\circ} \cdot y_2^{(2)\circ} = S(\alpha^{19}, \alpha^1, \alpha^{29}, \alpha^{17}),$$

$$y_3^{(3)} = g_3(R_3)^{-(3)\circ} \cdot y_3^{(2)\circ} = S(\alpha^{13}, \alpha^{13}, \alpha^0, \alpha^{16}),$$

$$D^{(4)}(R) = t_{0(4)} \circ^{(4)} y_2^{(3)} \circ^{(4)} t_{s(4)}^{-{(4)}} = S(\alpha^7, \alpha^2, \alpha^{25}, \alpha^{21}),$$

$$G^{(4)}(R) = \tau_{0(4)} \circ^{(3)} y_3^{(3)} \circ^{(4)} \tau_{s(4)}^{-{(4)}} = S(\alpha^{11}, \alpha^7, \alpha^0, \alpha^{16}),$$

$$D^{(3)}(R)' = D^{(4)}(R) \circ^{(4)} \hat{f}(G^{(4)}(R))^{-{(4)}} = S(0, 0, 0, \alpha^{29})$$

01010

We get $\beta_4(R_4) = \alpha^{29} = (01010)$. Perform inverse calculations $\beta_4(R_4)^{-1}$.

$$011010 R_3 = (*, *, 1)$$

$$001110 \text{ row 1 from } B_{3(4)}$$

$$011010 - 001110 = 011100 R_3 = (*, 1, 1)$$

$$001100 \text{ row 1 from } B_{2(4)}$$

$$011100 - 001100 = 0110100 R_3 = (2, 1, 1)$$

$$\text{We get } \beta_4(R_4)^{-1} = (2, 1, 1) = 14.$$

Receive a message $m = a'(R)^{-1}y_1 = S(\alpha^1, \alpha^2, \alpha^3, \alpha^4)$.

3 Security Parameters Analysis and Cost Estimation

Consider a brute force attack of key recovery. There are three possible schemes for such an attack.

Brute force attack on cipher text. By selecting $R = (R_1, R_2, \dots, R_l)$ try to decipher the text $y_1' = \alpha'(R') \cdot m = \alpha_1'(R_1') \cdot \alpha_2'(R_2') \dots \alpha_l'(R_l') \cdot m$. The covers $\alpha_k = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, \dots, a_{ij(k)}^{(l)})$ are selected randomly and the value is determined by multiplication in a group with no coordinate constraints. The resulting vector $\alpha'(R')$ depends on all components $\alpha_i'(R_i')$. Enumeration of key values $R = (R_1, R_2, \dots, R_l)$ has an estimation of complexity. For a practical attack, the message m is also unknown and has uncertainty to choose from q^l . This makes a brute-force attack on a key infeasible. If we take an attack model with a known text, then the attack complexity still remains the same and equal to q^l .

Brute force attack on the cyphertext y_2 . Select $R = (R_1, R_2, \dots, R_l)$ to match y_2 . The vector y_2 has a following definition over the components $\alpha_i'(R_i)$

$$y_2 = S \left(\sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} w_{ij(k)}^{(1)} + \sum_{i=1, j=R_i(1)}^{s(1)} \beta_{ij(1)}, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} w_{ij(k)}^{(2)} + \sum_{i=1, j=R_i(2)}^{s(2)} \beta_{ij(2)} + *, \dots, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} w_{ij(k)}^{(l)} + \sum_{i=1, j=R_i(l)}^{s(l)} \beta_{ij(l)} + * \right)$$

The values of the coordinates y_2 are defined by calculations over the vectors $w_1'(R_1), w_2'(R_2), \dots, w_l'(R_l)$. The keys $R = (R_1, R_2, \dots, R_l)$ are bound and changes in any of them leads to change y_2 . The brute force attack on key R has a complexity equal to q^l .

Brute force attack on the ciphertext y_3 . Select $R = (R_1, R_2, \dots, R_l)$ to match y_3 . The vector y_3 has a following definition over the components $\rho_i w_i'(R_i)$

$$y_3 = S \left(\sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} f(w_{ij(k)}^{(1)}) +, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} f(w_{ij(k)}^{(2)}) + *, \dots, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} f(w_{ij(k)}^{(l)}) + * \right).$$

The values of the coordinates y_3 are defined by calculations over the vectors $w_1'(R_1), w_2'(R_2), \dots, w_l'(R_l)$. The keys R_1, R_2, \dots, R_l are bound and changes in any of them leads to change y_3 . The brute force attack on key R has a complexity equal to q^l .

