On Minimal Length Factorizations of Finite Groups

María Isabel González Vasco[†1], Martin Rötteler[‡ *],
and Rainer Steinwandt[‡]

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

[*]Centre for Applied Cryptographic Research
Department of Combinatorics and Optimization
University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1
mroetteler@cacr.math.uwaterloo.ca

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

Abstract

Logarithmic signatures are a special type of group factorizations, introduced as basic components of certain cryptographic keys. Thus, *short* logarithmic signatures are of special interest. We deal with the question of finding logarithmic signatures of *minimal length* in finite groups. In particular, such factorizations exist for solvable, symmetric, and alternating groups.

We show how to use the known examples to derive minimal length logarithmic signatures for other groups. Namely, we prove the existence of such factorizations for several classical groups and—in parts by direct computation—for all groups of order $< 175\,560$ ($= \mathrm{ord}(J_1)$, where J_1 is Janko's first sporadic simple group). Whether there exists a minimal length logarithmic signature for each finite group still remains an open question.

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

1 Introduction

Public Key Cryptography nourishes on hard mathematical problems which very often, but not exclusively, arise from number theory. Already in the early 80's several authors have explored the possibility of using group theoretical problems for cryptography [Wagner and Magyarik, 1985; Wagner, 1990; Magliveras, 1986]. In particular owing to Magliveras et al. there are various proposals for cryptographic schemes which make use of special factorizations (so-called *logarithmic signatures*) of finite groups [Magliveras, 1986; Magliveras et al., 2002]. Besides inspiring further cryptographic research [González Vasco and Steinwandt, 2002; González Vasco et al., 2003; Birget et al., 2002; Bohli et al., 2002], these factorizations are interesting mathematical objects in themselves. E. g., Hajós' work on Minkowski's conjecture illustrates that for abelian groups this kind of factorization arises in the study of high dimensional tilings (see [Stein and Szabó, 1994]).

Defined to be used as keys within a cryptographic scheme, the question of finding *short* logarithmic signatures arises naturally. But also the logarithmic signatures of abelian groups considered in Rédei's theorem (see, e. g., [Stein and Szabó, 1994]) are examples of logarithmic signatures of minimal possible length.

In this contribution we study the existence of *minimal length* logarithmic signatures for several families of finite groups: in Section 2 we give the basic definitions and notations; Section 3 details a (constructive) proof of the existence of minimal logarithmic signatures for solvable groups and recalls some other known constructions. Thereafter, we discuss how to extend these results to obtain new examples. From the arguments in Section 3, one can conclude that the smallest group for which a minimal length logarithmic signature does not exist (if there should be any!) must be a simple group. Hence, we devote Section 4 to studying several families of simple groups. We start by pointing out that there are suitable factorizations for $\mathrm{PSL}_2(q)$ and some other classical groups. Next we prove—in part through direct computation with a computer algebra system—that all finite groups of order $< 175\,560$ (the order of Janko's first sporadic simple group) allow for a minimal length logarithmic signature. Whether such a factorization exists for all finite groups is to the best of our knowledge still an open problem. Some suggestions on possible directions for further research conclude the paper.

2 Preliminaries

In a series of works, Magliveras et al. [Magliveras, 2002, 1986; Magliveras and Memon, 1992; Magliveras et al., 2002] have explored the possibility of building symmetric and asymmetric cryptosystems using certain group factorizations. We next recall the definition of logarithmic signatures, which are one of the mainstays of their research. For the basic related notions and results see, for instance, [Cusack, 2000].

Definition 2.1 *Let G be a finite 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*

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

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 integer $\ell(\alpha) := \sum_{i=1}^{s} r_i$ as* length *of α.*

Of course, for each group G there always exists a trivial logarithmic signature $\alpha := [[g \,|\, g \in G]]$ consisting of a single block. Being precise, we actually obtain $\mathrm{ord}(G)!$ 'different' logarithmic signatures in this way, as a block of a signature is an (ordered) sequence and not just a set. The distinction of whether a block is a sequence or a set is mainly motivated by the use of logarithmic signatures in the public key scheme MST_1 [Magliveras et al., 2002], and as the subsequent discussion concerns only the length of logarithmic signatures, we can w. l. o. g. ignore this distinction.

Let us look at a more interesting example for a logarithmic signature: assume we know a subgroup chain

$$G = G_0 > G_1 > \cdots > G_s = \{e_G\},$$

where e_G denotes the unit element in G. Now take $\alpha = [\alpha_i \mid i = 1, \ldots, s]$ a sequence such that each $\alpha_i = [\alpha_{ij} \mid j = 0, \ldots, [G_{i-1} : G_i] - 1]$ is a complete system of left coset representatives of G_{i-1} modulo G_i. It is easy to check that α is a logarithmic signature for G. Such logarithmic signatures are called *exact (left) transversal.* Analogously, one can use right coset representatives to derive *exact (right) transversal* logarithmic signatures.

It is in general a non-trivial problem to check whether a group has logarithmic signatures of a fixed length. Luckily, we have at least a lower bound depending on the group order (first given in [González Vasco and Steinwandt, 2002]), which allows us to recognize the *shortest* ones:

Remark 2.2 *Let G be a finite group and $\operatorname{ord}(G) = \prod_{j=1}^{k} p_j^{a_j}$ the prime factorization of the order of G (with $p_1, \ldots, p_k$ different prime numbers). Moreover, denote by $\mathcal{B}(G) := \sum_{j=1}^{k} a_j p_j$ the sum of the prime divisors of $\operatorname{ord}(G)$ counting multiplicity. Then for each logarithmic signature α for G we have*

$$\ell(\alpha) \geq \mathcal{B}(G). \tag{1}$$

In the remaining part of the paper we dwell on the problem of finding logarithmic signatures α for which the latter inequality is tight, i. e., where $\ell(\alpha) = \mathcal{B}(G)$ holds. Trivial examples are provided by the 'empty' logarithmic signature $\alpha^{\{e\}} := []$ (of length 0) for the trivial group $\{e\}$ and by the logarithmic signature $\alpha^{C_p} := [[g \,|\, g \in C_p]]$ for a cyclic group C_p of prime order p. In the next section, we want to look at some more interesting examples.

3 Some examples and construction techniques

We start by proving that the bound (1) is met for solvable groups (this result can also be found in [González Vasco and Steinwandt, 2002]).

