Construction of strongly aperiodic logarithmic signatures

Tran van Trung
Institut für Experimentelle Mathematik
Universität Duisburg-Essen
Thea-Leymann-Straße 9
45127 Essen, Germany

Abstract

The aim of the paper is to present a general construction of strongly aperiodic logarithmic signatures (SALS) for elementary abelian p-groups. Their existence significantly extends the classes of tame logarithmic signatures which are used for the cryptosystem MST_3. They have particular characteristics that do not share with the well-known classes of transversal or fused transversal logarithmic signatures, and therefore will play a vital role for logarithmic signature based cryptosystems in practice. In theory, the construction of SALS is interesting in its own right as well.

Keywords. Aperiodic logarithmic signature, strongly aperiodic logarithmic signature, public-key cryptosystem MST_3.

2010 Mathematics Subject Classification. 94A60, 20K01.

1 Introduction

Logarithmic signatures (LS) and covers are a kind of factorization of a finite group $\mathcal{G}$ through its subsets and they induce surjective mappings from $\mathbb{Z}_{|\mathcal{G}|}$ onto $\mathcal{G}$. These mappings were used to building trapdoor one-way-functions for public key cryptosystems MST_1, MST_2 [7] and MST_3 [4, 12]. Logarithmic signatures for elementary abelian p-groups are particularly essential for an instantiation of cryptosystem MST_3. Before the papers [1] and [11] were published, periodic LS such as transversal or fused transversal were practically the only known classes, which had been analyzed for use in MST_3 [8, 2, 12, 15]. In a recent paper [10] Rybkin investigated the attack in [2] against the simple version MST_3 [4] and showed that the attack as described in [2] may have significant complexity. For the strengthened version of MST_3 [12], it has been shown that fused transversal LS withstand the powerful Matrix-Permutation attack. In [1] Baumeister and de Wiljes have proposed a method for constructing aperiodic LS for abelian groups based on the theory in Szabo's book about group factorizations [14]. Strong aperiodic LS have been introduced in [11]. Actually, the SALS class with its specific features that do not share with the known LS classes, is of vital significance for practical realizations of MST_3 and also for LS based cryptosystems. The construction of strongly aperiodic LS in [11] consists of two main steps. In the first step, construct a specific class of aperiodic LS on the basis of Baumeister-de Wiljes method. In the second step, show that the constructed class is strongly aperiodic. It should be noted that the logarithmic signatures constructed in the first step are generally not strongly aperiodic. The present paper shows a general construction of SALS with arbitrarily large block size for elementary abelian p-groups, which may be viewed as a generalization of a construction in [11]. The result thus establishes a non-periodic class of LS having particularly strong features which are relevant for cryptographic purposes.

2 Preliminaries

We briefly present notation, definitions and some basic facts about logarithmic signatures, covers for finite groups. For more details the reader is refered to [6], [7].

Let $\mathcal{G}$ be a finite group. We define the *width* of $\mathcal{G}$ to be the positive integer $w = \lceil \log_2 |\mathcal{G}| \rceil$. Suppose that $\alpha = [A_1, A_2, \ldots, A_s]$ is a sequence of ordered subsets $A_i = \{a_{i,1}, \ldots, a_{i,r_i}\}$ of $\mathcal{G}$ such that $\sum_{i=1}^{s} |A_i|$ is bounded by a polynomial in the width w of $\mathcal{G}$. Let $\mathcal{S}$ be a subset of $\mathcal{G}$. We say that α is a *cover* for $\mathcal{S}$, if every product $a_{1,j_1} \ldots a_{s,j_s}$ lies in $\mathcal{S}$ and if every $g \in \mathcal{S}$ can be expressed in at least one way as a product of the form

$$g = a_{1,j_1} \cdots a_{s,j_s} \tag{2.1}$$

with $a_{i,j_i} \in A_i$. If the expression in (2.1) is unique for every $g \in \mathcal{S}$, then α is called a *logarithmic signature* (LS) for $\mathcal{S}$. If $\mathcal{S} = \mathcal{G}$, α is called a cover, resp., a logarithmic signature for $\mathcal{G}$. The A_i are called the *blocks*, and the vector $(r_1, \ldots, r_s)$ with $r_i = |A_i|$ the *type* of α. We say that α is *proper* if $|A_i| \neq 1$ and $A_i \neq \mathcal{G}$ for $1 \leq i \leq s$; and we assume that all covers and logarithmic signatures are proper. The product $a_{1,j_1} \cdots a_{s,j_s}$ in (2.1) is called a *factorization* of g with respect to α. The sum $\ell(\alpha) = \sum_{i=1}^{s} r_i$ is defined as the *length* of α.

Let $\Gamma = \{(\mathcal{G}_i, \alpha_i)\}_{i \in \mathbb{N}}$ be a family of pairs, indexed by the security parameter i, where the $\mathcal{G}_i$ are groups in a common representation, and where α_i is a specific cover for $\mathcal{G}_i$ of length polynomial in w_i. We say that Γ is *tame* if there exists a probabilistic polynomial time algorithm $\mathcal{A}$ such that for each $g \in \mathcal{G}_i$, $\mathcal{A}$ accepts (α_i, g) as input, and outputs a factorization of g with respect to α_i (as in Equation (2.1)) 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 $g \in \mathcal{G}$ is negligible. Often we simply say α_i is tame or wild.

Let $\gamma : \mathcal{G} = \mathcal{G}_0 > \mathcal{G}_1 > \cdots > \mathcal{G}_s = 1$ be a chain of subgroups of a finite group $\mathcal{G}$, and let A_i be an ordered, complete set of right (or left) coset representatives of $\mathcal{G}_i$ in $\mathcal{G}_{i-1}$. Then it is clear that $[A_1, \ldots, A_s]$ forms a LS for $\mathcal{G}$, called an *(exact) transversal logarithmic signature* (TLS). It is shown in [13], for example, if $\mathcal{G}$ is abelian, then there is an algorithm for factoring each element $g \in \mathcal{G}$ with respect to a TLS in time complexity $O(w)$. Thus γ is tame. Suppose that $\mathcal{G}$ is a permutation group on the set $X = \{1, \ldots, n\}$. Consider a chain of nested point stabilizers $\mathcal{G} = \mathcal{G}_0 > \mathcal{G}_1 > \cdots > \mathcal{G}_s = 1$, where $\mathcal{G}_i$ fixes pointwise the symbols $1, 2, \ldots, i$, for any $i \geq 1$. It is shown in [6] that a specific constructed class of transversal logarithmic signatures from this chain of subgroups has a factorization in time complexity $O(n^2)$. In general, the problem of finding a factorization in Equation (2.1) with respect to a given cover is presumedly intractable. There is strong evidence in support of the hardness of the problem. For example, let $\mathcal{G}$ be a cyclic group and g be a generator of $\mathcal{G}$. Let $\alpha = [A_1, A_2, \ldots, A_s]$ be any cover for $\mathcal{G}$, for which the elements of A_i are written as powers of g. Then the factorization with respect to α amounts to solving the

Discrete Logarithm Problem in $\mathcal{G}$.

The main point making covers and LS interesting for use in cryptography is that they induce one-way functions when the factorization problem is intractable. In fact, they form the basis for private key crytosystem PGM [6], public key cryptosystems MST_1, MST_2 and MST_3 [7, 4, 12], and pseudorandom number generators in [5, 9].