Brute force attack on the vectors $(t_{0(k)}, \dots, t_{s(k)})$ and $(\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)})$. The brute force attack on $(t_{0(k)}, \dots, t_{s(k)})$ is a general for the MST cryptosystems and for the calculation in the field F_q over the group center $Z(G)$ has an optimistic complexity estimation equal to q . For the proposed algorithm all calculations are executed on whole group $|A_l(n, \theta)| = q^l$ and is a such case the complexity of the brute force attack on $(t_{0(k)}, \dots, t_{s(k)})$ and $(\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)})$ will be equal to q^l .

Attack on the Algorithm. The attack on the implementation algorithm of the MST cryptosystem based on the generalized Suzuki 2-group is multifaceted. Practical attacks look at the features of logarithmic signatures and random coverings known to a cryptanalyst. One solution is to use aperiodic logarithmic signatures. In the new cryptosystem with homomorphic encryption, random covers are a secret for the cryptanalyst. In this case, the known attacks based on the weakness of logarithmic signatures are impossible.

Let's estimate security and keys parameters for generalized Suzuki-2 group cryptosystem. We fix a generalized Suzuki 2-group $A_l(n, \theta) = \{S(a_1, a_2, \dots, a_l) | a_i \in F_q\}$, which is defined over the field F_q , $q = 2^n$. Then for l -parametric group we achieve $K = nl$ bit cryptography. Logarithmic signature array and random covers are known parameters that are used in encryption as follows

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_k = S\left(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, \dots, a_{ij(k)}^{(l)}\right),$$

$$h_{(k)} = [h_{1(k)}, \dots, h_{s(k)}] = S\left(h_{ij(k)}^{(1)}, h_{ij(k)}^{(2)}, \dots, h_{ij(k)}^{(l)}\right)$$

Also, we know random cover with homomorphic encryption

$$g_{(k)} = [g_{1(k)}, \dots, g_{s(k)}] = S\left(g_{ij(k)}^{(1)}, g_{ij(k)}^{(2)}, \dots, g_{ij(k)}^{(l)}\right)$$

for $k = \overline{1, l}$.

The number of vectors in arrays $\alpha_k, h_{(k)}, g_{(k)}$ is defined by the type of logarithmic signature. $(r_{1(k)}, \dots, r_{s(k)})$ and equals to $N = \sum_{k=1}^l (r_{1(k)} + r_{2(k)} + \dots + r_{s(k)})$

Since arrays $\alpha_k, g_{(k)}$ are random and can be constructed by random bits deterministic generator from some initial vector V , then we can define $\alpha_k, g_{(k)}$ over the vector V . Let's fix the vector length V to be equal to nl bits.

The array size $g_{(k)}$ equals to: $N_g = l \sum_{k=1}^l (r_{1(k)} + r_{2(k)} + \dots + r_{s(k)})$ n-bits words.

The secret parameters of the cryptosystem include vectors t, τ, ρ :

$$t_{0(k)}, \dots, t_{s(k)} \in A_l(n, \theta) \setminus Z, t_{i(k)} = S(t_{i1(k)}, \dots, t_{il(k)}),$$

$$\tau_{0(k)}, \dots, \tau_{s(k)} \in A_l(n, \theta) \setminus Z, \tau_{i(k)} = S(\tau_{i1(k)}, \dots, \tau_{il(k)}), \rho = (\rho_1, \rho_2, \dots, \rho_l), k = \overline{1, l}.$$

The number of vectors $t_{i(k)}, \tau_{i(k)}$ equals to: $N_t = N_\tau = l \sum_{k=1}^l s(k)$ n-bits words.

The length of the vector ρ equal to nl bits.

Obviously, that N_g, N_t, N_τ depends on type of $(r_{1(k)}, \dots, r_{s(k)})$.

Let the secrecy of cryptographic transformations be determined by K bits.

