On Minimal Logarithmic Signatures of Finite Groups

Wolfgang Lempken and Tran van Trung

CONTENTS

Logarithmic signatures (LS) are a kind of factorization of finite groups which are used as a main component of cryptographic keys for secret key cryptosystems such as PGM and public key cryptosystems like MST1. As such, logarithmic signatures of short length are of special interest. In the present paper we deal with the fundamental question of the existence of logarithmic signatures of shortest length, called minimal logarithmic signatures (MLS), for finite groups. Studies of the problem can be found in [Magliveras 02], [González Vasco and Steinwandt 02], and especially in [González Vasco et al. 03], where González Vasco, Rötteler, and Steinwandt show that minimal logarithmic signatures exist for all groups of order less than 175,560 by direct computation using the method of factorization of a group into "disjoint" subgroups. We introduce new approaches to deal with the question. The first method uses the double coset decomposition to construct minimal logarithmic signatures. This method allows one to prove, for instance, that if $\gcd(n, q-1) \in \{1, 4, p \mid p \text{ prime}\}$, then the projective special linear groups $L_n(q)$ have an MLS. Another main goal of this paper is to construct MLS for all finite groups of order $\leq 10^{10}$. Surprisingly, the method of double coset decomposition turns out to be very effective, as we can construct MLS for all groups in the range except eight groups. We are also able to prove that if an MLS for any of these eight groups exists, then it cannot be constructed by the method of double coset decomposition. We further discuss a method of construction of MLS for groups of the form $G = A.B$ with subgroups A, B and $A \cap B \neq 1$, by building suitable MLS for A and B and "gluing" them together.

1. INTRODUCTION

Most of the well-known public-key cryptosystems which are still unbroken are based on certain intractable problems in large finite abelian groups, such as the multiplicative group of units in the ring $\mathbb{Z}_{pq}$ with p, q primes, the multiplicative group of a finite field, or a cyclic subgroup of the group of rational points of an elliptic curve over a finite field. However, from the group-theoretic point of view, abelian groups have simple and well understood structures, and thus the intractability of the problems seems to be closer to number theory than group theory.

2000 AMS Subject Classification: Primary 20D99, 94A60

Keywords: Logarithmic signatures, group factorizations, double cosets, finite simple groups, cryptosystems

1058-6458/2005 $ 0.50 per page

One of the first symmetric-key cryptosytems exploiting the structure of nonabelian groups was proposed by Magliveras [Magliveras 86]. This cryptosystem, named PGM, makes use of a special type of factorization of nonabelian permutation groups which are called *logarithmic signatures* (LS). Recently, two possible approaches to constructing new public-key cryptosystems MST_1 and MST_2 using *group factorization* of finite groups were described by Magliveras, Stinson, and Tran van Trung [Magliveras et al. 02]. In particular, logarithmic signatures are used as the main component of the keys in MST_1. As such, the question of finding logarithmic signatures with *short length* emerges naturally and becomes more relevant regarding properties of cryptographic schemes involving logarithmic signatures. Moreover, logarithmic signatures of certain types are group-theoretically interesting structures of their own. The question of the existence of logarithmic signatures of minimum length, was first posed by González Vasco and Steinwandt in [González Vasco and Steinwandt 02], in which the authors derive a lower bound for the length of a logarithmic signature of a group G and show that finite solvable groups and symmetric groups S_n have logarithmic signatures achieving the bound. For short, we call a logarithmic signature achieving this bound a minimal logarithmic signature (MLS). It is also shown in [Magliveras 02] that the alternating groups A_n have minimal logarithmic signatures. In a recent paper [González Vasco et al. 03], González Vasco, Rötteler, and Steinwandt prove that minimal logarithmic signatures for all groups of order less than 175,560 exist. Essentially, the authors attempt to factorize each group G in the range into a product of "disjoint" subgroups with the property that each subgroup has a minimal logarithmic signature and thus obtain a desired MLS for G by joining the MLS of the subgroups together. In general, in order to obtain such a factorization, this method usually requires direct computations which rapidly become infeasible when the order of G gets large.

The purpose of the present paper is to introduce new approaches to deal with the above question. More precisely, we study the method of double coset decomposition (MDCD) and the method of subgroup product in its general setting. It turns out that the MDCD is a very effective tool for constructing minimal logarithmic signatures. For example, by applying the MDCD to special linear groups $SL_n(q)$ and to projective special linear groups $L_n(q)$ we show that if $\gcd(n, q-1) \in \{1, 4, p \mid p \text{ prime}\}$, then $SL_n(q)$ and $L_n(q)$ have an MLS. Our second main application of the MDCD is constructing minimal logarithmic signatures for all groups of order of at most 10^{10}. As a result, we prove that such an MLS exists for all groups in the range except a list of eight groups. For these eight groups we are able to prove that there are no MLS which can be obtained by the MDCD.

The second approach discusses the question of whether or not one can construct an MLS for a group $G = A.B$ from appropriate MLS of A and B, where A and B are subgroups of G and $A \cap B \neq 1$. Interestingly, in combining with the MDCD we succeed in analyzing several nontrivial examples showing that the question has a positive answer even for large groups with a complex structure such as $U_3(5)$ or J_2.

The paper is organized as follows. In Section 2, we give definitions, notation, and some basic results about logarithmic signatures. Section 3 shows that the general linear groups $GL_n(q)$ and the projective general linear groups $PGL_n(q)$ possess MLS. Section 4 presents the method of double coset decomposition and its application to $SL_n(q)$ and $L_n(q)$. In Section 5, we show, for the sake of completeness, that an MLS can be constructed for all groups G with $|G| < 175,560$ by the MDCD. This result is the content of the paper [González Vasco et al. 03] achieved by means of the group factorization into disjoint subgroups. In Section 6, we construct MLS for all groups G with $175,560 \leq |G| \leq 10^{10}$ except a list of eight groups. In Section 7, we prove that there are no MLS which can be constructed by the MDCD for these eight groups. Section 8 discusses the second approach of constructing MLS for groups which are the product of two nondisjoint subgroups. The paper closes with a conclusion in Section 9.

2. PRELIMINARIES

Logarithmic signatures (LS) are introduced as basic key components for some symmetric and asymmetric cryptosystems based on nonabelian finite groups. A logarithmic signature can be viewed as a certain type of "basis" for finite groups, in the sense that group elements are uniquely represented with respect to the basis. To be precise, we have the following definition.

Definition 2.1. Let G be a finite group. Let $\alpha = [\alpha_1, \ldots, \alpha_s]$ be a sequence of ordered subsets α_i of G such that $\alpha_i = [\alpha_{i_0}, \ldots, \alpha_{ir_i-1}]$ with $\alpha_{ij} \in G$, $(0 \leq j < r_i)$. Then α is called a logarithmic signature for G if each $g \in G$ is uniquely represented as a product

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

with $\alpha_{ij_i} \in \alpha_i$ $(1 \leq i \leq s)$.

The sequences α_i are called the blocks of α and the integer $\ell(\alpha) := \sum_{i=1}^{s} r_i$ the length of α.

In view of Definition 2.1 a logarithmic signature thus gives rise to a special type of factorization of a finite group. A simple method of constructing logarithmic signatures for a group G is the following: let

$$G = G_0 > G_1 > \cdots > G_s = 1$$

be a chain of subgroups. Take $\alpha = [\alpha_1, \ldots, \alpha_s]$, where $\alpha_i = [\alpha_{i_0}, \ldots, \alpha_{ir_i-1}]$ is the complete system of left (respectively right) coset representatives of G_i in G_{i-1}. It is easily checked that α is a logarithmic signature for G. Such logarithmic signatures are called *exact left (respectively right) transversal*. In particular, if $s = 1$ we have a trivial logarithmic signature α consisting of a single block, and therefore $\ell(\alpha) = |G|$.

