Weak Keys in MST_1

Jens-Matthias Bohli[1], María Isabel González Vasco[2], Consuelo Martínez[2], and Rainer Steinwandt[1]

[1]Institut für Algorithmen und Kognitive Systeme, Arbeitsgruppe Systemsicherheit, Prof. Dr. Th. Beth, Universität Karlsruhe, 76128 Karlsruhe, Germany
bohli@ira.uka.de, steinwan@ira.uka.de

[2]Departamento de Matemáticas, Universidad de Oviedo, c/Calvo Sotelo, s/n, 33007 Oviedo, Spain
mvasco@orion.ciencias.uniovi.es
chelo@pinon.ccu.uniovi.es

Abstract

The public key cryptosystem MST_1 has been introduced in [9]. Its security relies on the hardness of factoring with respect to wild logarithmic signatures. To identify 'wild-like' logarithmic signatures, the criterion of being totally-non-transversal has been proposed.

We give tame totally-non-transversal logarithmic signatures for the alternating and symmetric groups of degree ≥ 5. Hence, basing a key generation procedure on the assumption that totally-non-transversal logarithmic signatures are 'wild like' seems critical. We also discuss the problem of recognizing 'weak' totally-non-transversal logarithmic signatures, and demonstrate that another proposed key generation procedure based on permutably transversal logarithmic signatures may produce weak keys.

Keywords: public key cryptography, cryptanalysis, group factorizations, logarithmic signatures, finite permutation groups

[2]Work partially supported by project BFM2001-3239-C03-01.

1 Introduction

Nowadays, most practically used public key systems are based on the hardness of factoring large integers or computing discrete logarithms in a suitable cyclic group. It is indeed of interest to identify other mathematical primitives for public key schemes, specially due to the existence of efficient quantum algorithms for the above mentioned problems (see [12]).

The public key scheme MST_2 from [9] is an interesting step in this direction: it can be seen as a generalization of the ElGamal scheme to not necessarily abelian finite groups. However, despite its theoretical attractiveness, it still has not been possible to give any example of a concrete realization besides the original ElGamal scheme. In [4] it is shown that a generalization of the original MST_2 framework allows a uniform description of several public key systems, like the braid group based system from [6] or the MOR schemes [10, 11].

In this contribution we focus on the other public key scheme proposed in [9]: MST_1. The security of this system relies on the difficulty of computing factorizations with respect to certain *logarithmic signatures* for finite groups. Logarithmic signatures have already been used in cryptography before, e. g., in the symmetric scheme PGM [8]. Unfortunately, it is still unclear how to derive concrete instances of MST_1. Some potential problems are addressed in [5]; namely, there it is proven that a *totally-non-transversal* logarithmic signature may provide a factorization that is easy to compute. However, precisely this type of logarithmic signatures is supplied by the key generation procedure for MST_1 considered in [9].

Here we demonstrate that totally-non-transversal logarithmic signatures can in fact be tame. In other words, knowing that a logarithmic signature is totally-non-transversal does by no means guarantee that it is suitable for being used as a key in MST_1. In Section 3 we explicitly construct such 'weak' logarithmic signatures for the alternating and symmetric groups of degree ≥ 5. To support our conviction that these logarithmic signatures are far from being scarce, we also give examples of minimal length.

In Section 4 we discuss the problem of recognizing certain tame totally-non-transversal logarithmic signatures (and hence certain weak keys). Eventually, in the last section it is demonstrated that another key generation procedure for MST_1, based on so-called permutably transversal logarithmic signatures (cf. [2]), may produce weak keys.

2 The public key cryptosystem MST_1

We start by refreshing some basic terminology about logarithmic signatures which essentially follows from [8, 9, 5].

Recall that every finite group can be seen as a subgroup of some symmetric group S_n, and thus regarded as a permutation group of degree n. A *logarithmic signature* describes a kind of unique factorization of the elements in a finite permutation group G.

Definition 2.1 *Let G be a finite permutation group. Next, denote by $\alpha = [\alpha_1, \ldots, \alpha_s]$ a sequence of length $s \in \mathbb{N}_0$ such that each α_i $(1 \leq i \leq s)$ is itself a sequence $\alpha_i = [\alpha_{i0}, \ldots, \alpha_{ir_i-1}]$ with $\alpha_{ij} \in G$ $(0 \leq j < r_i)$ and $r_i \in \mathbb{N}_0$. Then we call α a* logarithmic signature *for G if each $g \in G$ is represented uniquely as a product*

$$g = \alpha_{1j_1} \cdots \alpha_{sj_s} \tag{1}$$

with $\alpha_{ij_i} \in \alpha_i$ $(1 \leq i \leq s)$.
We refer to the sequences α_i, $i = 1, \ldots, s$, as blocks *of α and to the vector $r = (r_1, \ldots, r_s)$ as* type *of α. Also, we call the integer $\ell(\alpha) = \sum_{i=1}^{s} r_i$* length *of α. Finally, we denote the set of all logarithmic signatures for G by $\Lambda(G)$.*

A typical method for constructing a logarithmic signature for a finite permutation group G is the following: denote by id the identity element in G, and consider some subgroup chain

$$G = G_0 > G_1 > \cdots > G_s = \{\mathrm{id}\}.$$

Now take $\alpha = [\alpha_1, \ldots, \alpha_s]$ such that each α_i is a complete system of left coset representatives of G_{i-1} modulo G_i. Under suitable assumptions on the representation of the elements in α, the factorizations (1) with respect to such a logarithmic signature can be computed easily (cf. [8]) for arbitrary $g \in G$. The public key system MST_1 is based on the idea that there are also logarithmic signatures such that computing the factorizations (1) for any given $g \in G$ is a very difficult algorithmic task.

