

Aperiodic logarithmic signatures

Barbara Baumeister and Jan-Hendrik de Wiljes

Abstract

In this paper we propose a method to construct logarithmic signatures which are not amalgamated transversal and further do not even have a periodic block. The latter property was crucial for the successful attack on the system MST_3 by Blackburn et al. [1]. The idea for our construction is based on the theory in Szabó's book about group factorizations [12].

1 Introduction

In the 80's Magliveras, Stinson and van Trung introduced two public key cryptosystems, MST_1 and MST_2 , based on factorizations, covers and logarithmic signatures, of finite nonabelian groups [9]. Recently, Lempken, Magliveras, van Trung and Wei [6] developed a third cryptosystem, MST_3 .

A main question is how to produce covers and logarithmic signatures for a group. Blackburn et al. [1] suggested a construction of so called amalgamated transversal logarithmic signatures from exact transversal logarithmic signatures (for the definition see Section 4.1). Based on the use of these amalgamated transversal logarithmic signatures they presented a successful attack on the system MST_3 .

In this paper we propose a method to construct logarithmic signatures which are not amalgamated transversal and further do not even have the property of being periodic, which was crucial for breaking the system MST_3 (see cases 2 and 3 in subsection 4.3 in [1]). The idea for this construction is based on the theory in Szabó's book about group factorizations [12].

The paper is organized as follows: In Section 2 covers and logarithmic signatures will be introduced and some basic facts will be presented. We shortly introduce the cryptosystem MST_3 , for further information see also [6] or [1]. Then we introduce the in [6] proposed platform groups, the Suzuki 2-groups. The question of how to construct logarithmic signatures will be the main issue of Section 4. In Section 5 we present the method for the construction of aperiodic logarithmic signatures. We will close with some final thoughts and remarks on further research in Section 6.

2 Covers and logarithmic signatures

The cryptosystem MST_3 is based on the use of covers and logarithmic signatures. We will introduce them in this section and give a short overview of necessary results. Further information can be found in [2], [6], [7], [8] and [9]. Throughout this paper, G denotes a finite group and every set is assumed to be finite.

Let $K \subseteq G$ and $\alpha = [A_1, \dots, A_s]$ be a sequence of sequences $A_i = [a_{i,1}, \dots, a_{i,r_i}]$ with $a_{i,j} \in G$, such that $\sum_{i=1}^s |A_i|$ is bounded by a polynomial in $\lceil \log |K| \rceil$. Then α is a *cover* for $K \subseteq G$, if every product $a_{1,j_1} \cdots a_{s,j_s}$ lies in K and if every $g \in K$ can be written as

$$g = a_{1,j_1} \cdots a_{s,j_s} \quad (1)$$

with $j_i \in \{1, \dots, |A_i|\}$. We denote the set of all covers for $K \subseteq G$ by $\mathcal{C}(K|G)$. If, moreover, the tuple (j_1, \dots, j_s) is unique for every $k \in K$ then α is called a *logarithmic signature* for K . The set of all logarithmic signatures for K is denoted by $\Lambda(K|G)$.

We call the product $a_{1,j_1} \cdots a_{s,j_s}$ in (1) a *factorization* of g w.r.t. α . Two factorizations $a_{1,j_1} \cdots a_{s,j_s}$ and $a_{1,h_1} \cdots a_{s,h_s}$ of g are *different* if $(j_1, \dots, j_s) \neq (h_1, \dots, h_s)$. (Note that for $\alpha = [[a, a], [b, b]]$ the element ab has four different factorizations $a \cdot b$.)

If $\alpha = [A_1, \dots, A_s] \in \mathcal{C}(K|G)$ with $r_i := |A_i|$ for all $i \in \{1, \dots, s\}$, then the sequence A_i is called a *block* of α and the sequence (r_1, \dots, r_s) the *type* of α . The *length* of α is

$$l(\alpha) := \sum_{i=1}^s r_i.$$

Covers of minimal length are noteworthy due to the fact that less memory capacity has to be used. The interested reader is referred to [7] for information on this issue.

For the application in cryptography the following distinction is made. A logarithmic signature $\beta \in \Lambda(K|G)$ is *tame* if every $g \in K$ can be factorized polynomial in $\lceil \log |K| \rceil$ w.r.t. to β , otherwise β is called *wild*.

The following map $\check{\alpha}$ is used during the encryption and decryption procedure of the cryptosystem MST_3 . Later on we will identify factorizing w.r.t. a cover α with inverting $\check{\alpha}$.

