UDC 621.391:519.2

Method of Security Improvement for MST3 Cryptosystem Based on Automorphism Group of Ree Function Field

Yevgen Kotukh[1], Gennady Khalimov[2], Maxim Korobchinskiy[3]

[1] *State Tax University, Irpin, Ukraine*
[2] *Kharkiv National University of Radioelectronics, Kharkiv, Ukraine*
[3] *Yevhen Bereznyak Military Academy, Kyiv, Ukraine*

Abstract

This article is a part of a research endeavor focused on creating a quantum-resistant cryptosystem for secure encryption and decryption. Our approach employs a challenging word problem while emphasizing cost-effective implementation. Previous research has involved the development of encryption schemes based on high-order groups, offering potential security enhancements. The choice of the non-abelian group is a critical factor in shaping the encryption algorithms, feasibility of implementation, and system parameters. Our central objective is to design a cryptosystem that effectively thwarts quantum cryptanalysis. To achieve this, we employ a logarithmic signature along with a random cover across an entire finite non-abelian group. Our unique contribution lies in optimizing finite group selection, parameters, and circuit solutions for the logarithmic signature to meet specific security and implementation criteria. Within this paper, we introduce an encryption scheme utilizing automorphisms of the Ree functional field and propose a method for enhancing resistance to cryptanalysis through the binding of session keys.

Keywords: MST3 cryptosystem, logarithmic signature, random cover, Ree function field, word problem

Introduction

In response to advancements in quantum computing, the American National Institute of Standards and Technology (NIST) initiated the process of standardizing cryptographic primitives in 2016. These primitives are designed to ensure security in the presence of powerful quantum computers. NIST aims to finalize these standards by the year 2024. An analysis of key and signature encapsulation mechanisms reveals contradictions concerning the criteria for assessing resistance to classical and quantum attacks, time and memory costs, and security levels. This contradiction primarily arises due to the absence of an analysis of the potential for quantum attacks on algorithms and the relationship between security levels and memory and time requirements. To address this contradiction, the development of post-quantum cryptographic algorithms with a demonstrable level of security and reasonable time and memory costs is imperative.

As previously noted in references [1,2,7], the stability of contemporary asymmetric cryptosystems relies on assumptions about the computational complexity of problems such as integer factorization and discrete logarithms. The emergence of Shor's quantum algorithm, capable of solving these problems with polynomial complexity in the presence of a quantum computer, underscores the urgency of identifying new mathematically challenging problems that remain computationally complex in the post-quantum era.

An essential characteristic of the post-quantum era in cryptography is the substantial uncertainty surrounding the initial data for cryptanalysis and countermeasures. This uncertainty pertains to the capabilities of quantum computers, their mathematical and software aspects, as well as the application of quantum cryptanalysis to existing cryptotransformations and cryptoprotocols, as mentioned in reference [7]. Mathematical methods of electronic signature (EP) have been selected as the primary approaches, undergoing extensive scrutiny and justification through rigorous research conducted by leading

cryptologists and mathematicians. These methods have been comprehensively documented and subjected to scrutiny during the initial phase of the US NIST international competition. In a subsequent stage, decisions were made to consolidate certain candidates for the post-quantum standards in terms of encryption and digital signatures. Nine candidates were retained for further investigation in the second stage: CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, QTESLA, Rainbow, and SPHINCS+. Among these, three (Dilithium, FALCON, and qTeSLA) are based on the stability of algebraic lattices (Lattice-based), four (GeMSS, LUOV, MQDSS, Rainbow) rely on multivariate transformations (multivariate), one (SPHINCS+) is a hash function, and one (Picnic) is grounded in the stability of the hash function and block stream ciphers. As emphasized in reference [7], the national post-quantum standard of Ukraine should encompass algorithms grounded in various types of mathematical transformations acknowledged by the global cryptographic community as capable of providing the requisite level of security in the face of quantum cryptanalysis.

One of the approaches to developing a cryptosystem resistant to quantum attacks involves utilizing a challenging word problem, a concept implemented in MST (Multiple Signatures and Thresholds) cryptosystems, which are founded on logarithmic signatures and random coverages [1,2]. Initial attempts to create cryptosystems based on logarithmic signatures and coverages date back to the late 1970s, with the most significant advancements occurring in the 21st century within the realm of public key cryptography. Over this period, various forms of cryptosystems based on logarithmic signatures and coverages have been proposed, encompassing encryption schemes, electronic signature schemes, and random number generation mechanisms. The authors of reference [2] acknowledge the pertinence of this approach to post-quantum cryptography. Crucial objectives within this domain encompass devising novel methodologies for constructing logarithmic signatures, achieving enhanced efficiency in terms of computational performance in cryptosystems, and devising tamper-resistant schemes. One notable advantage of implementing such cryptosystems lies in the simplicity of group operations for the majority of finite groups, potentially resulting in high calculation speeds. Nonetheless, challenges persist, including the substantial size of signatures, leading to large public key sizes, detailed cryptographic analyses, and optimization of implementation costs.

This article constitutes part of a dissertation research effort aimed at creating a quantum-resistant cryptosystem for directional encryption and decryption, relying on the utilization of a challenging word problem while optimizing implementation costs. The foundation of this endeavor is the MST cryptosystem, built upon logarithmic signatures and random coverages within multiparameter groups. The primary scientific and practical achievements of this project encompass the development of methodologies and algorithms for directional encryption and decryption based on the MST cryptosystem, implemented within finite groups of substantial order, software implementations of these algorithms, testing, and cost estimates to meet confidentiality requirements.