For cryptographic purposes, we are interested in logarithmic signatures having a *short* length. In general the problem of constructing logarithmic signatures of a given length is nontrivial. It is clear that for any logarithmic signature α of a finite group G we have $\ell(\alpha) \leq |G|$. A lower bound for $\ell(\alpha)$ is given by González Vasco and Steinwandt [González Vasco and Steinwandt 02].

Theorem 2.2. [González Vasco and Steinwandt 02] *Let G be a finite group and $|G| = \prod_{j=1}^{t} p_j^{a_j}$ be the order of G, where $p_1, \ldots, p_t$ are distinct primes. Then*

$$\ell(\alpha) \geq \sum_{j=1}^{t} a_j p_j$$

for any logarithmic signature α of G.

Proof: For any logarithmic signature $\alpha = [\alpha_1, \ldots, \alpha_s]$ with $|\alpha_i| = r_i$ we have $|G| = r_1 \cdots r_s$. Write $r_i = \prod_{j=1}^{t} p_j^{a_{ij}}$. Then $\sum_{i=1}^{s} a_{ij} = a_j$. The theorem now follows from $r_i \geq \sum_{j=1}^{t} a_{ij} p_j$, $(1 \leq i \leq s)$. □

Definition 2.3. A logarithmic signature α for a finite group G with $\ell(\alpha) = \sum_{j=1}^{t} a_j p_j$ is called a *minimal length logarithmic signature* or, for short, a *minimal logarithmic signature* (MLS).

González Vasco and Steinwandt show that solvable groups and symmetric groups have a minimal logarithmic signature [González Vasco and Steinwandt 02]. Magliveras proves the existence of an MLS for the alternating groups and also explores the problem for $L_2(q) = PSL_2(q)$ [Magliveras 02].

The following elementary results are useful and easy to verify.

Lemma 2.4. *Let G be a finite group with a normal subgroup N. If N and G/N have an MLS, then G has an MLS.*

Lemma 2.5. *Let G be a finite group. Suppose that G has subgroups H and K with $G = H.K$ and $H \cap K = 1$ such that H and K both have an MLS. Then*

1. *G has an MLS;*

2. *if N is a normal subgroup of G such that $N \leq K$ and K/N has an MLS, then G/N has an MLS;*

3. *the analogous statement is true if $N \leq H$.*

By using composition series it is easily seen that the question of the existence of MLS for finite groups is reduced to the question of the existence of MLS for finite simple groups. Accordingly, González Vasco, Rötteler and Steinwandt prove the existence of an MLS for all groups of order less than 175,560 (the order of J_1, the first Janko group) [González Vasco et al. 03]. The main tool in [González Vasco et al. 03] is to factorize a (simple) group in question as a product of a number of disjoint proper subgroups having an MLS. For example, using a result by Holt and Rowley [Holt and Rowley 93] that for any prime power q the groups $L_2(q)$ and $PGL_3(q)$ can be decomposed as a product of their Sylow p_i-subgroups, one concludes that $L_2(q)$ and $PGL_3(q)$ have an MLS.

In our paper, we intensively make use of the ATLAS, in particular we adopt its notation and its abbreviations for our discussion. For the reader's convenience we recall here some abbreviations frequently used in the ATLAS [Conway et al. 85].

- $[m]$ denoting an arbitrary group of order m;

- m denoting a cyclic group of order m;

- p^n, p is prime, indicates the elementary abelian group of that order;

- p^{1+2n} indicates an extraspecial group of that order.

For the rest of the paper we implicitly use the fact that solvable groups have an MLS.

3. THE GROUPS $GL_n(q)$, $PGL_n(q)$, $L_n(q) := PSL_n(q)$

In this section we show that for any $n \geq 2$ and any prime power q the general linear groups $GL_n(q)$ and the projective general linear groups $PGL_n(q)$ possess a product factorization of disjoint subgroups satisfying the condition of Lemma 2.5, and therefore have a minimal logarithmic signature.

Theorem 3.1. *Let $G := GL_n(q)$ for some $n \in \mathbb{N}$ and some prime power q. Then for any subgroup $Z \leq \mathbb{Z}(G)$ the group G/Z has a minimal logarithmic signature. So in particular, $GL_n(q)$ and $PGL_n(q)$ have MLS.*

Proof: Let V be an n-dimensional vector space over $GF(q)$ such that G acts as a group of linear tranformations on V. Let $H := G_v$ be the stabilizer of a nonzero vector $v \in V$. By a suitable choice of a basis for V, we see that the elements of H are matrices of the form:

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \alpha_2 & & & \\ \vdots & & A_1 & \\ \alpha_n & & & \end{pmatrix}$$

where A_1 is a nonsingular $(n-1) \times (n-1)$-matrix over $GF(q)$. The mapping $\varphi : \ A \to A_1$ is an epimorphism from H on $GL_{n-1}(q)$. The kernel of φ is an abelian group Q of order q^{n-1}. In particular, $H = Q : L$ is a semidirect product, where $L \cong GL_{n-1}(q)$ consists of all matrices of H with $\alpha_2 = \cdots = \alpha_n = 0$. Further, it is well-known that G contains a cyclic subgroup K of order $q^n - 1$ such that $\mathbb{C}_G(K) = K$ and K acts sharply transitive on $V - \{0\}$. Thus $H \cap K = 1$ and $G = H.K$.

Note that K has a minimal logarithmic signature. Since $GL_1(q)$ is solvable, we use an easy induction argument together with Lemma 2.4 to see that H has an MLS. Now $G = H.K$ has an MLS by Lemma 2.5.

Finally, let $Z \leq \mathbb{Z}(G)$. Then $K = \mathbb{C}_G(K) \geq \mathbb{Z}(G) \geq Z$. As K/Z is solvable and thus has an MLS, Lemma 2.5 shows that G/Z has an MLS. □

Corollary 3.2. *For every $n \geq 2$ and every prime power q with $\gcd(n, q-1) = 1$ the group $SL_n(q) \cong L_n(q)$ has a minimal logarithmic signature.*

Proof: The condition $\gcd(n, q-1) = 1$ is equivalent to $SL_n(q) \cong L_n(q) \cong PGL_n(q)$, hence the corollary follows. □

In general, the problem of decomposing finite nonsolvable groups as a product of disjoint subgroups appears to be difficult; it is not known whether such a decomposition is possible at all for a given nonabelian simple group, see for instance [Holt and Rowley 93], in which Holt and Rowley show that the simple group $U_3(3)$ does not have a factorization into Sylow subgroups. We also show in Section 5 that the first Janko simple group J_1 does not possess a factorization into a product of three disjoint subgroups.

In the next section, we develop a new method enabling further identification of $L_n(q)$ having an MLS.

4. METHOD OF DOUBLE COSET DECOMPOSITION (MDCD) FOR CONSTRUCTION OF MLS

In this section, we describe a new approach to construct minimal logarithmic signatures for a finite group G by using a double coset decomposition with respect to appropriate proper subgroups of G. Surprisingly, this method appears to be powerful in dealing with the problem. Especially, for groups of relatively "small" order, the double coset method gives a simple and elegant construction of minimal logarithmic signatures. Actually, the MDCD provides an easy way to prove the results in [González Vasco et al. 03], as we shall show.

Theorem 4.1. *Let G be a finite group with subgroups H and K such that $H \cap gKg^{-1} = 1$ for all $g \in G$. Let*

$$G = \bigcup_{i=1}^{n} Hg_iK$$

be the double coset decomposition of G with respect to H and K. Suppose that H and K each have a minimal logarithmic signature. If n is a prime number or $n \in \{1, 4\}$, then G has a minimal logarithmic signature.

Proof: It is known that $[G : K] = \sum_{i=1}^{n} [H : H \cap g_iKg_i^{-1}]$. As $H \cap g_iKg_i^{-1} = 1$ by the assumption, we have $[G : K] = |G|/|K| = n|H|$. Thus $|G| = n|H||K|$.

