J. Cryptol. (2009) 22: 62–74
DOI: 10.1007/s00145-008-9033-y

Journal of
CRYPTOLOGY

A Public Key Cryptosystem Based on Non-abelian Finite Groups

Wolfgang Lempken and Tran van Trung
Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Ellernstrasse 29, 45326 Essen, Germany
lempken@iem.uni-due.de; trung@iem.uni-due.de

Spyros S. Magliveras and Wandi Wei
Department of Mathematical Sciences, Center for Cryptology and Information Security,
Florida Atlantic University, Boca Raton, FL 33431, USA
spyros@fau.edu; wei@brain.math.fau.edu

Communicated by Stefan Wolf

Received 5 December 2005 and revised 16 October 2008
Online publication 11 November 2008

Abstract. We present a new approach to designing public-key cryptosystems based on covers and logarithmic signatures of non-abelian finite groups. Initially, we describe a generic version of the system for a large class of groups. We then propose a class of 2-groups and argue heuristically about the system's security. The system is scalable, and the proposed underlying group, represented as a matrix group, affords significant space and time efficiency.

Key words. Public-key cryptosystem, Logarithmic signature, Uniform cover, Trapdoor one-way function, Suzuki 2-group.

1. Introduction

At the writing of this paper, only a few asymmetric cryptographic primitives remain unbroken. Most of these are based on the perceived intractability of certain mathematical problems in very large finite abelian groups, in particular representations. Prominent hard problems are (i) the problem of factoring large integers, (ii) the *Discrete Logarithm Problem* (DLP) [1], in particular representations of large cyclic groups, and (iii) finding a short basis for a given integral lattice $\mathcal{L}$ of large dimension. Unfortunately, in view of P. Shor's quantum algorithms for integer factoring and solving the DLP [9], the known public-key systems will be insecure when quantum computers become practical. A recent report edited by P. Nguyen [8] identifies these and other problems facing the field of information security in the future.

This work was partially supported by a Federal Earmark grant for *Research in Secure Telecommunication Networks* (2004-05).

The theoretical foundations for many current asymmetric cryptographic primitives lie in the intractability of mathematical problems closer to number theory than group theory. Number theory deals mostly with abelian groups.

In this paper we introduce a new approach to designing trapdoor one-way functions based on non-abelian finite groups. Our primary motivation emerges from the observation that the security of public key cryptosystem MST_2 depends on the choice of a secret epimorphism. In particular, the public key in MST_2 consists of a *mesh* for a group $\mathcal{G}$ and its image under a certain epimorphism f from $\mathcal{G}$ onto a group $\mathcal{H}$, where f is the secret key [7]. Recommended usage is choosing f as conjugation by an element $g \in \mathcal{G}$. Indeed, in certain classes of groups, public knowledge of the mesh and its image under g reveals some information about g. This could be used to mount an attack against MST_2 for these classes of groups [7].

Our assumption is that *random covers* in finite groups induce one-way functions. Beginning with a random cover α for a subset of $\mathcal{G}$, we obtain a *two-sided transform* $\tilde{\alpha}$ of α. Then, using $\tilde{\alpha}$ and a secret, tame logarithmic signature β for the center of $\mathcal{G}$, we construct γ which covers a second subset of $\mathcal{G}$. We make α and γ public and keep secret the trap-door in the system β, as well as the information which produces $\tilde{\alpha}$ from α.

2. Preliminaries

In this section we briefly present notation, definitions and some basic facts about logarithmic signatures, covers for finite groups, and their induced mappings. For more details, the reader is referred to [6,7]. The group theoretic notation used is standard and can be found in [3].

Let $\mathcal{G}$ be 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 $X = [x_1, x_2, \ldots, x_r]$ and $Y = [y_1, y_2, \ldots, y_s]$ be two elements in $\mathcal{G}^{[\mathbb{Z}]}$. We define

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

Instead of $X \cdot Y$ we will also write $X \otimes Y$ as ordinary tensor product of matrices, or for short we will write XY. 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 $\log |\mathcal{G}|$. Let

$$\overline{A_1} \cdot \overline{A_2} \cdots \overline{A_s} = \sum_{g \in \mathcal{G}} a_g g, \quad a_g \in \mathbb{Z}. \tag{2.1}$$

Let $\mathcal{S}$ be a subset of $\mathcal{G}$. Then we say that α is

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

Let α be a cover. Define $\lambda_{\min} := \min\{a_g : g \in \mathcal{G}\}$, $\lambda_{\max} := \max\{a_g : g \in \mathcal{G}\}$, and $\lambda := \lambda_{\max}/\lambda_{\min}$. The ratio λ measures the degree of uniformity of α. We say that α is a *uniform cover* if $\lambda = 1$. In particular, a logarithmic signature is a uniform cover.

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

$$y = q_1 \cdot q_2 \dots q_{s-1} \cdot q_s \tag{2.2}$$

for $q_i \in A_i$.

Of course, for general covers, the factorization in (2.2) is not unique, and the problem of finding a factorization for a given $y \in \mathcal{G}$ is in general intractable.