3 Logarithmic signatures and basic transformations

We list some basic mappings that generally transform LS into LS. Let $\alpha = [A_1, \ldots, A_s]$ be an LS for a finite group $\mathcal{G}$. The following transformations can be applied on α.

(i) (*Element shuffle*): Permuting the elements within each block of α.

(ii) (*Block shuffle*): Permuting the blocks of α. If $\mathcal{G}$ is abelian, the block shuffle results in a logarithmic signature. If $\mathcal{G}$ is non-abelian, permuting two blocks of α may result in a cover for a certain subset of $\mathcal{G}$ and not an LS for $\mathcal{G}$.

(iii) (*Two sided transformation*): Let $g_0, g_1, \ldots, g_s \in \mathcal{G}$. Define a new logarithmic signature $\beta = [B_1, \ldots, B_s]$ by $B_i = g_{i-1}^{-1} A_i g_i$. Then β is called a *two sided transform* of α. When $g_0 = g_s = 1$, we say that β is a *sandwich* of α. When $g_0 = 1$, β, is said to be a *right translation* of α by g_s. If $g_s = 1$, then β is called a *left translation* of α by g_0.

(iv) (*Fusion*): If $\mathcal{G}$ is non-abelian, then replacing two consecutive blocks A_i and A_{i+1}, $1 \leq i \leq s-1$ by a single block $B = A_i A_{i+1} := \{xy \mid x \in A_i,\ y \in A_{i+1}\}$ will result in a logarithmic signature. B is called a *fused* block. If $\mathcal{G}$ is abelian, the fusion transformation can be done on any two blocks of α.

(v) (*Automorphism action*): If φ is an automorphism of $\mathcal{G}$, then $\beta = [B_1, \ldots, B_s]$ with $B_i = \varphi(A_i)$, $1 \leq i \leq s$, is a logarithmic signature for $\mathcal{G}$.

Recall that a logarithmic signature obtained from an exact transversal logarithmic signature by applying transformations (i), (ii), (iii), (iv) is called a *fused transversal logarithmic signature* (FTLS).

Definition 3.1 *A non-empty subset A of a group $\mathcal{G}$ is called* **periodic** *if there exists an element $g \in \mathcal{G} \setminus \{1_{\mathcal{G}}\}$ such that $gA = A$. Such an element g is called a* **period** *of A.*

The set of all periods of A will be denoted by $P(A)$, i.e. $P(A) = \{g \in \mathcal{G} \setminus \{1_{\mathcal{G}}\} \ : \ gA = A\}$.

Definition 3.2 *A logarithmic signature $\alpha = [A_1, \ldots, A_s]$ for a group $\mathcal{G}$ is called* **aperiodic** *if none of the blocks A_i is periodic.*

Note that the exact TLS and FTLS are examples of periodic LS.

4 Strongly aperiodic logarithmic signatures for abelian groups

A simple observation shows that aperiodicity property of an LS is preserved under the transformations described above, except the fusion. For fusing two or more blocks of an aperiodic logarithmic signature may result in a non-aperiodic logarithmic signature. The example below illustrates the situation.

Example 1 Let $\mathcal{G}$ be an elementary abelian 2-group of order 2^9 generated by $g_1, g_2, \ldots, g_9$. Then, it can be checked that $\beta = [B_1, B_2, B_3]$ with

$B_1 = \{1, g_1, g_2, g_1g_2, g_7, g_1g_3g_7, g_2g_4g_7, g_1g_3g_2g_4g_7\}$,

$B_2 = \{1, g_3, g_4, g_3g_4, g_8, g_1g_2g_3g_8, g_1g_4g_8, g_2g_3g_4g_8\}$,

$B_3 = \{1, g_5, g_6, g_5g_6, g_9, g_1g_3g_5g_9, g_2g_4g_6g_9, g_1g_2g_3g_4g_5g_6g_9\}$

is an aperiodic logarithmic signature of type $(8, 8, 8)$ for $\mathcal{G}$. However, when fusing blocks B_1 and B_2, we obtain a LS $\beta^* = [B^*, B_3]$ with $B^* = B_1.B_2$, which is no longer aperiodic, since block B^* is a subgroup and therefore periodic.

The SALS as introduced in [11] essentially require that the aperiodicity of an aperiodic LS should be preserved by all transformations listed above.

A word of caution is appropriate here. When fusing all the blocks of an LS for a group $\mathcal{G}$, we obtain one block equal $\mathcal{G}$, which is trivially a periodic LS. Therefore, when saying the aperiodicity of an LS is preserved under the fusion, we mean the resulting LS is nontrivial, i.e. the fusion is done on at most $s-1$ blocks, where s is the number of blocks of the LS.

In this paper we deal with LS for abelian p-groups, whose block size is at least p^3. Under this condition we may give a simple definition of strongly aperiodic LS as follows.

Definition 4.1 *Let $\mathcal{G}$ be an abelian p-group and let $\beta = [B_1, \ldots, B_s]$ be an aperiodic LS for $\mathcal{G}$ such that $|B_i| \geq p^3$ for $i = 1, \ldots, s$. The logarithmic signature β is called* **strongly aperiodic** *if any fusion of at most $s-1$ blocks of β always results in an aperiodic LS.*

Remark 4.1 When $|B_i| \leq p^2$ for some blocks of β, the definition of strong aperiodicity of an LS needs to be modified slightly, see [11]. It is due to results shown in the book of Szabó [14] *Topics of factorization of abelian groups.*

Remark 4.2 It seems not meaningful to extend Definition 4.1 to non-abelian groups. Because in this case a fusion of non-consecutive blocks would no longer yield an LS.

Here is a small example of SALS [11].

Example 2 Let $\mathcal{G}$ be the group given in Example 1. The following aperiodic LS $\beta = [B_1, B_2, B_3]$ of type $(8, 8, 8)$ for $\mathcal{G}$ with

$B_1 = \{1, g_1, g_2, g_1g_2, g_7, g_1g_2g_4g_6g_7, g_2g_3g_5g_7, g_1g_3g_4g_5g_6g_7\}$,

$B_2 = \{1, g_3, g_4, g_3g_4, g_8, g_1g_3g_8, g_2g_4g_8, g_1g_3g_2g_4g_8\},$

$B_3 = \{1, g_5, g_6, g_5g_6, g_9, g_1g_5g_9, g_2g_6g_9, g_1g_5g_2g_6g_9\},$

is strongly aperiodic. In fact, it can be checked that the fusion of any two blocks of β yields an aperiodic block.

The next lemma is useful for the proof of strong aperiodicity of an LS.

Lemma 1 ([11]) *Let $\mathcal{G}$ be an abelian group. Let $\beta = [B_1, \ldots, B_s]$ be a logarithmic signature for $\mathcal{G}$. Let $I \subseteq \{1, \ldots, s\}$. Suppose that the fused block $\prod_{i \in I} B_i$ is aperiodic. Then $\prod_{j \in J} B_j$ is aperiodic for any non-empty subset $J \subseteq I$.*

Remark 4.3 Lemma 1 is, in fact, very helpful. Suppose that we want to verify the strong aperiodicity of a logarithmic signature β having s blocks. Without Lemma 1, to fuse up to $s-1$ blocks we have to check all $\binom{s}{1} + \binom{s}{2} + \cdots + \binom{s}{s-1} = 2^s - 2$ possible fusions for the blocks of β. Whereas by using Lemma 1 we simply need to check $\binom{s}{s-1} = s$ fusions for all possible combinations of $s-1$ blocks of β.