Let α_H be an MLS for H and let α_K be an MLS for K. Since any element $g \in G$ can be written in the form $g = hg_ik$ with $h \in H$, $k \in K$, and $i \in \{1, \ldots, n\}$, it is clear that $\alpha = [\alpha_H, \{g_1, \ldots, g_n\}, \alpha_K]$ is an MLS for G, if $n \in \{1, 4\}$ or n is a prime number, as stated. □

Remark 4.2. If $n = 1$ in Theorem 4.1, then $G = H.K$ with $H \cap K = 1$ and consequently $G = H.K^g$ for any $g \in G$. Moreover, the block with double coset representatives of the logarithmic signature described in the theorem is reduced to a set with a single element, namely the identity, and therefore can be omitted. So we actually have a factorization of G into a product of two subgroups with trivial intersection.

The following result is an application of Theorem 4.1 to the special linear groups $SL_n(q)$ and the projective special linear groups $L_n(q)$.

Theorem 4.3. *Let $2 \leq n \in \mathbb{N}$ and q a prime power such that $\gcd(n, q-1) \in \{1, 4\}$ or $\gcd(n, q-1)$ is a prime number. Then the groups $L_n(q)$ and $SL_n(q)$ have an MLS.*

Proof: Let V be an n-dimensional vector space over $GF(q)$ and $G := GL(V) \cong GL_n(q)$ as well as $S := SL(V) \cong SL_n(q)$. Moreover, let $Z := \mathbb{Z}(G)$ and $\overline{G} := G/Z$. So, in particular, $Z_0 = Z \cap S$ is cyclic of order $d := \gcd(n, q-1)$ and $\overline{S} = SZ/Z \cong S/Z_0 \cong L_n(q)$.

Clearly,

$$H = \left\{ \left(\begin{array}{cccc} a_1 & 0 & \cdots & 0 \\ a_2 & & & \\ \vdots & & A_1 & \\ a_n & & & \end{array} \right) \middle| \; a_i \in GF(q), \right.$$

$$\left. a_1 \neq 0, \; A_1 \in GL_{n-1}(q) \right\}$$

is the stabilizer in G of a one-dimensional subspace of V; in particular, $H = Z \times Q : L$, where $Q \cong q^{n-1}$ and $L \cong GL_{n-1}(q)$ are as in the proof of Theorem 3.1.

Now $H_0 := H \cap S = Q : L_0$, where $L_0 := (Z \times L) \cap S \cong GL_{n-1}(q)$ with $L \trianglerighteq Z_0$. Similar to the proof of Theorem 3.1, let K be a cyclic subgroup of order $q^n - 1$ in G acting sharply transitive on $V \setminus \{0\}$ with $\mathbb{C}_G(K) = K$. Then $K_0 := K \cap S$ is cyclic of order $\frac{q^n-1}{q-1}$; moreover, $K_0 \cap Z = Z_0$. Since $\overline{K} = KZ/Z$ acts sharply transitive on the projective space $PG(V)$, the group $\overline{K}_0 = K_0/Z_0$ must act regularly on $PG(V)$. In particular, $\overline{H}_0 \cap \overline{K}_0^g = 1$ for all $g \in \overline{S}$.

Next, we observe that $\overline{H}_0 \cong H_0/Z_0$ is isomorphic to a semidirect product of Q and L_0/Z_0. Therefore, by Theorem 3.1 and Lemma 2.4, H_0 has an MLS. Clearly, $\overline{K}_0$ has an MLS. Since

$$\begin{aligned} |\overline{H}_0\overline{K}_0| &= |\overline{H}_0||\overline{K}_0| = \frac{q^{n-1}|GL_{n-1}(q)|}{d} \cdot \frac{q^n - 1}{d(q-1)} \\ &= \frac{|GL_n(q)|}{(q-1)d^2} = \frac{|\overline{S}|}{d}, \end{aligned}$$

the claim now follows from Theorem 4.1 and Lemma 2.4. □

Corollary 4.4. *For $n \in \{4, p \mid p \text{ prime}\}$ the groups $L_n(q)$ and $SL_n(q)$ have an MLS.*

5. MLS FOR SIMPLE GROUPS OF ORDER LESS THAN 175,560 CONSTRUCTED BY MDCD

As mentioned above, the MDCD works perfectly for finite simple groups G of small order. Here, we want to show this fact for $|G| < 175,560$. These groups have been treated in [González Vasco et al. 03] by the method of factorization into a product of disjoint subgroups.

In the following list, we show a pair of subgroups H and K for G that satisfies the condition of Theorem 4.1. However, we omit the alternating groups A_n; the projective special linear groups $L_2(q)$ for $q \in \{4, 5, 7, 9, 8, 11, 13, 17, 19, 16, 23, 25, 27, 31, 32, 37\}$; and $L_3(2)$, $L_3(3)$, and $L_4(2)$ since these groups are proved to have an MLS by Corollary 4.4. It should be mentioned that different pairs of H and K may exist. For instance, if $G = L_2(8)$, then the following pairs can be chosen: $(H = 2^3,\ K = 3^2)$, $(H = 2^3 : 7,\ K = 3)$, $(H = D_{18},\ K = 7)$, $(H = D_{14},\ K = 3^2)$. If the existence of H and K can essentially be read off from information in the ATLAS [Conway et al. 85], then we just present H and K without comments, otherwise we will prove their existence, for instance, as in the case of the group $G = U_3(5)$.

1. $G = U_3(3) \cong G_2(2)'$, $|G| = 6,048 = 2^5 \cdot 3^3 \cdot 7$,
   $H = 3^{1+2} : 8$, $K = 7$.

2. $G = M_{11}$, $|G| = 7,920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$,
   $H = A_6$, $K = 11$.

3. $G = U_4(2) \cong S_4(3)$, $|G| = 25,920 = 2^6 \cdot 3^4 \cdot 5$,
   $H = 2^4 : 2^2$, $K = 3^3 : 3$.

4. $G = Sz(8)$, $|G| = 29,120 = 2^6 \cdot 5 \cdot 7 \cdot 13$,
   $H = 2^{3+3} : 7$, $K = 13$.

5. $G = U_3(4)$, $|G| = 62,400 = 2^6 \cdot 3 \cdot 5^2 \cdot 13$,
   $H = 2^{2+4} : 15$, $K = 13$.

6. $G = M_{12}$, $|G| = 95,040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$,
   $H = 3^2 : 2S_4$, $K = 11.5$.

7. $G = U_3(5)$, $|G| = 126,000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7$,
   $H = A_7$, $K = 5^2$.

There are four classes of elements of order 5 in G, where four elements in the center of a Sylow 5-subgroup 5^{1+2} are of type 5A. There are three classes of maximal subgroups A_7 in G, the first class contains only elements of type 5B, the second elements of type 5C, and the third elements of type 5D. Now take $H = A_7$ containing elements of type 5B.

Further, G contains $S := Q : 8$ as a maximal subgroup with $Q = 5^{1+2}$. Let $L = A_7$ be the class of A_7-subgroups containing elements of type 5C. We have $X := S \cap L = D_{20} = 5\mathrm{C} : 4$. Let $\mathbb{Z}(Q) = \langle 5\mathrm{A} \rangle$ and let $K = \langle 5\mathrm{A}, 5\mathrm{C} \rangle$ be an elementary abelian group of order 5^2 with $5\mathrm{A} \in \mathbb{Z}(Q)$ and $5\mathrm{C} \in D_{20}$. As $K \trianglelefteq Q : 4$ and $\mathbb{C}_S(K) = K$, it follows that K contains 20 elements of type 5C and four elements of type 5A. In other words, $gKg^{-1} \cap H = 1$ for all $g \in G$. Thus we have a pair of subgroups (H, K) in G satisfying the condition of Theorem 4.1.

Here we want to make a remark about the first Janko group J_1 with order 175,560. By inspection of the list of maximal subgroups of J_1 we easily see that J_1 cannot be factored as a product of two proper subgroups A and B. The following result has been obtained by a computer search with the Magma algebra system [Bosma et al. 97].