Let $\alpha = [A_1, \dots, A_s]$ be a cover for $\mathcal{G}$ with $r_i = |A_i|$. Then the A_i are called the *blocks* of α and the vector $(r_1, \dots, r_s)$ of block lengths r_i the *type* of α. We define the *length* of α to be the integer $\ell = \sum_{i=1}^{s} r_i$. A uniform cover $\alpha = [A_1, \dots, A_s]$ of type $(r, r, \dots, r)$ is called an $[s, r]$-*mesh*. We say that α is *nontrivial* if $s \geq 2$ and $r_i \geq 2$ for $1 \leq i \leq s$; otherwise α is said to be *trivial*. We denote by $\mathcal{C}(\mathcal{G})$ and $\Lambda(\mathcal{G})$ the respective collections of *covers* and *logarithmic signatures* of group $\mathcal{G}$.

Let $\Gamma = \{(\mathcal{G}_\ell, \alpha_\ell)\}_{\ell \in \mathbb{N}}$ be a family of pairs indexed by the security parameter ℓ, where the $\mathcal{G}_\ell$ are groups in a common representation, and where α_ℓ is a specific cover for $\mathcal{G}_\ell$ of length polynomial in ℓ. We say that Γ is *tame* if there exists a probabilistic polynomial time algorithm $\mathcal{A}$ such that for each $g \in \mathcal{G}_\ell$, $\mathcal{A}$ accepts (α_ℓ, g) as input and outputs a factorization $\phi(g)$ of g with respect to α_ℓ (as in (2.2)) with overwhelming probability of success. We say that Γ is *wild* if for any probabilistic polynomial time algorithm $\mathcal{A}$, the probability that $\mathcal{A}$ succeeds in factorizing a random element g of $\mathcal{G}$ is negligible.

For finite groups, there are instances $\{(\mathcal{G}_\ell, \alpha_\ell)\}_\ell$ where the factorization in (2.2) is believed to be hard. For example, let q be a prime power for which the discrete logarithm problem in the multiplicative group of the finite field $\mathbb{F}_q$ is believed to be hard. Suppose that $2^{\ell-1} \leq q - 1 < 2^\ell$, and let $\mathcal{G}_\ell$ be the multiplicative group $\mathbb{F}_q^*$ just mentioned. Let f be a generator of $\mathcal{G}_\ell$. If $\alpha_\ell = [A_1, A_2, \dots, A_\ell]$, where $A_i = [1, f^{2^{i-1}}]$, then α_ℓ is a cover of $\mathcal{G}_\ell$, and factorization with respect to α_ℓ amounts to solving the discrete logarithm problem (DLP) in $\mathcal{G}_\ell$.

Suppose that $\alpha = [A_1, A_2, \dots, A_s]$ is a cover of a group $\mathcal{G}$. Let $g_0, g_1, \dots, g_s \in \mathcal{G}$ and consider $\beta = [B_1, B_2, \dots, B_s]$ with $B_i = g_{i-1}^{-1} A_i g_i$. We say that β is a *two-sided transform* of α by $g_0, g_1, \dots, g_s$; in the special case where $g_0 = 1$ and $g_s = 1$, β is called *a sandwich* of α. Notice that β is a cover for $\mathcal{G}$.

Let $\alpha = [A_1, A_2, \dots, A_s]$ be a cover of type $(r_1, r_2, \dots, r_s)$ for $\mathcal{G}$ with $A_i = [a_{i,1}, a_{i,2}, \dots, a_{i,r_i}]$, and let $m = \prod_{i=1}^{s} r_i$. Let $m_1 = 1$ and $m_i = \prod_{j=1}^{i-1} r_j$ for $i = 2, \dots, s$. Let τ denote the canonical bijection from $Z_{r_1} \oplus \mathbb{Z}_{r_2} \oplus \dots \oplus \mathbb{Z}_{r_s}$ on $\mathbb{Z}_m$, i.e.,

$$\tau : \mathbb{Z}_{r_1} \oplus \mathbb{Z}_{r_2} \oplus \dots \oplus \mathbb{Z}_{r_s} \to \mathbb{Z}_m,$$

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

Using τ, we now define the surjective mapping $\breve{\alpha}$ induced by α:

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

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

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

Conversely, given a cover α and an element $y \in \mathcal{G}$, to determine any element $x \in \breve{\alpha}^{-1}(y)$ it is necessary to obtain any one of the possible factorizations of type (2.2) for y and determine indices $j_1, j_2, \ldots, j_s$ such that $y = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$. This is possible if and only if α is tame. Once a vector $(j_1, j_2, \ldots, j_s)$ has been determined, $\breve{\alpha}^{-1}(y) = \tau(j_1, j_2, \ldots, j_s)$ can be computed efficiently.

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

2.1. *An Example*

We present a small example involving two logarithmic signatures α and β for the alternating group $\mathcal{A}_5$. The types of α and β are $(5, 2, 6)$ and $(3, 4, 5)$, respectively, and $|\mathcal{A}_5| = 5 \cdot 2 \cdot 6 = 3 \cdot 4 \cdot 5 = 60$. In Fig. 1 the blocks of α and β are listed vertically. To compute τ^{-1} and τ efficiently, we attach canonical logarithmic signatures τ_α and τ_β of the additive group $\mathbb{Z}_{60}$ to the left of α and to the right of β. The respective types of τ_α and τ_β are $(5, 2, 6)$ and $(3, 4, 5)$, just as for α and β.