Our research corpus comprises over a dozen papers [1-10]. One approach to establishing quantum-resistant cryptosystems, predicated on the word problem, hinges on the utilization of permutation groups. Several enhancements have been proposed, grounded in a distinct form of factorization of finite groups termed logarithmic signatures. The most recent variant, MST3, proposed on the Suzuki group algebra, has been examined. We assessed the feasibility of constructing an MST3 cryptosystem based on groups of higher order than Suzuki. Our efforts culminated in the construction of an MST3 cryptosystem predicated on generalized Suzuki groups, as well as groups of automorphisms of functional fields within multiparameter groups. Previous findings in cryptanalysis have indicated that computations within group algebra can introduce vulnerabilities in implementations. Previous works have seen us devise encryption schemes rooted in high-order groups, which hold the potential to enhance the security attributes of our proposal.

The fundamental structure of the MST3 cryptosystem comprises three essential components: a logarithmic signature, a random covering, and a finite non-abelian group, wherein the first two elements are nested.

A logarithmic signature constitutes a structured collection of data vectors with representations within a finite group, characterized by the property that calculating the vector sum (the sum of group elements) is

straightforward, and group factorization for the logarithmic signature on the group is tractable if one possesses the logarithmic signature. However, group factorization for a logarithmic signature on a group becomes a challenging problem for those without access to the logarithmic signature.

A random cover, defined as an array of random vectors (long-term key), serves the purpose of concealing the logarithmic signature.

The selection of the final non-Abelian group hinges on the feasibility of mapping the vectors of the logarithmic signature and the vectors of the random coverage onto the entire group.

Structural modifications within such a cryptosystem are conceivable across all three constituent elements. Notably, the construction of the array of logarithmic signature vectors assumes significance, with a parameter known as log signature type exerting a significant influence on the size of the log signature array. Concerns arise about cryptoresistance when implementing a minimum-size logarithmic signature, as indicated by existing estimates.

Random coverages are intrinsically associated with the logarithmic signature vectors, and their size is directly proportional to the dimensions of the logarithmic signature array.

The selection of the ultimate non-abelian group plays a pivotal role in determining the encryption algorithms, implementation feasibility, and the parameters of the cryptosystem.

As of 2019, comprehensive coverage of the Group Factorization Problem (GFP) pertaining to cryptosystems MST1, MST2, MST3, and eMST3, incorporating the construction of logarithmic signatures, is provided in reference [1]. The authors introduce an innovative enhancement to the eMST3 cryptosystem, which is based on the amalgamation of random coverages and logarithmic signatures. It is underscored that quantum resistance hinges upon the insolubility of the Group Factorization Problem (GFP) concerning the logarithmic signature within the Suzuki 2-group. The improvement in the eMST3 algorithm leads to a modification in the public key, rendering multiple ciphertexts independent of each other and simplifying the encryption process. In comparison to the eMST3 scheme, the proposed method is versatile, exhibits superior efficiency, and can be applied to file and image encryption.

Reference [2] provides an overview of directional encryption algorithms applicable to cryptosystems such as PGM, MST2, MST3, electronic signatures based on MST**, and a pseudorandom number generator, MSTg. Additionally, an exemplar of MST3 encryption rooted in the Suzuki 2-group is presented.

In [3], a comprehensive framework for the construction of Strongly Aperiodic Logarithmic Signatures (SALS) for elementary abelian p-groups is established. The introduction of SALS significantly broadens the spectrum of manual logarithmic signatures employed within the MST3 cryptosystem. These signatures possess characteristics that align with well-known categories of transversal or fusion transversal logarithmic signatures. It is posited that the property of "aperiodicity" plays a pivotal role in assessing the stability of MST cryptosystems.

Reference [4] delves into the issue of the existence of minimal logarithmic signatures for finite simple groups. The concept of minimality determines the nestedness of the logarithmic signature within the group without redundancy. Given that the construction of the logarithmic signature in the MST cryptosystem is centered around the group's core, it can be inferred that the core of the group is not excessively populated. This consideration influences the selection of the non-Abelian group for MST cryptosystem construction.

Reference [5] introduces an antiquantum MST3 PKE scheme tailored for remote sensing images. This scheme incorporates the use of a collision-resistant hash function, which enhances its resistance to quantum attacks. In comparison to prior MST encryption schemes, the proposed scheme exhibits heightened efficiency, as indicated by the authors.

Reference [6] provides estimates of the quantum resources required for potential attacks on AES-128, AES-192, and AES-256, along with quantum strategies for identifying Grover-based keys for AES encryption. In quantum computing, Grover's algorithm is invoked once an event is fixed, such as the key under investigation, and progressively refines measurement accuracy through iterations. The precise fixation of the sought-after event is pivotal, as it serves as the starting point for subsequent procedures. It is conceivable that the methodology employed in quantum analysis could find application in the development of the MST cryptosystem.

Reference [7] delves into the challenges related to post-quantum standards and the coordination thereof with national cryptographic standards. The meticulous implementation of

encryption algorithms and digital signatures within grid-based systems is examined in depth.

The foundational hypothesis of this study revolves around the notion that the problem of group factorization remains insoluble when applied to a logarithmic signature complemented by a random covering within a finite non-Abelian group. The intricate word problem serves as the cornerstone of MST cryptosystems and mitigates unknown attacks with reduced brute force complexity in the latest iteration of MST3. This forms a promising foundation for constructing a cryptosystem within the MST framework for the post-quantum era.