5 The Baumeister-de Wiljes construction of aperiodic LS

Constructing tame aperiodic LS for abelian groups is a problem of theoretical interest and of practical importance. For they form a class of LS beyond the well-known classes of transversal and their fused logarithmic signatures which are all periodic. With respect to cryptosystem MST_3 aperiodic logarithmic signatures appear to be specially significant.

In [1] Baumeister and de Wiljes present an interesting method for constructing aperiodic signatures for abelian groups, for short we call it BW-method or BW-construction. The BW-method is based on results in the book of Szabó [14], and describes an approach to constructing aperiodic logarithmic signatures. It should be stressed that the BW-construction as described below is not an algorithm, as it might appear, the reason is that the necessary conditions to be fulfilled, quickly forbids its computational feasibility even for groups of moderate order. However, its basic idea has proved to be useful.

Baumeister-de Wiljes construction

Let $\mathcal{G}$ be a finite abelian group. Let $\mathcal{H}$ be a subgroup of $\mathcal{G}$ and let $\mathcal{T}$ be a transversal of $\mathcal{H}$ in $\mathcal{G}$ (i.e. $\mathcal{T}$ is a complete set of coset representatives of $\mathcal{H}$ in $\mathcal{G}$).

(i) Let $\theta = [T_1, \ldots, T_s]$ be a logarithmic signature of type $(r_1, \ldots, r_s)$ for $\mathcal{T}$, where $T_i = \{t_{i,1}, \ldots, t_{i,r_i}\}$.

(ii) Suppose that for each i with $1 \leq i \leq s$ there exists a collection

$$\mathcal{L}_i = \{A_{i,1}, \ldots, A_{i,r_i}\}$$

of subsets $A_{i,j}$ of $\mathcal{H}$ such that any choice $[A_{1,j_1}, \ldots, A_{s,j_s}]$ with $A_{i,j_i} \in \mathcal{L}_i$ forms a logarithmic signature for $\mathcal{H}$.

(iii) Then $\beta := [B_1, \ldots, B_s]$ defined by $B_i = t_{i,1}A_{i,1} \cup \ldots \cup t_{i,r_i}A_{i,r_i}$, for $1 \leq i \leq s$ forms a logarithmic signature for $\mathcal{G}$.

The next proposition characterizes the aperiodicity of the constructed LS β.

For any subsets A, B of a group $\mathcal{G}$ we say that B is a *translate* of A if there is an element $g \in \mathcal{G}$ such that $gA = B$. The translate B is called *proper* if $A \neq B$.

Proposition 1 ([1]) *Suppose that $A_{i,j}$ is not a translate of $A_{i,k}$ for any $j, k \in \{1, \ldots, r_i\}$. Then B_i is periodic if and only if*

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

The main idea of the BW-construction is to find collections $\mathcal{L}_i$ satisfying condition (ii).

An interesting property of aperiodic LS constructed by the BW-method is that they are tame when certain conditions are satisfied [1], [3]. We record the result in the following theorem.

Theorem 1 *Let $\beta := [B_1, \ldots, B_s]$ be a logarithmic signature constructed by the BW-method. Assume that θ and all logarithmic signatures $[A_{1,j_1}, \ldots, A_{s,j_s}]$, $1 \leq j_i \leq r_i$ and $1 \leq i \leq s$, are tame. If θ and $\mathcal{L}_1, \ldots, \mathcal{L}_s$ are known, then β is tame.*

Proof. Let $g \in \mathcal{G}$ be an element that we want to factorize with respect to β. Then there exist unique elements $t \in \mathcal{T}$ and $h \in \mathcal{H}$ such that $g = ht$. Since θ is tame, we can find a factorization of $t = t_{1,j_1} \cdots t_{s,j_s}$ with respect to θ in time bounded by $O(w^{c_1})$, where $w = \lceil \log_2 |\mathcal{G}| \rceil$ and c_1 is a constant. Having obtained $(j_1, \ldots, j_s)$ we can determine the logarithmic signature $[A_{1,j_1}, \ldots, A_{s,j_s}]$ which is tame by the assumption. So, the complexity of factoring $h = a_{1,k_1} \cdots a_{s,k_s}$ with respect to $[A_{1,j_1}, \ldots, A_{s,j_s}]$ is bounded by $O(w^{c_2})$, where c_2 is a constant. Thus

$$g = ht = a_{1,k_1} \cdots a_{s,k_s}.t_{1,j_1} \cdots t_{s,j_s} = \underbrace{(a_{1,k_1}t_{1,j_1})}_{\in B_1} \cdots \underbrace{(a_{s,k_s}t_{s,j_s})}_{\in B_s}.$$

Since, finding $a_{i,k_i}t_{i,j_i} \in B_i$ only requires a time of $O(\log_2(|B_i|))$ when B_i is sorted. It follows that β is tame. □

The following observation about the fusion operation on a logarithmic signature obtained from the BW-construction is useful.

Lemma 2 *We use the notation as described in the BW-construction above. The fusion of blocks B_i and B_j, $i \neq j$, of β results in a logarithmic signature, which is again derived from the BW-construction, in which $\mathcal{L}_i$ and $\mathcal{L}_j$ are replaced by $\mathcal{L}_i\mathcal{L}_j$ and T_i and T_j by T_iT_j.*

From now on let $\mathcal{G}$ be an elementary abelian p-group of order p^f. We use additive notation for the group operation and 0 will denote the identity of $\mathcal{G}$. In fact we identify $\mathcal{G}$ with the additive group of the Galois field $\mathbb{F}_{p^f}$. In this way $\mathcal{G}$ is viewed as a vector space of dimension f over $\mathbb{F}_p$, and thus we may freely use the language of linear algebra with respect to $\mathcal{G}$. For example, a minimal generator set for $\mathcal{G}$ may be called a basis for $\mathcal{G}$.

6 A construction of SALS of type $(p^m, \dots, p^m)$ for elementary abelian groups of order p^{ms} with $m \geq 3$ and $s \geq 2$

In this section we first construct an aperiodic LS of type $(p^m, \dots, p^m)$ for an elementary abelian p-group $\mathcal{G}$ of order p^{ms}, where $p = 2$ or p is an odd prime with $m \geq 3$ and $s \geq 2$. Let $v_1, v_2, \dots, v_s, v_{s+1}, \dots, v_{2s}, \dots, v_{(m-1)s+1}, \dots, v_{ms}$ be a generator set of $\mathcal{G}$. By using the BW-method we define

(i) $\mathcal{T} = \langle v_{(m-1)s+1}, \dots, v_{ms} \rangle$ (a subgroup of order p^s of $\mathcal{G}$), $\theta = [T_1, \dots, T_s]$ an LS of $\mathcal{T}$ with $T_i = \{0, v_{(m-1)s+i}, 2v_{(m-1)s+i}, \dots, (p-1)v_{(m-1)s+i}\}$ for $i = 1, \dots, s$,

(ii) $\mathcal{H} = \langle v_1, \dots, v_{(m-1)s} \rangle$, a subgroup of order $p^{(m-1)s}$ of $\mathcal{G}$.