To give a more detailed description of MST_1 we first introduce some more notation: let G be a finite permutation group and $\alpha = [\alpha_1, \ldots, \alpha_s]$ a logarithmic signature for G. Say, $\alpha_i = [\alpha_{i0}, \ldots, \alpha_{ir_i-1}]$ $(1 \leq i \leq s)$, i. e., α is of type $r = (r_1, \ldots, r_s)$. For any natural number n, denote by $\mathbb{Z}_n$ the set of integers $\{0, 1, \ldots, n-1\}$. Then we can construct the mappings

$$\begin{array}{rccc} \lambda: & \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} & \longrightarrow & \mathbb{Z}_{|G|} \\ & (n_1, \ldots, n_s) & \longmapsto & \sum_{i=1}^{s} \left(n_i \cdot \prod_{j=1}^{i-1} r_j \right) \end{array} \quad \text{(“mixed radix repres.”)}$$

and

$$\begin{array}{rccc} \Theta_\alpha : & \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s} & \longrightarrow & G \\ & (n_1, \ldots, n_s) & \longmapsto & \alpha_{1n_1} \cdots \alpha_{sn_s} \end{array},$$

which are easily verified to be bijective. Thus, the functional composition of Θ_α and λ^{-1} yields a bijection

$$\begin{array}{rccc} \breve{\alpha} : & \mathbb{Z}_{|G|} & \longrightarrow & G \\ & n & \longmapsto & (\Theta_\alpha \lambda^{-1})(n) = \Theta_\alpha \left(\lambda^{-1}(n)\right), \end{array}$$

which plays an essential role in our setting. In fact, the security of the cryptosystem MST_1 relies on the assumption that inverting a certain mapping of this form is not feasible for the adversary. This motivates the following definitions (cf. [8]):

Definition 2.2 *Let G be a finite permutation group of degree n. Then we call two logarithmic signatures α, β for G* equivalent *if $\breve{\alpha} = \breve{\beta}$.*

Further on, we call a logarithmic signature α for G

- tame*, if $\breve{\alpha}^{-1}$ can be computed in polynomial time (of n);*
- supertame*, if $\breve{\alpha}^{-1}$ can be computed in time $\mathcal{O}(n^2)$;*
- wild*, if α is not tame.*

In a strict sense the (asymptotic) notions of wild and tame do only make sense when speaking about a family of groups. This imprecision will not cause problems in the sequel, as we will mainly consider families of groups (namely alternating and symmetric groups). Thus, we stick to the established terminology.

In the sequel, when writing down permutations in a symmetric group, we adopt the convention that the right-most permutation is applied first, i. e., for $\pi_1, \pi_2 \in S_n$ the product $\pi_1\pi_2$ is the permutation which maps each $1 \leq i \leq n$ to $(\pi_1 \circ \pi_2)(i) = \pi_1(\pi_2(i))$.

A logarithmic signature derived from a subgroup chain as described above is called *exact l-transversal.* The sequences constructed analogously by means of right coset representatives are called *exact r-transversals.* Similarly, one can construct *exact mixed transversals*, for which each block is either a complete sequence of left or right coset representatives of a quotient in the chain. The set of all exact l-, r-, or mixed transversal logarithmic signatures is referred to as the set of *exact transversal* logarithmic signatures for G and denoted by $\mathcal{E}(G)$. In the context of MST_1 also several other kinds of logarithmic signatures are of interest:

Definition 2.3 *A logarithmic signature α for a finite permutation group G is called*

- transversal*, if α is equivalent to a logarithmic signature of the same type in $\mathcal{E}(G)$;*
- non-transversal*, if it is not transversal;*
- permutably transversal*, if a transversal logarithmic signature can be obtained by permuting its blocks;*
- totally-non-transversal*, if none of its blocks is a coset of a non-trivial subgroup of G.*

The sets of all transversal, non-transversal, permutably transversal, and totally-non-transversal logarithmic signatures for a finite permutation group G are denoted by $\mathcal{T}(G)$, $\mathcal{NT}(G)$, $\mathcal{PT}(G)$, and $\mathcal{TNT}(G)$, respectively.
The following is a (toy) example of a logarithmic signature in $\mathcal{TNT}(S_4)$:

Example 2.4 *Let $\theta := [\theta_1, \theta_2, \theta_3]$, where the θ_i are sequences over S_4 defined as follows:*

$$\begin{aligned}
\theta_1 &:= [\mathrm{id}, (1,3,4,2)], \\
\theta_2 &:= [\mathrm{id}, (1,2), (1,2,4), (1,4)], \\
\theta_3 &:= [\mathrm{id}, (1,3), (2,3)].
\end{aligned}$$

Using a computer algebra system like GAP [3] or Magma [1], the sequence θ is easily verified to be a totally-non-transversal logarithmic signature for S_4.

It is convenient to introduce a canonical form for logarithmic signatures. For this we remind of the notion of a *sandwich* of a logarithmic signature:

Definition 2.5 *Denote by G some permutation group of degree n and let $\alpha = [\alpha_1, \dots, \alpha_s] \in \Lambda(G)$. Moreover, let $t_0 = t_s = \mathrm{id}$, $t_1, \dots, t_{s-1} \in G$ and set $\beta := [\beta_1, \dots, \beta_s]$ with $\beta_i := t_{i-1}^{-1}\alpha_i t_i$ $(1 \le i \le s)$. Then β is also a logarithmic signature for G, and we call β a* sandwich *of α.*

According to [8, Theorem 5.1], equivalent logarithmic signatures can now be characterized as follows:

Proposition 2.6 *Two logarithmic signatures of the same type are equivalent if and only if one is a sandwich of the other.*

Now, if we are given some logarithmic signature $\alpha = [\alpha_1, \ldots, \alpha_s]$ with

$$\alpha_i = [\alpha_{i0}, \ldots, \alpha_{i\,r_i-1}],$$

we can apply a sandwich with

$$(t_0, \ldots, t_s) = (\mathrm{id}, \alpha_{10}^{-1}, (\alpha_{10}\alpha_{20})^{-1}, \ldots, (\alpha_{10} \cdots \alpha_{s-1\,0})^{-1}, \mathrm{id})$$

to α. This results in an equivalent logarithmic signature where only in the right-most block, i. e. in $\beta_s := t_{s-1}^{-1}\alpha_s t_s$, the first element can differ from $\mathrm{id} \in G$. Such a logarithmic signature is said to be *l-canonical*. Analogously, one can construct an *r-canonical* equivalent to α. The justification for the name 'canonical' is given by the next proposition (see [2, Theorem 3.2 & Corollary 3.5]):

Proposition 2.7 *Let α be a logarithmic signature of type t. Then α has a unique l-canonical equivalent α^l of type t and a unique r-canonical equivalent α^r of type t. Moreover, if α is transversal, then α^l or α^r is exact transversal.*

To describe the setup of the MST_1 cryptosystem, let G be a finite permutation group, and assume that some supertame logarithmic signature η for G has been fixed. Both G and η are publicly known. By means of η to each $\alpha \in \Lambda(G)$ a permutation $\hat{\alpha} := \breve{\eta}^{-1}\breve{\alpha} \in S_{|G|}$ can be associated. Finally, the public and private key data are as follows:

Public key: Alice publishes a pair $(\alpha, \beta) \in \Lambda(G) \times \Lambda(G)$ such that α is wild and β is tame.