We now illustrate how $\breve{\alpha} : \mathbb{Z}_{60} \to \mathcal{A}_5$ is computed in practice. Any element $x \in \mathbb{Z}_{60}$ can be written uniquely as the sum of elements of τ_α, using exactly one element from each block. Determining this decomposition of x involves a greedy selection of components, one from each block, sequentially from the bottom block upwards, and essentially determines $\tau^{-1}(x) = (j_1, j_2, j_3)$. If x_i are the elements of $\mathcal{A}_5$ corresponding to the j_i, we compute $\breve{\alpha}(x) = x_1 x_2 x_3$. In particular if $x = 47$, we have: $47 = 40 + 5 + 2$, and the components $j_1 = 2$, $j_2 = 5$, and $j_3 = 40$ point to elements $x_1 = (1\,5\,4\,2\,3)$, $x_2 = (2\,4)(3\,5)$, and $x_3 = (1\,3\,2)$ of $\mathcal{A}_5$. We then compute: $\breve{\alpha}(47) = x_1 x_2 x_3 = (1\,5\,4\,2\,3) \cdot (2\,4)(3\,5) \cdot (1\,3\,2) = (1\,2\,5)$.

If we now factorize $y = \breve{\alpha}(x)$ with respect to the second logarithmic signature β, we obtain $y = y_1 y_2 y_3$. From the elements y_i the corresponding elements of the additive τ_β are obtained, and their sum is formed. In our particular case, $y = (1\,2\,5) = y_1 y_2 y_3 =$

	τ_α	α
	$\mathbb{Z}_{60}$	$\mathcal{A}_5$
	0	(1)(2)(3)(4)(5)
	1	(1 2 5 3 4)
$x_1 \to$	2	(1 5 4 2 3)
	3	(1 3 2 4 5)
	4	(1 4 3 5 2)
	0	(1 2 5 3 4)
$x_2 \to$	5	(2 4)(3 5)
	0	(1 3 5 4 2)
	10	(1 3)(2 4)(5)
	20	(1)(2)(3)(4)(5)
	30	(1 5)(2 3)(4)
$x_3 \to$	40	(1 3 2)(4)(5)
	50	(1 2 3)(4)(5)

$\mathcal{A}_5$

β	τ_β	
$\mathcal{A}_5$	$\mathbb{Z}_{60}$	
(1)(2)(3 4 5)	0	
(1)(2)(3 5 4)	1	$\leftarrow y_1$
(1)(2)(3)(4)(5)	2	
(1)(2 3)(4 5)	0	
(1)(2 5 3)(4)	3	$\leftarrow y_2$
(1)(2 4 3)(5)	6	
(1)(2)(3)(4)(5)	9	
(1 2 4)(3)(5)	0	$\leftarrow y_3$
(1)(2 3 5)(4)	12	
(1 3)(2)(4 5)	24	
(1 5 3 4 2)	36	
(1 4 3 2 5)	48	

Fig. 1. Two logarithmic signatures of $\mathcal{A}_5$.

(3 5 4)·(2 5 3)·(1 2 4), corresponding to the τ_β components 1, 3, 0, respectively. Thus, $\breve{\beta}^{-1}((1\ 2\ 5)) = 1 + 3 + 0 = 4$. We would like to mention that in this example, α and β belong to the class of tame log signatures, in fact β is supertame. Here, we do not explain further how the factorization $y = y_1\, y_2\, y_3$ is obtained efficiently. For further details, see [6].

When the underlying group is chosen appropriately, the bijections $\breve{\alpha}\breve{\beta}^{-1}$ can be used as cryptographic transformations with key (α, β) in symmetric cryptosystem PGM [5,6] or as cryptographic primitives in other systems.

3. Description of a New Public Key Cryptosystem

We presently describe a new cryptosystem, called MST_3. Let $\mathcal{G}$ be a finite non-abelian group with nontrivial center $\mathcal{Z}$ such that $\mathcal{G}$ does not split over $\mathcal{Z}$. Assume further 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 our cryptosystem, is that if $\alpha = [A_1, A_2, \ldots, A_s] := (a_{ij})$ is a random cover for a “large” subset $\mathcal{S}$ of $\mathcal{G}$, then finding a factorization

$$g = a_{1j_1} a_{2j_2} \cdots a_{sj_s}$$

for an arbitrary element $g \in \mathcal{S}$ with respect to α is, in general, an intractable problem.

3.1. *Setup*

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

(1) a tame logarithmic signature $\beta = [B_1, B_2, \ldots, B_s] := (b_{ij})$ of type $(r_1, r_2, \ldots, r_s)$ for $\mathcal{Z}$

(2) a random cover $\alpha = [A_1, A_2, \ldots, A_s] := (a_{ij})$ of the same type as β for a certain subset $\mathcal{J}$ of $\mathcal{G}$ such that $A_1, \ldots, A_s \subseteq \mathcal{G} \setminus \mathcal{Z}$.