Proposition 3.1 *Let G be a finite solvable group. Then there exists a logarithmic signature α for G of minimal length, i. e., such that $\ell(\alpha) = \mathcal{B}(G)$.*

Proof. Let G be a solvable group of order $\prod_{i=1}^{k} p_i$ with $p_1, \ldots, p_k$ not necessarily distinct prime numbers. As G is solvable, it allows for a composition series

$$\gamma :\equiv G = G_0 > G_1 > \cdots > G_k = \{e_G\}$$

where each $[G_{i-1} : G_i]$ is prime and $\prod_{i=1}^{k} [G_{i-1} : G_i] = \prod_{i=1}^{k} p_i$. Clearly, any exact transversal logarithmic signature derived from γ has length $\sum_{i=1}^{k} p_i$ and is thus of minimal length. $\square$

Remark 3.2 *For abelian groups there is an alternative construction which leads to a, in general different, minimal length logarithmic signature: let H be a cyclic group of order $\operatorname{ord}(H) = p^m$ for some prime p, and take a any* *generator of H. Then $\alpha = [\alpha_1, \ldots, \alpha_m]$ with $\alpha_i = [e_H, a^{p^{i-1}}, \ldots, a^{(p-1)p^{i-1}}]$ $(i = 1, \ldots, m)$ is a logarithic signature for H of length $m \cdot p = \mathcal{B}(H)$. Now just observe that the juxtaposition of minimal length logarithmic signatures for the cyclic p-primary factors of an abelian group G yields a minimal length logarithmic signature for G.*

As neither the definition of logarithmic signatures nor the proof of the bound in Remark 2.2 exploits the fact that a group allows for inverse elements, it might be worth pointing out that for finite commutative monoids minimal length factorizations do not always exist:

Example 3.3 *Using a computer algebra system, one easily checks by exhaustive search that there exist no 3-element subsets α_1, α_2 of the monoid $(\mathbb{Z}/9\mathbb{Z}, \cdot, 1)$ such that $\alpha_1 \cdot \alpha_2 = \mathbb{Z}/9\mathbb{Z}$ holds.*

Proofs of the tightness of the bound (1) for other families of groups often exploit peculiarities of the underlying group structure. This is the case for the symmetric and alternating groups; the existence of minimal length logarithmic signatures for the symmetric group S_n was first proven in [González Vasco and Steinwandt, 2002], and the tightness of the bound for the alternating group A_n was stated in [Magliveras, 2002]. Both proofs are constructive, and, moreover, in [Bohli et al., 2002] there are examples of minimal length logarithmic signatures for S_n and A_n which are in addition tame and totally-non-transversal (for the definitions of these notions see [Magliveras et al., 2002]).

The mentioned results for symmetric and alternating groups are in essence obtained by the same technique: given a permutation representation of a group G, identify a point $\mathtt{p}$ so that its stabilizer $G_{\mathtt{p}}$ can be factored through a minimal length logarithmic signature and such that there exists a complete set of representatives of G modulo $G_{\mathtt{p}}$ which moves $\mathtt{p}$ cyclically. Actually, analogously as in Remark 3.2, the underlying idea is to factor the group into a 'product of disjoint pieces' for which a minimal length logarithmic signature exists. For the case where the 'disjoint pieces' are finite groups, we can formalize this idea through the concept of a *knit product* of groups [Michor, 1989] (also called *Zappa-Szép product*).

Definition 3.4 *Let K and H be finite groups. Then we call two mappings $\kappa : H \times K \longrightarrow K$, $\hbar : K \times H \longrightarrow H$ an* automorphically knitted pair of actions for (K, H), *provided that*

1. *the mapping*

$$\begin{array}{rccc} \psi_\kappa : & H & \longrightarrow & S_K \\ & h & \longmapsto & \kappa_h(\cdot) := \kappa(h, \cdot) \end{array}$$

   is a group homomorphism,

2. *the mapping*

$$\begin{array}{rccc} \phi_\hbar : & K & \longrightarrow & S_H \\ & k & \longmapsto & \hbar_k(\cdot) := \hbar(k, \cdot) \end{array}$$

   is a group anti-homomorphism, namely $\hbar_{e_K} = \mathrm{id}_H$ *and* $\forall\, k_1, k_2 \in K :$ $\hbar_{k_1}\hbar_{k_2} = \hbar_{k_2 k_1}$,

3. $\forall\, k_1, k_2 \in K, h \in H :\ \kappa_h(k_1 k_2) = \kappa_h(k_1)\kappa_{\hbar_{k_1}(h)}(k_2)$, *and*

4. $\forall\, k_1, k_2 \in K, h \in H :\ \hbar_k(h_1 h_2) = \hbar_{\kappa_{h_2}(k)}(h_1)\hbar_k(h_2)$,

where S_X *denotes the group of permutations on the set* X *with functional composition as group operation, i. e., for* $\sigma, \tau \in S_X$ *we have* $(\sigma\tau)(x) := \sigma(\tau(x))$.

Definition 3.5 *Let* K*,* H *be groups, and* $(\kappa, \hbar)$ *an automorphically knitted pair of actions for* (K, H)*. Then the group defined over* $K \times H$ *with multiplication*

$$(k_1, h_1) \cdot (k_2, h_2) := (k_1 \kappa_{h_1}(k_2), \hbar_{k_2}(h_1)h_2),$$

and unit element (e_K, e_H) *is called* knit *or* Zappa-Szép product of K and H *and denoted by* $K \times_{(\kappa,\hbar)} H$.

Note that $K \times \{e_H\}$ and $\{e_K\} \times H$ are subgroups of $K \times_{(\kappa,\hbar)} H$, isomorphic respectively to K and H. Also, if $\psi_\kappa \equiv \mathrm{id}_K$ then $\{e_K\} \times H$ is a normal subgroup of $K \times_{(\kappa,\hbar)} H$, and thus we have a semidirect product (similarly, if $\phi_\hbar \equiv \mathrm{id}_H$). If both conditions hold, $K \times_{(\kappa,\hbar)} H$ is a direct product of $K \times \{e_H\}$ and $\{e_K\} \times H$. Actually, the Zappa-Szép product generalizes the notions of direct and semidirect product, and it is easy to see that Zappa-Szép products can be used to derive groups that allow for a minimal length logarithmic signature:

Proposition 3.6 *Let* G *be a Zappa-Szép product of two finite groups* K *and* H*, and suppose there are logarithmic signatures* α^K *for* K *and* α^H *for* H *such that* $l(\alpha^K) = \mathcal{B}(K)$ *and* $l(\alpha^H) = \mathcal{B}(H)$*. Then there exists a logarithmic signature* α^G *for* G *with* $l(\alpha^G) = \mathcal{B}(G)$.