Let $\alpha = [A_1, \dots, A_s] \in \mathcal{C}(K|G)$ be a cover for $K \subseteq G$ of type (r_1, \dots, r_s) with $A_i = [a_{i,1}, \dots, a_{i,r_i}]$ and let

$$m := \prod_{i=1}^s r_i, \quad m_1 := 1 \text{ and } m_i := \prod_{l=1}^{i-1} r_l \text{ for all } i \in \{2, \dots, s\}.$$

Let τ_α be the canonic bijection from $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$ to \mathbb{Z}_m , i. e.

$$\tau_\alpha : \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} \rightarrow \mathbb{Z}_m, \tau_\alpha(j_1, \dots, j_s) := \sum_{i=1}^s j_i m_i.$$

That is a generalization of n -ary representations. Let $\check{\alpha} : \mathbb{Z}_m \rightarrow K$ be the surjection:

$$\check{\alpha}(x) := a_{1,j_1+1} \cdots a_{s,j_s+1}, \text{ where } (j_1, \dots, j_s) = \tau_\alpha^{-1}(x).$$

Note that τ_α^{-1} can be computed efficiently (using Euclid's algorithm) and therefore the same is true for $\check{\alpha}$. Moreover, the map τ_α does only depend on the type of α , i. e. for $\alpha, \beta \in \mathcal{C}(K|G)$ we have

$$\tau_\alpha = \tau_\beta \Leftrightarrow \alpha \text{ and } \beta \text{ are of the same type.}$$

Let $g \in G$ and let α_g be the number of pairwise different factorizations $a_{1,j_1} \cdots a_{s,j_s}$ of g w.r.t. α . Then g has exactly α_g different preimages w.r.t. $\check{\alpha} \circ \tau_\alpha$, namely the tuples (j_1, \dots, j_s) with $g = a_{1,j_1} \cdots a_{s,j_s}$. That is the connection to equation (1). Therefore, a logarithmic signature $\beta \in \Lambda(K|G)$ is tame if we can compute $\check{\beta}^{-1}$ polynomial in $\lceil \log |K| \rceil$.

For $\mathcal{F} \in \{\mathcal{C}, \Lambda, \dots\}$ we use the notation

$$\mathcal{F}(G) := \mathcal{F}(G|G).$$

3 The cryptosystem MST₃

Alice chooses a public non-abelian group G with large center Z and generates

- a tame logarithmic signature $\beta = [B_1, \dots, B_s] \in \Lambda(Z)$ of type (r_1, \dots, r_s)
- and a random cover $\alpha = [A_1, \dots, A_s] \in \mathcal{C}(K|G)$ for a subset K of G with $a_{i,j_i} \in G \setminus Z$ for all $i \in \{1, \dots, s\}$ and $j_i \in \{1, \dots, r_i\}$, which is of the same type as β .

Then she chooses random elements $t_0, \dots, t_s \in G \setminus Z$ and computes the following covers:

- $\tilde{\alpha} = [\tilde{A}_1, \dots, \tilde{A}_s]$, whereat $\tilde{A}_i = t_{i-1}^{-1} A_i t_i$ for all $i \in \{1, \dots, s\}$,
- $\gamma := [H_1, \dots, H_s]$ with $H_i := [b_{i,1} \tilde{a}_{i,1}, \dots, b_{i,r_i} \tilde{a}_{i,r_i}]$ for all $i \in \{1, \dots, s\}$.

The public key is (α, γ) and the private key is (β, t_0, \dots, t_s) .

To encrypt an element $x \in \mathbb{Z}_{|Z|}$, Bob computes $y_1 = \check{\alpha}(x)$ and $y_2 = \check{\gamma}(x)$ and sends $y = (y_1, y_2)$ to Alice.

Alice decrypts y by calculating $\check{\beta}^{-1}(y_2 t_s^{-1} y_1^{-1} t_0)$ which equals x . As β is tame, the decryption-algorithm is efficient.

The cryptographic hypothesis is the problem of factorizing w.r.t. the random cover α . Furthermore it has to be hard for the attacker to reconstruct the private key by using the public key. For information on these two issues we refer the reader to [1], [3] and [10].

Remark 3.1 Lempken, Magliveras, van Trung and Wei [6] demand two additional properties.

Firstly the group G should not be a direct product of Z and a subgroup $U \leq G$, otherwise the system could be weakened using Schreier-trees [6].

The second assumption is $a_{i,j} a_{i,l}^{-1} \notin Z$ for all $i \in \{1, \dots, s\}$ and $j \neq l$. However, Blackburn et al. [1] didn't use that property for their attacks, because it holds for a large number of public keys and it is not required during the encryption and decryption process.