The central concept of this study is the development of a cryptosystem for encryption and decryption that exhibits resistance to quantum cryptanalysis. This is achieved through the propagation of a logarithmic signature, coupled with a random overlay, across the entirety of a finite non-Abelian group. The fundamental architecture of the MST3 cryptosystem incorporates a logarithmic signature with a random overlay situated at the core of the Suzuki 2-group. The selection of the Suzuki finite group is justified by its possession of the largest conceivable center among extant multiparameter finite groups. Calculations conducted within this center are commutative, facilitating the factorization of logarithmic signature group elements during decryption. Group calculations in this configuration are two-parameter, yielding a logarithmic signature with lesser computational power than that of the group itself. The strength of the logarithmic signature directly governs the security of the cryptosystem. To enhance the security of the MST3 cryptosystem without altering the power of the Suzuki 2-group, one potential approach is to extend the logarithmic signature to encompass the entire two-parameter group.

The novelty inherent in our approach to addressing the challenge of constructing a quantum-resistant cryptosystem lies in the optimization of finite group selection, parameters, and circuit solutions for the logarithmic signature, all aimed at achieving specified characteristics for security and implementation. Within this article, we explore an encryption scheme utilizing a group of automorphisms of the Ree functional field and propose a method for binding session keys to enhance resistance against cryptanalysis.

Our proposal

The implementation of the MST cryptosystem on the group of automorphisms of the Ree function field is predicated on the premise that optimal implementation and robust secrecy attributes can be achieved within a high-order multivariate group.

The group of automorphisms of the Ree function field is formally defined over a finite field F_q, $q = 3^{2s+1}$, where $s \in N \setminus \{0\}$ and $q_0 = 3^s$ [10].

The Ree function field F over K is defined as $S = K(x, y, z)$, where

$$y^q - y = x^{q_0}(x^q - x), z^q - z = x^{2q_0}(x^q - x).$$

It has $N = q^3 + 1$ rational places and genus $g = 3q_0(q-1)(q+q_0+1)/2$.

The automorphism group A of F is the Ree group $\mathrm{Ree}(q)$ and has order $|\mathrm{Ree}(q)| = q^3(q^3+1)(q-1)$.

Let P_∞ denote the unique pole x in F. Let

$A(P_\infty) := \{\sigma \in A | \sigma(P_\infty) = P_\infty\} \subset A$.

$A(P_\infty)$ consists of all automorphisms $\psi_{a,b,c,d}$ with $a,b,c,d \in K, a \neq 0$, which are defined as

$$\psi_{a,b,c,d} := \begin{cases} x \mapsto ax + b \\ y \mapsto a^{q_0+1}y + ab^{q_0}x + c \\ z \mapsto a^{2q_0+1}z - a^{q_0+1}b^{q_0}y + ab^{2q_0}x + d \end{cases}$$

We have $|A(P_\infty)| = q^3(q-1)$, and the subgroup $A(P_\infty)$ is a maximal subgroup of A.

Each element of $A(P_\infty)$ can be uniquely expressed.

$$A(P_\infty) = \{S(a,b,c,d) | a \in F_q^* := F_q \setminus \{0\}, c, b, d \in F_q\}$$

,

where $S(a,b,c,d) = [a,b,c,d]$ and group operation is defined as

$$S(a_1,b_1,c_1,d_1) \cdot S(a_2,b_2,c_2,d_2) =$$
$$S(\ a_1a_2, a_2b_1 + b_2, a_2^{q_0+1}c_1 + a_2b_1b_2^{q_0} + c_2, a_2b_1b_2^{2q_0} - a_2^{q_0+1}b_2^{q_0}c_1$$
$$+ a_2^{2q_0+1}d_1 + d_2\ )$$

The identity is the 4-triple $[1,0,0,0]$ and the inverse of $S(a,b,c,d)$ is

$$S(a,b,c,d)^{-1} = S(\ a^{-1}, -a^{-1}b, (a^{-1}b)^{q_0+1} - a^{-(q_0+1)}c,$$
$$-(a^{-1}b)^{2q_0+1} - a^{-(2q_0+1)}b^{q_0}c - a^{-(2q_0+1)}d\ ).$$

The encryption scheme founded upon the automorphism group of the Ree function field was introduced in reference [13]. Furthermore, the proposed algorithm's correctness has been substantiated through practical evaluation.

In the context of cryptanalysis of the encryption scheme, our investigation will encompass an examination of both the key generation and encryption phases.

Input: a large group on the field F_q, $q = 3q_0^2$, $q_0 = 3^s$

$$A(P_\infty) = \left\{ S(a,b,c,d) \middle| a \in F_q^* := F_q \setminus \{0\}, c,b,d \in F_q \right\}$$

.

Choose a tame logarithmic signatures $\beta_{(k)} = \left[B_{1(k)},...,B_{s(k)} \right] = \left(b_{ij} \right)_{(k)}$, $\left(b_{ij} \right)_{(k)} \in A(P_\infty)$ of type $\left(r_{1(k)},...,r_{s(k)} \right)$, $i = \overline{1,s(k)}$, $j = \overline{1,r_{i(k)}}$, $b_{ij(k)} \in F_q$, $k = \overline{1,3}$. Group element $\left(b_{ij} \right)_{(k)}$ has a value in only one coordinates b, c or d, respectively.

Select a random covers $\alpha_{(k)} = \left[A_{1(k)},...,A_{s(k)} \right] = \left(a_{ij} \right)_{(k)} = S\left(a_{ij(k)_1}, a_{ij(k)_2}, a_{ij(k)_3}, a_{ij(k)_4} \right)$ of the same type as $\beta_{(k)}$, where $a_{ij} \in A(P_\infty)$, $a_{ij(k)_1}, a_{ij(k)_2}, a_{ij(k)_3}, a_{ij(k)_4} \in F_q \setminus \{0\}$, $k = \overline{1,3}$.