Proof. Let α^K and α^H be of the form

$$\alpha^K = [\alpha_1^K, \ldots, \alpha_s^K], \quad \alpha_i^K = [\alpha_{i0}^K, \ldots, \alpha_{ir_i-1}^K] \ (i = 1, \ldots, s),$$

$$\alpha^H = [\alpha_1^H, \ldots, \alpha_t^H], \quad \alpha_i^H = [\alpha_{i0}^H, \ldots, \alpha_{il_i-1}^H] \ (i = 1, \ldots, t),$$

where $s, t \in \mathbb{N}_0$.
Then clearly

$$\alpha^G := [\alpha_1^G, \ldots, \alpha_s^G, \alpha_{s+1}^G, \ldots, \alpha_{s+t}^G]$$

where

$$\begin{aligned} \alpha_i^G &:= [(\alpha_{i0}^K, e_H), \ldots, (\alpha_{ir_i-1}^K, e_H)] \quad (i = 1, \ldots, s), \\ \alpha_{s+i}^G &:= [(e_K, \alpha_{i0}^H), \ldots, (e_K, \alpha_{il_i-1}^H)] \quad (i = 1, \ldots, t), \end{aligned}$$

is a minimal length logarithmic signature for G. □

Therefore, the bound in Remark 2.2 is in particular tight for any group G that is an extension of two groups K and H which have logarithmic signatures of minimal length—and thus for all direct and semidirect products of groups with that property. The same applies to groups which are (set theoretically) decomposable as the product of two disjoint proper subgroups meeting the bound of Remark 2.2.

Example 3.7 *In the following section we see that the groups* $\mathrm{PSL}_2(q)$ *have minimal length logarithmic signatures, and thus one concludes the tightness of (1) for the projective mock linear groups* $\mathrm{PML}_2(q)$ *(where* q *is an even power of an odd prime), for* $\mathrm{PSL}_2(q)$ *is a subgroup of* $\mathrm{PML}_2(q)$ *of index two. For further discussion on projective mock linear groups we refer to [Blackburn and Huppert, 1982, Chapter XI] and [Abhyankar, 1992].*

Starting again with $\mathrm{PSL}_2(q)$, one also verifies immediately the existence of minimal length logarithmic signatures for general linear groups $\mathrm{GL}_2(q)$:

Example 3.8 *As* $\mathrm{GL}_2(q)$ *is a cyclic extension of* $\mathrm{SL}_2(q)$*, and* $\mathrm{PSL}_2(q)$ *is* $\mathrm{SL}(2, q)$ *modulo its center, the bound (1) is tight for* $\mathrm{GL}_2(q)$*, too.*

Similarly, one easily sees that a finite group G has a minimal length logarithmic signature if it has a subnormal series whose factors do. Thus, for instance, the bound is tight for all nearly solvable groups[1]. As a result, if

[1] A group is *nearly solvable* if it admits a subnormal series so that each of its factors is a Möbius group; all Möbius groups are solvable, except from A_5.

there exists any finite group which does *not* have a minimal length logarithmic signature, then the smallest (w. r. t. the group order) counter-example must be a simple group. In the remaining part of this paper we therefore focus on simple groups.

4 Simple groups

Finite simple groups are indeed complex objects of study, but neatly classified [Gorenstein et al., 1998] and relatively well understood. Actually, much research has been devoted to the problem of factoring finite simple groups as a product of two proper subgroups; for a detailed survey see [Liebeck et al., 1990]. However, the factorizations we are dealing with are significantly different: they are comprised of blocks which impose a unique factorization in the sense of Definition 2.1 on the group, but the blocks are not necessarily subgroups and in fact may have no 'structure' at all. Of course, when trying to construct minimal length logarithmic signatures, we can in particular try to make use of known factorizations of finite simple groups and to exploit them for our purposes. To illustrate this approach, in the next section we consider factorizations of simple groups into a product of Sylow subgroups.

4.1 Factoring into a product of Sylow subgroups

In [Holt and Rowley, 1993] Rowley and Holt study which groups G can be written as a product $P_1 \cdots P_k$ where $p_1, \ldots, p_k$ are the different prime numbers dividing $\mathrm{ord}(G)$ and each P_i is a p_i-Sylow subgroup of G. They show that such a factorization is possible for several types of groups, including $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_3(q)$ for any prime power q. As all Sylow subgroups are solvable and therefore meet the bound (1), we conclude the tightness of (1) for all simple groups $\mathrm{PSL}_2(q)$ $(q > 3)$ and for all simple groups $\mathrm{PSL}_3(q)$ with $q \not\equiv 1 \pmod 3$ (and hence $\mathrm{PSL}_3(q) \simeq \mathrm{PGL}_3(q)$).[2]

Also for $q \equiv 1 \pmod 3$ such a factorization of $\mathrm{PSL}_3(q)$ into a product of Sylow subgroups—and thereby a logarithmic signature of minimal possible length—can be available: representing $\mathrm{PSL}_3(4)$ as subgroup $\langle \alpha, \beta \rangle \le S_{21}$

[2]For $\mathrm{PSL}_2(q)$ the existence of minimal length logarithmic signatures is also explored in [Magliveras, 2002]. However, the proof given there does not cover all choices of q. E. g., for $\mathrm{PSL}_2(13)$ no logarithmic signature can be obtained in this way.

with generators

$$\begin{aligned}\alpha &= (4,11,20)(5,15,17)(6,16,18)(7,14,13)(8,12,9)(10,21,19),\\ \beta &= (1,8,21,16,15,3,2)(4,10,20,18,17,9,7)(5,12,11,14,19,13,6),\end{aligned}$$

and choosing Sylow subgroups P_2, P_3, P_5, P_7 as given in Table 1, we can express $\mathrm{PSL}_3(4)$ as a product $\mathrm{PSL}_3(4) = P_7P_3P_2P_5$. At this, as always throughout the sequel, the product $(\sigma\pi) \in S_n$ of two permutations $\sigma, \pi \in S_n$ is understood to be the permutation that maps each $i \in \{1, \dots, n\}$ to $\pi(\sigma(i))$. The correctness of this factorization is easily checked by means of a computer algebra system like GAP [Team, 1997] or Magma [Bosma et al., 1997].

P_2	$=$	$\langle(2,15)(3,10,12,7)(4,11,21,13)(5,17)(6,8,20,9)(14,18,16,19),$ $(2,5)(3,19,8,13)(4,10,14,20)(6,21,7,16)(9,11,12,18)(15,17),$ $(2,5)(3,8)(4,16)(6,20)(7,10)(9,12)(14,21)(15,17),$ $(3,14)(4,8)(6,19)(7,13)(9,21)(10,11)(12,16)(18,20)\rangle \le \mathrm{PSL}_3(4)$
P_3	$=$	$\langle(1,12,5)(2,8,7)(3,13,15)(4,10,19)(6,14,18)(9,16,17),$ $(1,5,12)(2,13,9)(3,17,7)(6,14,18)(8,15,16)$ $(11,21,20)\rangle \le \mathrm{PSL}_3(4)$
P_5	$=$	$\langle(1,5,17,2,15)(3,21,4,8,6)(7,11,12,9,19)$ $(13,16,20,14,18)\rangle \le \mathrm{PSL}_3(4)$
P_7	$=$	$\langle(1,20,18,10,8,12,19)(2,13,6,4,17,15,3)$ $(5,21,16,9,14,11,7)\rangle \le \mathrm{PSL}_3(4)$