Lempken et al. [6] suggested the use of Suzuki 2-groups (see also [4] and [5]) as platform-groups for the system:

Let $\theta \neq id$ be an odd order field automorphism of \mathbb{F}_q ($q = 2^n$). We then define the Suzuki 2-group as

$$G := \{S(c, d) : c, d \in \mathbb{F}_q\},$$

where

$$S(c, d) := \begin{pmatrix} 1 & 0 & 0 \\ c & 1 & 0 \\ d & c^\theta & 1 \end{pmatrix}.$$

Lemma 3.2 *The center $Z(G) = \{S(0, d) : d \in \mathbb{F}_q\}$ is an elementary abelian 2-group.*

We will now concentrate on the construction of β and we will restrict us, motivated by the Lemma 3.2, to elementary abelian 2-groups, although all results in Section 5 hold for every abelian group.

4 Classes of logarithmic signatures

4.1 Exact transversal logarithmic signatures

A logarithmic signature $\beta = [B_1, \dots, B_s]$ for a group G is called *l-exact transversal* (*r-exact transversal*) if there is a subgroup chain

$$G = G_0 > G_1 > \dots > G_s = \{1\},$$

such that B_i is a left (right) transversal of G_i in G_{i-1} for all $i \in \{1, \dots, s\}$. A logarithmic signature is said to be *exact transversal* if it is l-exact transversal or r-exact transversal. We denote the set of all exact transversal logarithmic signatures for a group G by $\mathcal{ET}(G)$.

Remark 4.1 The block B_s of an exact transversal logarithmic signature β is a subgroup of G , more precisely $B_s = G_{s-1}$. Moreover, $[B_i, \dots, B_s]$ is an exact transversal logarithmic signature for G_{i-1} .

4.2 Amalgamated transversal logarithmic signatures

Let $\beta = [B_1, \dots, B_s]$ be an exact transversal logarithmic signature of type (r_1, \dots, r_s) for an abelian group G . Blackburn et al. [1] define the following operations on β :

- permute elements within each B_i ,
- permute the B_i ,
- replace B_i by a translate $B_i g$ for some $g \in G$,
- amalgamate two sets B_i and B_j by the single set $B_i \cdot B_j := \{gh \mid g \in B_i, h \in B_j\}$.

The logarithmic signatures that are constructed from an exact transversal logarithmic signature by applying a finite number of the four previous maps are called *amalgamated transversal* logarithmic signatures, see [1]. We will denote the set of amalgamated transversal logarithmic signatures for a group G by $\mathcal{AT}(G)$.

The amalgamated transversal logarithmic signatures have the special property of being periodic, which Blackburn et al. [1] used to break MST_3 under the assumption that the platform-group G is a Suzuki-2-group. A subset B of an abelian group G is called *periodic* if there exists a $g \in G \setminus \{1\}$ (the *period*) with $gB = B$. Let $P(B) := \{g \in G \setminus \{1\} : gB = B\}$ be the *set of periods* of B .

Proposition 4.2 (Blackburn et al. [1], Lemma 2.1) *Let G be an abelian group and $\beta \in \mathcal{AT}(G)$. Then at least one of the blocks B_i of β is periodic.*

Blackburn et al showed that every amalgamated transversal logarithmic signature can be used in MST_3 . Their proof is based on Proposition 4.2, see [1].

Theorem 4.3 (Blackburn et al. [1], Lemma 2.2) *Let G be an elementary abelian 2-group. Every logarithmic signature $\beta \in \mathcal{AT}(G)$ is tame.*

5 Constructing aperiodic tame logarithmic signatures

Since the usage of amalgamated transversal logarithmic signatures leaves the cryptosystem insecure, we are in need to find new ways of constructing tame logarithmic signatures, preferably some without periodic blocks. In this section we introduce an algorithm to construct tame logarithmic signatures without periodic blocks.

As in a logarithmic signature β every group element is at most once in a block and as the position of the element inside a block is irrelevant for the tameness of β , see Theorem 4.4, we will consider sets instead of sequences.

We call a logarithmic signature $\beta \in \Lambda(G)$ *aperiodic* if non of the blocks B_i is periodic. The set of all aperiodic logarithmic signatures for a group G is denoted by $\mathcal{A}(G)$.

Theorem 5.1 (Szabó [12], Theorem 7.3.1) *Let G be an elementary abelian 2-group. There exists an aperiodic logarithmic signature β of type (r_1, \dots, r_s) with $r_1 \geq \dots \geq r_s \geq 2$ if*

- $s = 2$ and $r_2 \geq 8$ or
- $s \geq 3$ and $r_1 \geq 8, r_s \geq 4$ holds.

There does not exist an aperiodic logarithmic signature of type (r_1, \dots, r_s) with $r_1 \geq \dots \geq r_s \geq 2$ if one of the following cases holds:

- $r_s = 2$,
- $s = 1$,
- $s = 2$ and $r_2 \nmid 4$,
- $s \geq 3$ and $r_1 \nmid 4, \dots, r_s \nmid 4$.

We are going to use the idea of the proof of this theorem to construct tame aperiodic logarithmic signatures for elementary abelian 2-groups, for example for the center of a Suzuki 2-Group.