Choose $t_{0(k)}, t_{1(k)},...,t_{s(k)} \in A(P_\infty) \setminus Z$,

$t_{i(k)} = S\left(t_{i(k)_1}, t_{i(k)_2}, t_{i(k)_3}, t_{i(k)_4} \right)$, $t_{i(k)_j} \in F^\times$, $i = \overline{0,s(k)}$, $j = \overline{1,4}$, $k = \overline{1,3}$. Let's $t_{s(1)} = t_{0(2)}$, $t_{s(2)} = t_{0(3)}$.

Construct a homomorphism f_k, $k = \overline{1,3}$ defined by

$$f_1\left(S(a_1,a_2,a_3,a_4) \right) = S(1,a_1,a_2,a_3),$$
$$f_2\left(S(a_1,a_2,a_3,a_4) \right) = S(1,0,a_2,a_3),$$
$$f_3\left(S(a_1,a_2,a_3,a_4) \right) = S(1,0,0,a_3).$$

Let's do the following calculations

$$\gamma_{(k)} = \left[h_{1(k)},...,h_{s(k)} \right] = t_{(i-1)(k)}^{-1} f_k\left(\left(a_{ij} \right)_{(k)} \right) \left(b_{ij} \right)_{(k)} t_{i(k)}$$

,

where $k = \overline{1,3}$, $i = \overline{1,s(k)}$, $j = \overline{1,r_{i(k)}}$,

$$f_1\left(\left(a_{ij} \right)_{(1)} \right) \left(b_{ij} \right)_{(1)} =$$
$$S\left(1, a_{ij(1)_1} + b_{ij(1)}, a_{ij(1)_2} + a_{ij(1)_1} b_{ij(1)}^{q_0}, a_{ij(1)_1} b_{ij(1)}^{2q_0} + a_{ij(1)_3} \right),$$
$$f_2\left(\left(a_{ij} \right)_{(2)} \right) \left(b_{ij} \right)_{(2)} = S\left(1,0, a_{ij(2)_2} + b_{ij(2)}, a_{ij(2)_3} \right),$$
$$f_3\left(\left(a_{ij} \right)_{(3)} \right) \left(b_{ij} \right)_{(3)} = S\left(1,0,0, a_{ij(3)_3} + b_{ij(3)} \right).$$

An output public key $\left[f_k, (\alpha_k, \gamma_k) \right]$, and a private key $\left[\beta_{(k)}, \left(t_{0(k)},...,t_{s(k)} \right) \right]$, $k = \overline{1,3}$.

Encryption. Let's define a message $m \in A(P_\infty)$, $m = S(m_1,m_2,m_3,m_4)$, $m_1 \in F_q \setminus \{0\}$, $m_2, m_3, m_4 \in F_q$, the public key $\left[f_k, (\alpha_k, \gamma_k) \right]$, $k = \overline{1,3}$, $R = R_1, R_2, R_3 \in Z_{|F_q|}$

Compute

$$y_1 = \alpha'(R) \cdot m = \alpha_1'(R_1) \cdot \alpha_2'(R_2) \cdot \alpha_3'(R_3) \cdot m,$$
$$y_2 = \gamma'(R) = \gamma_1'(R_1) \cdot \gamma_2'(R_2) \cdot \gamma_3'(R_3)$$
$$= S(*, a_{(1)_1}(R_1) + \beta_{(1)}(R_1) + *, a_{(2)_2}(R_2) + \beta_{(2)}(R_2) + *,$$
$$a_{(3)_3}(R_3) + \beta_{(2)}(R_3) + *).$$

In this context, the components are ascertained through cross-computations within the group operation of the product of $t_{0(k)},...,t_{s(k)}$ and the product of $a_{(k)_j}(R_k) + \beta_{(k)}(R_k)$.

Compute

$$y_3 = f_1\left(\alpha_1'(R_1) \right) = S\left(1, a_{(1)_1}(R_1), *, * \right),$$
$$y_4 = f_2\left(\alpha_2'(R_2) \right) = S\left(1,0, a_{(2)_2}(R_2), a_{(2)_3}(R_2) \right),$$
$$y_5 = f_3\left(\alpha_3'(R_3) \right) = S\left(1,0,0, a_{(3)_3}(R_3) \right).$$

Output $(y_1, y_2, y_3, y_4, y_5)$.

This encryption scheme exhibits a notable vulnerability. In the proposed instantiation of the algorithm, we have R_1 and R_2 as encryption keys. These elements are unrelated and permit a sequential key recovery attack. The keys can be restored on the basis of calculating the $\alpha_k'(R_k')$ for each $k = \overline{1,3}$ and comparing it with the y_3, y_4, y_5 according to the values of the corresponding coordinates.

$$y_3 = f_1\left(\alpha_1'(R_1) \right) = S\left(1, a_{(1)_1}(R_1), *, * \right),$$
$$y_4 = f_2\left(\alpha_2'(R_2) \right) = S\left(1,0, a_{(2)_2}(R_2), a_{(2)_3}(R_2) \right),$$
$$y_5 = f_3\left(\alpha_3'(R_3) \right) = S\left(1,0,0, a_{(3)_3}(R_3) \right).$$

The complexity of key recovery attack of $R = (R_1, R_2, R_3)$ is equivalent to $3q$.

In the revised implementation of the cryptosystem, we have modified the encryption algorithm to establish a binding between the keys of the logarithmic signatures, thereby fortifying it against a sequential recovery attack. Our proposal entails the utilization of the group of automorphisms associated with the Ree function field for encryption on the entire group $A(P_\infty) = \{S(a,b,c,d)\}$ while incorporating the

bound keys $R=(R_1,R_2,R_3)$. In such case, the brute force attack complexity is equivalent to q^3.

