Tatra Mt. Math. Publ. **41** (2008), 65–78

TATRA MOUNTAINS
*Mathematical Publications*

# ON THE SECURITY OF A REALIZATION OF CRYPTOSYSTEM $MST_3$

Spyros S. Magliveras — Pavol Svaba — Tran van Trung —
— Pavol Zajac

ABSTRACT. A new type of public key cryptosystem, called $MST_3$, has been recently developed on the basis of logarithmic signatures and covers of finite groups. The Suzuki 2-groups have been suggested for a possible realization of the generic version of $MST_3$. On one hand, due to their structure, the Suzuki 2-groups allow one to study the security of the system, on the other hand they possess a simple presentation allowing for an efficient implementation of the system. In this paper we present a detailed study of the security of this realization of $MST_3$. We prove a new general lower bound for the work effort required to determine the secret key in terms of the size of the underlying groups. This bound has size $q = 2^m$, where $q$ is the order of the finite field $\mathbb{F}_q$, on which the Suzuki 2-group $A(m, \theta)$ is defined. Further, by exploiting properties of the group operation in the Suzuki 2-groups, as well as a special property of canonical transversal logarithmic signatures for elementary abelian 2-groups, we show that canonical transversal logarithmic signatures are unfit to use in this realization of $MST_3$.

## 1. Introduction and preliminaries

In recent times, asymmetric cryptography has become essential to many information systems. New cryptosystems have been proposed, but only few of them remain unbroken. Security analysis is critical in the design of a new cipher, and all of its practical realizations.

The purpose of this paper is twofold. First we present a new, sharper bound on the work effort required to determine the secret key in terms of the size of the Suzuki 2-group $A(m, \theta)$ used for the realization of $MST_3$. Secondly, we present an attack on this realization when a special type of transversal logarithmic signatures, called canonical, is used as a basis for the private key. These kinds of

2000 Mathematics Subject Classification: 68P25, 94A60.
Keywords: public-key cryptosystem, logarithmic signature, random cover, Suzuki 2-group, cryptanalysis, $MST_3$.

logarithmic signatures are easily constructed and allow for very efficient factorization. However as we show in the present article, these transversal logarithmic signatures are unfit for use in the $MST_3$ realization based on the Suzuki 2-groups. The attack exploits strongly the distinguished features of the group operation of the Suzuki 2-groups and the structure of canonical logarithmic signatures.

In this section we briefly present definitions and some basic facts about logarithmic signatures, covers for finite groups and their induced mappings. For more details the reader is referred to [H63, M89, MM92, MST2, MST3].

For $\mathcal{G}$ a finite abstract group, we define the *width* of $\mathcal{G}$ to be the positive integer $w = \lceil \log |\mathcal{G}| \rceil$. Denote by $\mathcal{G}^{[\mathbb{Z}]}$ the collection of all finite sequences of elements in $\mathcal{G}$ and view the elements of $\mathcal{G}^{[\mathbb{Z}]}$ as single-row matrices with entries in $\mathcal{G}$. Let $X = [x_1, \ldots, x_r]$ and $Y = [y_1, \ldots, y_s]$ be two elements in $\mathcal{G}^{[\mathbb{Z}]}$. We define $XY \in \mathcal{G}^{[\mathbb{Z}]}$ by

$$XY = [x_1y_1, x_1y_2, \ldots, x_1y_s, x_2y_1, x_2y_2, \ldots, x_2y_s, \ldots, x_ry_1, x_ry_2, \ldots, x_ry_s].$$

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

Suppose that $\alpha = [A_1, A_2, \ldots, A_s]$ is a sequence of $A_i \in \mathcal{G}^{[\mathbb{Z}]}$, such that $\sum_{i=1}^{s} |A_i|$ is bounded by a polynomial in the width $w$ of $|\mathcal{G}|$. Let

$$\overline{A_1} \cdot \overline{A_2} \cdots \overline{A_s} = \sum_{g \in \mathcal{G}} a_g g, \qquad a_g \in \mathbb{Z}$$

and let $S$ be a subset of $\mathcal{G}$, then we say that $\alpha$ is

(i) a *cover* for $\mathcal{G}$ (or $S$), if $a_g > 0$ for all $g \in \mathcal{G}$ ($g \in S$),

(ii) a *logarithmic signature* for $\mathcal{G}$ (or $S$) if $a_g = 1$ for all $g \in \mathcal{G}$ ($g \in S$).

Note that if $\alpha = [A_1, \ldots, A_s]$ is a logarithmic signature for $\mathcal{G}$, then each element $y \in \mathcal{G}$ can be expressed uniquely as a product of the form

$$y = q_1 \cdot q_2 \cdots q_s \qquad \text{for} \quad q_i \in A_i. \tag{1.1}$$

Of course, for general covers the factorization in (1.1) is not unique, and the problem of finding a factorization for a given $y \in \mathcal{G}$ is, in general, intractable.

Let $\alpha = [A_1, \ldots, A_s]$ be a cover for $\mathcal{G}$ with $r_i = |A_i|$, then the $A_i$ are called the *blocks* of $\alpha$ and the vector $(r_1, \ldots, r_s)$ of block lengths $r_i$ the *type* of $\alpha$. We define the *length* of $\alpha$ to be the integer $\ell = \sum_{i=1}^{s} r_i$.