5.1 The algorithm

Now we are presenting the algorithm which constructs a new logarithmic signature out of a subgroup and a left transversal of that subgroup. The realization of some rather vague steps in the algorithm, namely the construction of δ and all $\alpha^{(j_1, \dots, j_s)}$, will be discussed in the last part of the paper.

Algorithm 5.2 We start with an abelian group G , choose a subgroup U of G and a transversal R of U in G . Then we generate

$$\delta = (D_1, \dots, D_s) \in \Lambda(R)$$

with

$$D_i = \{d_{i,1}, \dots, d_{i,r_i}\}$$

of type (r_1, \dots, r_s) and logarithmic signatures

$$\alpha^{(j_1, \dots, j_s)} := (A_1^{(j_1)}, \dots, A_s^{(j_s)}) \in \Lambda(U)$$

for all $(j_1, \dots, j_s) \in \{1, \dots, r_1\} \times \dots \times \{1, \dots, r_s\}$. We get $\beta := (B_1, \dots, B_s)$ by

$$\begin{aligned} B_1 &:= d_{1,1}A_1^{(1)} \cup \dots \cup d_{1,r_1}A_1^{(r_1)}, \dots, \\ B_s &:= d_{s,1}A_s^{(1)} \cup \dots \cup d_{s,r_s}A_s^{(r_s)}. \end{aligned}$$

Notice that we needed all the logarithmic signatures $\alpha^{(j_1, \dots, j_s)}$ to be able to produce an aperiodic logarithmic signature.

Example 5.3 We choose $G = \langle u, v, w, x, y, z \rangle = 2^6$, $U = \langle u, v, w, x \rangle$, $R = \{1, y, z, yz\}$ and set

$$D_1 := \{1, z\}, D_2 := \{1, y\}.$$

and

$$\begin{aligned} A_1^{(1)} &:= \{1, u, v, uv\}, A_1^{(2)} := \{1, w, x, wx\}, \\ A_2^{(1)} &:= \{1, uw, vx, uvwx\}, A_2^{(2)} := \{1, ux, uvw, vwx\}. \end{aligned}$$

We get

$$B_1 := \{1, u, v, uv, z, wz, xz, wxz\}, B_2 := \{1, uw, vx, uvwx, y, uxy, uvwy, vwx y\}.$$

Neither of these two blocks is periodic. It follows that $\beta \in \mathcal{A}(G)$ of type $(8, 8)$.

Theorem 5.4 The sequence β constructed by the algorithm 5.2 is a logarithmic signature for G of type (l_1, \dots, l_s) , where $l_i = \sum_{j=1}^{r_i} |A_i^{(j)}|$.

We denote a logarithmic signature which can be obtained from U and R by the construction above *decomposed and reunited* out of U and R , shortly *d.r.*, and we denote the set of logarithmic signatures for a group G which are d.r. by $\mathcal{DR}_G(U, R, \mathcal{E}(U|G), \mathcal{F}(R|G))$ where $\mathcal{E}, \mathcal{F} \in \{\Lambda, \mathcal{ET}, \mathcal{AT}, \dots\}$.

Remark 5.5 Every logarithmic signature $\beta = (B_1, \dots, B_s) \in \Lambda(G)$ is d.r. out of $U = G$ and $R = \{1\}$: Set $\delta = (1, \dots, 1)$ and $A_i^{(1)} = B_i$ for all $i = 1, \dots, s$.

An immediate question is how the choice of U and R influences the set $\mathcal{DR}_G(U, R, \mathcal{E}(U|G), \mathcal{F}(R|G))$. Another question is which logarithmic signatures are constructible out of the pair (U, R) when we choose γ and $\alpha^{(j_1, \dots, j_s)}$ to be for example exact transversal only.

It is possible to construct an aperiodic logarithmic signature by using only *total exact transversals*, i.e. exact transversals where every block is a subgroup, see Example 5.3 above.

Proposition 5.6 A logarithmic signature which is d.r. is tame if δ and all $\alpha^{(j_1, \dots, j_s)}$ are tame and if for every $g \in G$ the coset representative in R which lies in the same coset as g can be found efficiently.

5.2 Aperiodicity of β

From now on we assume that $\beta = (B_1, \dots, B_s)$ is constructed by the algorithm 5.2 and we use the notation introduced there. Next we summarize some basic facts. After that we show how to choose the sets $A_i^{(j)}$ to force the non-periodicity of B_i .