Theorem 5.1. *J_1 has no proper subgroups A, B, and C such that $J_1 = A.B.C$ and $|J_1| = |A| \cdot |B| \cdot |C|$.*

We do not know whether J_1 can be described as a product of more than three disjoint proper subgroups. But, in view of Theorem 5.1, the question of the existence of an MLS for J_1 on the basis of product of subgroups seems to be difficult. Below, we see however that the existence of an MLS for J_1 immediately follows by the double coset method.

6. MLS FOR SIMPLE GROUPS G OF ORDER $175,560 \leq |G| \leq 10^{10}$

The main aim of this section is to construct minimal logarithmic signatures by the MDCD for simple groups of order $\leq 10^{10}$. It turns out that, except for a few groups where the existence or the nonexistence of an MLS cannot be settled yet, the method works for almost all groups in the range. As in the previous section we present a pair of subgroups (H, K) of a simple group G satisfying the condition of Theorem 4.1. For each group G we give only one pair of (H, K), even though we know that other possibilities for such a pair exist or $G = A.B$ with $A \cap B = 1$. An item with × × means that the double coset method does not work for that group, and a proof is presented in the next section. Since the groups $L_n(q)$ with $|L_n(q)| \leq 10^{10}$ will have $n = 2, 3, 4, 5$, and therefore have an MLS by Corollary 4.4, these groups as well as the alternating groups are not included in the list below.

1. $G = J_1$, the first Janko group, $|G| = 175,560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$,
   $H = 2^3 : 7 : 3$, $K = 11 : 5$.

2. $G = M_{22}$, $|G| = 443,520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$,
   $H = L_3(4)$, $K = 11$.

3. $G = J_2$, the second Janko group, $|G| = 604,800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$,
   $H = U_3(3)$, $K = 5^2$.

4. $G = S_4(4)$, $|G| = 979,200 = 2^8 \cdot 3^2 \cdot 5^2 \cdot 17$,
   $H = 2^6 : (3 \times A_5)$, $K = 17$.

5. $G = S_6(2)$, $|G| = 1,451,520 = 2^9 \cdot 3^4 \cdot 5 \cdot 7$,
   $H = U_4(2) : 2$, $K = 7$.

6. $G = U_4(3)$, $|G| = 3,265,920 = 2^7 \cdot 3^6 \cdot 5 \cdot 7$,
   $H = L_3(4)$, $K = [3^4]$.

   Let $H = L_3(4)$ be a class of maximal subgroup of G. Now G has four conjugate classes 3A, 3B, 3C, 3D of elements of order 3. By inspection of the permutation character $1_H^G = 1a + 21a + 140a$, it follows that H only contains elements of type 3D. Now consider the first class of maximal subgroup $L = U_4(2)$ with the permutation character $1_L^G = 1a + 35a + 90a$. This shows that L does not contain elements of type 3D, in fact L contains elements of types 3A, 3B, and 3C. Now let $K = [3^4]$ be a Sylow 3-subgroup of L. Then $gKg^{-1} \cap H = 1$ for all $g \in G$. Thus we have a pair (H, K) in G satisfying the condition of Theorem 4.1, as required.

7. $G = G_2(3)$, $|G| = 4,245,696 = 2^6 \cdot 3^6 \cdot 7 \cdot 13$,
   $H = U_3(3) : 2$, $K = 3^{1+2}$.

   G contains five classes of elements of order 3. Let $H = U_3(3) : 2$ be a maximal subgroup of G with the permutation character $1_H^G = 1a + 168a + 182b$. Then H contains no 3-elements of type 3A, 3C, and 3D. Let $L = L_3(3) : 2$ be a maximal subgroup of G with the permutation character $1_L^G = 1a + 91c + 104a + 182a$. This shows that L only contains 3A- and 3D-elements. Let $K = 3^{1+2} \leq L$ be a Sylow 3-subgroup of L. Then $gKg^{-1} \cap H = 1$ for all $g \in G$. Thus an appropriate pair (H, K) in G satisfying the condition of Theorem 4.1 is found.

8. $G = S_4(5)$, $|G| = 4,680,000 = 2^6 \cdot 3^2 \cdot 5^4 \cdot 13$,
$H = 5^{1+2} : 2A_5$, $K = S_4$.

   Let $H_0 = 5^{1+2} : 4A_5$ be a maximal subgroup of G and let $H = (H_0)' = 5^{1+2} : 2A_5$ be the commutator group of H_0. Now G has two classes of involutions and two classes of elements of order 3. A consideration of the permutation character $1_{H_0}^G = 1a+65b+90a$ (see [Conway et al. 85, page 62]) shows that H contains no 2B-elements and no 3A-elements. Now consider a maximal subgroup $L = A_6$ of G. By the information in [Conway et al. 85] L contains 2B-elements and L contains two classes of S_4; one class contains 3A-elements and the other 3B elements. Now take $K = S_4 \leq L$ such that K only contains 3A-elements. Then $gKg^{-1} \cap H = 1$ for all $g \in G$. We therefore have a pair (H, K) in G satisfying the condition of Theorem 4.1.

9. $G = U_3(8)$, $|G| = 5,515,776 = 2^9 \cdot 3^4 \cdot 7 \cdot 19$,
$H = 2^{3+6} : 7$, $K = [3^4]$.

10. $G = U_3(7)$, $|G| = 5,663,616 = 2^7 \cdot 3 \cdot 7^3 \cdot 43$,
$H = 7^{1+2} : 3$, $K = [2^7]$.

11. $G = M_{23}$, $|G| = 10,200,960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$,
$H = 2^4 : A_7$, $K = 11$.

12. $G = U_5(2)$, $|G| = 13,685,760 = 2^{10} \cdot 3^5 \cdot 5 \cdot 11$,
$H = 2^{1+6} : 3^{1+2} : 2A_4$, $K = 11 : 5$.

13. $G = {}^2F_4(2)'$, the Tits group, $|G| = 17,971,200 = 2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$,
$\times\ \times$.

14. $G = Sz(32)$, the Suzuki group, $|G| = 32,537,600 = 2^{10} \cdot 5^2 \cdot 31 \cdot 41$,
$H = 2^{5+5} : 31$, $K = 25$.

15. $G = U_3(9)$, $|G| = 42,573,600 = 2^5 \cdot 3^6 \cdot 5^2 \cdot 73$,
$\times\ \times$.

16. $G = HS$, the Higman-Sims group, $|G| = 44,352,000 = 2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$,
$H = M_{22}$, $K = 5^2$.

   G has three classes 5A, 5B, and 5C of 5-elements. Let $H = M_{22}$ be a maximal subgroup of G. Then the permutation character $1_H^G = 1a+22a+77a$ shows that 5-elements in H are of type 5C. Consider $L = 5 : 4 \times A_5$, a maximal subgroup of G. The 5-elements in L are of type 5A and 5B only, for it can be seen in $O_5(C_G(5A)) = 5^{1+2}$ that the product of commuting 5A and 5B is of type 5B. Let $K = 5^2 \leq L$ be a Sylow 5-subgroup of L. Then $gKg^{-1} \cap H = 1$ for all $g \in G$. Hence the pair (H, K) can be used to construct an MLS for G.

17. $G = J_3$, the third Janko group, $|G| = 50,232,960 = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$,
$\times\ \times$.

18. $G = U_3(11)$, $|G| = 70,915,680 = 2^5 \cdot 3^2 \cdot 5 \cdot 11^3 \cdot 37$,
$H = 11^{1+2} : 5$, $K = (4^2 \times 3) : S_3$.

19. $G = S_4(7)$, $|G| = 138,297,600 = 2^8 \cdot 3^2 \cdot 5^2 \cdot 7^4$,
$H = 7^{1+2}(3 \times SL_2(7))$, $K = 5^2 : 4$.