We say that $\alpha$ is *nontrivial* if $s \geq 2$ and $r_i \geq 2$ for $1 \leq i \leq s$, otherwise $\alpha$ is said to be *trivial*. A cover $\alpha$ is called *tame* if the factorization in equation (1.1) can be achieved in time polynomial in the width $w$ of $\mathcal{G}$, otherwise, it is called *wild*. In particular, a logarithmic signature is called *supertame* if the factorization can be achieved in time $\mathcal{O}(w^2)$.

Suppose that $\alpha = [A_1, \ldots, A_s]$ is a cover. Let $g_0, g_1, \ldots, g_s \in \mathcal{G}$, and consider $\beta = [B_1, \ldots, B_s]$ with $B_i = g_{i-1}^{-1} A_i g_i$. We say that $\beta$ is a *two sided transform* of $\alpha$ by $g_0, \ldots, g_s$. In the special case, where $g_0 = 1$ and $g_s = 1$, $\beta$ is called a *sandwich* of $\alpha$. Notice that $\beta$ is cover for $\mathcal{G}$.

Let $\alpha = [A_1, \ldots, A_s]$, $A_i = [a_{i,1}, a_{i,2}, \ldots, a_{i,r_i}]$, be a cover of type $(r_1, \ldots, r_s)$ for $\mathcal{G}$ and let $m = \prod_{i=1}^{s} r_i$. Let $m_1 = 1$ and $m_i = \prod_{j=1}^{i-1} r_i$ for $i = 2, \ldots, s$. Let $\tau$ denote the canonical bijection from $\mathbb{Z}_{r_1} \oplus \cdots \oplus \mathbb{Z}_{r_s}$ onto $\mathbb{Z}_m$, i.e.,

$$\tau : \mathbb{Z}_{r_1} \oplus \cdots \oplus \mathbb{Z}_{r_s} \to \mathbb{Z}_m,$$

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

We define the surjective mapping $\check{\alpha}$ induced by $\alpha$,

$$\check{\alpha} : \mathbb{Z}_m \to \mathcal{G},$$

$$\check{\alpha}(x) := a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s},$$

where $(j_1, j_2, \ldots, j_s) = \tau^{-1}(x)$. Since $\tau$ and $\tau^{-1}$ are efficiently computable, the mapping $\check{\alpha}(x)$ is efficiently computable.

Conversely, given a cover $\alpha$ and an element $y \in \mathcal{G}$, to determine any element $x \in \check{\alpha}^{-1}(y)$ it is necessary to obtain any one of the possible factorizations of type (1.1) for $y$ and determine indices $j_1, \ldots, j_s$ such that $y = a_{1,j_1} \cdots a_{s,j_s}$. This is possible if $\alpha$ is tame. Once a vector $(j_1, \ldots, j_s)$ has been determined, $\check{\alpha}^{-1}(y) = \tau(j_1, \ldots, j_s)$ can be computed efficiently.

Two covers (logarithmic signatures) $\alpha$, $\beta$ are said to be *equivalent* if $\check{\alpha} = \check{\beta}$.

Here we present definitions and some facts about the special type of logarithmic signatures for vector spaces over $\mathbb{F}_2$ used in the realization of $MST_3$ based on the Suzuki 2-groups.

**Definition 1.1.** Let $V$ be a vector space of dimension $m$ over the finite field $\mathbb{F}_2$. Further, let $\mathcal{P} = C_1 \cup \cdots \cup C_s$, $|C_i| = k_i$, $\sum_{i=1}^{s} k_i = m$, be a random partition of the set $\{1, \ldots, m\}$. A logarithmic signature $\beta = [B_1, \ldots, B_s]$ for $V$ is said to be **canonical** if for each $i \in \{1, \ldots, s\}$, block $B_i$ consists of all possible $2^{k_i}$ vectors with bits set on the positions defined by the subset $C_i$ and zeros elsewhere.

A canonical signature $\beta$ for $V$ of the type $(r_1, r_2, \ldots, r_s)$, $r_i = 2^{k_i}$, can be created by the following algorithm:

**Algorithm 1.1.** (Construction of a canonical logarithmic signature $\beta = [B_1, \ldots, B_s]$ for $V$.)

1. Create a random partition $\mathcal{P} = C_1 \cup \cdots \cup C_s$ of the set $\{1, \ldots, m\}$ with $|C_i| = k_i$.
2. Now, for each $i = \{1, \ldots, s\}$, construct the block $B_i$ by taking all possible $2^{k_i}$ vectors in $V$ having bits equal to 0 at positions with index not in $C_i$.

**Definition 1.2.** Let $V$ be a vector space of dimension $m$ over $\mathbb{F}_2$. We say that a canonical logarithmic signature $\beta = [B_1, \ldots, B_s] := (b_{i,j})$ for $V$ is in **standard form**, if it also fulfils the following conditions:

1. $C_1 = \{1, \ldots, k_1\}$, $C_2 = \{k_1 + 1, \ldots, k_1 + k_2\}, \ldots, C_s = \{k_1 + \cdots + k_{s-1} + 1, \ldots, m\}$
   (i.e., the lowest $k_1$ bits are used for block $B_1$, the next $k_2$ bits for $B_2$, etc.)
2. for all $i,\ j_1 < j_2 :\ b_{i,j_1} < b_{i,j_2}$
   (i.e., the vectors within $B_i$ are sorted by their integer values).

It is clear that $\beta$ forms a logarithmic signature for $V$.