Lemma 5.7 *We have $d_{i,j}^{-1}d_{i,k} \notin U$ for all $i = 1, \dots, s$ and $j, k = 1, \dots, r_i$ with $j \neq k$.*

Proof. We assume that there are i and $j \neq k$ with $d_{i,j}^{-1}d_{i,k} \in U$. We consider the two factorizations

$$d_{1,1} \cdots d_{i-1,1} d_{i,j} d_{i+1,1} \cdots d_{s,1} \quad \text{and} \quad d_{1,1} \cdots d_{i-1,1} d_{i,k} d_{i+1,1} \cdots d_{s,1}.$$

These elements of R are in different cosets of U in G . On the other hand we have

$$(d_{1,1} \cdots d_{i-1,1} d_{i,j} d_{i+1,1} \cdots d_{s,1})^{-1} d_{1,1} \cdots d_{i-1,1} d_{i,k} d_{i+1,1} \cdots d_{s,1} = d_{i,j}^{-1} d_{i,k} \in U,$$

which is not possible. \square

Lemma 5.8 *Let $A, B \leq G$. Then $A = B$ if and only if there exists an element $g \in G$ with $gA = B$.*

Lemma 5.9 *If B_i is periodic with period $g \in G$, then for every $d_{i,j}A_i^{(j)}$ there is a $k \in \{1, \dots, r_i\}$, such that*

$$gd_{i,j}A_i^{(j)} = d_{i,k}A_i^{(k)}.$$

If additionally $A_i^{(j)}, A_i^{(k)} \leq G$ holds, then $A_i^{(j)} = A_i^{(k)}$.

Proof. Assume there is no such k . Then we have $a_1, a_2 \in A_i^{(j)}$ with $a_1 \neq a_2$ and $b \in A_i^{(e)}, c \in A_i^{(l)}$ for $e \neq l$, such that $gd_{i,j}a_1 = d_{i,e}b$ and $gd_{i,j}a_2 = d_{i,l}c$. From that it follows $d_{i,l}^{-1}d_{i,e} = ca_2^{-1}a_1b^{-1} \in U$, which is a contradiction to Lemma 5.7. This shows the first statement. The second part follows from Lemma 5.8. \square

To describe the periodic signatures β we introduce for $i \in \{1, \dots, s\}$ the set

$$D_i^{(j)} := \left\{ d_{i,k} : A_i^{(k)} = A_i^{(j)} \right\}$$

of elements $d_{i,k}$ that have the same corresponding subset $A_i^{(k)}$. Then we immediately obtain the following:

Lemma 5.10 *B_i is periodic if one of the following holds:*

$$(i) \quad \bigcap_{j=1}^{r_i} P\left(A_i^{(j)}\right) \neq \emptyset.$$

$$(ii) \quad \bigcap_{j=1}^{r_i} P\left(D_i^{(j)}\right) \neq \emptyset.$$

The special case $r_i = 2$ or 3 and pairwise different subgroups $A_i^{(j)}$ of the following theorem was proven in cooperation with Anja Nuss [11].

Theorem 5.11 *Let $A_i^{(j)} \leq G$ for all $j \in \{1, \dots, r_i\}$. Then B_i is periodic if and only if*

$$\bigcap_{j=1}^{r_i} P\left(X^{(j)}\right) \neq \emptyset$$

holds for at least one r_i -tuple $(X^{(1)}, \dots, X^{(r_i)}) \in \{A_i^{(1)}, D_i^{(1)}\} \times \dots \times \{A_i^{(r_i)}, D_i^{(r_i)}\}$.

Proof. One part of the equivalence follows from Lemmas 5.9 and 5.10.

Now assume that B_i is periodic. Let $g \in G$ be a period of B_i . By Lemma 5.9 we have for every j and $D_i^{(j)} = \{d_{i,j_1}, \dots, d_{i,j_k}\}$ that

$$g\left(d_{i,j_1}A_i^{(j)} \cup \dots \cup d_{i,j_k}A_i^{(j)}\right) = d_{i,j_1}A_i^{(j)} \cup \dots \cup d_{i,j_k}A_i^{(j)}.$$

Moreover, every $d_{i,j_l}A_i^{(j)}$ is mapped to a $d_{i,j_c}A_i^{(j)}$ by multiplication with g . Therefore g must be either an element of $A_i^{(j)}$, i. e. $g \in P\left(A_i^{(j)}\right)$ or g permutes the elements of $D_i^{(j)}$, i. e. $g \in P\left(D_i^{(j)}\right)$. \square

An immediate consequence is the following equivalence.

Corollary 5.12 *Let $A_i^{(j)} \leq G$ for all $j \in \{1, \dots, r_i\}$ and $A_i^{(j)} \neq A_i^{(k)}$ for all $j, k \in \{1, \dots, r_i\}$ with $j \neq k$. Then B_i is periodic if and only if*

$$\bigcap_{j=1}^{r_i} P\left(A_i^{(j)}\right) \neq \emptyset.$$

\square

If at least one $A_i^{(j)}$ is not a subgroup of G , then the statement of Theorem 5.11 does not hold anymore. The following example shows that we can already get a periodic block when $r_i = 2$.