Let $u \in \{1, \dots, p-1\} = \mathbb{F}_p \setminus \{0\}$ be a chosen parameter. For $i = 1, \dots, s$ define a collection

$$\mathcal{L}_i = \{A_{i,0}, A_{i,1}, \dots, A_{i,(p-1)}\}$$

as follows.

$$\begin{aligned}
&A_{1,0} = \langle v_1, \dots, v_{m-1} \rangle, \\
&A_{1,j} = \langle v_1 + v_2 + j \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+1},\ v_1 + v_3 + j \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+2},\ \dots, \\
&\qquad v_1 + v_{m-1} + j \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+(m-2)},\ u \cdot v_{m-2} + j \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+(m-1)} \rangle, \\
&\qquad j \in \{1, \dots, p-1\},
\end{aligned}$$

$$\begin{aligned}
&A_{i,j} = \langle v_{(m-1)(i-1)+1} + jv_1,\ v_{(m-1)(i-1)+2} + jv_2,\ \dots,\ v_{(m-1)(i-1)+(m-1)} + jv_{m-1} \rangle, \\
&\qquad i \in \{2, \dots, s\},\ j \in \{0, \dots, p-1\}.
\end{aligned}$$

Remark 6.1 Note that in (i) we may replace $\mathcal{T}$ by any transversal $\mathcal{TR}$ of $\mathcal{H}$. Here $\mathcal{TR}$ is not a subgroup in general. In fact, it is simple to create an LS for a transversal of $\mathcal{H}$ by passing to the quotient group $\bar{\mathcal{T}} = \mathcal{G}/\mathcal{H}$. Namely, let $\bar{\theta} = [\bar{T}_1, \dots, \bar{T}_s]$ be an LS for $\bar{\mathcal{T}}$, where $\bar{T}_i = [x_{i,0}\mathcal{H}, \dots, x_{i,(p-1)}\mathcal{H}]$, $1 \leq i \leq s$. Note that there are $|\mathcal{H}|$ possibilities for choosing $x_{i,j}$ as coset representatives. By lifting $\bar{\theta}$ to $\mathcal{G}$ we obtain an LS $\theta = [T_1, \dots, T_s]$ with $T_i = [x_{i,0}, \dots, x_{i,(p-1)}]$ for a certain transversal $\mathcal{TR}$ of $\mathcal{H}$.

We now prove that the subsets $A_{i,j}$ of $\mathcal{L}_i$, $1 \leq i \leq s$ satisfy condition (ii) of the BW-construction. This means that for any $(j_1, j_2, \ldots, j_s) \in \{0, 1, \ldots, p-1\}^s$ the collection $[A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}]$ forms a logarithmic signature for $\mathcal{H}$. This is equivalent to say that the basis elements of $A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}$ are linearly independent.

We consider two cases: $j_1 = 0$ and $j_1 \neq 0$.

Case $j_1 = 0$.

Since $j_1 = 0$, we have

$$\begin{aligned}
A_{1,0} &= \langle v_1, \ldots, v_{m-1} \rangle, \\
A_{2,j_2} &= \langle v_{(m-1)+1} + j_2 v_1, v_{(m-1)+2} + j_2 v_2, \ldots, v_{(m-1)+(m-1)} + j_2 v_{m-1} \rangle, \\
A_{3,j_3} &= \langle v_{2(m-1)+1} + j_3 v_1, v_{2(m-1)+2} + j_3 v_2, \ldots, v_{2(m-1)+(m-1)} + j_3 v_{m-1} \rangle, \\
&\vdots \\
A_{s,j_s} &= \langle v_{(s-1)(m-1)+1} + j_s v_1, v_{(s-1)(m-1)+2} + j_s v_2, \ldots, v_{(s-1)(m-1)+(m-1)} + j_s v_{m-1} \rangle
\end{aligned}$$

By forming a linear combination of the basis elements of $A_{1,0}, A_{2,j_2}, \ldots, A_{s,j_s}$ for the zero element we obtain

$$\begin{aligned}
0 &= \lambda_{1,1}.v_1 + \cdots + \lambda_{1,(m-1)}.v_{m-1} \\
&+ \lambda_{2,1}.(v_{(m-1)+1} + j_2 v_1) + \cdots + \lambda_{2,(m-1)}.(v_{(m-1)+(m-1)} + j_2 v_{m-1}) + \cdots \\
&+ \lambda_{s,1}.(v_{(s-1)(m-1)+1} + j_s v_1) + \cdots + \lambda_{s,(m-1)}.(v_{(s-1)(m-1)+(m-1)} + j_s v_{m-1})
\end{aligned} \tag{6.2}$$

with $\lambda_{i,j} \in \mathbb{F}_p$. The matrix form of Equation (6.2) is given by

$$(\lambda_{1,1}, \ldots, \lambda_{1,(m-1)}, \lambda_{2,1}, \ldots, \lambda_{2,(m-1)}, \ldots, \lambda_{s,1}, \ldots, \lambda_{s,(m-1)})M = (0, 0, \ldots, 0),$$

where M is the following $((m-1)s \times (m-1)s)$-matrix over $\mathbb{F}_p$

$$
M = \begin{pmatrix}
1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\
0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\
0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\
& & & & & & & & & & & & & & & & \\
j_2 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\
0 & j_2 & \dots & 0 & 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\
0 & 0 & \dots & j_2 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\
& & & & & & & & & & & & & & & & \\
j_3 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\
0 & j_3 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\
0 & 0 & \dots & j_3 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 & \dots & 0 & 0 & \dots & 0 \\
& & & & & & & & & & & & & & & & \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\
& & & & & & & & & & & & & & & & \\
j_s & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 1 & 0 & \dots & 0 \\
0 & j_s & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & 1 & \dots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots \\
0 & 0 & \dots & j_s & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 1
\end{pmatrix}
$$

Since M is a lower triangular matrix with all 1 on the main diagonal, M is invertible and Equation (6.2) has $\lambda_{i,j} = 0$ for all $1 \leq i \leq s$ and $1 \leq j \leq m-1$ as the unique solution. Thus the basis elements of $A_{1,0}, A_{2,j_2}, \dots, A_{s,j_s}$ are linearly independent. In other words $[A_{1,0}, A_{2,j_2}, \dots, A_{s,j_s}]$ forms a logarithmic signature for $\mathcal{H}$.

Case $j_1 \neq 0$.