Our first step is a key generation stage.

Input: a large group on the field F_q, $q=3q_0^2$, $q_0=3^s$

$$A(P_\infty)=\left\{S(a,b,c,d)\middle| a\in F_q^*:=F_q\setminus\{0\},c,b,d\in F_q\right\}$$

.

Choose a tame logarithmic signatures $\beta_{(k)}=\left[B_{1(k)},...,B_{s(k)}\right]=\left(b_{ij}\right)_{(k)}$, $\left(b_{ij}\right)_{(k)}\in A(P_\infty)$ of type $\left(r_{1(k)},...,r_{s(k)}\right)$, $i=\overline{1,s(k)}$, $j=\overline{1,r_{i(k)}}$, $b_{ij(k)}\in F_q$, $k=\overline{1,3}$. Group element $\left(b_{ij}\right)_{(k)}$ has a value in only one coordinates b, c or d, respectively.

For example $\left(b_{ij}\right)_{(1)}=S\left(1,b_{ij(k)_a},0,0\right)$.

Select a random covers $\alpha_{(k)}=\left[A_{1(k)},...,A_{s(k)}\right]=\left(a_{ij}\right)_{(k)}=S\left(a_{ij(k)_a},a_{ij(k)_b},a_{ij(k)_c},a_{ij(k)_d}\right)$ of the same types as $\beta_{(k)}$, where $a_{ij}\in A(P_\infty)$, $a_{ij(k)}\in F_q\setminus\{0\}$, $i=\overline{0,s(k)}$, $j=\overline{1,r_{i(k)}}$, $k=\overline{1,3}$.

Choose $t_{i(k)}=S\left(t_{i(k)_a},t_{i(k)_b},t_{i(k)_c},t_{i(k)_d}\right)$ $t_{i(k)}\in A(P_\infty)\setminus Z$, $t_{i(k)_a},t_{i(k)_b},t_{i(k)_c},t_{i(k)_d}\in F_q/\{0\}$, $i=\overline{0,s(k)}$, $k=\overline{1,3}$.

Let's $t_{s(k-1)}=t_{0(k)}$, $k=\overline{1,3}$.

Construct a homomorphisms defined by

$f_1\left(S(a,b,c,d)\right)=S(1,b,c,d)$,

$f_2\left(S(a,b,c,d)\right)=S(1,0,c,d)$,

$f_3\left(S(a,b,c,d)\right)=S(1,0,0,d)$.

Let's do the following calculations

$\gamma_{(k)}=\left[h_{1(k)},...,h_{s(k)}\right]=t_{(i-1)(k)}^{-1}f_k\left(\left(a_{ij}\right)_{(k)}\right)\left(b_{ij}\right)_{(k)}t_{i(k)}$,

$i=\overline{1,s(k)}$, $j=\overline{1,r_{i(k)}}$, $k=\overline{1,3}$

and

$f_1\left(\left(a_{ij}\right)_{(1)}\right)\left(b_{ij}\right)_{(1)}=$

$S\left(1,a_{ij(1)_b}+b_{ij(1)_b},a_{ij(1)_c}+a_{ij(1)_b}b_{ij(1)_b}^{q_0},a_{ij(1)_b}b_{ij(1)_b}^{2q_0}+a_{ij(1)_d}\right)$,

$f_2\left(\left(a_{ij}\right)_{(2)}\right)\left(b_{ij}\right)_{(2)}=S\left(1,0,a_{ij(2)_c}+b_{ij(2)_c},a_{ij(2)_d}\right)$,

$f_3\left(\left(a_{ij}\right)_{(3)}\right)\left(b_{ij}\right)_{(3)}=S\left(1,0,0,a_{ij(3)_d}+b_{ij(3)_d}\right)$.

An output public key $[f_k,(\alpha_k,\gamma_k)]$, and a private key $\left[\beta_{(k)},\left(t_{0(k)},...,t_{s(k)}\right)\right]$, $k=\overline{1,3}$.

The next step is encryption stage.

Input: a message $m\in A(P_\infty)$, $m=S(m_1,m_2,m_3,m_4)$, $m_1\in F_q\setminus\{0\}$, $m_2,m_3,m_4\in F_q$ and the public key $\left[f_k,f_1,f_2,(\alpha_k,\gamma_k)\right]$, $k=\overline{1,3}$.

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

Choose a random $R=(R_1,R_2,R_3)$, $R_k\in Z_{|Z|}$, $k=\overline{1,3}$.

Let's set the encryption key through the mapping

$R'=\pi(R_1,R_2,R_3)=(R_1',R_2',R_3')$.

Compute

$y_1=\alpha'(R')\cdot m=\alpha_1'(R_1')\cdot\alpha_2'(R_2')\cdot\alpha_3'(R_3')\cdot m$.

Compute component y_2.

$\gamma(R)=\gamma_1'(R_1)\cdot\gamma_2'(R_2)\cdot\gamma_3'(R_3)=$

$S\Big(1,\sum_{i=1,j=R_{i(1)}}^{s(1)}\left(a_{ij(1)_b}+\beta_{ij(1)_b}\right)+*,\sum_{i=1,j=R_{i(2)}}^{s(2)}\left(a_{ij(2)_c}+\beta_{ij(2)_c}\right)+*,$

$\sum_{i=1,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_c}+\beta_{ij(3)_c}\right)+*\Big)$.

In this context, the components are ascertained through cross-computations within the group operation of the product of $t_{0(k)},...,t_{s(k)}$ and the product of $a_{(k)}(R_k)+\beta_{(k)}(R_k)$.