Table 1: factorization $\mathrm{PSL}_3(4) = P_7P_3P_2P_5$

Similar factorizations can be obtained for $\mathrm{PSU}_4(2)$ and $\mathrm{PSU}_3(4)$. Namely, representing $\mathrm{PSU}_4(2)$ as subgroup $\langle\gamma, \delta\rangle \le S_{45}$ with generators

$$\begin{aligned}\gamma &= (2,5,3)(4,12,7)(6,17,10)(8,21,14)(9,19,13)(11,29,20)(16,30,25)\\ &\quad (18,28,27)(22,26,32)(23,36,31)(33,35,39)(34,37,41)(40,42,43),\\ \delta &= (1,2,4,8,15,24)(3,6,11,21,31,37)(5,9,16,14,23,34)\\ &\quad (7,13,22,33,40,20)(10,18,25)(12,17,26,35,42,30)(19,28,29)\\ &\quad (32,38,43)(36,41,45)(39,44),\end{aligned}$$

and choosing Sylow subgroups P_2, P_3, P_5 as listed in Table 2, we can express $\mathrm{PSU}_4(2)$ as a product $\mathrm{PSU}_4(2) = P_3P_2P_5$. Juxtaposing minimal length logarithmic signatures for these solvable factors yields the required minimal length logarithmic signature for $\mathrm{PSU}_4(2)$.

P_2	$=$	$\langle(1,30,45,23)(2,28,3,42)(4,17,16,19)(5,11)(6,9,26,35)$ $(7,43,20,27)(8,31,41,12)(10,44,39,18)(13,40,32,38)$ $(14,36,37,29)(15,24,34,21)(22,33),$ $(1,15,17,6)(2,44,31,13)(3,32,12,18)(4,40,23,39)(5,22)(7,20)$ $(8,9,42,24)(10,30,38,16)(11,33)(14,37)(19,34,45,26)$ $(21,28,35,41)(27,29)(36,43),$ $(1,21,17,35)(2,10,31,38)(3,40,12,39)(4,32,23,18)(5,33)$ $(6,41,15,28)(7,20)(8,26,42,34)(9,19,24,45)(11,22)$ $(13,16,44,30)(14,37)(27,36)(29,43)\rangle \leq \mathrm{PSU}_4(2)$
P_3	$=$	$\langle(1,27,3,19,16,12,11,34,25)(2,32,26,17,8,21,33,24,36)$ $(4,30,22,37,43,45,10,35,31)(5,41,29)$ $(6,20,44,28,13,14,40,38,23)(7,42,18)(9,39,15),$ $(2,44,34)(3,40,24)(4,22,30)(5,42,41)(6,32,12)(7,18,39)$ $(8,25,28)(9,15,29)(10,31,35)(13,20,38)(14,27,17)(16,33,23)$ $(21,36,26)(37,45,43)\rangle \leq \mathrm{PSU}_4(2)$
P_5	$=$	$\langle(1,30,40,34,20)(2,42,21,18,37)(3,23,10,13,7)(4,35,15,27,17)$ $(5,11,33,22,25)(6,14,45,28,9)(8,38,26,36,19)(12,16,24,32,43)$ $(29,31,41,39,44)\rangle \leq \mathrm{PSU}_4(2)$

Table 2: factorization $\mathrm{PSU}_4(2) = P_3 P_2 P_5$

Based on the representation $\mathrm{PSU}_3(4) = \langle \epsilon, \zeta \rangle \leq S_{65}$ with

$$\begin{aligned}
\epsilon \;=\;& (2,9,50,12,61,38,14,3,15,4,27,63,52,23,6)\\
& (5,32,21,10,53,33,18,11,55,45,22,47,30,16,8)\\
& (7,62,39,29,51,25,60,17,43,42,49,44,28,34,36)\\
& (13,48,57,59,46,41,24,20,37,54,58,35,40,19,26)(56,64,65),\\
\zeta \;=\;& (1,2,4,8,18,39,26,48,59,44,22,21,6,15,31)\\
& (3,7,10,23,33,47,27,16,34,9,20,41,61,40,58)\\
& (5,12,17,37,55,54,60,38,32,56,28,52,63,62,64)\\
& (11,25,43,45,51,46,49,50,57,65,13,14,29,19,42)(24,35,36),
\end{aligned}$$

in Table 3 a respective factorization $\mathrm{PSU}_3(4) = P_{13}P_5P_2P_3$ of $\mathrm{PSU}_3(4)$ into Sylow subgroups is specified.

In general, we certainly cannot expect that a logarithmic signature of minimal length for a given finite (simple) group can be obtained by means of a factorization into Sylow subgroups. Actually, Holt and Rowley prove in [Holt and Rowley, 1993] that such a factorization does not exist for the simple group $\mathrm{PSU}_3(3)$. At the moment we do not know whether there exists a finite simple group—or equivalently any finite group—for which no logarithmic signature at all meeting the bound (1) exists. In the next section we show that in particular for all sporadic simple Mathieu groups a minimal length logarithmic signature exists, and thereafter we prove that all simple groups of order $< 175\,560$ (the order of Janko's first sporadic simple group) allow for a minimal length logarithmic signature, too. This implies that the bound (1) must be tight for arbitrary (not necessarily simple) groups of order $< 175\,560$.

4.2 Mathieu groups

Among the sporadic simple groups the five Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, and M_{24} already have been constructed two centuries ago. They are highly transitive permutation groups and can be obtained as the automorphism groups of Steiner systems. More precisely, M_{12} is the sharply 5-transitive automorphism group of a Steiner system $S(5,6;12)$ and M_{24} is the 5-transitive automorphism group of a Steiner system $S(5,8;24)$. We refer to [Beth et al., 1999] for notations and the realization of the Mathieu groups as automorphism groups of Steiner systems. In the following we employ a more direct construction which allows to obtain the Mathieu groups as symmetries of the projective geometries $\mathrm{PG}(2,\mathbb{F}_{11})$ and $\mathrm{PG}(2,\mathbb{F}_{23})$, respectively.