Secret key: Alice knows a (short) sequence $[\theta_1, \ldots, \theta_k] \in \mathcal{T}(G)^k$ such that

$$\hat{\beta}^{-1}\hat{\alpha} = \hat{\theta}_1 \cdots \hat{\theta}_k.$$

Encryption: to send the plaintext $m \in \mathbb{Z}_{|G|}$ to Alice, Bob transmits the ciphertext

$$c = \hat{\beta}^{-1}\hat{\alpha}(m) \in \mathbb{Z}_m.$$

Decryption: Alice recovers (in polynomial time) the plaintext

$$m = \hat{\alpha}^{-1}\hat{\beta}(c) = \hat{\theta}_k^{-1} \cdots \hat{\theta}_1^{-1}(c).$$

Theoretically, the above scheme is rather appealing, but for deriving concrete instances one has to clarify how precisely the parameters in the above description should be chosen. In particular, a key generation procedure for producing private key/public key pairs is required. So far these problems are still unsolved, but the authors of MST_1 make several suggestions in this direction.

A key point is the construction of the public wild logarithmic signature α along with a trapdoor (the factorization into the tame logarithmic signatures θ_i $(1 \leq i \leq k)$). For deciding whether a given logarithmic signature $\alpha \in \Lambda(G)$ is 'wild-like', the key generation procedure described in [9] tests whether $\alpha \in \mathcal{TNT}(G)$ holds. In the next section we show that this criterion is rather critical; namely, we prove that totally-non-transversal logarithmic signatures can be tame. If such a logarithmic signature is used in Alice's public key, then an attacker can decrypt arbitrary messages without having to know Alice's trapdoor information.

3 Tame totally-non-transversal signatures

It is well-known that under suitable assumptions transversal logarithmic signatures are tame (cf. [8, 9]). Therefore, intuitively a wild logarithmic signature should be 'far from being transversal'. In the definition of totally-non-transversal logarithmic signatures this idea is reflected in the requirement that not a single block is allowed to be a coset of a non-trivial subgroup.

However, this approach is rather critical: let $\alpha = [\alpha_1, \ldots, \alpha_s]$ be an exact transversal logarithmic signature for some finite permutation group G with $\alpha_i \neq G$ for all $i \in \{1, \ldots, s\}$. Then we know that there exists an index $i \in \{1, \ldots, s\}$, so that the block α_i is a non-trivial subgroup of G. In general we cannot expect that any block α_j with $i \neq j$ is a coset of some non-trivial subgroup of G, too. Hence, let us suppose only the block α_i prevents $\alpha \in \mathcal{E}(G)$ from being totally-non-transversal.
Now assume that $\gamma = [\gamma_1, \ldots, \gamma_t] \in \mathcal{TNT}(\alpha_i)$ where $1 < |\gamma_j| < |\alpha_i|$ $(1 \leq j \leq t)$. Then

$$\tilde{\alpha} := [\alpha_1, \ldots, \alpha_{i-1}, \gamma_1, \ldots, \gamma_t, \alpha_{i+1}, \ldots, \alpha_s]$$

is in $\mathcal{TNT}(G)$, but of course if $|\alpha_i|$ is small, inverting $\tilde{\alpha}$ is easy. Namely, to factor $g \in G$ with respect to $\tilde{\alpha}$ we can proceed as follows:

1. After *fusing* the blocks $\gamma_1, \ldots, \gamma_t$ to a single block α_i we can easily

determine the factorization $g = \alpha_{1j_1} \cdots \alpha_{sj_s}$ of g with respect to the exact transversal logarithmic signature α.

2. Replacing α_{ij_i} in the latter product with the factorization of α_{ij_i} with respect to γ yields the desired factorization of g. If $|\alpha_i|$ is small, then factoring along γ can be done through a brute-force approach.

The above discussion illustrates that the difference between a transversal and a totally-non-transversal logarithmic signature can be extremely 'local'. In the following proposition we apply this observation to the alternating and symmetric groups: by means of the subgroup chain

$$A_n > A_{n-1} > \cdots > A_5 > \{\mathrm{id}\},$$

we construct tame logarithmic signatures in $\mathcal{TNT}(A_n)$ and $\mathcal{TNT}(S_n)$ for all $n \geq 5$.

Proposition 3.1 *For $n \geq 5$ there are tame totally-non-transversal logarithmic signatures for all alternating groups A_n and symmetric groups S_n.*

Proof. To prove the statement for the alternating groups A_n, $n \geq 5$ we define, for each $5 < i \leq n$, a sequence $\beta_i = [\beta_{i0}, \ldots, \beta_{i\,i-1}]$ with $\beta_{ij} \in A_i$, $j = 0, \ldots, i-1$, in the following way:

$$\beta_{ij} := \begin{cases} \mathrm{id} & \text{, if } j = 0 \\ (2,3,\ldots,i)^j & \text{, if } 0 < j < i-1 \text{ and } (2,3,\ldots,i)^j \in A_i \\ (2,3,\ldots,i)^j(2,3) & \text{, if } 0 < j < i-1 \text{ and } (2,3,\ldots,i)^j \notin A_i \\ (2,3)(1,i) & \text{, if } j = i-1. \end{cases}$$