$y_2=\gamma(R)\cdot f_2\left(\alpha_3'(R_3)\right)\cdot f_1\left(\alpha_3'(R_3)\right)\cdot f_1\left(\alpha_2'(R_2)\right)$

,

where

$f_1\left(\alpha_k'(R_k)\right)=\prod_{i=1,j=R_{i(k)}}^{s(k)}S\left(1,a_{ij(k)_b},0,0\right)$, $k=2,3$

$f_2\left(\alpha_k'(R_k)\right)=\prod_{i=1,j=R_{i(k)}}^{s(k)}S\left(1,0,a_{ij(k)_c},0\right)$, $k=3$

and

$y_2=S\Bigg(1,\sum_{k=1}^{3}\sum_{i=1,j=R_{i(1)}}^{s(1)}a_{ij(k)_b}+\sum_{i=1,j=R_{i(1)}}^{s(1)}\beta_{ij(1)_b}+*,$

$\sum_{i=1,j=R_{i(2)}}^{s(2)}\left(a_{ij(2)_c}+\beta_{ij(2)_c}\right)+\sum_{i=1,j=R_{i(3)}}^{s(3)}a_{ij(3)_c}+*,$

$\sum_{i=1,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_d}+\beta_{ij(3)_d}\right)+*\Bigg)$.

Compute component y_3.

$\lambda(R)=f_1\left(\alpha_1'(R_1)\right)\cdot f_2\left(\alpha_2'(R_2)\right)\cdot f_2\left(\alpha_3'(R_3)\right)$,

$y_3=\lambda(R)\,f_1\left(\alpha_3'(R_3)\right)\cdot f_1\left(\alpha_2'(R_2)\right)$,

where

$f_1\left(\alpha_k'(R_k)\right)=\prod_{i=1,j=R_{i(k)}}^{s(k)}S\left(1,a_{ij(k)_b},a_{ij(k)_c},a_{ij(k)_d}\right)$,

$k=1$

$$f_2\left(\alpha_k{}'(R_k)\right)=\prod_{i=1,\,j=R_{i(k)}}^{s(k)} S\left(1,0,a_{ij(k)_c},a_{ij(k)_d}\right),$$

$k=2,3$

and

$$y_3=S\left(1,\sum_{k=1}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)_b},\right.$$

$$\left.\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)_c}+*,\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)_d}+*\right).$$

Output (y_1,y_2,y_3).

Let's decrypt. *Input*: a ciphertext (y_1,y_2,y_3) and private key $\left[\beta_{(k)},\left(t_{0(k)},...,t_{s(k)}\right)\right]$, $k=\overline{1,3}$.

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

Compute

$$D(R_1,R_2,R_3)=t_{0(1)}y_2y_3{}^{-1}t_{s(3)}^{-1}=S\left(1,\sum_{i=1,\,j=R_{i(1)}}^{s(1)}\beta_{ij(1)_a},*,*\right)$$

Restore R_1 with $\beta_{(1)}(R_1)=\sum_{i=1,\,j=R_{i(1)}}^{s(1)}\beta_{ij(1)_b}$ using $\beta_{(1)}(R_1)^{-1}$, because β_1 is simple. For further calculation, it is necessary to remove the component $\gamma_1{}'(R_1)$ from y_2 and $\alpha_1{}'(R_1)$ from y_3

Compute

$$y_2^{(1)}=\gamma_1{}'(R_1)^{-1}y_2=S\left(1,\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)_b}+*,\right.$$

$$\left.\sum_{i=1,\,j=R_{i(2)}}^{s(2)}\left(a_{ij(2)_c}+\beta_{ij(2)_c}\right)+*,\sum_{i=1,\,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_d}+\beta_{ij(3)_d}\right)+*\right)$$

and

$$y_3{}^{(1)}=f_1\left(\alpha_1{}'(R_1)\right)^{-1}y_3=S\left(1,\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)_a},\right.$$

$$\left.\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)_b}+*,\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)_c}+*\right).$$

Repeat the calculations for $D(R_2,R_3)$

$$D(R_2,R_3)=t_{0(2)}y_2{}^{(1)}\left(y_3{}^{(1)}\right)^{-1}t_{s(3)}^{-1}=$$

$$S\left(1,0,\sum_{i=1,\,j=R_{i(2)}}^{s(2)}\beta_{ij(2)_c},\sum_{i=1,\,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_d}+\beta_{ij(3)_d}\right)+*\right).$$

Restore R_2 with $\beta_{(2)}(R_2)=\sum_{i=1,\,j=R_{i(1)}}^{s(2)}\beta_{ij(1)_c}$ using $\beta_{(2)}(R_2)^{-1}$, because β_2 is simple. Remove the component $\gamma_2{}'(R_2)$ from $y_2^{(1)}$ and $f_1\left(\alpha_2{}'(R_2)\right)$ from $y_3{}^{(1)}$.

$$y_2^{(2)}=\gamma_2{}'(R_2)^{-1}y_2^{(1)}=S\left(1,\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)_b}+*,\right.$$

$$\left.\sum_{i=1,\,j=R_{i(3)}}^{s(3)} a_{ij(3)_c}+*,\sum_{i=1,\,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_d}+\beta_{ij(3)_d}\right)+*\right)$$

and

$$y_3{}^{(2)}=f_2\left(\alpha_2{}'(R_2)\right)^{-1}y_3{}^{(1)}=S\left(1,\sum_{k=2}^{3}\sum_{i=1,\,j=R_{i(k)}}^{s(k)} a_{ij(k)_b},\right.$$

$$\left.\sum_{i=1,\,j=R_{i(3)}}^{s(3)} a_{ij(3)_c}+*,\sum_{i=1,\,j=R_{i(3)}}^{s(3)}\left(a_{ij(3)_d}+\beta_{ij(3)_d}\right)+*\right).$$

Compute

$$D(R_3)=t_{0(3)}y_2{}^{(2)}\left(y_3{}^{(2)}\right)^{-1}t_{s(3)}^{-1},$$

$$D(R_3)=t_{0(3)}y_2{}^{(2)}\left(y_3{}^{(2)}\right)^{-1}t_{s(3)}^{-1}==S\left(1,0,0,\sum_{i=1,\,j=R_{i(3)}}^{s(3)}\beta_{ij(3)_d}\right).$$

Restore R_3 with $\beta_{(3)}(R_3)$ using $\beta_{(3)}(R_3)^{-1}$.