**Proposition 1.1.** *Canonical signatures are tame.*

Proof. From Definition 1.1, the elements of block $B_i$ act only on the bits of $C_i$, and each $B_i$ contains a complete set of $2^{k_i}$ vectors of dimension $k_i$ on the positions of $C_i$. To "factorize" element $y \in V$ in the form $y = b_{1,j_1} b_{2,j_2} \ldots b_{s,j_s}$ we split the bits of $y$ into vectors $b_{i,j_i}$ with respect to partition $\mathcal{P}$ as follows. We copy the bits of $y$ on the positions determined by $C_i$ to appropriate vector $b_{i,j_i}$, and set the rest of the bits of $b_{i,j_i}$ to zero. The position of such created vector $b_{i,j_i}$ within the block $B_i$ then defines index $j_i$.

If the vectors in each $B_i$ are sorted in ascending order, then the integer value, with respect to Radix 2, of the subvector $u_i$ constructed from $b_{i,j_i}$ by concatenation of the bits on the positions of $C_i$ is equal to the index of $b_{i,j_i}$ within the block $B_i$ (starting with index 0). This factorization procedure has time complexity $\mathcal{O}(1)$. □

**Proposition 1.2.** *A canonical logarithmic signature $\beta := (b_{i,j})$ for $V$ can be written as a linear transformation of the canonical signature $\varepsilon := (e_{i,j})$ of the same type for $V$ in standard form. In other words, there exists a matrix $M \in GL(m, 2)$ such that $\beta := (b_{i,j}) = (e_{i,j}M)$.*

Sketch of Proof. Any canonical logarithmic signature can be transformed to standard form by permuting elements between subsets $C_i$ and by sorting vectors within each block $B_i$. Both transformations induce permutation matrices acting on bits of block elements represented as binary vectors. □

The following statement follows naturally:

**Proposition 1.3.** *Transforming a canonical logarithmic signature of $V$ by means of a non-singular linear transformation results in a tame logarithmic signature for $V$.*

Sketch of proof. As this transformation is reversible, factorization is tame. □

Using this proposition we may construct tame logarithmic signatures.

**Algorithm 1.2.** (Construction of tame logarithmic signature for $V$.)

1. Create a canonical logarithmic signature $\beta := (b_{i,j})$ of a given type for $V$ over the field $\mathbb{F}_{2^m}$ (using Algorithm 1.1).
2. Generate a random matrix $M \in GL(m, 2)$ and transform $\beta$ to a tame logarithmic signature $\beta^* := (b^*_{i,j}) = (b_{i,j}M)$.

The use of random matrices in Algorithm 1.2 for tame signature generation introduces some level of randomness essential for the cryptography. However, as we show in later sections, it does not prevent an attack that exploits the special structure of canonical signatures used in this algorithm.

**Proposition 1.4.** *Let $\beta = [B_1, B_2, \ldots, B_s]$ be a canonical logarithmic signature for $V$. Let $\beta^* := (b^*_{i,j})$, where $b^*_{i,j} = b_{i,j} + d_i$ with $d_i \in B_i$, then $\beta^*$ is also canonical for $V$.*

Proof. From Definition 1.1, the blocks of $\beta$ act on disjoint sets of bits $C_i$, and every block $B_i$ contains the complete set of $2^{k_i}$ vectors with bits set on the positions of $C_i$. If we add a fixed element $d_i \in B_i$, to all elements of $B_i$, we switch the bits in the positions of 1's in $d_i$ in each of $2^{k_i}$ possible vectors, so $B_i$ remains the same up to order, and $\beta$ remains canonical for $V$. □

In general we have

**Proposition 1.5.** *Let $\mathcal{G}$ be a finite group. Let $\beta = [B_1, B_2, \ldots, B_s] := (b_{i,j})$ be a tame logarithmic signature for $\mathcal{G}$. Let $\beta^* := (b^*_{i,j})$, where $b^*_{i,j} = b_{i,j}d_i$, $d_i \in \mathcal{G}$. Then $\beta^*$ is tame, if one of the following conditions is fulfilled:*

1. *$d_i \in \mathbb{Z}(\mathcal{G})$ for $i = 1, \ldots, s$;*
2. *$d_i \in \mathcal{G}_{i-1}$ for $i = 1, \ldots, s$, if $\beta$ is exact-transversal for $\mathcal{G}$ with a chain of subgroups $\gamma : 1 = \mathcal{G}_0 < \mathcal{G}_1 < \cdots < \mathcal{G}_s = \mathcal{G}$, and $B_i$ a complete set of right (left) coset representatives of $\mathcal{G}_{i-1}$ in $\mathcal{G}_i$.*

Sketch of proof. In Case 1., the elements $b_{i,j}$ and $d_i$ commute, so we can find logarithmic signature $\beta' = (b'_{i,j})$ equivalent to $\beta^*$ such, that

$$b'_{i,j} = \begin{cases} b_{i,j} & \text{for all } i = 1, \ldots, s-1, \\ b_{s,j}d & \text{where } d = d_1 d_2 \ldots d_s\,. \end{cases}$$

Then, if we are able to factorize in $s$ blocks of $\beta$, we are able to factorize in the first $s-1$ blocks and find the last index $j_s$ by exhaustive search.