   Using Magma, we can verify that $H := \mathbb{N}_G(\langle 7A \rangle) = 7^{1+2}(3 \times SL_2(7))$ of order $2^4 \cdot 3^2 \cdot 7^4$ contains involutions of type 2A only, whereas $K := \mathbb{N}_G(5^2) = 5^2 : 4$ only has involutions of type 2B. Thus H and K are a pair of subgroups of G satisfying the condition of Theorem 4.1.

20. $G = O_8^+(2)$, $|G| = 174,182,400 = 2^{12} \cdot 3^5 \cdot 5^2 \cdot 7$,
$H = S_6(2)$, $K = A_5$.

   First note that G has five classes of involutions, five classes of 3-elements and three classes of 5-elements. Let $H = S_6(2)$ be a maximal subgroup of G with the permutation character $1_H^G = 1a + 35a + 84a$. Then H contains no elements of type 2C, 2D, 3B, 3C, 5B, 5C. Further, there is a subgroup $K = A_5$ in G containing 2B-elements, 3B-elements and 5B-elements only. Thus $gKg^{-1} \cap H = 1$ for all $g \in G$. Thus H and K are the desired pair.

21. $G = O_8^-(2)$, $|G| = 197,406,720 = 2^{12} \cdot 3^4 \cdot 5 \cdot 7 \cdot 17$,
$H = 2^6 : U_4(2)$, $K = 17$.

22. $G = {}^3D_4(2)$, $|G| = 211,341,312 = 2^{12} \cdot 3^4 \cdot 7^2 \cdot 13$,
$\times\ \times$.

23. $G = M_{24}$, $|G| = 244,823,040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$,
$H = 2^4 : A_8$, $K = 23 : 11$.

24. $G = G_2(4)$, $|G| = 251,596,800 = 2^{12} \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13$,
$\times\ \times$.

25. $G = U_3(13)$, $|G| = 811,273,008 = 2^4 \cdot 3 \cdot 7^2 \cdot 13^3 \cdot 157$,
$\times\ \times$.

26. $G = M^cL$, the McLaughlin group, $|G| = 898,128,000 = 2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$,
$\times\ \times$.

27. $G = U_4(4)$, $|G| = 1,018,368,000 = 2^{12} \cdot 3^2 \cdot 5^3 \cdot 13 \cdot 17$,
$H = 2^8 : (3 \times L_2(16))$, $K = 5^2$.

Let S be a Sylow 2-subgroup of G. Consider $H = \mathbb{N}_G(\mathbb{C}_S(S')) \cong 2^8 : (3 \times L_2(16))$ of order $2^{12} \cdot 3^2 \cdot 5 \cdot 17$. Let F be a Sylow 5-subgroup of G. Then $N = \mathbb{N}_G(F) = 5^3 : S_4$. Let $T \in Syl_3(N)$. Define $K = [F, T] \cong 5^2$. Using Magma one shows that the 5-elements in K are not conjugate to 5-elements in H. Thus H and K are a desired pair.

28. $G = S_4(8)$, $|G| = 1,056,706,560 = 2^{12} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 13$, $H = L_2(64) : 2$, $K = L_2(8)$.

By using Magma we see that G contains a pair of subgroups $H \cong L_2(64) : 2$ of order $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$ and $H \cong L_2(8)$ of order $2^3 \cdot 3^2 \cdot 7$ such that $H \cap K^g = 1$ for all $g \in G$.

29. $G = S_4(9)$, $|G| = 1,721,606,400 = 2^8 \cdot 3^8 \cdot 5^2 \cdot 41$, $H = 3^{2+4} : \hat{2}A_6$, $K = 5 \times D_{16}$.

Let $S \in Syl_3(G)$. Then $\mathbb{Z}(S) \cong 3^2$ and $N := \mathbb{N}_G(\mathbb{Z}(S)) \cong 3^{2+4}(8 * \hat{2}A_6)$. Define $H := N' = 3^{2+4} : \hat{2}A_6$, which is of order $2^4 \cdot 3^8 \cdot 5$. By using Magma we see that 5-elements of H are of type 5AB and involutions of H are of type 2A. Further G contains 5-elements of type 5CD such that $\mathbb{N}_G(\langle 5CD \rangle) \cong (\langle 5CD \rangle \times PGL_2(9)) : 2$ and $\mathbb{C}_G(5CD) \geq K \cong \langle 5CD \rangle \times D_{16}$ with involutions in K all of type 2B. So $H \cap K^g = 1$ for all $g \in G$.

30. $G = U_3(17)$, $|G| = 2,317,678,272 = 2^6 \cdot 3^4 \cdot 7 \cdot 13 \cdot 17^3$, × × .

31. $G = He$, the Held group, $|G| = 4,030,387,200 = 2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$,
$H = S_4(4) : 2$, $K = 7^2 : D_{21}$.

Note that G has two classes of involutions and two classes of 3-elements. Let $H = S_4(4) : 2$ be a maximal subgroup of G. An inspection of the permutation character 1_H^G shows that H contains no 3-elements of type 3B. Let $L = 7^2 : 2L_2(7)$ be a maximal subgroup of G. We have $H \cap L \leq 2.S_4$. Now G contains only one class of elements of order 8, with fourth power of type 2B. Hence the involutions in $H \cap L$ are of type 2B. Any element in G of order 3 which commutes with a 2B-element is of type 3B. Thus 3-elements in L are of type 3B. Now let $K = 7^2 : F_{21} \leq L$. Then the pair (H, K) satisfies the condition of Theorem 4.1.

32. $G = U_3(16)$, $|G| = 4,279,234,560 = 2^{12} \cdot 3 \cdot 5 \cdot 17^2 \cdot 241$, $H = [2^{12}] : 255$, $K = 241$.

Here H is the normalizer of a Sylow 2-subgroup in G.

33. $G = O_7(3)$, $|G| = 4,585,351,680 = 2^9 \cdot 3^9 \cdot 5 \cdot 7 \cdot 13$, $H = G_2(3)$, $K = A_6$.

G contains three classes of involutions and seven classes of 3-elements. Let $H = G_2(3)$ be a class of maximal subgroup of G having the permutation character $1_H^G = 1a + 260a + 891a$. Then H contains no involutions of type 2A and 2B and no 3-elements of type 3B, 3C, and 3E. Let $L = (S_4 \times S_6)$ be a maximal subgroup of G and let $K = (S_4 \times S_6)^{(\infty)} \cong A_6$. A computation with the Magma algebra system [Bosma et al. 97] shows that the involutions in K are of type 2B and the 3-elements are of type 3B or 3C. Thus $gKg^{-1} \cap H = 1$ for all $g \in G$. Hence G has an MLS.

34. $G = S_6(3)$, $|G| = 4,585,351,680 = 2^9 \cdot 3^9 \cdot 5 \cdot 7 \cdot 13$, $H = 3^{1+4} : 2U_4(2)$, $K = (7 \times 2) : 2$.

Let $H = 3^{1+4} : 2U_4(2)$. A consideration of the permutation character 1_H^G shows that H contains no involutions of type 2B. Let $L = (7 \times 2) : 6$ be the normalizer of a Sylow 7-subgroup in G. By the information in [Conway et al. 85] all involutions in L are of type 2B. Now take $K = (7 \times 2) : 2 \leq L$, then $gKg^{-1} \cap H = 1$ for all $g \in G$. The pair (H, K) gives an MLS for G.

35. $G = G_2(5)$, $|G| = 5,859,000,000 = 2^6 \cdot 3^3 \cdot 5^6 \cdot 7 \cdot 31$, $H = U_3(3) : 2$, $K = [5^6]$.

36. $G = U_6(2)$, $|G| = 9,196,830,720 = 2^{15} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11$, $H = 2^9 : L_3(4) : 2$, $K = [3^4]$.