It is easy to see that the elements in β_i cannot form a complete coset of a non-trivial subgroup of A_i: we have $\mathrm{id} \in \beta_i$, and hence β_i had to be a group. But as for $k \in \{0,1\}$ the sequence β_i does not contain the product

$$(2,3,\ldots,i)(2,3)^k \cdot (2,3)(1,i) = \begin{cases} (1,2,4,5,\ldots,i) & \text{, if } k = 0 \\ (1,\ldots,i) & \text{, if } k = 1 \end{cases}$$

this is impossible. Next, suppose that two (left) cosets $\beta_{ij_1}A_{i-1}$ and $\beta_{ij_2}A_{i-1}$ coincide for some $0 \leq j_1 < j_2 < i$. The case $j_1 = 0$ cannot arise, as β_{ij_2} does not stabilize i for $0 < j_2 \leq i-1$. So for some $0 < j_1 < j_2 < i$ and $k_1, k_2 \in \{0,1\}$ one of the following situations must arise:

- $(2,3)^{k_1}(2,3,\ldots,i)^{j_2-j_1}(2,3)^{k_2} \in A_{i-1}$ or

- $(2,3,\ldots,i)^{j_1}(2,3)^{k_1} \cdot (2,3)(1,i) \in A_{i-1}$

But i is not stabilized by any of these permutations, so this is impossible. Consequently, β_i is a complete system of (left) coset representatives of A_{i-1} in A_i and $\beta := [\beta_n, \beta_{n-1} \ldots, \beta_6, A_5]$ is an exact (left) transversal logarithmic signature for A_n. In particular, β is tame, and replacing (independently of n) the $5!/2 = 60$ elements in the last block with the logarithmic signature from [8, Figure 5] (which is in $\mathcal{TNT}(A_5)$) yields a tame logarithmic signature in $\mathcal{TNT}(A_n)$.

Now it is easy to construct from β a tame logarithmic signature in $\mathcal{TNT}(S_n)$ for each $n \geq 5$: the sequence $[\mathrm{id}, (1,2)^n(1,\ldots,n)]$ is a complete set of (left) coset representatives of S_n modulo A_n, and it is obviously not a group. Thus, for each $n \geq 5$, we obtain a tame logarithmic signature in $\mathcal{TNT}(S_n)$ from the sequence

$$\alpha := \big[[\mathrm{id}, (1,2)^n(1,\ldots,n)], \beta_n, \beta_{n-1}, \ldots, \beta_6, A_5\big],$$

just by replacing A_5 with the logarithmic signature from [8, Figure 5]. $\square$

Remark 3.2 *Note that for the symmetric groups S_n we could easily have given a construction similar to the one for A_n, taking, for instance, blocks $\alpha_i = [\alpha_{i0}, \ldots, \alpha_{i\,i-1}]$, $\alpha_{ij} \in S_i, j = 0, \ldots, i-1$, with*

$$\alpha_{ij} := \begin{cases} (2,3,\ldots,i)^j & , \text{ if } 0 \leq j < i-1 \\ (1,i) & , \text{ if } j = i-1 \end{cases}$$

and building

$$\tilde{\alpha} := [\alpha_n, \alpha_{n-1}, \ldots, \alpha_5, \theta_1, \theta_2, \theta_3],$$

where $[\theta_1, \theta_2, \theta_3]$ is the logarithmic signature in $\mathcal{TNT}(S_4)$ from Example 2.4. In fact, this method would give us a tame logarithmic signature in $\mathcal{TNT}(S_n)$ for each $n \geq 4$.

Remark 3.3 *Proposition 3.1 should be seen as an asymptotic result; i. e., what we actually give is a family $\Gamma = \{\gamma_n\}_{n\geq 5}$ of totally-non-transversal logarithmic signatures for the family of groups $\{A_n\}_{n\geq 5}$ resp. $\{S_n\}_{n\geq 5}$. The* tameness *of the logarithmic signatures is stated by the existence of an algorithm $\mathcal{A}$ which on input of a permutation $\sigma \in A_m$ resp. $\sigma \in S_m$ for some $m \geq 5$ outputs a factorization of σ with respect to γ_m in time* $\mathrm{poly}(m)$.

For cryptographic purposes, it is often desirable to use *short* logarithmic signatures. In [5] the following lower bound for the length of a logarithmic signature is given:

Remark 3.4 *Let G be a finite permutation group and $|G| = \prod_{j=1}^{t} p_j^{a_j}$ the prime factorization of the order of G (with $p_1, \ldots, p_t$ the different prime factors of $|G|$). Then for any $\alpha \in \Lambda(G)$ we have $\ell(\alpha) \geq \sum_{j=1}^{t} a_j p_j$.*

A construction of *minimal length* logarithmic signatures (i. e., logarithmic signatures for which the previous bound is sharp) for solvable and symmetric groups is given in [5]. The sharpness of the bound for alternating groups and for groups $PSL_2(q)$ is proven in [7].

Here we show that for $n \geq 5$ constructing tame minimal length logarithmic signatures in $\mathcal{TNT}(A_n)$ and $\mathcal{TNT}(S_n)$ is also possible.

Proposition 3.5 *For $n \geq 5$ there are tame totally-non-transversal minimal length logarithmic signatures for all alternating groups A_n and symmetric groups S_n.*

Proof. Let $[\theta_1, \theta_2, \theta_3]$ be the following sequence:

$$\begin{aligned}
\theta_1 &:= [(2,3,4),(1,2,4,5,3),(1,2,3,5,4),(1,5)(2,4),(2,5,3)],\\
\theta_2 &:= [\mathrm{id},(1,2)(4,5),(1,3,2,4,5),(1,3)(2,5)],\\
\theta_3 &:= [\mathrm{id},(2,3)(4,5),(1,4,2,5,3)].
\end{aligned}$$

With a computer algebra system it is easy to verify that θ is a (tame) minimal length logarithmic signature in $\mathcal{TNT}(A_5)$. Now we proceed by induction on n, namely, given a tame minimal length logarithmic signature in $\mathcal{TNT}(A_{n-1})$, $\theta = [\theta_1, \ldots, \theta_s]$, we construct a tame minimal length logarithmic signature in $\mathcal{TNT}(A_n)$, for $n > 5$.