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

(3) $\tilde{\alpha} = [\tilde{A}_1, \tilde{A}_2, \ldots, \tilde{A}_s]$, where $\tilde{A}_i = t_{i-1}^{-1}\, A_i\, t_i$ for $i = 1, \ldots, s$

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

Alice publishes her public key $(\alpha = (a_{ij}), \gamma = (h_{ij}))$, keeping $(\beta = (b_{ij}), (t_0, \ldots, t_s))$ as her private key.

3.2. *Encryption*

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

(i) computes $y_1 = \breve{\alpha}(x)$ and $y_2 = \breve{\gamma}(x)$

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

3.3. *Decryption*

Now, Alice knows y_2, figures that

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

and can therefore compute

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

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

3.4. *Remark*

1. Let $\alpha = [A_1, \ldots, A_s]$ be a cover for $\mathcal{J}$ satisfying Setup condition (2) so that

$$\overline{A_1}\cdot\overline{A_2}\cdots\overline{A_s} = \sum_{h\in\mathcal{J}} a_h h,$$

and let $\lambda = \frac{1}{|\mathcal{J}|}\sum_{h\in\mathcal{J}} a_h$. The assumption that Alice is able to construct a cover α of the same type as β implies that $\lambda|\mathcal{J}| \leq |\mathcal{Z}|$.

Note also that for the construction of MST_3, the cryptographic hypothesis that $\breve{\alpha}$ and $\breve{\gamma}$ are one-way functions is still necessary, in general. However, we will show below that the hypothesis for α can be removed if $\lambda_{\min} := \min\{a_h : h \in \mathcal{J}\}$ is sufficiently large.

2. The assumption that $\mathcal{G}$ does not split over $\mathcal{Z}$ implies that there is no subgroup $\mathcal{H} < \mathcal{G}$ with $\mathcal{H} \cap \mathcal{Z} = 1$ such that $\mathcal{G} = \mathcal{Z}\cdot\mathcal{H}$ ($=\mathcal{Z}\times\mathcal{H}$, since $\mathcal{Z}$ is the center of $\mathcal{G}$). Without this assumption the system may be vulnerable to attacks based on permutation group algorithms. In particular, if our group is a direct product $\mathcal{G} = \mathcal{Z}\times\mathcal{H}$ and can be represented as a permutation group of reasonable degree (e.g., ≤ 100000), then using an appropriate strong generating set for $\mathcal{G}$ and Schreier trees, one could extract b_{ij} from h_{ij}. The system will consequently be weakened.

The encryption as described is a deterministic encryption: the same plaintext will give the same ciphertext by each encryption. However, a randomized encryption can be realized as follows:

To encrypt a message $x \in \mathbb{Z}_{|\mathcal{Z}|}$, Bob chooses a random number $R \in \mathbb{Z}_{|\mathcal{Z}|}$, $R \neq 0$, and

(i) computes $y_0 = x + R$, where the computation is carried out in $\mathbb{Z}_{|\mathcal{Z}|}$
(ii) computes $y_1 = \breve{\alpha}(R)$ and $y_2 = \breve{\gamma}(R)$

(iii) sends $y = (y_0, y_1, y_2)$ to Alice.

To decrypt $y = (y_0, y_1, y_2)$, Alice first recovers R from (y_1, y_2) as described above and then obtains $x = y_0 - R$.

4. Realization of MST_3 and Its Security

In this section we propose a class of groups for the generic version of our public-key cryptosystem MST_3. Here, the crucial point is the fact that for arbitrary members $\mathcal{G}$ in this family, we can show the security and strength of the system. To make the analysis below understandable, we include some basic notation and definitions concerning finite p-groups and describe the structure of the Suzuki 2-groups in some details.

4.1. *Suzuki-2 Groups*

To begin with, we recall some basic facts about finite p-groups, where p denotes a prime number. A finite group $\mathcal{G}$ of order a power of p is called a *p-group*, i.e., $|\mathcal{G}| = p^n$ for a certain positive integer n. The least common multiple of the orders of the elements of $\mathcal{G}$ is called the *exponent* of $\mathcal{G}$. An abelian (commutative) p-group $\mathcal{G}$ of exponent p is said to be *elementary abelian*. The set $\mathbb{Z}(\mathcal{G}) = \{z \in \mathcal{G} : zg = gz\ \forall g \in \mathcal{G}\}$ is called the *center* of $\mathcal{G}$. It is well known that $\mathbb{Z}(\mathcal{G})$ is a normal subgroup of order at least p for any p-group $\mathcal{G}$. The subgroup $\mathcal{G}'$ generated by all the elements of the form $x^{-1}y^{-1}xy$ with $x, y \in \mathcal{G}$ is called the *commutator subgroup* of $\mathcal{G}$. The so-called *Frattini* subgroup of $\mathcal{G}$, denoted by $\Phi(\mathcal{G})$, is by definition the intersection of all the maximal subgroups of $\mathcal{G}$. If $\mathcal{G}$ is a p-group, then the factor group $\mathcal{G}/\Phi(\mathcal{G})$ is elementary abelian. In particular, if $\mathcal{G}$ is a 2-group, then $\Phi(\mathcal{G}) = \langle g^2 \mid g \in \mathcal{G}\rangle$. Finally, an element of order 2 in a group is called an *involution*.