In Case 2., suppose we are able to factorize $g = b_{1,j_1} b_{2,j_2} \ldots b_{s,j_s}$ with respect to $\beta$, and trying to factorize $g^* = b^*_{1,j_1} b^*_{2,j_2} \ldots b^*_{s,j_s}$ with respect to $\beta^*$. As $B^*_i = B_i d_i$ with $d_i \in \mathcal{G}_{i-1}$, it follows that $b_{i,j}$ and $b^*_{i,j}$ are in the same coset of $\mathcal{G}_{i-1}$ in $\mathcal{G}_i$.

We start the factorization of $g^* = b^*_{1,j_1} \ldots b^*_{s,j_s}$ with respect to the block $B^*_s$.

Because $b^*_{1,j_1} \dots b^*_{s-1,j_{s-1}} \in \mathcal{G}_{s-1}$, $g^*$ and $b^*_{s,j_s}$ are in the same coset of $\mathcal{G}_{s-1}$ in $\mathcal{G}_s$. This means we can identify the coset of $g^*$, say $b^*_{s,j_s}\mathcal{G}_{s-1}$ uniquely. Thus, we have found the first factor of $g^*$, namely $b^*_{s,j_s}$. We continue with the factorization of $g^*(b^*_{s,j_s})^{-1}$ with respect to the block $B^*_{s-1}$ and identify element $b^*_{s-1,j_{s-1}}$, etc. □

## 2. Generic version of $MST_3$

We presently describe cryptosystem $MST_3$ in its generic form. Let $\mathcal{G}$ be a finite non-abelian group with nontrivial center $\mathcal{Z}$ such that $\mathcal{G}$ does not split over $\mathcal{Z}$, i.e., there is no subgroup $\mathcal{H} < \mathcal{G}$ with $\mathcal{H} \cap \mathcal{Z} = 1$ such that $\mathcal{G} = \mathcal{Z} \cdot \mathcal{H}$. Assume also that $\mathcal{Z}$ is sufficiently large so that exhaustive search problems are computationally not feasible in $\mathcal{Z}$.

The cryptographic hypothesis, which forms the security basis of cryptosystem $MST_3$, is that if $\alpha = [A_1, A_2, \dots, A_s] := (a_{i,j})$ is a random cover for a "large" subset $S$ of $\mathcal{G}$, then finding a factorization

$$g = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,js}$$

for an arbitrary element $g \in S$ with respect to $\alpha$ is an intractable problem see [MST3].

### 2.1. Setup

Alice chooses a large group $\mathcal{G}$ as described above and generates:

(1) *a tame logarithmic signature* $\beta = [B_1, \dots, B_s] := (b_{i,j})$ of type $(r_1, \dots, r_s)$ for $\mathcal{Z}$.

(2) *a random cover* $\alpha = [A_1, \dots, A_s] := (a_{i,j})$ of the same type as $\beta$ for a certain subset $\mathcal{J}$ of $\mathcal{G}$ such that $A_1, \dots, A_s \subseteq \mathcal{G} \setminus \mathcal{Z}$.

She then chooses elements $t_0, t_1, \dots, t_s \in \mathcal{G} \setminus \mathcal{Z}$ and computes:

(3) $\tilde{\alpha} = [\tilde{A}_1, \dots, \tilde{A}_s] := (\tilde{a}_{i,j})$, where $\tilde{a}_{i,j} = t_{i-1}^{-1} a_{i,j} t_i$ for $i = 1, \dots, s$ and $j = 1, \dots, r_i$.

(4) $\gamma := (h_{i,j}) = (b_{i,j}\tilde{a}_{i,j})$.

Alice publishes her public key $[\alpha, \gamma]$, keeping $\big[\beta, (t_0, \dots, t_s)\big]$ as her private key.

### 2.2. Encryption

If Bob wants to send a message $x \in \mathbb{Z}_{|\mathcal{Z}|}$ to Alice, he

(1) computes values $y_1 = \check{\alpha}(x)$ and $y_2 = \check{\gamma}(x)$, and

(2) sends $y = (y_1, y_2)$ to Alice.

### 2.3. Decryption

Alice knows $y$, figures that

$$\begin{aligned} y_2 &= \check{\gamma}(x) \\ &= b_{1,j_1}\tilde{a}_{1,j_1} \cdot b_{2,j_2}\tilde{a}_{2,j_2} \cdots b_{s,j_s}\tilde{a}_{s,j_s} \\ &= b_{1,j_1}t_0^{-1}a_{1,j_1}t_1 \cdots b_{s,j_s}t_{s-1}^{-1}a_{s,j_s}t_s \\ &= b_{1,j_1}b_{2,j_2} \cdots b_{s,j_s}t_0^{-1}a_{1,j_1}a_{2,j_2} \cdots a_{s,j_s}t_s \\ &= \check{\beta}(x) \cdot t_0^{-1}\check{\alpha}(x)t_s \\ &= \check{\beta}(x) \cdot t_0^{-1}y_1t_s \end{aligned}$$

and can therefore compute

$$\check{\beta}(x) = y_2t_s^{-1}y_1^{-1}t_0.$$

Alice then recovers $x$ from $\check{\beta}(x)$ using $\check{\beta}^{-1}$ which is efficiently computable as $\beta$ is tame.

## 3. Realization of $MST_3$

In this section we present details of the only known realization of the cryptosystem $MST_3$ described in [MST3].