We have

$$
\begin{aligned}
A_{1,j_1} &= \langle v_1 + v_2 + j_1 \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+1},\ v_1 + v_3 + j_1 \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+2},\ \dots, \\
&\qquad v_1 + v_{m-1} + j_1 \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+(m-2)},\ u \cdot v_{m-2} + j_1 \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+(m-1)} \rangle \\
A_{2,j_2} &= \langle v_{(m-1)+1} + j_2 v_1, v_{(m-1)+2} + j_2 v_2, \dots, v_{(m-1)+(m-1)} + j_2 v_{m-1} \rangle, \\
A_{3,j_3} &= \langle v_{2(m-1)+1} + j_3 v_1, v_{2(m-1)+2} + j_3 v_2, \dots, v_{2(m-1)+(m-1)} + j_3 v_{m-1} \rangle, \\
&\ \vdots \\
A_{s,j_s} &= \langle v_{(s-1)(m-1)+1} + j_s v_1, v_{(s-1)(m-1)+2} + j_s v_2, \dots, v_{(s-1)(m-1)+(m-1)} + j_s v_{m-1} \rangle
\end{aligned}
$$

and obtain a linear combination of the zero element from the basis elements of $A_{1,j_1}, A_{2,j_2}, \ldots, A_{s,j_s}$ as follows.

$$
\begin{aligned}
0 = {} & \lambda_{1,1}.(v_1 + v_2 + j_1 \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+1}) + \cdots + \lambda_{1,(m-2)}.(v_1 + v_{m-1} + j_1 \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+(m-2)}) \\
& + \lambda_{1,(m-1)}.(u \cdot v_{m-2} + j_1 \cdot \sum_{\ell=1}^{s-1} v_{(m-1)\ell+(m-1)}) \\
& + \lambda_{2,1}.(v_{(m-1)+1} + j_2 v_1) + \cdots + \lambda_{2,(m-1)}.(v_{(m-1)+(m-1)} + j_2 v_{m-1}) + \cdots \\
& + \lambda_{s,1}.(v_{(s-1)(m-1)+1} + j_s v_1) + \cdots + \lambda_{s,(m-1)}.(v_{(s-1)(m-1)+(m-1)} + j_s v_{m-1})
\end{aligned}
\tag{6.3}
$$

The coefficient matrix M of Equation (6.3) has the form

$$
M = \begin{pmatrix}
1 & 1 & 0 & \ldots & 0 & 0 & j_1 & 0 & \ldots & 0 & 0 & \ldots & j_1 & 0 & \ldots & 0 & 0 \\
1 & 0 & 1 & \ldots & 0 & 0 & 0 & j_1 & \ldots & 0 & 0 & \ldots & 0 & j_1 & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
1 & 0 & 0 & \ldots & 0 & 1 & 0 & 0 & \ldots & j_1 & 0 & \ldots & 0 & 0 & \ldots & j_1 & 0 \\
0 & 0 & 0 & \ldots & u & 0 & 0 & 0 & \ldots & 0 & j_1 & \ldots & 0 & 0 & \ldots & 0 & j_1 \\
 & & & & & & & & & & & & & & & & \\
j_2 & 0 & 0 & \ldots & 0 & 0 & 1 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 \\
0 & j_2 & 0 & \ldots & 0 & 0 & 0 & 1 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 0 & j_2 & 0 & 0 & \ldots & 0 & 1 & \ldots & 0 & 0 & \ldots & 0 & 0 \\
 & & & & & & & & & & & & & & & & \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
 & & & & & & & & & & & & & & & & \\
j_s & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 1 & 0 & \ldots & 0 & 0 \\
0 & j_s & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 1 & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 0 & j_s & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 1
\end{pmatrix}
$$

- By subtracting j_1 times the rows $(m-1)+1$, $2(m-1)+1$, …, $(s-1)(m-1)+1$ from the first row,
- j_1 times the rows $(m-1)+2$, $2(m-1)+2$, …, $(s-1)(m-1)+2$ from the second row, and so on, up to
- j_1 times the rows $(m-1)+(m-1)$, $2(m-1)+(m-1)$, …, $(s-1)(m-1)+(m-1)$ from the $(m-1)^{th}$-row

we obtain an $s(m-1) \times s(m-1)$-matrix M' of the form

$$M' = \begin{pmatrix}
1\text{-}J & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\
1 & \text{-}J & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
1 & 0 & 0 & \dots & \text{-}J & 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\
0 & 0 & 0 & \dots & u & \text{-}J & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\
 & & & & & & & & & & & & & & & & \\
j_2 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\
0 & j_2 & 0 & \dots & 0 & 0 & 0 & 1 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \dots & 0 & j_2 & 0 & 0 & \dots & 0 & 1 & \dots & 0 & 0 & \dots & 0 & 0 \\
 & & & & & & & & & & & & & & & & \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
 & & & & & & & & & & & & & & & & \\
j_s & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 1 & 0 & \dots & 0 & 0 \\
0 & j_s & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 1 & \dots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \dots & 0 & j_s & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 1
\end{pmatrix}$$

where $J = j_1(j_2 + \cdots + j_s)$.

Thus we have det M = det M' = det M_{m-1}, where

$$M_{m-1} = \begin{pmatrix}
1\text{-}J & 1 & 0 & \dots & 0 & 0 \\
1 & \text{-}J & 1 & \dots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
1 & 0 & 0 & \dots & \text{-}J & 1 \\
0 & 0 & 0 & \dots & u & \text{-}J
\end{pmatrix}$$

is an $(m-1) \times (m-1)$-matrix over $\mathbb{F}_p$. We will compute the determinant of M_{m-1}. Set $n = m-2$. Since $m \geq 3$, we have $n \geq 1$.

If $m = 3$, i.e. $n = 1$, we obtain

$$M_2 = \begin{pmatrix} 1\text{-}J & 1 \\ u & \text{-}J \end{pmatrix}$$

and det $M_2 = J^2 - J - u$.

Now assume that $n = m - 2 \geq 2$.

Define two $n \times n$-matrices P_n and Q_n as follows.

$$P_n = \begin{pmatrix}
\text{-}J & 1 & 0 & \dots & 0 & 0 \\
0 & \text{-}J & 1 & \dots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \dots & \text{-}J & 1 \\
0 & 0 & 0 & \dots & u & \text{-}J
\end{pmatrix},$$

$$Q_n = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 1 & \text{-}J & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & 0 & 0 & \dots & \text{-}J & 1 \\ 0 & 0 & 0 & \dots & u & \text{-}J \end{pmatrix}.$$

Then

$$\det M_{m-1} = (1-J)\det P_n - \det Q_n.$$

Further

$$\det P_n = (-J)\det P_{n-1}.$$

As

$$P_2 = \begin{pmatrix} \text{-}J & 1 \\ u & \text{-}J \end{pmatrix},$$

we have

$$\det P_n = (-J)^{n-2}(J^2-u).$$

For computing $\det Q_n$ we observe that

$$\det Q_n = \det P_{n-1} - \det Q_{n-1}.$$

Here

$$Q_2 = \begin{pmatrix} 1 & 1 \\ 0 & \text{-}J \end{pmatrix},$$

so $\det Q_2 = -J$. The recursion for $\det Q_n$ gives

$$\begin{aligned} \det Q_n &= (-1)^0 \det P_{n-1} + (-1)^1 \det P_{n-2} + (-1)^2 \det P_{n-3} + \cdots + (-1)^{n-4}\det P_3 \\ &\quad + (-1)^{n-3}\det P_2 + (-1)^{n-2}\det Q_2 \\ &= (-1)^0(-J)^{n-3}(J^2-u) + (-1)^1(-J)^{n-4}(J^2-u) + \cdots + (-1)^{n-4}(-J)(J^2-u) \\ &\quad + (-1)^{n-3}(J^2-u) + (-1)^{n-2}(-J) \\ &= (-1)^{n-3}(J^2-u)[J^{n-3} + J^{n-4} + \cdots + J + 1] + (-1)^{n-2}(-J). \end{aligned}$$

Substituting the values of $\det P_n$ and $\det Q_n$ in

$$\det M_{m-1} = (1-J)\det P_n - \det Q_n,$$

and simplifying gives

$$\det M_{m-1} = (-1)^{n-2}(J^2-u)[-J^{n-1} + J^{n-2} + J^{n-3} + \cdots + J + 1] + (-1)^{n-2}J.$$

Recall that our goal is to show that for any given m we can choose a $u \in \mathbb{F}_p \setminus \{0\}$ such that $\det M' = \det M_{m-1} \neq 0$ for any J, i.e. for any possible choices of $(j_1, j_2, \dots, j_s) \in \{0, 1, \dots, p-1\}^s$.