Suppose $n = p_1 \cdots p_k$, with p_i, $i = 1, \ldots, k$, not necessarily distinct primes. Consider the sequence of blocks $[\beta_1, \ldots, \beta_k]$ defined as follows:

$$\beta_1 \;:=\; \left[\mathrm{id}, \beta_{1,1}, \ldots, \beta_{1,p_1-2}, (n-2, p_1-1, n)\right]$$

where $\beta_{1,j} := (j+1, j, n) \quad (1 \leq j \leq p_1 - 2)$, and for $i = 2, \ldots, k$ we set

$$\beta_i := \left[\mathrm{id}, \beta_{i,1}, \ldots, \beta_{i,p_i-2}, \beta_{i,p_i-1}\right],$$

where for $j = 1, \ldots, p_i - 2$

$$\beta_{i,j} := \big((j+1)p_1 \cdots p_{i-1}, jp_1 \cdots p_{i-1}, n\big) \circ \prod_{1 \leq l < p_1 \cdots p_{i-1}} \big((j+1)p_1 \cdots p_{i-1}, jp_1 \cdots p_{i-1} + l, l\big)$$

and

$$\beta_{i,p_i-1} := \big(n-1, (p_i - 1)p_1 \cdots p_{i-1}, n\big) \circ \prod_{1 \leq l < p_1 \cdots p_{i-1}} \big(p_1 \cdots p_i, (p_i - 1)p_1 \cdots p_{i-1} + l, l\big).$$

It is easy to check that $\alpha = [\theta_1, \ldots, \theta_s, \beta_1, \ldots, \beta_k]$ is a logarithmic signature for A_n. Just recall that $A_n = \bigcup_{i=1}^{n} A_{n-1} g_i$, where g_i is any even permutation such that $g_i(i) = n$ for $i = 1, \ldots, n$, and observe that each product of the form $\beta_{1j_1} \cdots \beta_{kj_k}$ with $\beta_{ij_i} \in \beta_i$ defines an even permutation that maps a different $i \in \{1, \ldots, n\}$ to n (cf. [5, proof of Proposition 3.2]). By construction α has minimal length.
To verify it is also totally-non-transversal, we only have to check that the new blocks $\beta_1, \ldots, \beta_k$ are not cosets of any proper subgroup of A_n. That is straightforward to see, as each of the blocks contains the identity element and is not a group:

- β_1: as $|\beta_1| = p_1$ is a prime and (up to the identity) all elements in β_1 are 3-cycles, β_1 being a group would imply $|\beta_1| = 3$ and $\beta_{1,1} = (2, 1, n)$—in contradiction to $n - 2 > 3$.

- β_i $(i = 2, \ldots, k)$: if $p_i \neq 2$ or $i < k$, the permutation $\beta_{i,1}$ maps $p_1 \cdots p_{i-1}$ to n, and no permutation in β_i maps n to $p_1 \cdots p_{i-1}$. If both $p_i = 2$ and $i = k$, we conclude that $p_1 \cdots p_{i-1} \geq 3$ and $\beta_{k,1}(2) = p_1 \cdots p_{i-1} + 1$. However, $\beta_{k,1}(p_1 \cdots p_{i-1} + 1) = 1$, i. e., $\beta_{k,1}^2 \neq \mathrm{id}$, and thus $\beta_k = [\mathrm{id}, \beta_{k,1}]$ is not a group.

Moreover, analogously as in the proof of Proposition 3.1 we can reason that α is tame. Thus, the statement holds for A_n.

To get a minimal length logarithmic signature in $\mathcal{TNT}(S_n)$, it suffices to append the block $[\mathrm{id}, (1, 2)^n (1, \ldots, n)]$ to a tame minimal length logarithmic signature in $\mathcal{TNT}(A_n)$. □

Of course, the alternating and symmetric groups are just examples, and one can think of identifying tame totally-non-transversal signatures in other families of groups, too. We do not elaborate on this topic here, as in our opinion already the above discussion gives ample evidence that being totally-non-transversal is not really a suitable criterion for characterizing 'wild-like' logarithmic signatures. In the next section we explore the question of how to recognize at least some 'weak' logarithmic signatures (and hence keys) in MST_1.

4 Recognizing weak keys

Let $\alpha = [\alpha_1, \ldots, \alpha_s] \in \Lambda(G)$ for some finite permutation group G. Denoting the type of α by $r = (r_1, \ldots, r_s)$, for $1 \leq i \leq j \leq s$ we define $M^{\alpha}_{i,j} \in \{0, 1\}$ as follows:

$$M^{\alpha}_{i,j} := \begin{cases} 1, & \text{if } \alpha_i \cup \cdots \cup \alpha_j \text{ generates a subgroup of order } r_i \cdots r_j \\ 0, & \text{otherwise.} \end{cases}$$

For computing the values $M^{\alpha}_{i,j}$ we can use the method suggested in [2, Section 3.5] for computing the values $M[i, j]$ considered there. The key observation is that for small values of $r_i + \cdots + r_j$, the order of the subgroup generated by $\alpha_i \cup \cdots \cup \alpha_j$ can be computed efficiently. In particular, if $\ell(\alpha)$ is not 'too large' (having in mind that α is supposed to serve as part of the public key in MST_1, this assumption seems reasonable), we can determine the elements $M^{\alpha}_{i,j}$ $(1 \leq i \leq j \leq s)$ efficiently. The use of these values is summarized in the next somewhat technically looking remark (cf. [2, Section 3.5]):

Remark 4.1 *Let $\alpha = [\alpha_1, \ldots, \alpha_s] \in \Lambda(G)$ for some finite permutation group G. Then we have $\alpha \in \mathcal{E}(G)$ if and only if there is a sequence of pairs $(i_1, j_1), \ldots, (i_s, j_s) \in \{1, \ldots, s\}^2$ such that $M^{\alpha}_{i_k,j_k} = 1$ $(1 \leq k \leq s)$, $i_1 = j_1$, and for all $1 < k \leq s$ we have $(i_k, j_k) \in \{(i_{k-1} - 1, j_{k-1}), (i_{k-1}, j_{k-1} + 1)\}$.*

Proof. Let $\alpha \in \mathcal{E}(G)$, and let

$$G = G_0 > G_1 > \cdots > G_s = \{\mathrm{id}\}$$

be the subgroup chain corresponding to α. Then some block α_{i_1} of α is the group G_{s-1}, and consequently we have $M^{\alpha}_{i_1,i_1} = 1$. If $s = 1$, then we are done. Otherwise one of the following cases must hold:

- $i_1 < s$ and α_{i_1+1} is a right-transversal of α_{i_1} in the subgroup generated by $\alpha_{i_1} \cup \alpha_{i_1+1}$ (G_{s-2});

- $1 < i_1$ and α_{i_1-1} is a left-transversal of α_{i_1} in the subgroup generated by $\alpha_{i_1-1} \cup \alpha_{i_1}$ (G_{s-2}).