Example 5.13 We choose $G := \langle u, v, w, x, y, z \rangle = 2^6$, $U = \langle u, v, w, x \rangle$ and set

$$A_1^{(1)} := \{1, u, v, uvw\}, A_1^{(2)} := \{u, 1, uv, vw\} = u^{-1}A_1^{(1)}$$

and

$$D_1 := \{1, y\}.$$

Then we get

$$B_1 = d_{1,1}A_1^{(1)} \cup d_{1,2}A_1^{(2)} = \{1, u, v, uvw, uy, y, uvy, vwy\},$$

which has the period uy . But the other conditions of Theorem 5.11 are fulfilled because of

$$P\left(D_1^{(1)}\right) = P\left(D_1^{(2)}\right) = P\left(A_1^{(1)}\right) = P\left(A_1^{(2)}\right) = \emptyset.$$

If we set

$$A_2^{(1)} := A_2^{(2)} := \{1, w, x, wx\} \text{ and } D_2 := \{1, z\},$$

then we get a logarithmic signature for G .

Next we generalize Theorem 5.11. For G a group and $A, B \subseteq G$ we say that A is a *multiple* of B if there is a $g \in G$ with $gA = B$. Notice if B is a subgroup of G and A a multiple of B , then A is a left coset of B in G . We say that a multiple A of B is *proper*, if $A \neq B$.

Lemma 5.14 *If B_i is periodic with period $g \in G$, if $A_i^{(j)}$ is not a proper multiple of $A_i^{(k)}$ and if $gd_{i,j}A_i^{(j)} = d_{i,k}A_i^{(k)}$, then $A_i^{(j)} = A_i^{(k)}$.*

Proof. That follows immediately from the previous definition, because of $d_{i,k}^{-1}gd_{i,j}A_i^{(j)} = A_i^{(k)}$. \square

Theorem 5.15 *Suppose that $A_i^{(j)}$ is not a proper multiple of $A_i^{(k)}$ for all $j, k \in \{1, \dots, r_i\}$. Then B_i is periodic if and only if*

$$\bigcap_{j=1}^{r_i} P(X^{(j)}) \neq \emptyset$$

for at least one r_i -tuple $(X^{(1)}, \dots, X^{(r_i)}) \in \{A_i^{(1)}, D_i^{(1)}\} \times \dots \times \{A_i^{(r_i)}, D_i^{(r_i)}\}$.

Proof. The proof is analog to the one of Theorem 5.11 but we have to use Lemma 5.14 instead of Lemma 5.9. \square

Corollary 5.16 *Suppose that $A_i^{(j)}$ is not a multiple of $A_i^{(k)}$ for all $j, k \in \{1, \dots, r_i\}$. Then B_i is periodic if and only if*

$$\bigcap_{j=1}^{r_i} P(A_i^{(j)}) \neq \emptyset.$$

5.3 Concret construction for G elementary abelian of order 2^n .

We will construct aperiodic logarithmic signatures for elementary abelian 2-groups G . Such a logarithmic signature has already been constructed in Example 5.3 for $G = 2^6$. Now we generate one for $G = 2^7$ and then use these two logarithmic signatures to construct tame aperiodic logarithmic signatures for all groups 2^n with $n \geq 6$.

Example 5.17 (see also Szabó [12], Theorem 7.3.1) We choose $G = \langle t, u, v, w, x, y, z \rangle = 2^7$, $U = \langle u, v, w, x, y, z \rangle$, $R = \{1, t\}$ and set

$$\begin{aligned} A_1^{(1)} &:= \{1, v, wx, vwx\}, & A_1^{(2)} &:= \{1, w, vz, vwz\}, \\ A_2^{(1)} &:= \{1, x, y, xyz\}, \\ A_3^{(1)} &:= \{1, z, u, zuw\}. \end{aligned}$$

and

$$D_1 := \{1, t\}, \quad D_2 := \{1\}, \quad D_3 := \{1\}.$$

The resulting logarithmic signature β is aperiodic of type $(8, 4, 4)$.