We first outline an elementary construction of the Mathieu groups M_{11} and M_{12} based on the projective geometry $\mathrm{PG}(2,\mathbb{F}_{11})$. Let

$$P = \{0,1,2,3,4,5,6,7,8,9,10,\infty\}$$

denote the points of the standard coordinatization of $\mathrm{PG}(2,\mathbb{F}_{11})$. Then M_{12} can be obtained as a permutation group on the set P. Namely, consider the following mappings (cf. [Gorenstein, 1982, Chapter 2.2]) which permute the set P:

$$f : x \mapsto x+1, \quad g : x \mapsto -\frac{1}{x}, \quad h : x \mapsto 4x^2 - 3x^7.$$

P_2	$=$	$\langle(1,40,29,21)(2,23,15,20)(3,49,34,12)(4,27,46,54)$
		$(5,50,30,26)(6,32,47,38)(7,35,65,25)(8,41,62,13)$
		$(9,44,36,52)(10,28,45,56)(11,53,59,17)(14,61,24,63)$
		$(16,19,43,37)(22,60,48,31)(33,39,58,55)(42,51,64,57),$
		$(1,27,24,6)(2,8,22,37)(3,51,52,33)(4,21,38,61)(5,25,45,11)$
		$(7,50,53,56)(9,64,49,39)(10,59,30,35)(12,55,36,42)$
		$(13,20,43,31)(14,47,29,54)(15,62,48,19)(16,60,41,23)$
		$(17,28,65,26)(32,63,46,40)(34,57,44,58),$
		$(1,2,14,48)(3,30,44,45)(4,16,32,13)(5,52,10,34)(6,62,54,37)$
		$(7,42,17,39)(8,27,19,47)(9,28,12,50)(11,58,35,51)$
		$(15,24,22,29)(20,63,60,21)(23,61,31,40)(25,57,59,33)$
		$(26,36,56,49)(38,41,46,43)(53,55,65,64),$
		$(1,57,14,33)(2,35,48,11)(3,6,44,54)(4,12,32,9)(5,37,10,62)$
		$(7,31,17,23)(8,30,19,45)(13,26,16,56)(15,25,22,59)$
		$(20,65,60,53)(21,42,63,39)(24,58,29,51)(27,34,47,52)$
		$(28,41,50,43)(36,46,49,38)(40,64,61,55)\rangle \leq \mathrm{PSU}_3(4)$
P_3	$=$	$\langle(1,21,22)(2,14,40)(3,62,42)(4,65,49)(5,41,25)(6,33,56)$
		$(7,9,32)(8,55,44)(10,13,11)(12,38,53)(15,29,61)(16,59,30)$
		$(17,36,46)(19,39,34)(23,31,60)(24,63,48)(26,47,51)$
		$(27,57,28)(35,45,43)(37,64,52)(50,54,58)\rangle \leq \mathrm{PSU}_3(4)$
P_5	$=$	$\langle(1,40,52,42,30)(2,51,60,38,8)(3,55,10,24,63)$
		$(4,37,22,33,23)(5,29,21,44,64)(6,53,43,28,9)(7,13,26,49,27)$
		$(12,54,65,41,50)(14,61,34,39,45)(15,57,31,32,62)$
		$(16,56,36,47,17)(19,48,58,20,46),$
		$(1,47,54,5,15)(2,51,60,38,8)(3,53,49,34,22)(4,24,9,13,14)$
		$(6,26,61,37,63)(7,45,23,10,28)(11,59,25,35,18)$
		$(12,64,62,30,36)(16,41,21,31,52)(17,65,29,57,40)$
		$(19,58,46,48,20)(27,39,33,55,43)$
		$(32,42,56,50,44)\rangle \leq \mathrm{PSU}_3(4)$
P_{13}	$=$	$\langle(1,3,48,30,53,6,58,18,60,56,16,55,38)$
		$(2,65,21,61,13,46,45,19,10,59,42,8,64)$
		$(4,54,14,50,27,44,26,15,22,34,25,29,32)$
		$(5,47,35,28,39,51,31,37,36,9,62,33,20)$
		$(7,49,24,43,40,57,23,63,17,52,12,41,11)\rangle \leq \mathrm{PSU}_3(4)$

Table 3: factorization $\mathrm{PSU}_3(4) = P_{13}P_5P_2P_3$

Note that by convention $\infty = 1/0$ and $0 = 1/\infty$. The elements f and g generate the group $\mathrm{PSL}_2(11)$ which is contained in $M_{12} := \langle f, g, h\rangle$. Explicitly, f, g, and h give rise to the following permutations σ, τ, and π of P:

$$\begin{array}{rcl}\sigma &=& (0,1,2,3,4,5,6,7,8,9,10),\\ \tau &=& (0,\infty)(1,10)(2,5)(3,7)(4,8)(6,9),\\ \pi &=& (2,6,10,7)(3,9,4,5).\end{array}$$

Now M_{12} is a simple group of order 95 040 which is sharply 5-transitive on the points P. Furthermore, M_{11} is defined as the stabilizer of the point 0. Hence $\mathrm{ord}(M_{11}) = 7920$ and a direct calculation shows that

$$M_{12} = K_{12} \cdot M_{11}, \tag{2}$$

where $K_{12} \leq M_{12}$ is the subgroup of order 12 generated by

$$\begin{array}{rcl}\alpha &:=& (0,7)(1,8)(2,6)(3,\infty)(4,10)(5,9),\\ \beta &:=& (0,1)(2,9)(3,4)(5,6)(7,8)(10,\infty),\\ \gamma &:=& (0,6,4,8,9,\infty)(1,5,3,7,2,10).\end{array}$$

In terms of the generators σ, τ, and π we obtain the factorizations $\alpha = \pi\sigma^2\tau\pi^{-1}\tau\pi\tau^{-1}\sigma^{-2}\pi^{-1}$, $\beta = \pi^{-1}\tau\sigma^2\tau^{-1}\sigma\pi$, and $\gamma = \sigma^{-1}\pi\sigma^{-1}\pi^{-1}\sigma\pi\tau^{-1}$.

Since K_{12} is an abelian group isomorphic to a product $C_2 \times C_6$ of two cyclic groups, we obtain from equation (2) that M_{12} has a logarithmic signature of minimal length if we can find one for M_{11}. To put it another way, we have that M_{12} is a Zappa-Szép product of K_{12} and M_{11} (see Section 3).

Focusing on M_{11}, we consider the stabilizer of the point 1 and obtain a group M_{10} of order 720 which is known to have a composition series $\{e_{M_{10}}\} < A_6 < M_{10}$. Since A_6 allows for a logarithmic signature meeting the bound (1) [Magliveras, 2002; González Vasco and Steinwandt, 2002] and the factor group is isomorphic to C_2, we obtain that M_{10} has a logarithmic signature of minimal length, and because of M_{11} being isomorphic to a Zappa-Szép product

$$M_{11} = C_{11} \cdot M_{10},$$

we can also construct minimal length logarithmic signatures for the small Mathieu groups M_{11} and M_{12}.