We obtain $R'=\pi(R_1,R_2,R_3)=(R_1',R_2',R_3')$ and recovery the message $m=\alpha'(R_1',R_2',R_3')^{-1}\cdot y_1$.

Conclusions and security check

Our assessment of such an attack remains applicable to the implementation of the MST3 cryptosystem, irrespective of the non-commutative group employed, and necessitates a distinct analysis. This attack entails numerous intricacies that are interconnected with vulnerabilities in the logarithmic signature and potentially the group operation.

Let us examine a brute-force attack aimed at key recovery, for which three potential schemes exist. By selecting $R=(R_1,R_2,R_3)$ try to decipher the text $y_1'=\alpha'(R')\cdot m=\alpha_1'(R_1')\cdot\alpha_2'(R_2')\cdot\alpha_3'(R_3')\cdot m$. The covers $\alpha_{(k)}=\left(a_{ij}\right)_{(k)}=S\left(a_{ij(k)_a},a_{ij(k)_b},a_{ij(k)_c},a_{ij(k)_d}\right)$ are chosen randomly, and their values are determined through multiplication within a group devoid of coordinate constraints. The resultant vector $\alpha'(R')$ depends on all of its components $\alpha_1'(R_1'),\alpha_2'(R_2'),\alpha_3'(R_3')$. Enumeration of key values $R=(R_1,R_2,R_3)$ has an estimation of complexity. For a practical attack, the message m is also unknown and has uncertainty to choose from q^3. This renders a brute-force attack on a key unfeasible. If we consider an attack model with known plaintext, the complexity of a brute-

force attack on the ciphertext remains unchanged and is equivalent to q^3.

Brute force attack on the cyphertext y_2. Select $R=(R_1,R_2,R_3)$ to match y_2. The vector y_2 has a following definition over the components $\alpha_i'(R_i)$

$$y_2 = S\left(1, \sum_{k=1}^{3}\sum_{i=1,\, j=R_{i(1)}}^{s(1)} a_{ij(k)_b} + \sum_{i=1,\, j=R_{i(1)}}^{s(1)} \beta_{ij(1)_b} + *, \right.$$
$$\sum_{i=1,\, j=R_{i(2)}}^{s(2)} \left(a_{ij(2)_c} + \beta_{ij(2)_c}\right) + \sum_{i=1,\, j=R_{i(3)}}^{s(3)} a_{ij(3)_c} + *,$$
$$\left. \sum_{i=1,\, j=R_{i(3)}}^{s(3)} \left(a_{ij(3)_d} + \beta_{ij(3)_d}\right) + * \right)$$

The values of the coordinates y_2 are defined by calculations over the vectors $\alpha_1'(R_1), \alpha_2'(R_2), \alpha_3'(R_3)$. The keys R_1, R_2, R_3 are bound and changes in any of them leads to change y_2. The brute force attack on key $R=(R_1,R_2,R_3)$ has a complexity equal to q^3.

Brute force attack on the ciphertext y_3. Select $R=(R_1,R_2,R_3)$ to match y_3. The vector y_3 has a following definition over the components $\alpha_i'(R_i)$

$$y_3 = S\left(1, \sum_{k=1}^{3}\sum_{i=1,\, j=R_{i(k)}}^{s(k)} a_{ij(k)_b}, \right.$$
$$\left. \sum_{k=2}^{3}\sum_{i=1,\, j=R_{i(k)}}^{s(k)} a_{ij(k)_c} + *, \sum_{k=2}^{3}\sum_{i=1,\, j=R_{i(k)}}^{s(k)} a_{ij(k)_d} + * \right).$$

The values of the coordinates y_2 are defined by calculations over the vectors $\alpha_1'(R_1), \alpha_2'(R_2), \alpha_3'(R_3)$. The keys R_1, R_2, R_3 are bound and changes in any of them leads to change y_2. The brute force attack on key $R=(R_1,R_2,R_3)$ has a complexity equal to q^3.

Brute force attack on the $\left(t_{0(k)},...,t_{s(k)}\right)$. The brute force attack on $\left(t_{0(k)},...,t_{s(k)}\right)$ 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 $|G|=q^3$ and is a such case the complexity of the brute force attack on $\left(t_{0(k)},...,t_{s(k)}\right)$ will be equal to q^3.

Our proposition involves employing the automorphism group of the Ree function field for full group $A(P_\infty)$ encryption along with associated keys $R=(R_1,R_2,R_3)$ and evaluating the complexity of a brute-force attack. We have enhanced the encryption algorithm to establish key bindings within the logarithmic signature, thereby fortifying it against sequential recovery attacks. The complexity of a brute-force attack for key recovery is assessed as q^3. The examination of selected text attacks also warrants consideration.