Let $H = 2^9 : L_3(4) : 2$ be a maximal subgroup of G. An inspection of the permutation character 1_H^G shows that the 3-elements of H are of type 3C. Let $C = C_G(9A) = S_3 \times \langle 9A \rangle$ be the centralizer of a 9A-element in G and let $T = O_3(C)$. Then $L = N_G(T)$ has the order $2 \cdot 3^5$. The Sylow 3-subgroup of L contains a subgroup $K = [3^4]$ such that $T < K$ and K contains no 3C-elements. Thus $gKg^{-1} \cap H = 1$ for all $g \in G$. Hence the pair (H, K) satisfies the condition of Theorem 4.1.

7. SIMPLE GROUPS OF ORDER $\leq 10^{10}$ HAVING NO MLS BY THE MDCD

In this section, we present a proof that the method of double coset decomposition does not provide an MLS for the eight groups marked by × × in the list of Section 6. Thereby, we show that further methods need to be developed in order to prove or disprove the existence of an MLS for finite simple groups in general.

In each of the following eight cases we assume by way of contradiction that G has a double coset decomposition $G = \cup_{i=1}^{r} Hg_iK$ with subgroups H and K satisfying the condition of Theorem 4.1; so, in particular, we assume that $r \in \{1,4\}$ or r is a prime.

7.1 $G = {}^2F_4(2)'$, The Tits Group, $|G| = 17,971,200 = 2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$

Since G has only one class of 3-elements, we may assume that $3^2 \mid |H|$ and $3 \nmid |K|$. By inspection of possible maximal subgroups M containing H in G we have $M \in \{L_3(3):2,\ A_6.2^2\}$.

If $|H|_3 = 3^2$, then $r = 3$, $|H| \mid 2^5 \cdot 3^2 \cdot 5$, and $2^6 \cdot 5 \cdot 13 \mid |K|$. Since G has no subgroups of order divisible by $2^6 \cdot 5 \cdot 13$, we derive a contradiction. Therefore $|H|_3 = 3^3$ and $M = L_3(3):2$; in particular, $3^3 \mid |H| \mid 2^5 \cdot 3^3 \cdot 13$ and $2^4 \cdot 5 \mid |K|$.

Note that G has no subgroups of order divisible by $2^4 \cdot 5 \cdot 13$ or $2^6 \cdot 5^2$. Therefore $r \neq 13$ and $M' \leq H \leq M$ with $|H| \in \{2^4 \cdot 3^3 \cdot 13, 2^5 \cdot 3^3 \cdot 13\}$.

If $r \in \{2,4\}$, we get $K = 5^2 : [2^4]$, $r = 4$, and $H = M$; this is a contradiction, because then K contains representatives of each class of involutions in G. Thus we have $r = 5$ and $(|H|,|K|) \in \{(2^4{\cdot}3^3{\cdot}13, 2^7{\cdot}5), (2^5{\cdot}3^3{\cdot}13, 2^6{\cdot}5)\}$. In any case, H contains only involutions of type $2B$ in G, and so K contains only involutions of type $2A$. Let $X \in Syl_5(K)$ and observe that $N_G(X) = P : X_2$ with $P \in Syl_5(G)$ and $X_2 \equiv Z_4 \times Z_2$; moreover, any subgroup of order 4 in X_2 contains involutions of type $2B$. This in turn implies that $|N_K(X)| \in \{5, 5{\cdot}2\}$. As this contradicts Sylow's theorem, the claim follows.

7.2 $G = U_3(9)$, $|G| = 42,573,600 = 2^5 \cdot 3^6 \cdot 5^2 \cdot 73$

Since G has only one class of involutions, we may assume that $2^3 \mid |H|$ and that $|K|$ is odd.

If $r \in \{2,4\}$, then an inspection of the subgroup structure of G reveals that $73 \mid |K| \mid 73 \cdot 3$ and hence $2^5{\cdot}3^5{\cdot}5^2 \mid |H|$. Since G has no subgroups of order divisible by $2^5 \cdot 3^5 \cdot 5^2$, we have reached a contradiction. Therefore r is an odd prime and $2^5 \mid |H|$; furthermore, if L is a maximal subgroup of G containing H, then $L \equiv 5 \times 2.A_6.2$ and $2^5 \mid |H| \mid 2^5 \cdot 3^2 \cdot 5^2$. Now we get $3^3 \mid |K|$ and thus $73 \nmid |K|$; hence $r = 73$ and $3^4 \mid |K| \mid 3^6 \cdot 5^2$. An inspection of the maximal subgroups of G now shows that $K \leq M \equiv 3^{2+4} : 5$. This in turn implies $5 \mid |H|$.

Assume now that $5 \mid |K|$. Since elements of order 5 in M act irreducibly on $O_3(M)/Z(O_3(M)) \equiv 3^4$, we get $K = M$ and $H = O_5(L) \times L_2$ with $L_2 \in Syl_2(L)$. We have derived a contradiction, because the Sylow 5-subgroups of M are conjugate to $O_5(L)$ in G.

We have shown that $5^2 \mid |H|$ and consequently $H = L$. This in turn implies $|K| = 3^4$. Since elements of order 3 in H commute with an involution, they are all of type $3A$ in G. On the other hand, $K \cap Z(O_3(M)) \neq 1$ and the nontrivial elements of $Z(O_3(M))$ are of type $3A$ in G as well. This gives the desired final contradiction.

7.3 $G = J_3$, The Third Janko Group, $|G| = 50,232,960 = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$

Since G has one class of involutions we may assume that $2^5 \mid |H|$ and that $|K|$ is odd. If $|H|_2 = 2^5$ or 2^6, then $3^5{\cdot}5{\cdot}17{\cdot}19 \mid |K|$, which is a contradiction to the orders of maximal subgroups in G. Thus we have $|H|_2 = 2^7$ and H is contained in either $2^{1+4} : A_5$ or $2^{2+4} : (3 \times S_3)$, which are maximal subgroups of G. It follows that $|H|_3 \mid 3^2$. Therefore $3^2 \mid |K|_3$. If $r = 3$, then $17 \cdot 19 \mid |K|$, a contradiction to the orders of maximal subgroups in G. So we have $r \neq 3$ and $|K|_3 \geq 3^3$. Since the number of double coset representatives with respect to H and K is 1, 4, or prime, we get $17 \mid |K|$ or $19 \mid |K|$, again a contradiction to the orders of maximal subgroups in G.

7.4 $G = {}^3D_4(2)$, $|G| = 211,341,312 = 2^{12} \cdot 3^4 \cdot 7^2 \cdot 13$

First note that G has nine classes of maximal subgroups, namely (1) $2^{1+8} : L_2(8)$, (2) $2^2.[2^9] : (7 \times S_3)$, (3) $U_3(3) : 2$, (4) $S_3 \times L_2(8)$, (5) $(7 \times L_2(7)) : 2$, (6) $3^{1+2} : 2S_4$, (7) $7^2 : 2A_4$, (8) $3^2 : 2A_4$, (9) $13 : 4$.

Assume $H \leq 2^{1+8} : L_2(8)$, or $H \leq 2^2.[2^9] : (7 \times S_3)$. Assume $|H|$ is even. As G has no subgroup of order divisible by $3 \cdot 7 \cdot 13$, we see that $3^2 \mid |H|$. If $|K|_3 = 3^2$, then $|H|_3 = 3^2$; this implies $H \leq 2^{1+8} : L_2(8)$ and then H must be a proper subgroup of $2^{1+8} : L_2(8)$, because G has no subgroup of odd order divisible by $3^2 \cdot 7$ or $3^2 \cdot 13$. Since $|H|_3 = 3^2$, we have $H \leq 2^{1+8} : D_{18}$, and thus $2 \mid |K|$; it follows that either $2 \cdot 3^2 \cdot 7 \cdot 13 \mid |K|$ or $2 \cdot 3^2 \cdot 7^2 \mid |K|$ and we obtain a contradiction because G has no such proper subgroups K. This proves that $2 \nmid |H|$. As the role of H and K may be interchanged, we conclude that K is neither a subgroup of even order of $2^{1+8} : L_2(8)$ nor of $2^2.[2^9] : (7 \times S_3)$.