4.2.1 The Mathieu groups M_{22}, M_{23}, and M_{24}

Similarly to the construction of M_{12} one may obtain M_{24} as a permutation group acting on the projective geometry $\mathrm{PG}(2, \mathbb{F}_{23})$. This time we start from

$\mathrm{PSL}_2(23)$ which is generated by $f : x \mapsto x+1$ and $g : x \mapsto -\frac{1}{x}$. The mapping (see [Gorenstein, 1982])

$$h : x \mapsto -3x^{15} + 4x^4,$$

defines a permutation of the points of $\mathrm{PG}(2, \mathbb{F}_{23})$. The Mathieu group M_{24} is defined as $M_{24} := \langle \sigma, \tau, \pi \rangle$, where the permutations σ, τ, and π are obtained from f, g, and h. Explicitly, we have

$$\begin{aligned}
\sigma &= (0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22),\\
\tau &= (0,\infty)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20)(10,16)\\
&\quad (12,21)(14,18),\\
\pi &= (2,16,9,6,8)(3,12,13,18,4)(7,17,10,11,22)(14,19,21,20,15).
\end{aligned}$$

Note that M_{24} can be written as a Zappa-Szép product in the following way:

$$M_{24} = S_4 \cdot M_{23},$$

where M_{23} denotes the stabilizer of the point 0 in M_{24}. The symmetric group $S_4 := \langle \alpha, \beta \rangle \leq M_{24}$ is generated by the permutations

$$\begin{aligned}
\alpha &:= (0,2)(1,14)(3,8)(4,\infty)(5,20)(6,17)(7,10)(9,21)(11,18)(12,16)\\
&\quad (13,15)(19,22),\\
\beta &:= (0,1,\infty,12)(2,7,3,9)(4,18,13,22)(5,10,16,19)(6,11,14,21)\\
&\quad (8,20,15,17).
\end{aligned}$$

We can descend one more step to M_{22} since the corresponding transversal can be chosen to be a cyclic group of order 23. More precisely, we have $M_{23} = C_{23} \cdot M_{22}$, where M_{22} stabilizes the points 0 and 1, and C_{23} is a cyclic group of order 23. In fact, as generator of C_{23} we can choose an arbitrary element of order 23 in M_{23}.

Finally, M_{22} can be realized as follows: we define the subgroups $C_{11} := \langle (2,19,9,7,18,12,\infty,5,11,16,21)(3,17,8,10,13,20,22,14,6,4,15) \rangle \leq M_{22}$ and $C_2 := \langle (2,10)(3,19)(4,11)(7,13)(8,21)(9,15)(12,14)(16,17) \rangle \leq M_{22}$. Then the subset $A := C_2 \cdot C_{11}$ of M_{22} has the property that for each point $x \in \{2,\ldots,22,\infty\}$ there is an element $\rho \in A$ such that $\rho(2) = x$. On the other hand the stabilizer of the points 0, 1, and 2 inside M_{24} is isomorphic to the simple group $\mathrm{PSL}_3(4)$ of order 20 160. Thus, using the result that $\mathrm{PSL}_3(4)$ has a logarithmic signature of minimal possible length (see Table 1), we also obtain a logarithmic signature for $M_{22} = \mathrm{PSL}_3(4) \cdot A$ that meets the bound (1). Hence, by the previous arguments also M_{23} and M_{24} have logarithmic signatures of minimal possible length.

4.3 A lower bound for the size of a counter-example

In Table 4 the simple groups for which we know already that the bound in Remark 2.2 is tight are listed.

group	order	possible minimal length factorization
C_p (p prime)	p	trivial: $[[g \mid g \in C_p]]$
A_n ($n\geq 5$)	$n!/2$	stabilizer chain (see [Magliveras, 2002] and [Bohli et al., 2002])
$\mathrm{PSL}_2(q)$ ($q>3$)	$\frac{q\cdot(q^2-1)}{\gcd(2,q-1)}$	product of Sylow subgroups (Section 4.1)
$\mathrm{PSL}_3(q)$ ($q\not\equiv_3 1$)	$q^3(q^3-1)(q^2-1)$	product of Sylow subgroups (Section 4.1)
$\mathrm{PSL}_3(4)$	20 160	product of Sylow subgroups (Table 1)
$\mathrm{PSU}_4(2)$	25 920	product of Sylow subgroups (Table 2)
$\mathrm{PSU}_3(4)$	62 400	product of Sylow subgroups (Table 3)
M_{11}	7 920	product of subgroups: $C_{11} \cdot A_6 \cdot C_2$
M_{12}	95 040	product of subgroups: $(C_2 \times C_6) \cdot M_{11}$
M_{22}	443 520	product of subgroups: $\mathrm{PSL}_3(4) \cdot C_2 \cdot C_{11}$
M_{23}	10 200 960	product of subgroups: $C_{23} \cdot M_{22}$
M_{24}	244 823 040	product of subgroups: $S_4 \cdot M_{23}$

Table 4: simple groups meeting the bound in Remark 2.2

In particular, this list covers all simple groups of order $\leq 2^{17}$ up to the following three exceptions:

- $\mathrm{PSU}_3(3)$ (of order 6048)
- $\mathrm{Sz}(8)$ (of order 29120)
- $\mathrm{PSU}_3(5)$ (of order 126000)

Subsequently we give a logarithmic signature for each of these three groups. They have been found and verified by means of the computer algebra system Magma.

4.3.1 $\mathrm{PSU}_3(3)$

We represent $\mathrm{PSU}_3(3)$ as a subgroup $\langle\alpha,\beta\rangle \le S_{28}$ with generators

$$\begin{aligned}
\alpha &= (2,7,23,26,17,13,6,3)(4,19,11,28,25,24,16,9)\\
&\quad (5,18,10,14,15,8,20,12)(21,27),\\
\beta &= (1,2,4,10,8,16,13,22)(3,7,9,17,6,12,21,5)\\
&\quad (11,19,26,14,15,23,24,25)(27,28).
\end{aligned}$$

Then $\mathrm{PSU}_3(3)$ can be factored into a product $\langle\alpha,\beta\rangle = G_1C_4C_7$ where G_1 is the stabilizer of 1, and C_4 resp. C_7 is a cyclic group of order 4 resp. 7. Precise choices for C_4 and C_7 are given in Table 5.
As the stabilizer G_1 (of order $216 = \mathrm{ord}(\mathrm{PSU}_3(3))/(4\cdot 7)$) is solvable, we immediately obtain a minimal length logarithmic signature for $\mathrm{PSU}_3(3)$ by juxtaposing minimal length logarithmic signatures for the three subgroups G_1, C_4, and C_7.