General construction. Let $G = 2^n$ be an elementary abelian group of order n and let $\mathcal{B} = \{g_1, \dots, g_n\}$ be a generating set for G . We now decompose G in the following way:

$$G = \underbrace{U_1 \times \dots \times U_s}_{=U} \times \underbrace{D_1 \times \dots \times D_s}_{=R}$$

where $U_1 \times D_1$ is a small group with a known aperiodic logarithmic signature β' (see Examples 5.13 and 5.17) and $2 \leq |D_i| < \prod_{j=1}^{i-1} |U_j|$ for $i \in \{2, \dots, s\}$. Then we choose for every $i \in \{2, \dots, s\}$ a subset $K_i := \{k_i^{(1)}, \dots, k_i^{(r_i)}\} \subseteq (U_1 \times \dots \times U_{i-1})^\#$ of size $r_i := |D_i|$. We construct the logarithmic signature $\beta = [\beta', B_2, \dots, B_s]$ using Algorithm 5.2 by setting

$$\begin{aligned} \delta &:= [D_2, \dots, D_s], \\ A_i^{(j)} &:= \{1\} \cup \{k_i^{(j)} u : u \in U_i^\#\}, \text{ for } i = 2, \dots, s \text{ and } j = 1, \dots, r_i. \end{aligned}$$

Then no $A_i^{(j)}$ is the multiple of an $A_i^{(l)}$ for some $l \neq j$. Therefore, Corollary 5.16 implies that the resulting logarithmic signature β for G is aperiodic.

For security and storage issues it seems to be reasonable to choose small subgroups U_i and D_i . Further, one should apply some of the operations from subsection 4.2 to β to hide the subgroup $U_1 \times D_1$, more precisely, the blocks of the logarithmic signature β' , otherwise an attacker could obtain a periodic (and therefore tame) logarithmic signature for $G/(U_1 \times D_1)$.

If we want to store this logarithmic signature we are only in need to store a minimal generating set $\mathcal{B} = \cup_{l=1}^{2s} \mathcal{B}_l$ of G such that the subsets \mathcal{B}_l generate U_i and D_i , respectively, and the information which elements of \mathcal{B} generate which subgroups U_i and D_i . The latter can be provided for example by a tuple $v \in \mathbb{Z}^{2s}$, and a strict total order on the \mathbb{F}_2 -vector space \mathbb{F}_2^n , e.g. the lexicographical order, because the position of the elements is needed for the factorization.

Factorization. We define $V_i := \sum_{k=1}^i v_k$ and use the following algorithm:

```

Let  $y = \mathcal{K}_{\mathcal{B}}(g)$  be the coordinate vector of  $g$  w.r.t.  $\mathcal{B}$ 
Let  $j \in \mathbb{Z}^{s-1}$  be the tuple consisting only of ones
for  $i = s+1$  to  $2s-1$  do
  for  $l = 1 + V_i$  to  $V_{i+1}$  do
    if  $y_l = 0$  then
       $j_{i-s} = j_{i-s} + 2^{v_i - (l - V_i)}$ 
Let  $h \in \mathbb{Z}^{s-1}$  be the tuple consisting only of ones
for  $i = 1$  to  $s-1$  do
   $h_i = h_i + (j_i - 1)2^{v_{i+1}}$ 
  for  $l = 1 + V_i$  to  $V_{i+1}$  do
    if  $y_l = 0$  then
       $h_i = h_i + 2^{v_i - (l - V_i)}$ 

```

Now we need to factorize the projection y' of y onto $U_1 \times R_1$ which yields $x = \tau_{\beta'}^{-1}(g')$ where $y' = \mathcal{K}_{\mathcal{B}'}(g')$ and $\mathcal{B}' \subseteq \mathcal{B}$ a generating set of $U_1 \times R_1$.

Altogether we get $\tau_\beta^{-1}(g) = (x, h_1, \dots, h_{s-1})$ and from that we receive $\check{\beta}^{-1}(g)$.

Note that we have to treat β' differently, but since $U_1 \times D_1$ is small, we get the requested element in the factorization efficiently (meaning in $O(\log_2|G|)$) by an exhaustive search.

Complexity. Under the assumption, that comparison and arithmetic in \mathbb{Z} can be done in $O(1)$, we can compute the complexity of the factorization-algorithm in the following way (worst case):

$$\begin{aligned}
& \sum_{i=s+1}^{2s-1} \sum_{l=1+V_i}^{V_{i+1}} (v_i - l + V_i + 4) + \sum_{i=1}^{s-1} \left(v_{i+1} + 3 + \sum_{l=1+V_i}^{V_{i+1}} (v_i - l + V_i + 4) \right) \\
&= \sum_{i=1}^{2s-1} \sum_{l=1+V_i}^{V_{i+1}} (v_i - l + V_i + 4) - \sum_{l=1+V_s}^{V_{s+1}} (v_s - l + V_s + 4) + \sum_{i=1}^{s-1} (v_{i+1} + 3) \\
&= \sum_{i=1}^{2s-1} \left(v_{i+1}(v_i + V_i + 4) - \sum_{l=1+V_i}^{V_{i+1}} l \right) - \left(v_{s+1}(v_s + V_s + 4) - \sum_{l=1+V_s}^{V_{s+1}} l \right) + X \\
&= \sum_{i=1}^{2s-1} \left(v_{i+1}(v_i + V_i + 4) - \left(v_{i+1}V_i + \sum_{l=1}^{v_{i+1}} l \right) \right) - Y + X \\
&= \sum_{i=1}^{2s-1} \left(v_{i+1} \left(v_i - \frac{1}{2}v_{i+1} \right) \right) + \sum_{i=1}^{2s-1} \left(\frac{7}{2}v_{i+1} \right) - Y + X \\
&\leq M \cdot n + \frac{7}{2}n - Y + X \quad \left(\text{where } M = \max_i \left| v_i - \frac{1}{2}v_{i+1} \right| \right)
\end{aligned}$$