Let $q = 2^m$ with $3 \leq m \in \mathbb{N}$ odd, and let $\theta$ be a nontrivial automorphism of odd order of the field $\mathbb{F}_q$. Now let $\mathcal{G}$ be the Suzuki 2-group $A(m,\theta)$ of order $q^2$ as given in [H63]. $\mathcal{G}$ is a special 2-group of exponent 4 such that $\mathcal{Z} := \mathbb{Z}(\mathcal{G}) = \Phi(\mathcal{G}) = \mathcal{G}' = \Omega_1(\mathcal{G})$, where $\Phi(\mathcal{G})$ denotes by definition the intersection of all the maximal subgroups of $\mathcal{G}$, and $\Omega_1(\mathcal{G}) = \langle g \in \mathcal{G} : g^2 = 1\rangle$. The groups $\mathcal{Z}$ and $\mathcal{G}/\mathcal{Z}$ are elementary abelian of order $q$. Moreover, $o(g) = 4$ for every $g \in \mathcal{G} \setminus \mathcal{Z}$.

Within each block $A_i$ of cover $\alpha$, elements are selected according to the following property: *For every $A_i$, $i = 1, \ldots, s$, if $x \neq y$, $x, y \in A_i$, then $xy^{-1}$ is an element of order 4 in $\mathcal{G}$.* This means that distinct elements $x$ and $y$ of $A_i$ are not in the same coset of $\mathcal{Z}$.

Group $\mathcal{G}$ can be described as a subgroup of $GL(3,q)$ as follows. Let $a, b \in \mathbb{F}_q$ and define

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

Then

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

and

$$\mathcal{Z} = \mathbb{Z}(\mathcal{G}) = \Phi(\mathcal{G}) = \mathcal{G}' = \Omega_1(\mathcal{G}) = \big\{S(0,b) \mid b \in \mathbb{F}_q\big\}.$$

It is easily verified that the multiplication of two elements in $\mathcal{G}$ is given by rule

$$S(a_1, b_1)S(a_2, b_2) = S\big(a_1 + a_2,\ b_1 + b_2 + a_1^\theta a_2\big).$$

Particularly, if we store elements $S(a, b)$ as a triple $\big(a, b, a^\theta\big)$ and identify the product $S\big(a_1, b_1, a_1^\theta\big)S\big(a_2, b_2, a_2^\theta\big)$ with the triple $\big(a_1{+}a_2,\ b_1{+}b_2{+}a_1^\theta a_2,\ a_1^\theta{+}a_2^\theta\big)$, we are able to realize each group operation in just a single multiplication and four additions in $\mathbb{F}_q$.

For efficiency reasons, the Frobenius automorphism has been chosen for $\theta$ to minimize the number of squaring operations needed to extend a group element to its triple representation.

The reduced storage requirement and operation efficiency are significant for the realization of $MST_3$ using group $\mathcal{G} = A(m, \theta)$.

An important requirement of the realization of $MST_3$ is efficient factorization with respect to tame logarithmic signature $\beta$.

**Remark 3.1.** As elements of the center $\mathcal{Z}$ are of the form $S(0, b)$, we can identify the center with the additive group of the field $\mathbb{F}_q$, i.e., with a vector space $V$ of dimension $m$ over $\mathbb{F}_2$.

Then we can use canonical logarithmic signatures for $V$ as a basis for key generation. In this realization of $MST_3$, Algorithm 1.2 is used to generate a tame logarithmic signature $\beta$ which is a part of Alice's private key. This reduces the complexity of factorizing with respect to $\beta$ to $\mathcal{O}(1)$.

## 4. Attack on $MST_3$

In this section we present details of an attack on the realization of cryptosystem $MST_3$ described in the previous section.

### 4.1. Used notation

Here we define notation used below and note some facts resulting from the usage of the Suzuki 2-group $A(m, \theta)$ in the realization of $MST_3$.

If $g = S(x, y) \in \mathcal{G},\ \ x, y \in \mathbb{F}_q$, we denote $x$ by $g_{.a}$, and $y$ by $g_{.b}$, that is, we denote the projections of $g \in \mathcal{G}$ along the first and second coordinates by $g_{.a}$ and $g_{.b}$, respectively. Thus, we write $g = S(g_{.a}, g_{.b})$.

Accordingly, we denote the elements of the public key $\alpha := (a_{i,j})$, $\gamma := (h_{i,j})$, known to the adversary, by pairs $S(a_{(i,j).a},\ a_{(i,j).b})$, and $S(h_{(i,j).a},\ h_{(i,j).b})$, respectively. Similarly, the private key elements $\beta := (b_{i,j})$, $(t_0, \ldots, t_s)$ are denoted by pairs $S\big(b_{(i,j).a},\ b_{(i,j).b}\big)$, and $S\big(t_{(i).a},\ t_{(i).b}\big)$.

We define an action of $GL(m,2)$ on $\mathcal{G}$ as follows: If $M \in GL(m,2)$ and $g = S(g_{.a}, g_{.b}) \in \mathcal{G}$, we define a "transformation"

$$gM = S(g_{.a}, g_{.b})M := S(g_{.a}, g_{.b}M).$$

Thus, $M \in GL(m,2)$ acts on the second coordinate, and fixes the first coordinate of the elements of $\mathcal{G}$.