Formally, a *Suzuki 2-group* is defined as a nonabelian 2-group with more than one involution having a cyclic group of automorphisms which permutes its involutions transitively. This class of 2-groups was studied and characterized by G. Higman [2]. In particular, in any Suzuki 2-group $\mathcal{G}$ we have $\mathbb{Z}(\mathcal{G}) = \Phi(\mathcal{G}) = \mathcal{G}' = \Omega_1(\mathcal{G})$, where $\Omega_1(\mathcal{G}) = \langle g \in \mathcal{G} \mid g^2 = 1\rangle$ and $|\mathbb{Z}(\mathcal{G})| = q = 2^m, m > 1$. It is shown in [2] that the order of $\mathcal{G}$ is either q^2 or q^3. Thus all the involutions of $\mathcal{G}$ are in the center of $\mathcal{G}$, therefore $\mathbb{Z}(\mathcal{G})$ and the factor group $\mathcal{G}/\Phi(\mathcal{G})$ are elementary abelian. Consequently, all elements not in $\mathbb{Z}(\mathcal{G})$ have order 4, i.e., $\mathcal{G}$ is of exponent 4. It is known that $\mathcal{G}$ has an automorphism ξ of order $q-1$ cyclically permuting the involutions of $\mathcal{G}$ [2] (see also [4]).

In our realization of MST_3 we only consider the class of Suzuki 2-groups having order q^2. Using Higman's notation, a Suzuki 2-group of order q^2 will be denoted by $A(m,\theta)$. Let $q = 2^m$ with $3 \le m \in \mathbb{N}$ such that the field $\mathbb{F}_q$ has a nontrivial automorphism θ of odd order. This implies that m is not a power of 2. Then the groups $A(m,\theta)$ do exist.

In fact, if we define

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

where

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

is a 3 × 3-matrix over $\mathbb{F}_q$, then it is shown that the group $\mathcal{G}$ is isomorphic to $A(m,\theta)$. Thus $\mathcal{G}$ has order q^2, and we have

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

Since the center $\mathbb{Z}(\mathcal{G})$ is elementary abelian of order q, it can be identified with the additive group of the field $\mathbb{F}_q$. Also the factor group $\mathcal{G}/\Phi(\mathcal{G})$ is an elementary abelian group of order q. It is then easily verified that the multiplication of two elements in $\mathcal{G}$ is given by the rule

$$S(a_1,b_1)S(a_2,b_2) = S\big(a_1+a_2, b_1+b_2+a_1^{\theta}a_2\big). \tag{4.1}$$

In this matrix-form representation, the Suzuki 2-groups $A(m,\theta)$ can be considered as subgroups of the *general linear* group $GL(3,q)$ over $\mathbb{F}_q$.

Remark 4.1. It has been shown in [2] that the groups $A(m,\theta)$ and $A(m,\phi)$ are isomorphic if and only if $\phi = \theta^{\pm 1}$.

The security analysis of the realization of MST_3 with Suzuki 2-groups $\mathcal{G} = A(m,\theta)$, as carried out below, does not require the explicit representation of $\mathcal{G}$ in the matrix form above. In fact we can view G just as a nonabelian 2-group of order q^2, $q = 2^m$, $m > 1$, having exponent 4 such that $\mathcal{Z} := \mathbb{Z}(\mathcal{G}) = \Phi(\mathcal{G}) = \mathcal{G}'$ with $\mathbb{Z}(\mathcal{G})$ elementary abelian of order q. The arguments strongly exploit the structure of $\mathcal{G}$. For instance, any two elements x, $y \in \mathcal{G}$ of order 4 belonging to distinct cosets of the center $\mathbb{Z}(\mathcal{G})$ do not commute, i.e., $xy \neq yx$.

In this realization we choose the elements for the cover α according to the following:

Property DC. *For every A_i, $i = 1, \ldots, s$, elements of A_i are selected so that 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 $\mathcal{Z}$.

4.2. *Security of the Given Realization of MST_3*

We can envisage the following types of attacks against MST_3.

4.2.1. *Attack 1*

The first attack attempts to extract information about $(t_0, \ldots, t_s)$ and $\beta = (b_{ij})$ from the public knowledge of $\alpha = (a_{ij})$ and $\gamma = (h_{ij})$. However, it is sufficient for the attacker to obtain a logarithmic signature β' *equivalent* to β, i.e., any convenient β' which is a *sandwich* transform of β. Thus, without loss of generality, by applying a sandwich transformation, we can assume that the first element of each block, except for the last block of β, is the identity $1 \in \mathcal{G}$. The attacker considers the general equations

$$h_{i,j} = b_{i,j} t_{i-1}^{-1} a_{i,j} t_i, \quad i = 1, \dots, s, \ 1 \le j \le r_i, \tag{4.2}$$

where the $h_{i,j}$ and $a_{i,j}$ are public.

Since $b_{1,1} = 1$, (4.2) yields

$$h_{1,1} = t_0^{-1} a_{1,1} t_1. \tag{4.3}$$

Since $t_0 \in \mathcal{G} \setminus \mathcal{Z}$, the attacker has $q^2 - q$ choices for t_0, and for each such choice, t_1 is completely determined from (4.3). Further, having selected a t_0, since a_{1j} and h_{1j} are known, the attacker can compute b_{1j} from $h_{1j} = b_{1j} t_0^{-1} a_{1j} t_1$ for each $j \in \{2, \dots, r_1\}$. Thus, the choice of t_0 determines uniquely all further elements of block B_1.