Setting $(i_2, j_2) := (i_1, i_1 + 1)$ resp. $(i_2, j_2) := (i_1 - 1, i_1)$ accordingly, we have $M^a_{i_2,j_2} = 1$ as required. If $s = 2$ then we are done, and for $s > 2$ the definition of an exact transversal logarithmic signature guarantees that we can repeat the above argument with the group $\alpha_{i_1} = G_{s-1}$ being replaced by the group $\alpha_{i_2} \cdot \alpha_{j_2} = G_{s-2}$: in the construction of α either α_{j_2+1} must have served as right-transversal of $\alpha_{i_2} \cdot \alpha_{j_2}$ or α_{i_2-1} must have served as left-transversal of $\alpha_{i_2} \cdot \alpha_{j_2}$. Defining (i_3, j_3) acordingly and going on in this way, we finally obtain a sequence $(i_1, j_1), \ldots, (i_s, j_s)$ as specified in the remark.

Now assume we are given a sequence $(i_1, j_1), \ldots, (i_s, j_s)$ as specified in the remark. Then we know that α_{i_1} is a group. Next, if $(i_2, j_2) = (i_1 - 1, i_1)$, then the residue classes $g\alpha_{i_1}$ $(g \in \alpha_{i_2})$ must be pairwise different: as α is a logarithmic signature we have

$$\alpha_{i_1-1} \cdot \alpha_{i_1} = \biguplus_{g \in \alpha_{i_1-1}} g\alpha_{i_1}.$$

Moreover, from $M^\alpha_{i_1-1,i_1} = 1$ we know that $\alpha_{i_1-1} \cdot \alpha_{i_1}$ is a group. Similarly, for $(i_2, j_2) = (i_1, i_1 + 1)$, we identify α_{i_1+1} as right-transversal of α_{i_1} in the group $\alpha_{i_1} \cdot \alpha_{i_1+1}$. In the same way, for $s > 2$ we next recognize α_{i_3} or α_{j_3} as left- resp. right-transversal of $\alpha_{i_2} \cdot \alpha_{j_2}$ in $\alpha_{i_3} \cdots \alpha_{j_3}$: the disjointness of the cosets follows from α being a logarithmic signature, and $M^\alpha_{i_3,j_3} = 1$ guarantees that $\alpha_{i_3} \cdots \alpha_{j_3}$—the union of the cosets—is a group. Continuing in this way with $(i_4, j_4), \ldots, (i_s, j_s)$, we finally identify α as an element of $\mathcal{E}(G)$. $\square$

If we write down the values $M^\alpha_{i,j}$ for an exact transversal logarithmic signature α in matrix form, the above lemma guarantees the existence of a continuous 'staircase of 1's' starting at the diagonal element $M^\alpha_{i_1,j_1}$ and ending in the upper right corner $M^\alpha_{i_s,j_s} = M^\alpha_{s,1}$:

Example 4.2 *Using the left-transversal* $\alpha_1 := [\mathrm{id}, (1,5), (2,5), (3,5), (4,5)]$ *of* S_4 *in* S_5*, the right-transversal* $\alpha_4 := [\mathrm{id}, (1,2,3,4)]$ *of* A_4 *in* S_4*, and the left-transversal* $\alpha_2 := [\mathrm{id}, (1,2)(3,4), (1,3,4), (2,3,4)]$ *of* A_3 *in* A_4*, we obtain an exact transversal logarithmic signature* $\alpha := [\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ *of* S_5 *where the third block* $\alpha_3 := A_3$ *is a group. The following table depicts the corresponding* *values of $M^{\alpha}_{i,j}$, and the 'staircase of 1's' is clearly visible:*

$i \diagdown j$	1	2	3	4
1	0	0	0	**1**
2		0	**1**	**1**
3			**1**	0
4				0

On the other hand, if for some logarithmic signature α we have such a 'staircase from a diagonal element to the upper right corner', then we know that α is exact transversal. So assume that we have computed the values $M^{\alpha}_{i,j}$ of some totally-non-transversal logarithmic signature α in l- or r-canonical form. Then we know that all 'diagonal entries' $M^{\alpha}_{i,i}$ must vanish, but nevertheless large parts of the 'staircase' can be present already. In fact, by looking at the values $M^{\alpha}_{i,j}$ in more detail we may find some blocks that can be fused to close the gaps in the 'staircase':

Example 4.3 *The following logarithmic signature $\alpha = [\alpha_1, \ldots, \alpha_7]$ can easily be verified to be in $\mathcal{TNT}(S_7)$:*

$$\begin{aligned}
\alpha_1 &:= [\mathrm{id}, (1,7), (2,7), (3,7), (4,7), (5,7), (6,7)], \\
\alpha_2 &:= [\mathrm{id}, (1,3)(2,6), (1,5)(4,6)], \\
\alpha_3 &:= [\mathrm{id}, (1,2,6)], \\
\alpha_4 &:= [\mathrm{id}, (1,5), (2,5), (3,5), (4,5)], \\
\alpha_5 &:= [\mathrm{id}, (1,3,4,2)], \\
\alpha_6 &:= [\mathrm{id}, (1,2), (1,2,4), (1,4)], \\
\alpha_7 &:= [\mathrm{id}, (1,3), (2,3)].
\end{aligned}$$

Using a computer algebra system, the corresponding values $M^{\alpha}_{i,j}$ can be determined easily:

$i \diagdown j$	1	2	3	4	5	6	7
1	0	0	0	0	0	0	**1**
2		0	0	0	0	0	**1**
3			0	0	0	0	0
4				0	0	0	**1**
5					0	0	**1**
6						0	0
7							0