The following lemma is quite easy to see:

**Lemma 4.1.** *In terms of the notation introduced thus far we have:*

i) *The inverse of $g = S(g_{.a}, g_{.b}) \in \mathcal{G}$ is given by rule*

$$S(g_{.a}, g_{.b})^{-1} = S(g_{.a}, g_{.b} + {g_{.a}}^{\theta} g_{.a})\,.$$

ii) *Both operations, inversion and matrix transformation, keep the ".a-part" of an element $g$ invariant.*

iii) *Elements from the same coset of the center $\mathcal{Z}$, have identical ".a-part" projections, i.e., if $t_j \in t_i\mathcal{Z}$ then,*

$$t_{(i).a} = t_{(j).a}\,.$$

We identify a canonical logarithmic signature $\varepsilon := (e_{i,j})$ for $V$ with a logarithmic signature $\beta := (b_{i,j})$ for $\mathcal{Z}$, where $b_{i,j} := S(0, e_{i,j})$.

### 4.2. Attack on $t_0$

In this attack, an adversary attempts to extract information about the private key $\big[\beta, (t_0, \ldots, t_s)\big]$ from the knowledge of the public key $\big[\alpha, \gamma\big]$. We will show that if the adversary can determine the coset of $t_0\mathcal{Z}$, then he can construct an alternative secret key $\big[\beta^*, (t_0^*, \ldots, t_s^*)\big]$ satisfying the equation

$$h_{i,j} = b_{i,j}^* t_{i-1}^{*-1} a_{i,j} t_i^* \tag{4.1}$$

for all $i = 1, \ldots, s$ and $j = 1, \ldots, r_i$, such that $\big[\beta^*, (t_0^*, \ldots, t_s^*)\big]$ can be used to decrypt any ciphertext correctly.

**Assumption 4.1.** Assume that the coset $t_0\mathcal{Z}$ is known to the adversary.

In the following we prove that any choice of $t_0^* \in t_0\mathcal{Z}$ provides enough information to determine $\big[\beta^*,\ (t_0^*, \ldots, t_s^*)\big]$ satisfying equation (4.1).

Let $t_0 = t_0^* z_0$ for some $z_0 \in \mathcal{Z}$ (by Assumption 4.1). In this attack the adversary will construct $\beta^* = (b_{i,j}^*)$ with $b_{i,1}^* = id$ (i.e. zero vector), for $i = 1, \ldots, s$. Now let $b_{i,j} = b_{i,j}^*\ d_{i,j}$ for some $d_{i,j} \in \mathcal{Z}$. As $b_{i,1}^* = id$ we have $d_{i,1} = b_{i,1}$ for every $i = 1, \ldots, s$.

Starting with the first block of $\gamma$ we write equations:

$$\begin{aligned}
h_{1,1} &= b^*_{1,1}\ d_{1,1}\ t_0^{*-1}\ z_0\ a_{1,1}\ t_1 \\
&= b^*_{1,1}\ t_0^{*-1}\ a_{1,1}\ (t_1\ d_{1,1}\ z_0) \quad \Rightarrow \quad t^*_1 = t_1\ d_{1,1}\ z_0 \\
&\qquad\qquad \text{(i.e., } t^*_1 \text{ and } t_1 \text{ are in the same coset of } \mathcal{Z}\text{)}, \\
h_{1,j} &= b_{1,j}\ t_0^{*-1}\ z_0\ a_{1,j}\ t^*_1\ d_{1,1}\ z_0 \quad \text{for all } j = 2, \ldots, r_1\,, \\
&= (b_{1,j}\ d_{1,1})\ t_0^{*-1}\ a_{1,j}\ t^*_1\,, \\
b^*_{1,j} &= b_{1,j}\ d_{1,j} = \ b_{1,j}\ d_{1,1} \quad \Rightarrow \quad d_{1,j} = d_{1,1} = b_{1,1}\,.
\end{aligned}$$

Using $t^*_1$ we compute $t^*_2$ and $d_{2,j}$ from the second block:

$$\begin{aligned}
h_{2,1} &= b^*_{2,1}\ d_{2,1}\ t_1^{*-1}\ d_{1,1}\ z_0\ a_{2,1}\ t_2 \\
&= b^*_{2,1}\ t_1^{*-1}\ a_{2,1}\ (t_2\ d_{2,1}\ d_{1,1}\ z_0) \quad \Rightarrow \quad t^*_2 = t_2\ d_{2,1}\ d_{1,1}\ z_0 \\
&\qquad\qquad \text{(i.e., } t^*_2 \text{ and } t_2 \text{ are in the same coset of } \mathcal{Z}\text{)}, \\
h_{2,j} &= b_{2,j}\ t_1^{*-1}\ d_{1,1}\ z_0\ a_{2,j}\ t^*_2\ d_{2,1}\ d_{1,1}\ z_0 \qquad \text{for all } j = 2, \ldots, r_2\,, \\
&= (b_{2,j}\ d_{2,1})\ t_1^{*-1}\ a_{2,j}\ t^*_2\,, \\
b^*_{2,j} &= b_{2,j}\ d_{2,j} = \ b_{2,j}\ d_{2,1} \quad \Rightarrow \quad d_{2,j} = d_{2,1} = b_{2,1}\,. \\
&\ \ \vdots
\end{aligned}$$

Continuing this process we determine all $t^*_1, \ldots, t^*_s$. It follows that $d_{i,j} = d_{i,1} = b_{i,1},$ for all $i = 1, \ldots, s$. Denote $d_{i,j} = d_i$. Notice that $t^*_i = t_i\ z_0 \prod_{k=1}^{i} d_k$, i.e., $t^*_i$ and $t_i$ are in the same coset of $\mathcal{Z}$ in $\mathcal{G}$, $i = 1, \ldots, s$.