Now, we consider $\det M_{m-1}$ as a polynomial $f_u^{(n)}(J)$ over $\mathbb{F}_p$, i.e.

$$f_u^{(1)}(J) := J^2 - J - u,$$

and for $n \geq 2$

$$f_u^{(n)}(J) := (-1)^{n-2}(J^2 - u)[-J^{n-1} + J^{n-2} + J^{n-3} + \cdots + J + 1)] + (-1)^{n-2}J.$$

Hence the statement that $\det M' \neq 0$ for a suitable choice of $u \in \mathbb{F}_p \setminus \{0\}$ is equivalent to the statement that $f_u^{(n)}(J)$ has no root in $\mathbb{F}_p$. We first prove the following lemma.

Lemma 3 *Let $u_1, u_2 \in \mathbb{F}_p^\times := \mathbb{F}_p \setminus \{0\}$ with $u_1 \neq u_2$. Suppose that there exist $a_1, a_2 \in \mathbb{F}_p$ such that $f_{u_1}^{(n)}(a_1) = 0$ and $f_{u_2}^{(n)}(a_2) = 0$. Then $a_1 \neq a_2$.*

Proof. First consider case $n = 1$. Suppose that $a_1 = a_2$. Then

$$\begin{aligned}
0 &= f_{u_1}^{(1)}(a_1) \\
&= a_1^2 - a_1 - u_1 \\
&= f_{u_2}^{(1)}(a_2) \\
&= f_{u_2}^{(1)}(a_1) \\
&= a_1^2 - a_1 - u_2.
\end{aligned}$$

It follows that $u_1 = u_2$, a contradiction.

Assume that $n \geq 2$. Again suppose that $a_1 = a_2$. Then

$$\begin{aligned}
0 &= f_{u_1}^{(n)}(a_1) \\
&= (-1)^{n-2}(a_1^2 - u_1)[-a_1^{n-1} + a_1^{n-2} + a_1^{n-3} + \cdots + a_1 + 1)] + (-1)^{n-2}a_1 \\
&= f_{u_2}^{(n)}(a_2) \\
&= f_{u_2}^{(n)}(a_1) \\
&= (-1)^{n-2}(a_1^2 - u_2)[-a_1^{n-1} + a_1^{n-2} + a_1^{n-3} + \cdots + a_1 + 1)] + (-1)^{n-2}a_1.
\end{aligned}$$

Set $Z = [-a_1^{n-1} + a_1^{n-2} + a_1^{n-3} + \cdots + a_1 + 1)]$.

It follows that $u_1 Z = u_2 Z$ or $(u_1 - u_2)Z = 0$.

Since $u_1 \neq u_2$ we have $Z = 0$.

So

$$\begin{aligned}
f_{u_1}^{(n)}(a_1) &= (-1)^{n-2}(a_1^2 - u_1)Z + (-1)^{n-2}a_1 \\
&= (-1)^{n-2}a_1 \\
&= 0.
\end{aligned}$$

Thus $a_1 = 0$, but this is a contradiction, since $f_u^{(n)}(0) = (-1)^{n-2}(-u) \neq 0$, as $u \in \mathbb{F}_p^\times$. $\square$

We evaluate the values of $f_u^{(n)}(J)$ at $0, 1, 2, u$.

Assume $n \geq 2$. Using

$$\frac{J^n - 1}{J - 1} = J^{n-1} + \cdots + J + 1$$

for $J \neq 1$, the polynomial $f_u^{(n)}(J)$ will be simplified to

$$f_u^{(n)}(J) = (-1)^{n-2}\frac{(J^2-u)}{(J-1)}[-J^n + 2J^{n-1} - 1] + (-1)^{n-2}J.$$

We find

$$\begin{aligned}
f_u^{(n)}(0) &= (-1)^{n-1}u, \\
f_u^{(n)}(1) &= (-1)^{n-2}(-(n-2)u + n - 1), \\
f_u^{(n)}(2) &= (-1)^{n-2}(u-2), \\
f_u^{(n)}(u) &= (-1)^{n-2}u^n(-u+2).
\end{aligned}$$

For $n = 1$. We have

$$\begin{aligned}
f_u^{(1)}(0) &= -u, \\
f_u^{(1)}(1) &= -u, \\
f_u^{(1)}(2) &= (2-u), \\
f_u^{(1)}(u) &= u(u-2).
\end{aligned}$$

The next proposition shows that det $M' \neq 0$ for an appropriate choice of $u \in \mathbb{F}_p^\times$.

Proposition 2 *For any given $n \geq 1$, there is a $u \in \mathbb{F}_p^\times$ such that $f_u^{(n)}(J)$ has no root in $\mathbb{F}_p$.*

Proof. Assume $n \geq 2$. We distinguish case $p = 2, 3$ from case $p \geq 5$. It is clear that the proposition is true for $p = 2, 3$, as we may choose $u = 1$. Thus, for $p = 2$ we have

$$\begin{aligned}
f_1^{(n)}(0) &= (-1)^{n-1}1 \neq 0, \\
f_1^{(n)}(1) &= (-1)^{n-2}1 \neq 0,
\end{aligned}$$

and for $p = 3$ we find

$$\begin{aligned}
f_1^{(n)}(0) &= (-1)^{n-1}1 \neq 0, \\
f_1^{(n)}(1) &= (-1)^{n-2}1 \neq 0, \\
f_1^{(n)}(2) &= (-1)^{n-2}(-1) \neq 0.
\end{aligned}$$

Now assume that $p \geq 5$.

Consider $(p-2)$ polynomials

$$f_1^{(n)}(J), f_3^{(n)}(J), f_4^{(n)}(J), \ldots, f_{p-1}^{(n)}(J),$$

i.e. all polynomials $f_u^{(n)}(J)$ with $u \neq 2$.

Suppose by contradiction that each of these polynomials have a root in $\mathbb{F}_p$. Then these roots are in $\mathbb{F}_p \setminus \{0, 2, u\}$, this is because $f_u^{(n)}(0) \neq 0$, $f_u^{(n)}(2) \neq 0$, $f_u^{(n)}(u) \neq 0$ for all $u \neq 2$. By Lemma 3 these $(p-2)$ roots are pairwise distinct. But this is a contradiction, as $|\mathbb{F}_p \setminus \{0, 2, u\}| = p - 3$. It follows that there is a value $u \in \mathbb{F}_p^\times \setminus \{2\}$ such that $f_u^{(n)}(J)$ has no root in $\mathbb{F}_p$.

For case $n = 1$ the proof is similar, and therefore is omitted. $\square$

Proposition 2 finally shows that β is a LS of type $(p^m, \ldots, p^m)$ for $\mathcal{G}$. By using Proposition 1 and the fact that $A_{i,j} \cap A_{i,k} = \{0\}$ for any $A_{i,j}, A_{i,k} \in \mathcal{L}_i$ with $j \neq k$, $1 \leq i \leq s$, we find that β is aperiodic. We record the result in the following theorem.