As $M^{\alpha}_{2,7} = 1$, we can 'eliminate' the gap $M^{\alpha}_{3,7} = 0$ by fusing the blocks α_2 and α_3 to a single block $\tilde{\alpha}_2 := [\alpha_{2i}\alpha_{3j} : 1 \le i \le 3, 1 \le j \le 2]$ of size $|\alpha_2| \cdot |\alpha_3| = 6$. Analogously, to get rid of the values $M^{\alpha}_{6,7} = 0$ and $M^{\alpha}_{7,7} = 0$, we can fuse the blocks α_5, α_6, and α_7 to

$$\tilde{\alpha}_4 := [\alpha_{5i}\alpha_{6j}\alpha_{7k} : 1 \le i \le 2, 1 \le j \le 4, 1 \le k \le 3]$$

of size 24. Permuting the elements in $\tilde{\alpha}_2$ and $\tilde{\alpha}_4$ accordingly, the resulting signature $\tilde{\alpha} := [\tilde{\alpha}_1, \ldots, \tilde{\alpha}_4]$ (where $\tilde{\alpha}_1 := \alpha_1$, $\tilde{\alpha}_3 := \alpha_4$) is both equivalent to α and exact transversal. The corresponding values $M^{\tilde{\alpha}}_{i,j}$ are depicted below:

$i \diagdown j$	1	2	3	4
1	0	0	0	**1**
2		0	0	**1**
3			0	**1**
4				**1**

To prevent an attacker from transforming a totally-non-transversal logarithmic signature α into an equivalent exact transversal logarithmic signature by just fusing some (small) blocks, one has to ensure 'that the gaps in the staircase are large enough'. We do not try to give a criterion for identifying 'truly wild' logarithmic signatures here, but the above discussion illustrates that the requirement of being totally-non-transversal is clearly not sufficient.

5 Permutably transversal signatures

In [2] C. Cusack explores the possibility of using sandwiches of permutably transversal logarithmic signatures as keys for MST_1. Such a logarithmic signature η is constructed as follows:

1. Obtain from a subgroup chain

$$G = G_0 > G_1 > \cdots > G_s = \{\mathrm{id}\}, \tag{2}$$

   an exact transversal logarithmic signature $\alpha = [\alpha_1, \ldots, \alpha_s] \in \mathcal{E}(G)$.

2. Transform α into a transversal logarithmic signature $\beta = [\beta_1, \ldots, \beta_s]$ for G through sandwiching α with some $t := (t_0, \ldots, t_s) \in G^s$ (where $t_0 = t_s = \mathrm{id}$).

3. Transform β into another logarithmic signature $\gamma \in \Lambda(G)$ by permuting the blocks of β with some $\sigma \in S_s$: $\gamma := [\beta_{\sigma^{-1}(1)}, \ldots, \beta_{\sigma^{-1}(s)}]$.
4. Finally, by sandwiching γ with some $u := (u_0, \ldots, u_s) \in G^s$ (where $u_0 = u_s = \mathrm{id}$) derive a logarithmic signature $\eta = [\eta_1, \ldots, \eta_s]$ for G.

Here we give some evidence that such logarithmic signatures provide, in principle, very few security guarantees. We restrict our attention to finite abelian groups, as non-abelian groups are already excluded in Cusack's proposal (see [2, Section 3.7]). Thus, the above constructed logarithmic signature η can be written in the form

$$\eta = [g_1\alpha_{\sigma^{-1}(1)}, \ldots, g_s\alpha_{\sigma^{-1}(s)}],$$

where $g_i \in G, (1 \le i \le s)$ such that $g_1 \cdots g_s = 1$.

Cusack does not make concrete suggestions on how to choose the abelian group; he only points out the possibility of using such a logarithmic signature η as a public key corresponding to the private key α, and thus letting σ and $(g_1, \ldots, g_1)$ be the trapdoor information.

However, by construction some block α_{i_1} of α is equal to the subgroup G_{s-1} of G. Consequently, η contains the block

$$\eta_{\sigma(i_1)} = g_{\sigma(i_1)}\alpha_{i_1}$$

and we can try to recover α_{i_1} by identifying an index $1 \le j_1 \le s$ such that $\eta_{j_1} \cdot \eta_{j_1 0}^{-1}$ is a group (where as usual $\eta_{j_1 0}^{-1}$ denotes the first element of η_{j_1}). Having found the correct index $j_1 = \sigma(i_1)$, we can continue in this manner to identify—up to a multiple in G_{s-2}—the transversal α_{i_2} of G_{s-1} in G_{s-2} used in the construction of α: the logarithmic signature η contains the block

$$\eta_{\sigma(i_2)} = g_{\sigma(i_2)}\alpha_{i_2}.$$

So after multiplying $\eta_{\sigma(i_2)}$ with $\eta_{\sigma(i_2)0}^{-1}$ we obtain a transversal of G_{s-1} in G_{s-2} that—possibly up to a multiple in G_{s-2}—coincides with α_{i_2}. Hence, to recover α_{i_2} (up to a multiple in G_{s-2}) we look for an index $1 \le j_2 \le s$ such that $\eta_{j_2} \cdot \eta_{j_2 0}^{-1}$ is a complete system of coset representatives of $G_{s-1} = \eta_{j_1} \cdot \eta_{j_1 0}^{-1}$ in the group generated by G_{s-1} and $\eta_{j_2} \cdot \eta_{j_2 0}^{-1}$. Equivalently, we can check whether the group generated by $\eta_{j_1} \cdot \eta_{j_1 0}^{-1}$ and $\eta_{j_2} \cdot \eta_{j_2 0}^{-1}$ is of size $|\eta_{j_1}| \cdot |\eta_{j_2}|$.

Having identified the correct index $j_2 = \sigma(i_2)$, we know in particular the group $G_{s-2} = \eta_{j_1}\eta_{j_1 0}^{-1} \cdot \eta_{j_2}\eta_{j_2 0}^{-1}$, and in case of $s > 2$ we can iterate the above procedure: next we try to recover the index i_3 of the transversal α_{i_3} of G_{s-2} in G_{s-3} used in the construction of α. For this we check for which $1 \leq j_3 \leq s$ the group generated by $\eta_{j_1} \cdot \eta_{j_1 0}^{-1}$, $\eta_{j_2}^{-1} \cdot \eta_{j_2 0}^{-1}$, and $\eta_{j_3} \cdot \eta_{j_3 0}^{-1}$ is of size $|\eta_{j_1}| \cdot |\eta_{j_2}| \cdot |\eta_{j_3}|$. Continuing in this way, we should finally obtain the complete subgroup chain (2). Moreover, each recovered transversal $\alpha'_{i_k} := \eta_{\sigma(i_k)} \cdot \eta_{\sigma(i_k)0}^{-1}$ $(1 \leq k \leq s)$ of G_{s-k+1} in G_{s-k} is equal to the 'corresponding original one' α_{i_k} up to a multiple in G_{s-k}.