Assume $H \leq 7^2 : 2A_4$, $3^2 : 2A_4$, or $13 : 4$. Then $|H|_2 \leq 2^3$ and $2^7 \mid |K|$. Hence K is contained in either $2^{1+8} : L_2(8)$ or $2^2.[2^9] : (7 \times S_3)$, a contradiction.

Assume $H \leq S_3 \times L_2(8), (7 \times L_2(7)) : 2$, or $3^{1+2} : 2S_4$. Then $|H|_2 \leq 2^4$ and $2^6 \mid |K|$. If $|K|_2 = 2^6$, then $13 \mid |K|$, a contradiction to the order of subgroups in G. Therefore

$2^7 \mid |K|$. This in turn implies that K is a subgroup of $2^{1+8} : L_2(8)$ or of $2^2.[2^9] : (7 \times S_3)$, a contradiction.

Finally, assume $H \leq U_3(3) : 2$. Then $2^4 \mid |K|$. As K cannot be a subgroup of $2^{1+8} : L_2(8)$ or of $2^2.[2^9] : (7 \times S_3)$, it follows that $|K|_2 \leq 2^6$. The cases $|K|_2 = 2^4$ or 2^5 are easily ruled out. Thus $|K|_2 = 2^6$. This implies that $3 \cdot 7 \mid |K|$ and $K \leq U_3(3) : 2$ and therefore $K = U_3(3) : 2$. Thus $gKg^{-1} \cap H \neq 1$ for some $g \in G$, a contradiction.

7.5 $G = G_2(4)$, $|G| = 251,596,800 = 2^{12} \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13$

Suppose first that $r \neq 13 \mid |K|$. Then K is isomorphic to one of the following groups: 13, 13:2, 13:3, 13:6, $L_2(13)$ $(2^2 \cdot 3 \cdot 7 \cdot 13)$, $U_3(4)$ $(2^6 \cdot 3 \cdot 5^2 \cdot 13)$, $U_3(4).2$ $(2^7 \cdot 3 \cdot 5^2 \cdot 13)$. This implies that $|K|_3 = 3$ and 3-elements in K are of type 3B (by inspection of permutation characters). Since any subgroup of order 3^2 in G contains elements of type 3A and type 3B, we get $r = |H|_3 = |K|_3 = 3$; and the 3-elements in H are of type 3A and $|H| = \frac{|G|}{3 \cdot |K|} \in \{2^{12} \cdot 3 \cdot 5^2 \cdot 7,\ 2^{11} \cdot 3 \cdot 5^2 \cdot 7,\ 2^{10} \cdot 3 \cdot 5^2,\ 2^6 \cdot 3 \cdot 7,\ 2^5 \cdot 3 \cdot 7\}$. The first three possibilities are excluded by inspection of the orders of maximal subgroups of G. This leaves $|H| \in \{2^6 \cdot 3 \cdot 7,\ 2^5 \cdot 3 \cdot 7\}$ and so H must be conjugate to a subgroup of $U_3(3).2$, $\hat{3}L_3(4).2_3$, or J_2; since none of these three maximal subgroups of G contains a subgroup of order $|H|$, we have reached a contradiction. We have shown that $13 \nmid |K|$. Clearly, by symmetry, $13 \nmid |H|$ and so $r = 13$.

Since any subgroup of order 3^2 in G contains elements of type 3A and type 3B, we may assume without loss of generality that $3^3 \mid |H|$. In particular, H is conjugate to a subgroup of J_2 $(2^7 \cdot 3^3 \cdot 5^2 \cdot 7)$, $L := \hat{3}L_3(4).2_3$ $(2^7 \cdot 3^3 \cdot 5 \cdot 7)$, or $U := U_3(3).2$ $(2^6 \cdot 3^3 \cdot 7)$ and $2^5 \mid |K|$. Observe that each of J_2, L, and U contains involutions of type 2A and type 2B. Therefore H must be conjugate to a proper subgroup of J_2, L, or U.

Assume next that $3^3 \cdot 7 \mid |H|$. An inspection of the subgroup structure of J_2, L, and U then shows that H is isomorphic to $\hat{3}L_3(4)$ or $U_3(3)$; in particular, $(|H|, |K|) \in \{(2^6 \cdot 3^3 \cdot 5 \cdot 7\ ,\ 2^6 \cdot 5),\ (2^5 \cdot 3^3 \cdot 7\ ,\ 2^7 \cdot 5^2)\}$ and the involutions of H are of type 2A. Since neither J_2 nor $U_3(3).2$ contains subgroups of order $2^7 \cdot 5^2$, G contains no subgroup of order $2^7 \cdot 5^2$. So we conclude that $H \cong \hat{3}L_3(4)$ and $|K| = 2^6 \cdot 5$ and all involutions in K are of type 2B. Since the 5-elements in H are of type 5AB, the 5-elements in K are of type 5CD. By Sylow's theorem we find that $2 \mid |C_K(K_5)|$ for $K_5 \in Syl_5(K)$; this in turn implies that K contains elements of type 2A, a contradiction. We have shown that $7 \nmid |H|$ and hence $7 \mid |K|$.

Now $2^5 \cdot 7 \mid |K|$ and so K is conjugate to a proper subgroup of J_2, L, or U. In particular, $2^5 \mid |K|_2 \mid 2^7$ and thus $2^5 \mid |H|_2 \mid 2^7$. Now we easily see that in any case H and K contain involutions of the same type, thereby obtaining a final contradiction.

7.6 $G = U_3(13)$, $|G| = 811,273,008 = 2^4 \cdot 3 \cdot 7^2 \cdot 13^3 \cdot 157$

To deal with the group $G = U_3(13)$ we need various facts about conjugacy classes and subgroups of G which are not recorded in the literature, so we collect these facts in the following lemma.

Lemma 7.1. *Let $G = U_3(13)$.*

(i) Let X_p denote a representative of a G-conjugacy class of a prime order subgroup in G. We have

X_p	$\lvert X_p \rvert$	$\mathbb{C}_G(X_p)$	$\mathbb{N}_G(X_p)$
X_2	2	$7 \times (SL_2(13) : 2)$	$7 \times (SL_2(13) : 2)$
X_3	3	$8 \times 3 \times 7$	$(8 \times 3 \times 7) : 2$
X_{7A}	7	$7 \times (SL_2(13) : 2)$	$7 \times (SL_2(13) : 2)$
X_{7B}	7	$7 \times 7 \times 2^2$	$(7 \times 7 \times 2^2) : 3$
X_{7C}	7	$7 \times 7 \times 2^2$	$(7 \times 7 \times 2^2) : 3$
X_{13A}	13	$13^{1+2} : (2 \times 7)$	$13^{1+2} : (8 \times 3 \times 7)$
X_{13B}	13	13^2	$13^2 : (4 \times 3)$
X_{157}	157	157	$157 : 3$

(ii) G has a Sylow 7-normalizer isomorphic to $(7 \times 7 \times 2^2) : S_3$.

(iii) G has a Sylow 13-normalizer isomorphic to $13^{1+2} : (8 \times 3 \times 7)$.

(iv) If $X \lneqq G$ with $157 \mid |X|$, then $X \leq 157 : 3$.

(v) If $X \lneqq G$ with $13^2 \mid |X|$, then X is contained in a Sylow 13-normalizer of G.