with $X := \sum_{i=1}^{s-1} (v_{i+1} + 3)$, $Y := \left(v_{s+1}(v_s + V_s + 4) - \sum_{l=1+V_s}^{V_{s+1}} l \right)$ and

$$\begin{aligned}
-Y + X &= - \left(v_{s+1}v_s + 4v_{s+1} - \left(\frac{1}{2}(v_{s+1})(v_{s+1} + 1) \right) \right) + \sum_{i=1}^{s-1} (v_{i+1} + 3) \\
&= 3s + \sum_{i=1}^{s-1} v_{i+1} - \left(v_s + \frac{7}{2} - \frac{1}{2}v_{s+1} \right) v_{s+1} - 3 \\
&\leq 4n - \left(v_s + \frac{7}{2} - \frac{1}{2}v_{s+1} \right) v_{s+1}
\end{aligned}$$

Since every v_i is supposed to be small, especially v_{s+1} , M will also be small and $v_s + \frac{7}{2} - \frac{1}{2}v_{s+1}$ will be nonnegative, independent of n . So in that case the runtime of the factorization-algorithm is $O(n) = O(\log_2|G|)$ and, therefore, β is tame.

6 Conclusion

We presented a new way to construct tame logarithmic signatures. The advantage of this method is the possibility to produce aperiodic logarithmic signatures

which resist the attack proposed in [1]. Although, one is in need to store δ and all $\alpha^{(j_1, \dots, j_s)}$ to factorize with respect to β , this is also an aspect of security, because an attacker doesn't know those elements used during the construction but is in need to find them for being able to factorize w.r.t. β , as far as we know.

Further, we showed how to get a huge number of aperiodic tame logarithmic signatures by using the proposed algorithm. Although, those might not be enough, the fact that we mainly used exact transversal logarithmic signatures for the construction of our examples implies the assumption that many more aperiodic logarithmic signatures might be gained when using for example amalgamated transversal logarithmic signatures.

Still, it is not clear if the proposed algorithm has any weaknesses in view of the reconstruction of δ and the $\alpha^{(j_1, \dots, j_s)}$ from a given β because of the known structure of the algorithm, although we conjecture that keeping the used generating set \mathcal{B} a secret makes it hard to extract any information. Further, we don't know if β is tame whether or not one knows δ and $\alpha^{(j_1, \dots, j_s)}$, which is also an important issue for an attacker.

References

- [1] S. R. Blackburn, C. Cid, and C. Mullan. Cryptanalysis of the mst3 public key cryptosystem. *Journal Math. Cryptology*, 3(4):321-328, 2009.
- [2] C. A. Cusack. Group factorizations in cryptography. University of Nebraska, Dissertation, 2000.
- [3] M. I. González Vasco, A. L. Pérez del Pozo, and P. Taborda Duarte. A note on the security of mst3. Cryptology ePrint Archive (<http://eprint.iacr.org/2009/096.pdf>), 2009.
- [4] B. Huppert and N. Blackburn. *Finite Groups II*. Springer, 1982.
- [5] B. Huppert and N. Blackburn. *Finite Groups III*. Springer, 1982.
- [6] W. Lempken, S. S. Magliveras, T. van Trung, and W. Wei. A public key cryptosystem based on non-abelian finite groups. *Journal of Cryptology*, 22(1):62-74, 2009.
- [7] W. Lempken and T. van Trung. On minimal logarithmic signatures of finite groups. *Experimental Mathematics*, 14(3):257-269, 2005.
- [8] S. S. Magliveras and N. D. Menon. Algebraic properties of cryptosystem pgm. *Journal of Cryptology*, 5(3):167-183, 1992.
- [9] S. S. Magliveras, D. R. Stinson, and T. van Trung. New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. *Journal of Cryptology*, 15(4):285-297, 2002.
- [10] S. S. Magliveras, P. Svaba, T. van Trung, and P. Zajac. On the security of a realization of cryptosystem mst3. *Tatra Mt. Math. Publ.*, 41:65-78, 2008.
- [11] A. Nuss. pers. comm. Tuebingen, 2009-2010.

- [12] S. Szabó. *Topics in Factorization of Abelian Groups*. Birkhaeuser, 2004.