Theorem 2 *The construction above yields an aperiodic LS β of type $(p^m, \ldots, p^m)$ for $\mathcal{G}$.*

Remark 6.2 In the proof of Proposition 2 we observe that for $p = 2, 3$ we may choose $u = 1$ for every $n \geq 1$. However for $p \geq 5$, the choice $u \in \mathbb{F}_p^\times$ actually depends on n. Consider $p = 5$, for example. It is straightforward to check that we may choose u as follows.

$$\begin{cases} u = 1 & \text{if } n \text{ even,} \\ u = -1 & \text{if } n \text{ odd and } n \not\equiv 4 \bmod 5 \text{ ,} \\ u = 3 & \text{if } n \text{ odd and } n \equiv 4 \bmod 5. \end{cases}$$

Now we proceed to prove that β is strongly aperiodic.

Theorem 3 *The above constructed LS β of type $(p^m, \ldots, p^m)$ for the elementary abelian p-group $\mathcal{G}$ of order p^{ms} is strongly aperiodic.*

Proof. Recall that Lemma 2 states that fusing any two blocks of β results in an LS, which is again obtained from the BW-construction. By using Lemma 1 we simply need to show that the fusion of any $(s-1)$ blocks of $\beta = [B_1, \ldots, B_s]$ forms an aperiodic block. The proof is done by showing that the fusion of any $(s-1)$ collections $\mathcal{L}_i$ yields a collection of subgroups of $\mathcal{G}$ having only the identity element 0 of $\mathcal{G}$ in their intersection.

We consider three cases.

Case 1: Fusing $\mathcal{L}_2, \ldots, \mathcal{L}_s$.

Let $\mathcal{L}_2 + \cdots + \mathcal{L}_s$ denote the collection of subgroups obtained by fusing $\mathcal{L}_2, \ldots, \mathcal{L}_s$. The subsets of $\mathcal{L}_2 + \cdots + \mathcal{L}_s$ are of the form $(A_{2,j_2} + A_{3,j_3} + \cdots + A_{s,j_s})$ with $(j_2, j_3, \ldots, j_s) \in \{0, 1, \ldots, p-1\}^{s-1}$

We show that

$$\bigcap_{\substack{(j_2, j_3, \ldots, j_s) \\ \in \{0,1,\ldots,p-1\}^{s-1}}} (A_{2,j_2} + A_{3,j_3} + \cdots + A_{s,j_s}) = \{0\}.$$

Observe that

$$\begin{aligned}
& (A_{2,0}+A_{3,0}+\cdots+A_{s,0})\cap(A_{2,1}+A_{3,0}+\cdots+A_{s,0}) \\
= \; & \langle v_{(m-1)+1},\ldots,v_{(m-1)+(m-1)},\ldots,v_{(s-1)(m-1)+1},\ldots,v_{(s-1)(m-1)+(m-1)}\rangle \\
& \cap\langle v_{(m-1)+1}+v_1,\ldots,v_{(m-1)+(m-1)}+v_{m-1},v_{2(m-1)+1},\ldots,v_{2(m-1)+(m-1)},\ldots, \\
& v_{(s-1)(m-1)+1},\ldots,v_{(s-1)(m-1)+(m-1)}\rangle \\
= \; & \langle v_{2(m-1)+1},\ldots,v_{2(m-1)+(m-1)},\ldots,v_{(s-1)(m-1)+1},\ldots,v_{(s-1)(m-1)+(m-1)}\rangle \\
= \; & A_{3,0}+A_{4,0}+\cdots+A_{s,0}.
\end{aligned}$$

Similarly, we find

$$\begin{aligned}
& (A_{2,0}+A_{3,0}+A_{4,0}+\cdots+A_{s,0})\cap(A_{2,0}+A_{3,1}+A_{4,0}+\cdots+A_{s,0}) \\
= \; & A_{2,0}+A_{4,0}+\cdots+A_{s,0}, \\
\vdots & \\
& (A_{2,0}+A_{3,0}+\cdots+A_{s-1,0}+A_{s,0})\cap(A_{2,0}+A_{3,0}+\cdots+A_{s-1,1}+A_{s,0}) \\
= \; & A_{2,0}+A_{3,0}+\cdots+A_{s-2,0}+A_{s,0},
\end{aligned}$$

and

$$\begin{aligned}
& (A_{2,0}+A_{3,0}+\cdots+A_{s-1,0}+A_{s,0})\cap(A_{2,0}+A_{3,0}+\cdots+A_{s-1,0}+A_{s,1}) \\
= \; & A_{2,0}+A_{3,0}+\cdots+A_{s-1,0}.
\end{aligned}$$

It is clear that the intersection of the elements on the right hand side of the equalities is equal to $\{0\}$.

Case 2: Fusing $\mathcal{L}_1,\mathcal{L}_2,\ldots,\mathcal{L}_{s-1}$.

We show that

$$\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1}) \\ \in\{0,1,\ldots,p-1\}^{s-1}}} \left(A_{1,j_1}+A_{2,j_2}+\cdots+A_{s-1,j_{s-1}}\right)=\{0\}.$$

First, we have

$$\begin{aligned}
& (A_{1,0}+A_{2,0}+\cdots+A_{s-1,0})\cap(A_{1,1}+A_{2,0}+\cdots+A_{s-1,0}) \\
= \; & \langle v_1,\ldots,v_{(m-1)},v_{(m-1)+1},\ldots,v_{(m-1)+(m-1)},\ldots,v_{(s-2)(m-1)+1},\ldots,v_{(s-2)(m-1)+(m-1)}\rangle \\
& \cap\langle v_1+v_2+\sum_{\ell=1}^{s-1}v_{(m-1)\ell+1},v_1+v_3+\sum_{\ell=1}^{s-1}v_{(m-1)\ell+2},\ \ldots, \\
& v_1+v_{m-1}+\sum_{\ell=1}^{s-1}v_{(m-1)\ell+(m-2)},\ u\cdot v_{m-2}+\sum_{\ell=1}^{s-1}v_{(m-1)\ell+(m-1)}, \\
& v_{(m-1)+1},\ldots,v_{(m-1)+(m-1)},\ldots,v_{(s-2)(m-1)+1},\ldots,v_{(s-2)(m-1)+(m-1)}\rangle \\
= \; & A_{2,0}+A_{3,0}+\cdots+A_{s-1,0}.
\end{aligned}$$

Consider further intersection:

$$
\begin{aligned}
& (A_{2,0}+A_{3,0}+\cdots+A_{s-1,0}) \cap (A_{1,1}+A_{2,1}+A_{3,0}\cdots+A_{s-1,0}) \\
= \; & (A_{2,0}+A_{3,0}+\cdots+A_{s-1,0}) \cap (A_{2,1}+A_{3,0}\cdots+A_{s-1,0}) \\
= \; & v_{(m-1)+1},\ldots,v_{(m-1)+(m-1)},\ldots,v_{(s-2)(m-1)+1},\ldots,v_{(s-2)(m-1)+(m-1)}\rangle \\
& \cap\langle v_{(m-1)+1}+v_1, v_{(m-1)+2}+v_2,\ldots,v_{(m-1)+(m-1)}+v_{m-1}, \\
& v_{2(m-1)+1},\ldots,v_{2(m-1)+(m-1)},\ldots,v_{(s-2)(m-1)+1},\ldots,v_{(s-2)(m-1)+(m-1)}\rangle \\
= \; & \langle v_{2(m-1)+1},\ldots,v_{2(m-1)+(m-1)},\ldots,v_{(s-2)(m-1)+1},\ldots,v_{(s-2)(m-1)+(m-1)}\rangle \\
= \; & A_{3,0}+A_{4,0}+\cdots+A_{s-1,0}.
\end{aligned}
$$