Now let $(\breve{\alpha}(x),\ \breve{\gamma}(x))$ be a cipher of a message $x \in \mathbb{Z}_{|\mathcal{Z}|}$, i.e.,

$$\begin{aligned}
\breve{\gamma}(x) &= \breve{\beta}(x)\ t_0^{-1}\ \breve{\alpha}(x)\ t_s \\
&= \breve{\beta}(x)\ t_0^{*-1}\ z_0\ \breve{\alpha}(x)\ t^*_s\ z_0 \prod_{k=1}^{s} d_k \\
&= \Big(\breve{\beta}(x) \prod_{k=1}^{s} d_k\Big)\ t_0^{*-1}\ \breve{\alpha}(x)\ t^*_s\,.
\end{aligned}$$

Now if $\breve{\beta}(x) = b_{1,x_1}\ b_{2,x_2}\ \ldots b_{s,x_s}$ and $\beta^* := (b^*_{i,j})$ where $b^*_{i,j} = b_{i,j}\ d_i$, then

$$\begin{aligned}
\breve{\beta}^*(x) &= b^*_{1,x_1}\ b^*_{2,x_2}\ \ldots b^*_{s,x_s} \\
&= b_{1,x_1}\ d_1\ b_{2,x_2}\ d_2\ \ldots b_{s,x_s}\ d_s \\
&= (\breve{\beta}(x) \prod_{k=1}^{s} d_k).
\end{aligned}$$

And therefore

$$\breve{\beta}^*(x) = \breve{\gamma}(x)\ t_s^{*-1}\ \breve{\alpha}(x)^{-1}\ t_0^*\,.$$

This shows that factorization of $\breve{\beta}^*(x)$ with respect to $\beta^*$ provides the correct message $x$. Moreover, as $\beta^*$ is tame, after Proposition 1.5 (1.), this factorization can be done efficiently.

**Conclusion 1.** From the above, in the Suzuki 2-group realization of $MST_3$, it is sufficient for an adversary to obtain an element $t_0^* \in t_0\mathcal{Z}$. This knowledge enables him to compute an alternative private key $[\beta^*, (t_0^*, \ldots, t_s^*)]$ , where $\beta^*$ is tame. With this key he can decrypt any message correctly and efficiently. As there are $q = |\mathcal{G}/\mathcal{Z}|$ possible choices for $t_0^*$ in $t_0\mathcal{Z}$, the complexity of this attack is $q$.

### 4.3. Attack on $MST_3$ when canonical signature is used

In this section we show that if the canonical transversal logarithmic signature is used in the realization of $MST_3$ with the Suzuki 2-groups, then the system can be broken.

Assume that the canonical signature $\beta$ is used with the Suzuki 2-group $\mathcal{G} = A(m, \theta)$, where $\theta$ is a nontrivial automorphism of odd order of the field $\mathbb{F}_q$, $q = 2^m$. ($\theta$ is not necessary the Frobenius automorphism.) We show how an adversary can determine the correct coset $t_0\mathcal{Z}$, and hence can break the system as described in Section 4.2.

In this attack, we have to step down from group $\mathcal{G}$ to underlying field $\mathbb{F}_q$.

For the first block of $\gamma$:

$$h_{1,j} = b_{1,j}\ t_0^{-1}\ a_{1,j}\ t_1\,.$$

Particularly, for each part

$$\begin{aligned} h_{(1,1).a} &= t_{(0).a}^{-1} + a_{(1,1).a} + t_{(1).a} \\ h_{(1,j).b} &= b_{(1,j).b} + t_{(0).b}^{-1} + a_{(1,j).b} + t_{(1).b} + \left(t_{(0).a}\right)^{\theta} a_{(1,j).a} \\ &\quad + (t_{(0).a})^{\theta} t_{(1).a} + \left(a_{(1,j).a}\right)^{\theta} t_{(1).a}\,. \end{aligned}$$

For an index set $J$ yet to be determined, with $|J|$ even

$$\begin{aligned}\sum_{j\in J} h_{(1,j).b} &= \sum_{j\in J} b_{(1,j).b} \sum_{j\in J} a_{(1,j).b} + \big(t_{(0).a}\big)^{\theta} \sum_{j\in J} a_{(1,j).a} \\ &\quad + t_{(1).a} \sum_{j\in J} \big(a_{(1,j).a}\big)^{\theta} \\ &= \sum_{j\in J} b_{(1,j).b} + \sum_{j\in J} a_{(1,j).b} + \big(t_{(0).a}\big)^{\theta} \sum_{j\in J} a_{(1,j).a} \\ &\quad + \big(h_{(1,1).a} + t_{(0).a} + a_{(1,1).a}\big) \sum_{j\in J} \big(a_{(1,j).a}\big)^{\theta}.\end{aligned}$$

We end up with trinomial:

$$A\big(t_{(0).a}\big)^{\theta} + B\big(t_{(0).a}\big) + C = 0, \tag{4.2}$$

where

$$\begin{aligned}A &= \sum_{j\in J} a_{(1,j).a}\,, \\ B &= \sum_{j\in J} (a_{(1,j).a})^{\theta}, \\ C &= \sum_{j\in J} b_{(1,j).b} + \sum_{j\in J} h_{(1,j).b} + \sum_{j\in J} a_{(1,j).b} \\ &\quad + \big(h_{(1,1).a} + a_{(1,1).a}\big) \sum_{j\in J} \big(a_{(1,j).a}\big)^{\theta}.\end{aligned}$$

The question here is how to choose $J$. The unknown in this trinomial is $\sum_{j\in J} b_{(1,j).b}$, i.e., the sum of elements of the first block of $\beta$. As it is part of the private key, and to guess it is infeasible, we choose $J$ such that $\sum_{j\in J} b_{(1,j).b}$ will sum up to zero.