By analogy, knowledge of t_1 and the fact that $b_{2,1} = 1$ determine t_2 and all elements $b_{2,j}$ for $j \in \{2, \dots, r_2\}$. Iteratively, having chosen t_0, the attacker can compute $t_1, \dots, t_{s-1}$, all possible $b_{i,j}$ for $i \in \{1, \dots, s-1\}$, and corresponding $j \in \{1, \dots, r_i\}$.

Now, the first element $b_{s,1}$ of the last block B_s is in $\mathcal{Z}$ but otherwise indeterminate. There are q choices for $b_{s,1}$, and for each such choice, t_s and all elements of the last block are completely determined. Thus, there are $q^2 - q$ choices for t_0 and q choices for $b_{s,1}$, i.e., $(q-1)q^2$ choices for $(t_0, b_{s,1})$, each of which completely determines $(t_0, \dots, t_s; \beta)$.

If t_0 is replaced by $t_0 z$, where $z \in \mathcal{Z}$, while keeping the public keys α and γ, as well as the private β invariant, it is easy to verify from (4.2) that $(t_0, t_1, \dots, t_s)$ is replaced by $(t_0 z, t_1 z, \dots, t_s z)$. Thus, from the point of view of the attacker, the choices for $(t_0, \dots, t_s)$ fall into equivalence classes, each of size $|\mathcal{Z}| = q$. More precisely, it suffices to choose one t_0 from each distinct coset of $\mathcal{G}$ modulo $\mathcal{Z}$. It follows that an attacker actually has

$$\frac{(q-1)q^2}{q} = q(q-1)$$

possible choices for the controlling pair $(t_0, b_{s,1})$. Since q is assumed to be very large, this type of attack is not feasible.

4.2.2. *Attack 2*

The goal of the following *chosen plaintext attack* is to determine β and (t_0, t_s) from the equations

$$y_2 = \breve{\beta}(x) t_0^{-1} y_1 t_s, \quad x \in \mathbb{Z}_{|\mathcal{Z}|}, \tag{4.4}$$

or equivalently,

$$\breve{\beta}(x) = y_2 t_s^{-1} y_1^{-1} t_0, \tag{4.5}$$

where $y_1 = \breve{\alpha}(x)$ and $y_2 = \breve{\gamma}(x)$.

The attacker attempts to compute enough values $\breve{\beta}(x_i)$ in order to reconstruct β using Proposition 4.1 in [7]: The proposition states that if $\mathcal{G}$ is a permutation group of degree N and if β is of known type $(r_1, \dots, r_s)$, then one can reconstruct a logarithmic signature equivalent to β by using certain $1 - s + \sum_{i=1}^{s} r_i$ properly selected values $\breve{\beta}(x_i)$.

We note incidentally that the conclusion of Proposition 4.1 remains valid for abstract groups, i.e., the condition that $\mathcal{G}$ be a permutation group is not used or needed in the proof of the proposition.

Let $\{x_1, \dots, x_n\}$ be a collection of plaintexts, chosen by the attacker, from which information about β is to be derived. We have

$$\breve{\beta}(x_i) = y_{i,2} t_s^{-1} y_{i,1}^{-1} t_0, \quad i = 1, \dots, n, \tag{4.6}$$

where $y_{i,1} := \breve{\alpha}(x_i)$ and $y_{i,2} := \breve{\gamma}(x_i)$.

The attacker tries to compute or guess the n distinct values $\breve{\beta}(x_i)$ in order to reconstruct β. Note that in each of (4.6) only $y_{i,1}$ and $y_{i,2}$ are known. First of all we have

$$y_{i,2}\left(y_{i,1}^{-1}\right)^{t_s} t_s^{-1} t_0 = y_{i,2} y_{i,1}^{-1} y_{i,1} \left(y_{i,1}^{-1}\right)^{t_s} t_s^{-1} t_0 \in \mathcal{Z}.$$

Since $y_{i,1}(y_{i,1}^{-1})^{t_s} \in \mathcal{G}' = \mathcal{Z}$, it follows that

$$t_0^{-1} t_s \in y_{i,2}\, y_{i,1}^{-1} \mathcal{Z}$$

or, equivalently,

$$t_s \in t_0 y_{i,2} y_{i,1}^{-1} \mathcal{Z}, \quad \text{for } i = 1, \dots, n. \tag{4.7}$$

Suppose that

$$y_{i,2} y_{i,1}^{-1} \mathcal{Z} \neq y_{j,2} y_{j,1}^{-1} \mathcal{Z} \quad \text{for a pair } i \neq j.$$

Then,

$$t_s \in t_0 y_{i,2} y_{i,1}^{-1} \mathcal{Z} \cap t_0 y_{j,2} y_{j,1}^{-1} \mathcal{Z} = \emptyset,$$

which is a contradiction to the fact that there is at least one pair (t_0, t_s) satisfying (4.6). Hence, we have

$$y_{i,2} y_{i,1}^{-1} \in y_{1,2} y_{1,1}^{-1} \mathcal{Z}, \quad \text{for } i = 1, \dots, n.$$

Set $w := y_{1,2} y_{1,1}^{-1}$.