$C_4 = \langle(1,7,13,21)(2,8,19,4)(3,24,22,18)(5,6,10,14)(9,23)(11,20,28,15)(12,16)(17,27,25,26)\rangle \le \mathrm{PSU}_3(3)$
$C_7 = \langle(1,11,8,14,20,27,2)(3,5,12,21,18,4,28)(6,23,24,26,22,9,13)(7,25,16,17,10,15,19)\rangle \le \mathrm{PSU}_3(3).$

Table 5: factors C_4 and C_7 of the factorization $\mathrm{PSU}_3(3) = G_1C_4C_7$

4.3.2 Sz(8)

We represent the Suzuki group Sz(8) as subgroup $\langle \alpha, \beta \rangle \leq S_{65}$ with generators

$$\begin{aligned}
\alpha &= (1,2)(3,4)(5,7)(6,9)(8,12)(10,13)(11,15)(14,19)(16,21)(17,23) \\
&\quad (18,25)(20,28)(22,31)(24,33)(26,35)(27,32)(29,37)(30,39)(34,43) \\
&\quad (36,46)(38,48)(41,51)(42,44)(45,55)(47,50)(49,58)(52,60)(53,61) \\
&\quad (54,59)(56,62)(57,63)(64,65), \\
\beta &= (1,3,5,8)(4,6,10,14)(7,11,16,22)(9,12,17,24)(13,18,26,36) \\
&\quad (15,20,29,38)(19,27,31,28)(21,30,40,50)(23,32,41,52) \\
&\quad (25,34,44,54)(33,42,53,43)(35,45,56,63)(37,47,51,46) \\
&\quad (39,49,59,60)(48,57,55,58)(61,64,62,65).
\end{aligned}$$

Then Sz(8) can be factored into a product $\mathrm{Sz}(8) = G_1 C_5 C_{13}$ where G_1 is the stabilizer of 1, and C_5 resp. C_{13} is cyclic of order 5 resp. 13. Concrete choices for the cyclic groups C_5 and C_{13} are given in Table 6.
As the stabilizer G_1 (of order 448=ord(Sz(8))/$(5 \cdot 13)$) is solvable, we immediately obtain the required minimal length logarithmic signature for Sz(8) by juxtaposing minimal length logarithmic signatures for the three factors G_1, C_5, and C_{13}.

C_5	$=$	$\langle(1,38,43,40,64)(2,50,32,63,44)(3,18,10,65,61)$ $(4,7,15,24,12)(5,19,33,54,17)(6,8,36,27,13)$ $(9,31,48,47,30)(11,49,51,20,23)(14,60,16,53,57)$ $(21,39,56,35,37)(22,46,58,45,59)(25,34,62,26,41)$ $(28,55,29,42,52)\rangle \leq \mathrm{Sz}(8)$
C_{13}	$=$	$\langle(1,46,21,18,47,51,22,31,15,4,39,6,41)$ $(2,56,32,27,5,49,3,20,40,54,50,59,23)$ $(7,42,48,61,37,65,53,36,19,8,17,45,43)$ $(9,52,55,29,38,12,62,25,57,24,11,58,30)$ $(10,63,26,14,44,35,13,34,33,16,64,28,60)\rangle \leq \mathrm{Sz}(8)$

Table 6: factors C_5 and C_{13} of the factorization $\mathrm{Sz}(8) = G_1 C_5 C_{13}$

4.3.3 $\mathrm{PSU}_3(5)$

We represent $\mathrm{PSU}_3(5)$ as a subgroup $\langle\alpha,\beta\rangle \leq S_{126}$ with generators

$$
\begin{aligned}
\alpha \;=\; & (1,2,4,10,25)(3,7,17,41,19)(5,13,33,68,111)(6,14,36,34,70)\\
& (8,20,47,81,48)(9,22,32,61,106)(11,28,37,40,82)(12,30,24,55,65)\\
& (15,38,77,29,64)(16,39,43,85,73)(18,44,75,118,109)\\
& (21,49,93,126,120)(23,53,42,83,52)(26,58,104,122,101)\\
& (27,60,105,110,124)(31,35,72,116,66)(45,87,123,108,96)\\
& (46,89,95,100,59)(50,94,57,76,103)(51,97,114,71,107)\\
& (54,88,74,63,98)(56,102,117,99,121)(62,86,78,90,80)\\
& (67,79,112,92,125)(69,113,84,115,119),\\
\beta \;=\; & (2,13,112,108,24,93,45,7)(3,32,53,102,54,65,75,16)\\
& (4,41,52,104,11,68,99,30)(5,81,122,18,56,34,19,63)\\
& (6,17,72,69,101,10,55,31)(8,29,100,40,84,67,37,57)\\
& (9,36,98,124,27,94,117,66)(12,120,42,43,33,15,26,106)\\
& (14,76,64,85,86,96,70,97)(20,73,82,83,125,50,39,113)\\
& (21,74,87,23,59,105,110,61)(22,60,88,123,78,62,90,116)\\
& (28,118,77,79,44,46,115,121)(35,80,109,48,95,49,114,126)\\
& (38,91,47,92,51,107,71,119)(58,103,89,111).
\end{aligned}
$$

Then $\mathrm{PSU}_3(5)$ can be factored into a product $\langle\alpha,\beta\rangle = C_7C_3^{(1)}C_3^{(2)}C_2G_1$ where G_1 is the stabilizer of 1, C_2 is a cyclic group of order 2, both $C_3^{(1)}$ and $C_3^{(2)}$ are cyclic groups of order 3, and C_7 is a cyclic group of order 7. Precise choices for the four cyclic factors are given in Table 7. As the stabilizer G_1 (of order $1000 = \mathrm{ord}(\mathrm{PSU}_3(5))/(2\cdot3\cdot3\cdot7)$) is solvable, we immediately obtain a minimal length logarithmic signature for $\mathrm{PSU}_3(5)$ by juxtaposing minimal length logarithmic signatures for the five subgroups G_1, C_2, $C_3^{(1)}$, $C_3^{(2)}$, and C_7.

Thus, if there is any finite group G such that no logarithmic signature for G meets the bound in Remark 2.2, then the smallest counter-example (w. r. t. the group order) has to be both simple and of order $> 2^{17}$. Further on, we can exclude all simple groups covered by Table 4, and thus the smallest group for which the tightness of (1) is open, is Janko's first sporadic group J_1 of oder 175 560.