Here the special structure of the canonical logarithmic signature used as a basis for $\beta$ can be exploited. As $\beta := (b_{i,j}) = (e_{i,j}M)$, for some canonical signature $\varepsilon := (e_{i,j})$ and $M \in GL(m, 2)$, it is true that

$$\sum_{j\in J} b_{(1,j).b} = \sum_{j\in J} e_{(1,j).b} M = \left(\sum_{j\in J} e_{(1,j).b}\right) M.$$

The block of canonical logarithmic signature $\varepsilon$ consists of a complete set of $2^{k_i}$ vectors, so we are always able to find $J \subseteq \{1, \ldots, r_1\}$ such that

$$\sum_{j\in J} e_{(1,j).b} = 0.$$

From the structure of the canonical logarithmic signature we see that the sum of all vectors in the block $B_1$ is a zero vector. Therefore we can choose $J = \{1, \ldots, r_1\}$, i.e., indices of all elements in the first block of $\beta$ [1].

Now, breaking the system reduces to the problem of finding the root of the trinomial in equation (4.2) over $\mathbb{F}_q$. Well known results of Berlekamp or Shoup solve the problem of factoring a polynomial of degree $n$ over $\mathbb{Z}_p[x]$ in time polynomial in $n$ and $p$ [B70, S90].

**Conclusion 2.** From the above, if the canonical logarithmic signature is used in the realization of $MST_3$ with Suzuki 2-groups, then the adversary can determine the coset $t_0\mathcal{Z}$ with the complexity equivalent to that of finding the roots of a trinomial over $\mathbb{F}_q$. In particular, when $\theta$ is the Frobenius automorphism the complexity of this attack is $\mathcal{O}(1)$.

### 4.4. Conclusions

We have studied the realization of $MST_3$ using the Suzuki 2-groups. The main contributions of this paper are twofold. First, we have sharpened the bound on the security complexity of $MST_3$. Our new bound provides a valuable estimate of the strength of $MST_3$. Secondly, we have proved that the canonical logarithmic signatures are not suitable for use in this realization. From the proof we gain a good insight into the structure of $MST_3$ with the underlying Suzuki 2-groups. Particularly, it becomes clear that the class of suitable logarithm signatures for this $MST_3$ realization has to possess certain additional properties. Further, the results of the paper implicitly suggest a method of modifying the canonical logarithmic signatures to be fit into a secure implementation of $MST_3$. We will present these methods in a future work.

**Acknowledgements.** The authors would like to thank the anonymous reviewers for their helpful comments.

REFERENCES

[H63] HIGMAN, G.: *Suzuki 2-groups,* Illinois J. Math. **7** (1963), 79–96.

[M89] MEMON, N. D.: *On Logarithmic Signatures and Applications,* Dissertation, University of Nebraska, USA, 1989.

[MM92] MAGLIVERAS, S. S.—MEMON, N. D.: *Algebraic properties of cryptosystem PGM,* J. Cryptology **5** (1992), 167–183.

[MST2] MAGLIVERAS, S. S.—STINSON, D. R.—TRAN VAN TRUNG: *New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups,* J. Cryptology **15** (2002), 285–297.

[1] The attack described above can be applied to any block $B_i$ of $\beta$ to identify a coset of $t_{i-1}$. Knowing the coset of $t_{i-1}$ we can determine the coset of $t_0$ uniquely.

[MST3] LEMPKEN, W.—MAGLIVERAS, S. S.—TRAN VAN TRUNG—WEI, W.: *A public key cryptosystem based on non-abelian finite groups* J. Cryptology, online version, `http://www.springerlink.com/content/f50820g6h8152822/fulltext.pdf`.

[B70] BERLEKAMP, E.: *Factoring polynomials over large finite fields,* Math. Comp. **24** (1970), 713–735.

[S90] SHOUP, V.: *On the deterministic complexity of factoring polynomials over finite fields,* Inform. Process. Lett. **33** (1990), 261–267.

Received September 28, 2007

*S. S. Magliveras*
*Department of Mathematical Sciences*
*Center for Cryptology and*
*Information Security*
*Florida Atlantic University*
*Boca Raton, FL 33431*
*U.S.A.*
*E-mail*: spyros@fau.edu

*P. Svaba*
*Tran van Trung*
*Institut für Experimentelle Mathematik*
*Universität Duisburg-Essen*
*Ellernstrasse 29*
*D-45326 Essen*
*GERMANY*
*E-mail*: svaba@iem.uni-due.de
trung@iem.uni-due.de

*P. Zajac*
*Department of Applied Information and*
*Information Technology*
*Slovak University of Technology*
*Ilkovičova 3*
*SK-812-19 Bratislava*
*SLOVAKIA*
*E-mail*: pavol.zajac@stuba.sk