For factoring a given $g \in G$ with respect to η we can now proceed as follows: start by factoring $g \cdot \prod_{k=1}^{s} \eta_{k0}^{-1}$ with respect to the exact transversal logarithmic signature $\alpha' := [\alpha'_{i_1}, \ldots, \alpha'_{i_s}]$ for G to obtain an expression of the form

$$g \cdot \prod_{k=1}^{s} \eta_{k0}^{-1} = \alpha'_{i_1 l_1} \cdots \alpha'_{i_s l_s} \quad (\text{with } \alpha'_{i_k l_k} \in \alpha'_{i_k}).$$

Then the factorization of g with respect to η can be obtained by multiplying each $\alpha'_{i_k l_k}$ with the corresponding $\eta_{\sigma(i_k)0}$ $(1 \leq k \leq s)$:

$$g = \prod_{k=1}^{s} \underbrace{\left(\eta_{j_k 0} \cdot \alpha'_{i_k l_k}\right)}_{\in \eta_{j_k}} \quad (\text{where } j_k = \sigma(i_k)).$$

Clearly, it could happen that we are already mistaken in our choice of j_1 in the first step, namely, that the logarithmic signature α has several blocks which are groups, and we pick one different from G_{s-1}. In the same way we may commit errors in the subsequent steps, and in some cases we may even end up with a subgroup chain different from (2).

A problem arises if at some step the above approach yields a subgroup chain that cannot be continued by means of one of the remaining blocks of η, and we must replace previously guessed blocks, say by a backtracking approach. If there are too many such backtracking steps, then the attack can become infeasible. However, in our experiments with groups of order $\approx 48!$ (the group size proposed in [9]) the above simple approach turned out to work quite satisfactorily: lacking a concrete suggestion, for our experiments we used several logarithmic signatures for the groups $(\mathbb{Z}/10\mathbb{Z})^{61}$ and $\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/48\mathbb{Z}$. Here deriving a corresponding exact transversal logarithmic signature with the above attack did not pose any difficulties. On the other hand, it is certainly possible that for some carefully chosen groups and logarithmic signatures our attack fails to succeed. Thus, our results do not imply that permutably transversal logarithmic signatures cannot be used at all for deriving keys in MST_1, but as it stands Cusack's construction does not guarantee acceptable security.

6 Conclusions

The above discussion illustrates various obstacles that arise when one attempts to derive practical instances of MST_1. As we already pointed out in [5], we believe that the appropriate (but unfortunately non-constructive) criterion for choosing logarithmic signatures as keys is that they are not only 'non-tame', but provide factorizations which are *almost always* hard to compute. Thus, we believe that the definition of wild adopted from [8] (Definition 2.2) should be modified in that sense.

In [9] the authors assume that totally-non-transversal logarithmic signatures provide hard factorizations. We give strong evidence against that assumption by supplying several examples of tame logarithmic signatures that are totally-non-transversal, including some of minimal length. Also, we demonstrate that several (sandwiches of) permutably transversal signatures can be inverted efficiently. Thus, we are rather pessimistic with respect to the existence of a reliable key generation procedure for MST_1 based on the above mentioned types of logarithmic signatures.

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma Algebra System I: The User Language, *Journal of Symbolic Computation*, vol. 24 (1997), pp. 235–265.

[2] C. A. Cusack, Group Factorizations in Cryptography, *PhD Thesis*, University of Nebraska, 2000.

[3] The GAP Team, GAP–Groups, Algorithms, and Programming, *Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, Univ. St. Andrews, Scotland*, (1997).

[4] M. I. González Vasco, C. Martínez and R. Steinwandt, Towards a Uniform Description of Several Group Based Cryptographic Primitives, sub-

mitted. See also *Cryptology ePrint Archive: Report 2002/048*, (2002). Available electronically at `http://eprint.iacr.org/2002/048/`.

[5] M. I. González Vasco and R. Steinwandt, Obstacles in Two Public Key Cryptosystems Based on Group Factorizations, to appear in *Cryptology*, Tatra Mountains Mathematical Publications vol. 25, (2002).

[6] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J.-S. Kang, C. Park, New Public-Key Cryptosystem Using Braid Groups, *Advances in cryptology — CRYPTO 2000*, M. Bellare, editor, Lecture Notes in Computer Science, vol. 1880, Springer, (2000), pp. 166–183.

[7] S.S. Magliveras, Secret- and Public-key Cryptosystems from Group Factorizations, to appear in *Cryptology*, Tatra Mountains Mathematical Publications vol. 25 (2002). Available electronically at `http://zeus.math.fau.edu/spyros/prints/tatras.ps`.

[8] S. S. Magliveras and N. D. Memon, Algebraic Properties of Cryptosystem PGM, *Journal of Cryptology*, vol. 5 (1992), pp.167–183.

[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, to appear in *Journal of Cryptology*.

[10] S. H. Paeng, K. C. Ha, J. H. Kim, S. Chee and C. Park, New Public Key Cryptosystem Using Finite Non Abelian Groups, *Advances in cryptology, Proc. CRYPTO 2001*, J. Kilian, editor, Lecture Notes in Computer Science, vol. 2139, Springer, (2001), pp. 470–485.

[11] S. H. Paeng, D. Kwon, K. C. Ha and J. H. Kim, Improved public key cryptosystem using finite non abelian groups, *Cryptology ePrint Archive: Report 2001/066*, (2001). Available electronically at `http://eprint.iacr.org/2001/066/`.

[12] P. W. Shor, Polynomial time algorithms for prime factorization and discrete logarithms on quantum computer, *SIAM Journal on Computing*, vol. 26, no. 5 (1997), pp. 1484–1509.