References

[1] Yue Cong, Haibo Hong, Jun Shao, Song Han, Jianhong Lin, Shuai Zhao. A New Secure Encryption Scheme Based on Group Factorization Problem. IEEE Access, 7:168728-168735, 2019 (https://www.researchgate.net/publication/337405245_A_New_Secure_Encryption_Scheme_Based_On_Group_Factorization_Problem)

[2] T. van Trung, ‘‘Construction of strongly aperiodic logarithmic signatures,’’ J. Math. Cryptol., vol. 12, no. 1, pp. 23–35, 2018. https://www.degruyter.com/document/doi/10.1515/jmc-2017-0048/html

[3] A. R. Rahimipour, A. R. Ashrafi The Existence of Minimal Logarithmic Signatures for some Finite Simple Unitary Groups Group Theory (math.GR) pp. 1–12, 2019 https://arxiv.org/pdf/1908.04125.pdf

[4] Xianmin Wang, Jing Li, Hongyang Yan An improved anti-quantum MST3 public key encryption scheme for remote sensing images April 2019 Enterprise Information Systems 15(1):1-15 DOI:10.1080/17517575.2019.1600040 https://www.tandfonline.com/doi/abs/10.1080/17517575.2019.1600040?journalCode=teis20

[5] Brandon Langenberg, Hai Pham and Rainer Steinwandt Reducing the Cost of Implementing AES as a Quantum Circuit IEEE Transactions on Quantum Engineering (Volume: 1) 16 January 2020, ISSN: 2689-1808 DOI: 10.1109/TQE.2020.2965697 https://ieeexplore.ieee.org/document/8961201

[6] G. Khalimov, Y. Kotukh, S.Khalimova Improved encryption scheme based on the automorphism group of the Ree function field field" 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE Xplore: 14 May 2021, DOI: 10.1109/IEMTRONICS52119.2021.9422514 https://ieeexplore.ieee.org/document/9422514

[7] G. Khalimov, Y. Kotukh, S.Khalimova Encryption scheme based on the automorphism group of the Ree function field" 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020, 2020, 9340192 IEEE Xplore: 02 February 2021 10.1109 / IOTSMS52051.2020.9340192 https://ieeexplore.ieee.org/document/9340192

[8] Gennady Khalimov, Yevgen Kotukh, ;Ibraim Didmanidze, Oleksandr Sievierinov, Svitlana Khalimova, Andrii Vlasov Towards three-parameter group encryption scheme for MST3 cryptosystem improvement IEEE Xplore: 19 August 2021, Page(s): 204 –211 DOI: 10.1109/WorldS451998.2021.9514009 https://ieeexplore.ieee.org/document/9514009

[9] Khalimov, G., Kotukh, Y., Shonia, O., Sievierinov, O., Khalimova, S. Encryption Scheme Based on the Automorphism Group of the Suzuki Function Field 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedings, 2021, стр. 383–387, 9468089 https://ieeexplore.ieee.org/document/9468089

[10] G. Khalimov, Y. Kotukh, S.Khalimova "Improved encryption scheme based on the automorphism group of the Ree function field field" 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE Xplore: 14 May 2021, DOI: 10.1109/ IEMTRONICS52119.2021. 9422514; https://ieeexplore.ieee.org/document/9422514

[11] 11. G. Khalimov, Y. Kotukh, S.Khalimova "Encryption scheme based on the automorphism group of the Ree function field" 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020, 2020, 9340192 IEEE Xplore: 02 February 2021 DOI: 10.1109 / IOTSMS52051.2020.9340192; https://ieeexplore.ieee.org/document/9340192

[12] Khalimov, G., Kotukh, Y., Khalimova, S. MST3 cryptosystem based on a generalized Suzuki 2 - Groups CEUR Workshop Proceedings, 2020, 2711, стр. 1–15 http://ceur-ws.org/Vol-2711/paper1.pdf

[13] Khalimov, G., Kotukh, Y., Khalimova, S. MST3 cryptosystem based on the automorphism group of the hermitian function field 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, стр. 865–868, 9061290 IEEE Xplore: 09 April 2020 DOI: 10.1109/PICST47496.2019.9061290 https://ieeexplore.ieee.org/document/9061290

[14] Gennady Khalimov, Yevgen Kotukh, Ibraim Didmanidze; Oleksandr Sievierinov, Svitlana Khalimova Encryption scheme based on small Ree groups ACM International Conference Proceeding Series, 2021, pp.33–37 https://dl.acm.org/doi/10.1145/3477911.3477917

[15] N.R. Wagner and M.R. Magyarik, A public-key cryptosystem based on the word problem", Proc. Advances in Cryptology – CRYPTO 1984, LNCS 196, Springer-Verlag (1985), 19–36.

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

[17] A. Caranti and F. D. Volta, ``The round functions of cryptosystem PGM generate the symmetric group," Des. Codes Cryptogr., vol. 38, no. 1,pp. 147_155, 2006.

[18] W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei, "A public key cryptosystem based on non-abelian finite groups", J. of Cryptology, 22 (2009), 62–74.

[19] 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.

[20] P. Svaba and T. van Trung, "Public key cryptosystem MST3 cryptanalysis and realization", Journal of Mathematical Cryptology,vol.4,no.3,pp.271–315,2010.

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

[22] Magliveras S.S., Svaba P., van Trung T., et al. On the security of a realization of cryptosystem MST3. Tatra Mt Math Publ, 2008, 41: 1–13

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

[24] W. Lempken and T. van Trung, "On minimal logarithmic signatures of finite groups," Experimental Mathematics,vol.14, no. 3, pp. 257–269, 2005.

[25] P. Svaba, "Covers and logarithmic signatures of finite groups in cryptography", Dissertation, https://bit.ly/2Ws2D24