Since $t_0 \in \mathcal{G} \setminus \mathcal{Z}$, there are $q^2 - q$ possibilities for t_0. If t_0 is chosen, then $t_s \in t_0 w \mathcal{Z}$, i.e., there are q possibilities for t_s. Thus, we have $q(q-1)q$ "admissible" pairs (t_0, t_s).

Further, it is clear that if (t_0, t_s) satisfies (4.7), so does the pair $(t_0 z, t_s z)$ with $z \in \mathcal{Z}$; in other words, for each solution pair (t_0, t_s) of (4.6), one has q associated solutions $(t_0 z, t_s z)$ with $z \in \mathcal{Z}$.

Suppose now that (τ_0, τ_s) and (t_0, t_s) satisfy

$$y_{i,2} t_s^{-1} y_{i,1}^{-1} t_0 = z = \breve{\beta}(x_i) = y_{i,2} \tau_s^{-1} y_{i,1}^{-1} \tau_0.$$

Thus, we have

$$\tau_0^{-1} y_{i,1} \tau_s = t_0^{-1} y_{i,1} t_s \quad \text{for } i = 1, \dots, n.$$

Therefore,

$$\tau_0^{-1} y_{i,1} y_{j,1}^{-1} \tau_0 = t_0^{-1} y_{i,1} y_{j,1}^{-1} t_0, \quad \forall i, j = 1, \dots, n. \tag{4.8}$$

If there are enough pairs (i, j) such that the different elements $y_{i,1}y_{j,1}^{-1}$ generate $\mathcal{G}$ (at least m such elements are needed), then τ_0 and t_0 induce the same inner automorphism of $\mathcal{G}$, i.e.,

$$\tau_0 \equiv t_0 \bmod \mathcal{Z}. \tag{4.9}$$

Hence, $\tau_0 = t_0 z$ and then $\tau_s = t_s z$ for some $z \in \mathcal{Z}$. Thus, the number of admissible pairs (t_0, t_s) yielding distinct $\breve{\beta}(x_i)$ is

$$\frac{q^2(q-1)}{q} = q(q-1).$$

The result of this analysis shows that the attacker has to construct at least $q(q-1)$ solution tuples $(\breve{\beta}(x_1), \ldots, \breve{\beta}(x_n))$. Among these possible solutions, only one is correct. In other words the success probability of the attacker is $\frac{1}{q(q-1)}$. Interestingly the number $q(q-1)$ of solution tuples for $(\breve{\beta}(x_1), \ldots, \breve{\beta}(x_n))$ is exactly the number of non-associated solutions (t_0, t_s) for (4.6).

Remark 4.2.

1. If the attacker does not have enough equations of type (4.8), to conclude (4.9), then there are more possibilities for (t_0, t_s) and therefore more possible solution tuples $(\breve{\beta}(x_1), \ldots, \breve{\beta}(x_n))$. Since only one of those possible solutions is the correct one, the probability of a successful attack is even smaller than $\frac{1}{q(q-1)}$.
2. According to Proposition 4.1 of [7], one needs $1 - s + \sum_{i=1}^{s} r_i$ different values $\breve{\beta}(x)$ to reconstruct a logarithmic signature equivalent to β. Now, β is a logarithmic signature of type $(r_1, \ldots, r_s)$ for $\mathcal{Z}$, and $|\mathcal{Z}| = q = 2^m$. Let $r_i = 2^{e_i}$ for $i = 1, \ldots, s$. Then

$$2^m = 2^{e_1} \cdots 2^{e_s}, \quad \text{and} \quad \sum_{i=1}^{s} e_i = m.$$

Now,

$$\begin{aligned}\sum_{i=1}^{s} r_i - s + 1 &= \sum_{i=1}^{s} \bigl(2^{e_i} - 1\bigr) + 1\\ &> \sum_{i=1}^{s} e_i\\ &= m.\end{aligned}$$

This inequality validates a statement mentioned in the analysis of Attack 2.

4.3. *Space and Time Complexity for Computing with $\mathcal{G}$*

In this section we discuss space and time requirements when computing with $\mathcal{G} = A(m, \theta)$ in matrix-form representation. As before, let $q = 2^m$, where $m \geq 3$ is not a power of 2, and let θ be a nontrivial odd-order automorphism of the field $\mathbb{F}_q$. Recall that $\mathcal{G}$ consists of all 3×3 matrices of the form

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

with $a, b \in \mathbb{F}_q$. The center $\mathcal{Z} := \mathbb{Z}(\mathcal{G}) = \{S(0,b) | b \in \mathbb{F}_q\}$ of $\mathcal{G}$ is an elementary abelian group of order q. Hence $\mathcal{Z}$ may be viewed a vector space of dimension m over $\mathbb{F}_2$.