C_2	$=$	$\langle(1,60)(3,6)(4,27)(5,21)(7,94)(8,59)(9,12)(10,83)(11,42)$ $(13,30)(14,84)(15,58)(16,47)(17,32)(18,74)(19,115)(20,77)$ $(22,54)(23,78)(24,120)(25,82)(26,43)(28,114)(29,100)(31,76)$ $(33,106)(34,35)(36,45)(37,80)(38,39)(40,105)(41,98)(44,55)$ $(46,67)(48,79)(49,116)(50,61)(52,124)(53,71)(56,91)(57,70)$ $(62,97)(63,119)(64,92)(65,88)(66,111)(68,103)(69,109)$ $(72,96)(73,101)(75,126)(81,122)(86,107)(87,113)(90,110)$ $(93,108)(95,125)(102,121)(104,112)(118,123)\rangle \leq \mathrm{PSU}_3(5)$
$C_3^{(1)}$	$=$	$\langle(1,81,13)(2,119,26)(3,16,105)(4,121,97)(5,120,109)$ $(6,24,113)(7,10,28)(8,40,74)(9,66,94)(11,39,49)(12,112,62)$ $(14,60,83)(15,126,122)(17,123,56)(18,76,33)(19,69,91)$ $(20,101,45)(21,87,61)(22,78,104)(23,100,65)(25,43,72)$ $(27,67,75)(29,58,36)(30,51,38)(31,118,108)(32,59,89)$ $(34,41,55)(35,82,71)(37,103,110)(42,63,86)(44,114,107)$ $(46,48,116)(47,85,115)(50,90,80)(52,77,70)(53,124,111)$ $(54,98,102)(57,84,117)(64,79,88)(68,93,106)(73,95,99)$ $(92,125,96)\rangle \leq \mathrm{PSU}_3(5)$
$C_3^{(2)}$	$=$	$\langle(1,8,6)(2,57,56)(3,88,104)(4,79,9)(5,22,97)(7,30,67)$ $(10,58,54)(11,28,27)(12,75,106)(13,19,94)(14,50,51)$ $(15,68,66)(16,34,44)(17,36,73)(18,25,32)(20,93,112)$ $(21,26,70)(23,87,24)(29,64,111)(31,47,116)(33,105,91)$ $(35,98,84)(37,72,121)(38,83,40)(39,59,78)(41,110,71)$ $(42,43,69)(45,108,123)(46,95,102)(48,100,77)(49,115,55)$ $(52,80,63)(53,125,96)(60,82,89)(61,124,76)(62,113,74)$ $(65,126,117)(81,114,118)(85,90,119)(86,120,92)$ $(99,109,101)(103,107,122)\rangle \leq \mathrm{PSU}_3(5)$
C_7	$=$	$\langle(1,108,125,9,17,95,64)(2,39,63,34,111,25,60)$ $(3,33,68,30,74,47,107)(4,5,32,52,67,57,62)$ $(6,23,78,28,80,46,122)(7,24,50,100,48,104,15)$ $(8,18,85,93,44,51,16)(10,116,113,22,90,126,65)$ $(11,55,72,26,42,124,14)(12,77,121,75,120,84,59)$ $(13,92,56,88,118,94,73)(19,36,45,103,35,21,54)$ $(20,98,110,69,82,29,87)(27,112,109,70,117,97,89)$ $(31,99,96,79,66,81,123)(37,61,91,101,71,102,58)$ $(38,115,105,106,40,114,76)(41,119,53,49,43,86,83)\rangle$

Table 7: cyclic factors of the factorization $\mathrm{PSU}_3(5) = C_7C_3^{(1)}C_3^{(2)}C_2G_1$

5 Conclusions and further research

Motivated by the question of finding short keys for the public key cryptosystem MST_1, we have shown that various finite groups allow for logarithmic signatures of minimal possible length. Unfortunately, so far we could not answer the question whether there is any finite group for which the bound (1) is not tight, but we have shown that there can be no such group of cardinality smaller than Janko's first sporadic simple group.

Both from the mathematical and the cryptographic point of view it would be desirable to identify further families of—not necessarily simple—groups for which the bound (1) is tight. On the cryptographic side, also the question arises whether logarithmic signatures of minimal length can be found, where effectively factoring group elements along the logarithmic signature is computationally hard. Such logarithmic signatures would be desirable for realizing the MST_1 public key cryptosystem.

Acknowledgement

We thank Consuelo Martínez for helpful comments and discussions.

References

S.S. Abhyankar. Galois Theory on the Line in Nonzero Characteristic. *Bulletin of the American Mathematical Society*, 27(1):68–133, 1992.

Th. Beth, D. Jungnickel, and H. Lenz. *Design Theory*, volume I. Cambridge University Press, 2. edition, 1999.

J.-C. Birget, S.S. Magliveras, and W. Wei. Trap doors from subgroup chains and recombinant bilateral transversals. In S. González Jiménez and C. Martínez López, editors, *Actas de la VII Reunión Española de Criptología y Seguridad de la Información; Tomo I*, pages 31–48, 2002.

N. Blackburn and B. Huppert. *Finite Groups III.* Die Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin-New York, 1982.

J.-M. Bohli, M.I. González Vasco, C. Martínez, and R. Steinwandt. Weak Keys in MST_1. Cryptology ePrint Archive: Report 2002/070, 2002.

W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: The User Language. *Journal of Symbolic Computation*, 24:235–265, 1997.

C.A. Cusack. *Group Factorizations in Cryptography.* PhD thesis, University of Nebraska, 2000.

M.I. González Vasco, C. Martínez, and R. Steinwandt. Towards a Uniform Description of Several Group Based Cryptographic Primitives. To appear in Designs, Codes and Cryptography, 2003.

M.I. González Vasco and R. Steinwandt. Obstacles in Two Public-Key Cryptosystems Based on Group Factorizations. In *Cryptology. Editors: K. Nemoga, O. Grošek*, volume 25 of *Tatra Mountains Mathematical Publications*, pages 23–37, 2002. To appear.

D. Gorenstein. *Finite Simple Groups.* University series in mathematics. Plenum Press, New York, 1982.

D. Gorenstein, R. Lyons, and R. Solomon. *The Classification of the Finite Simple Groups*, volume 40(1) of *Mathematical Surveys and Monographs.* AMS, Providence, RI, 1998.

D.F. Holt and P. Rowley. On products of Sylow subgroups in finite groups. *Archiv der Mathematik*, 60(2):105–107, 1993.

M.W. Liebeck, C.E. Praeger, and J. Saxl. *The maximal factorizations of the finite simple groups and their automorphism groups*, volume 86(432) of *Memoirs of the AMS.* AMS, Providence, RI, 1990.

S.S. Magliveras. A cryptosystem from logarithmic signatures of finite groups. In *Proceedings of the 29'th Midwest Symposium on Circuits and Systems*, pages 972–975. Elsevier Publishing Company, 1986.

S.S. Magliveras. Secret- and Public-key Cryptosystems from Group Factorizations. In *Cryptology. Editors: K. Nemoga, O. Grošek*, volume 25 of *Tatra Mountains Mathematical Publications*, pages 11–22, 2002. To appear.

S.S. Magliveras and N.D. Memon. Algebraic Properties of Cryptosystem PGM. *Journal of Cryptology*, 5:167–183, 1992.

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.

P.W. Michor. Knit Products of Graded Lie Algebras and Groups. In *Proceedings of the Winter School on Geometry and Physics, Srni 1988*, Ser. II, 22, pages 171–175. Suppl. Rendiconti Circolo Matematico di Palermo, 1989.

S.K. Stein and S. Szabó. *Algebra and Tiling. Homomorphisms in the Service of Geometry.* Number 25 in The Carus Mathematical Monographs. The Mathematical Association of America, 1994.

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.

N.R. Wagner. Searching for Public-Key Cryptosystems. In *Proceedings of the 1984 Symposium on Security and Privacy (SSP '84)*, pages 91–98, Los Angeles, Ca., USA, 1990. IEEE Computer Society Press.

N.R. Wagner and M.R. Magyarik. A Public Key Cryptosystem Based on the Word Problem. In G. R. Blakley and D. Chaum, editor, *Advances in Cryptology. Proceedings of CRYPTO 1984*, volume 196 of *Lecture Notes in Computer Science*, pages 19–36. Springer, 1985.