Let's define a type of $(r_{1(k)}, \dots, r_{s(k)}) = (2, \dots, 2)$, then $s(k) = n$ over the field $F(2^n)$. We get the following values

$$N_g = nl \sum_{k=1}^l (r_{1(k)} + r_{2(k)} + \dots + r_{s(k)}) = 2n^2 l^2 = 2K^2 \text{ bit}$$

$$N_t = N_\tau = nl \sum_{k=1}^l s(k) = n^2 l^2 = K^2 \text{ bit}$$

The length of vectors V, ρ equals to $N_V = N_\rho = nl = K$ bit. Let's define a type of $(r_{1(k)}, \dots, r_{s(k)}) = (2^8, \dots, 2^8), s(k) = n/8$ over field $F(2^n)$. We achieve

$$N_g = nl \sum_{k=1}^l (r_{1(k)} + r_{2(k)} + \dots + r_{s(k)}) = 2^5 n^2 l^2 = 2^5 K^2 \text{ bit}$$

$$N_t = N_\tau = nl \sum_{k=1}^l s(k) = n^2 l^2 / 8 = 2^{-3} K^2 \text{ bit}$$

Estimated implementation costs are presented in the table below.

Memory costs for arrays of shared and secret parameters do not depend on the field $F(2^n)$ and the number of parameters of the generalized Suzuki group. Selection of field F_q and parameters of the Suzuki group will define the speed of calculations on the group and depends on the software implementation (Table 10).

Table 10. Estimated implementation costs

$K = 256, (r_{1(k)}, \dots, r_{s(k)}) = (2, \dots, 2)$			
$F(2^n)$	N_g Kbyte	$N_t(N_\tau)$, Kbyte	$N_V(N_\rho)$, bit
$F(2^8), \dots, F(2^{256})$	4	2	256
$K = 256, (r_{1(k)}, \dots, r_{s(k)}) = (2^8, \dots, 2^8)$			
$F(2^8), \dots, F(2^{256})$	64	0.25	256
$K = 512, (r_{1(k)}, \dots, r_{s(k)}) = (2^8, \dots, 2^8)$			
$F(2^8), \dots, F(2^{512})$	64	32	512
$K = 512, (r_{1(k)}, \dots, r_{s(k)}) = (2^8, \dots, 2^8)$			
$F(2^8), \dots, F(2^{512})$	1024	8	512

4 Conclusions

Generalized Suzuki 2-groups are multiparameter groups and may have an arbitrarily large order. MST cryptosystems based on generalized Suzuki 2-group have an advantage over other schemes implementations in secrecy and realization. We can build a highly secure cryptosystem with group computation in a small finite field. Applying homomorphic encryption to random coverings in a logarithmic signature provides protection against known attacks on logarithmic signature implementations. To build a cryptosystem, you can use secure logarithmic signatures of a simple design, which leads to low costs for the general parameters of the cryptosystem. The proposed cryptosystem with homomorphic encryption is a good candidate for post-quantum cryptography.

Acknowledgements. This publication is based on work supported by a grant from the U.S. Civilian Research & Development Foundation (CRDF Global).

References

1. Wagner, N.R., Magyarik, M.R.: A public-key cryptosystem based on the word problem. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 19–36. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_3
2. Magliveras, S.S.: 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 (1986)
3. Lempken, W., Magliveras, S.S., van Trung, T., Wei, W.: A public key cryptosystem based on non-abelian finite groups. *J. Cryptol.* **22**, 62–74 (2009)
4. Magliveras, S.S., Svaba, P., van Trung, T., et al.: On the security of a realization of cryptosystem MST3. *Tatra Mt. Math. Publ.* **41**, 1–13 (2008)
5. Svaba, P., van Trung, T.: Public key cryptosystem MST3 cryptanalysis and realization. *J. Math. Cryptol.* **4**(3), 271–315 (2010)
6. van Trung, T.: Construction of strongly aperiodic logarithmic signatures. *J. Math. Cryptol.* **12**(1), 23–35 (2018)
7. Khalimov, G., Kotukh, Y., Khalimova, S.: MST3 cryptosystem based on the automorphism group of the Hermitian function field. In: IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, pp. 865–868 (2019)
8. Khalimov, G., Kotukh, Y., Khalimova, S.: MST3 cryptosystem based on a generalized Suzuki 2 – Groups. *CEUR Workshop Proc.* **2711**, 1–15 (2020)
9. Khalimov, G., Kotukh, Y., Khalimova, S.: Encryption scheme based on the automorphism group of the Ree function field. In: 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020, 9340192 (2020)
10. Hanaki, A.: A condition on lengths of conjugacy classes and character degrees Osaka *J. Math.* **33**, 207–216 (1996)
11. P. Svaba, “Covers and logarithmic signatures of finite groups in cryptography”, Dissertation, <https://bit.ly/2Ws2D24>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