As mentioned in Sect 4.1 above, the multiplication of two elements in $\mathcal{G}$ is given by the rule

$$S(a_1,b_1)S(a_2,b_2) = S\big(a_1 + a_2, b_1 + b_2 + a_1^{\theta} a_2\big). \tag{4.10}$$

We could store the group elements $S(a,b)$ as pairs (a,b), but this would require that we compute some a^{θ} each time we compute a product of group elements. In turn, each computation a^{θ} requires $O(m)$ multiplications in $\mathbb{F}_q$. It is therefore more time efficient to store the group elements as triples (a, b, a^{θ}). Thus, the product $S(a_1,b_1) \cdot S(a_2,b_2)$ is identified with the triple

$$\big(a_1 + a_2, b_1 + b_2 + a_1^{\theta} a_2, a_1^{\theta} + a_2^{\theta}\big),$$

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

The reduced storage requirement for group elements and the highly efficient operation in the 2-group $\mathcal{G}$ are significant positive factors for the realization of the cryptosystem with underlying group $\mathcal{G} = A(m,\theta)$.

4.4. *MST_3 without the Cryptographic Hypothesis for α*

One striking fact emerges when comparing MST_3 with MST_2. This fact lies in our cryptographic hypothesis that "*randomly generated covers for large finite groups induce one-way functions*."

For MST_2, the cryptographic hypothesis is fundamental. However, for MST_3, the cryptographic hypothesis for random cover α may be dropped without impairing the security of the system if α is constructed appropriately.

The value $|\mathcal{Z}|/|\mathcal{J}|$ can be viewed as the average number of representations for each element of $\mathcal{J}$ with respect to cover α. This implies that any $y \in \mathcal{J}$ will have, on average, $|\mathcal{Z}|/|\mathcal{J}|$ preimages in $\mathbb{Z}_{|\mathcal{Z}|}$ with respect to $\breve{\alpha} : \mathbb{Z}_{|\mathcal{Z}|} \to \mathcal{J}$. When the cryptographic hypothesis for α is removed, MST_3 remains secure if $|\mathcal{Z}|/|\mathcal{J}|$ is large. For, if $\breve{\alpha}$ is not a one-way function, i.e., for any given $y \in \mathcal{J}$, finding $z \in \mathbb{Z}_{|\mathcal{Z}|}$ such that $\breve{\alpha}(z) = y$ is computationally feasible, then using an oracle $\varOmega$ that outputs $z \in \mathbb{Z}_{|\mathcal{Z}|}$ for a given input $y \in \mathcal{J}$ such that $\breve{\alpha}(z) = y$ will break MST_3 after $|\mathcal{Z}|/2|\mathcal{J}|$ queries on average.

Assume that $x \in \mathbb{Z}_{|\mathcal{Z}|}$ is a cleartext and $y_1 := \breve{\alpha}(x)$. Now, if $|\mathcal{Z}| \geq 2|\mathcal{J}|^2$, then the oracle $\varOmega$ needs at least $|\mathcal{J}|$ queries for input y_1 in order to find x with probability $\geq 1/2$. As $\mathcal{J}$ is large, any computation with time complexity $O(|\mathcal{J}|)$ is intractable, and the condition $|\mathcal{Z}| \geq 2|\mathcal{J}|^2$ simply means that the cryptographic hypothesis for α need not be made.

5. Conclusions

We have presented a new approach to designing a public-key cryptosystem based on covers and logarithmic signatures of nonabelian finite groups in a particular class. As a realization of the generic version of the system, a class of special 2-groups is proposed, which allows us to carry out a detailed analysis showing the strength of the system. We obtain lower bounds on the work effort for two types of attacks against the system. The results show, as desired, that the cryptosystem is secure against these attacks if the order of the chosen 2-group is sufficiently large. Further, when the underlying 2-group is presented as a matrix group, it has an efficient representation permitting a minimal storage space for its elements and, even more significantly, a shortest possible time for group element multiplications.

Acknowledgements

The third author wishes to express his thanks to the Department of Mathematical Sciences and to the Center for Cryptology and Information Security, Florida Atlantic University, USA, for their hospitality he enjoyed while carrying out parts of this research.

References

[1] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **31**, 469–472 (1985)

[2] G. Higman, Suzuki 2-groups. *Ill. J. Math.* **7**, 79–96 (1963)

[3] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967)

[4] B. Huppert, N. Blackburn, *Finite Groups II* (Springer, Berlin, 1982)

[5] S.S. Magliveras, A cryptosystem from logarithmic signatures of finite groups. In *Proceedings of the 29th Midwest Symposium on Circuits and Systems* (Elsevier, Amsterdam, 1986), pp. 972–975

[6] S.S. Magliveras, N.D. Memon, The algebraic properties of cryptosystem PGM. *J. Cryptol.* **5**, 167–183 (1992)

[7] S.S. Magliveras, D.R. Stinson, T. van Trung, New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. *J. Cryptol.* **15**, 285–297 (2002)

[8] P. Nguyen, Editor, *New Trends in Cryptology*, European project "STORK—Strategic Roadmap for Crypto"—IST-2002-38273. http://www.di.ens.fr/~pnguyen/pub.html#Ng03

[9] P. Shor, Polynomial time algorithms for prime factorization and discrete logarithms on quantum computers. *SIAM J. Comput.* **26**(5), 1484–1509 (1997)