Similarly, we find

$$
\begin{aligned}
& (A_{3,0}+\cdots+A_{s-1,0}) \cap (A_{1,1}+A_{2,0}+A_{3,1}+A_{4,0}+\cdots+A_{s-1,0}) \\
= \; & (A_{3,0}+\cdots+A_{s-1,0}) \cap (A_{2,0}+A_{3,1}+A_{4,0}+\cdots+A_{s-1,0}) \\
= \; & A_{4,0}+\cdots+A_{s-1,0}.
\end{aligned}
$$

Clearly, this process can further be iterated so that we eventually get $\{0\}$ as the intersection.

Case 3: Fusing $\mathcal{L}_1,\ldots,\mathcal{L}_{k-1},\mathcal{L}_{k+1},\ldots,\mathcal{L}_s$ for all $k\in\{2,3,\ldots,s-2,s-1\}$.

We claim that

$$
\bigcap_{\substack{(j_1,\ldots,j_{k-1},j_{k+1},\ldots,j_s)\\ \in\{0,1,\ldots,p-1\}^{s-1}}} \left(A_{1,j_1}+\cdots+A_{k-1,j_{k-1}}+A_{k+1,j_{k+1}}+\cdots+A_{s,j_s}\right)=\{0\}
$$

Define an automomorphism Φ of $\mathcal{G}$ as follows

$$
\Phi(v_i)=\begin{cases} v_{(s-1)(m-1)+j} & \text{if } i=(k-1)(m-1)+j,\ j=1,\ldots,m-1 \\ v_{(k-1)(m-1)+j} & \text{if } i=(s-1)(m-1)+j,\ j=1,\ldots,m-1 \\ v_i & \text{otherwise} \end{cases}
$$

Thus Φ interchanges

$$
\begin{aligned}
& v_{(k-1)(m-1)+1} \text{ with } v_{(s-1)(m-1)+1}, \\
& v_{(k-1)(m-1)+2} \text{ with } v_{(s-1)(m-1)+2}, \\
& \vdots \\
& v_{(k-1)(m-1)+(m-1)} \text{ with } v_{(s-1)(m-1)+(m-1)},
\end{aligned}
$$

and fixes the remaining generators of $\mathcal{G}$. We have

$$
\Phi(A_{i,j_i})=\begin{cases} A_{i,j_i} & \text{if } i\neq k,s \\ A_{s,j_k} & \text{if } i=k \\ A_{k,j_s} & \text{if } i=s \end{cases}
$$

From

$$
\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1})\\ \in\{0,1,\ldots,p-1\}^{s-1}}} \left(A_{1,j_1}+A_{2,j_2}+\cdots+A_{s-1,j_{s-1}}\right)=\{0\}
$$

in Case 2, we obtain

$$\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1})\\ \in\{0,1,\ldots,p-1\}^{s-1}}} \left(\Phi\left(A_{1,j_1}\right)+\Phi\left(A_{2,j_2}\right)+\cdots+\Phi\left(A_{s-1,j_{s-1}}\right)\right)=\{0\}$$

This gives

$$\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1})\\ \in\{0,1,\ldots,p-1\}^{s-1}}} \left(A_{1,j_1}+\cdots+A_{k-1,j_{k-1}}+\Phi\left(A_{k,j_k}\right)+A_{k+1,j_{k+1}}+\cdots+A_{s-1,j_{s-1}}\right)=\{0\}.$$

So we have

$$\bigcap_{\substack{(j_1,j_2,\ldots,j_{s-1})\\ \in\{0,1,\ldots,p-1\}^{s-1}}} \left(A_{1,j_1}+\cdots+A_{k-1,j_{k-1}}+A_{s,j_k}+A_{k+1,j_{k+1}}+\cdots+A_{s-1,j_{s-1}}\right)=\{0\},$$

which shows the claim. This completes the proof. □

7 Conclusion

We have presented a general construction of strongly aperiodic LS for elementary abelian p-groups. The existence of SALS has significantly extended the key space for LS-based cryptosystems, in particular for cryptosystem MST_3. Their favourable features would also enhance the security of those systems. Moreover, the question of existence of strongly aperiodic logarithmic signatures for abelian groups in general is a challenging and interesting problem that is worth studying.

References

[1] B. Baumeister and J.-H. de Wiljes, Aperiodic logarithmic signatures, *J. Math. Cryptol.* **6** (2012), 21–37.

[2] S. R. Blackburn, C. Cid, C. Mullan, Cryptanalysis of the MST_3 Public Key Cryptosystem, *J. Math. Cryptol.* **3** (2009), 321–338.

[3] D. Janiszczak, Konstruktion aperiodischer logarithmischer Signaturen elementarabelscher p-Gruppen und Untersuchung ihrer Faktorisierungseigenschaft, Diplomarbeit, Fakultät für Mathematik der Universität Duisburg-Essen, 2012.

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

[5] S. S. Magliveras, B. A. Oberg and A. J. Surkan, A New Random Number Generator from Permutation Groups, In *Rend. del Sem. Matemat. e Fis. di Milano* **LIV** *(1984)*, 203–223.

[6] S. S. Magliveras and N. D. Memon, The Algebraic Properties of Cryptosystem PGM, *J. of Cryptology* **5** (1992), pp. 167-183.

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

[8] S. S. Magliveras, P. Svaba, Tran van Trung and P. Zajac, On the security of a realization of cryptosystem MST_3, *Tatra Mt. Math. Publ.* **41** (2008), 1-13.

[9] P. Marquardt, P. Svaba and Tran van Trung, Pseudorandom number generators based on random covers for finite groups, *Des. Codes Cryptogr.* **64** (2012), 209–220

[10] A. S. Rybkin, Investigation of the cryptosystem MST_3 based on a Suzuki 2-group, *Discrete Math. Appl.* **25(3)** (2015), 157–177.

[11] R. Staszewski and Tran van Trung, Strongly aperiodic logarithmic signatures, *J. Math. Cryptol.* **7** (2013), 147–179.

[12] P. Svaba and Tran van Trung, Public key cryptosystem MST3: cryptanalysis and realization, *J. Math. Cryptol.* **4** (2010), 271–315.

[13] P. Svaba, Tran van Trung and P. Wolf, Logarithmic signatures for abelian groups and their factorization, *Tatra Mt. Math. Publ.* **57** (2013), 1–13.

[14] Sándor Szabó, Topics in Factorization of Abelian Groups, Birkhäuser Verlag, Basel - Boston - Berlin 2004.

[15] M. I. G. Vasco, A. I. P. del Pozo, P. T. Duarte, A note on the security of MST_3, *Des. Codes Cryptogr.* **55** (2010), 189–200.