Proof: The claims can be verified by means of Magma. □

In order to prove that $G = U_3(13)$ has no MLS by a double coset decomposition, we show first that $r = 157$ and without loss of generality $2^4 \mid |H|$. This in turn implies $13^{1+2} \leq K \leq 13^{1+2} : (3 \times 7)$ and $2^4 \cdot 7 \mid |H| \mid 2^4 \cdot 3 \cdot 7^2$. Using Lemma 7.1 we then derive $O_2(H) = O_3(H) = O_7(H) = 1$ and show that H is nonsolvable. Since the only nonabelian simple $\{2, 3, 7\}$-groups are $L_2(7)$ $(2^3 \cdot 3 \cdot 7)$, $L_2(8)$ $(2^3 \cdot 3^2 \cdot 7)$, and $U_3(3)$ $(2^5 \cdot 3^3 \cdot 7)$, we finally conclude that $H \cong Aut(L_2(7)) \cong L_2(7) : 2$. But then the Sylow 2-subgroups of H are dihedral of order 16, contrary to the fact that the Sylow 2-subgroups of G are semidihedral of order 16.

7.7 $G = M^cL$, the McLaughlin Group, $|G| = 898,128,000 = 2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$

As G has only one class of involutions, we may assume that $2^5 \mid |H|$ and that $|K|$ is odd.

Assume $|H|_2 = 2^5$ or 2^6. By an inspection of possible maximal subgroups M containing H in G we have $M \in \{U_4(3),\ M_{22},\ 2.A_8,\ 2^4 : A_7\}$. If $M = U_4(3)$, then $5^2 \cdot 11 \mid |K|$; if $M = M_{22}$, then $3^4 \cdot 5^2 \mid |K|$; if $M = 2.A_8$ or $2^4 : A_7$, then $3^4 \cdot 5^2 \cdot 11 \mid |K|$; all these cases give a contradiction. Thus we have $|H|_2 = 2^7$. We have the following possibilities: (1) $5^2 \mid |K|$, (2) $5 \cdot 11 \mid |K|$, (3) $3^4 \cdot 5 \mid |K|$, (4) $3^3 \cdot 5^2 \cdot 11 \mid |K|$, (5) $3^4 \cdot 5^2 \mid |K|$, and (6) $3^4 \cdot 5 \cdot 11 \mid |K|$. Cases (3), (4), (5), and (6) immediately lead to a contradiction. Case (2) is ruled out, since the 5-elements in K and H are of the same type, namely 5B. Case (1) is also not possible, since any group of order 5^2 contains 5-elements of both types 5A and 5B, we cannot have $gKg^{-1} \cap H = 1$ for all $g \in G$. Thus, we have reached the desired contradiction.

7.8 $G = U_3(17)$, $|G| = 2,317,678,272 = 2^6 \cdot 3^4 \cdot 7 \cdot 13 \cdot 17^3$

The following lemma collects information about the group $G = U_3(17)$ that is needed for our discussion and that cannot be found in the literature.

Lemma 7.2. *Let $G = U_3(17)$.*

(i) Let X_p denote a representative of a G-conjugacy class of a prime order subgroup in G. We have

X_p	$\lvert X_p \rvert$	$\mathbb{C}_G(X_p)$	$\mathbb{N}_G(X_p)$
X_2	2	$3 \times (SL_2(17) : 2)$	$3 \times (SL_2(17) : 2)$
X_{3A}	3	$3 \times (SL_2(17) : 2)$	$3 \times (SL_2(17) : 2)$
X_{3B}	3	$(3 \times 9 \times 2^2) : 3$	$(3 \times 9 \times 2^2) : S_3$
X_7	7	7×13	$(7 \times 13) : 3$
X_{13}	13	7×13	$(7 \times 13) : 3$
X_{17A}	17	$17^{1+2} : (2 \times 3)$	$17^{1+2} : (2^5 \times 3)$
X_{17B}	17	17^2	$17^2 : 16$
X_{17C}	17	17^2	$17^2 : 16$
X_{17D}	17	17^2	$17^2 : 16$

(ii) The Sylow 2-subgroups of G are semidihedral of order 64.

(iii) If $X \leq G$ with $|X| = 17^2$, then $\mathbb{N}_G(X) \cong 17^{1+2} : 16$. Moreover, apart from one subgroup of type X_{17A}, the group X contains 17 further subgroups of order 17, all of which have the same type.

(iv) If $X \leq G$ with $|X| = 17^3$, then $\mathbb{N}_G(X) \cong 17^{1+2} : (2^5 \times 3)$.

(v) If X is a proper subgroup of G with $17^2 \mid |X|$, then X is contained in a Sylow 17-normalizer of G.

Proof: The claims can easily be verified by means of Magma. □

We now prove that $G = U_3(17)$ has no MLS by a double coset decomposition. Since G has only one class of involutions we may assume without loss of generality that $2^4 \mid |H|$ and that $|K|$ is odd.

Using the information in Lemma 7.2 we then deduce that $17 \mid |K|$ and consequently $2^4 \cdot 17^2 \mid |H|$. This in turn leads to $r \in \{2, 4\}$, $7^{1+2} : 2^4 \leq H \leq 7^{1+2} : (2^5 \times 3)$, and $3^3 \cdot 7 \cdot 13 \mid |K| \mid 3^4 \cdot 7 \cdot 13$. Obviously, $O_7(K) = O_{13}(K) = 1$. As K is solvable, we get $Q := O_3(K) \neq 1$. Since $7 \nmid |GL_3(3)|$, we easily verify now that Q is centralized by an element of order 7. As this contradicts the information in Lemma 7.2, the desired result follows.

8. GROUPS HAVING A FACTORIZATION AS PRODUCT OF TWO NONDISJOINT SUBGROUPS

Let G be a finite group such that $G = H.K$ for some proper subgroups H and K. As a special case of the double coset method, we know by Theorem 4.1 that if $H \cap K = 1$ and if both H and K have an MLS, then G evidently has an MLS. In other words, we can "glue" MLS of H and K together to form an MLS for G. In this section, we attempt to explore the case $H \cap K \neq 1$. Here, the general question whether or not G has an MLS, when H and K do, seems to be difficult. A solution of the problem obviously depends on the subgroup structure of H and K and also on the structure of their MLS. It turns out that with an appropriate factorization of $G = H.K$ the "gluing method" actually works. We will illustrate the method by several nontrivial examples. Interestingly, in our examples the method of double coset decomposition still appears to be crucial.

8.1 $G = A_6$

In $G = A_6$ there are two classes of maximal subgroups isomorphic to A_5 having non-conjugate 3-elements. Let $H \cong A_5$ be in the first class and $K \cong A_5$ be in the second class. Obviously, $G = H.K$ and $W := H \cap K \cong D_{10}$. Let $X = 3$ be a subgroup of H and $Y = 3$ be a subgroup of K. Let α_W be an MLS for W, α_X an MLS for X, and α_Y an MLS for Y. By using the double coset method for H with the pair (W, X) we obtain an MLS α_H for H of the form

$$\alpha_H = \alpha_X \cup \{1, h\} \cup \alpha_W.$$

Similarly, using the pair (W, Y) for the double coset method we also obtain an MLS α_K for K with

$$\alpha_K = \alpha_W \cup \{1, k\} \cup \alpha_Y.$$

This shows that

$$\alpha_G := \alpha_X \cup \{1, h\} \cup \alpha_W \cup \{1, k\} \cup \alpha_Y$$

is an MLS for G obtained by gluing α_H and α_K together.

8.2 $G = U_3(5)$

It is easy to see that $G = H.K$, where $H = Q : L$, $Q = 5^{1+2}$, $L = 8$, and $K = A_7$. Thus $X := H \cap K = D_{20}$.

Let $Z = \mathbb{Z}(Q) = 5$. The elements of Z are of type 5A, whereas the elements in $Q \setminus Z$ are of type 5B, 5C, or 5D. As the 5-elements of X are not of type 5A we may assume without loss of generality that the elements of X are of type 5B. Now take P a subgroup of order 5 of Q consisting of 5C-elements only. Then $A = Z.P = 5^2$ contains only elements of type 5A and 5C. Thus $A \cap X^h = 1$ for all $h \in H$. So we can construct an MLS α_H for H by using an MLS α_A for A and an MLS α_X for X, namely

$$\alpha_H = \alpha_A \cup \{1, g\} \cup \alpha_X.$$

By inspection of the maximal subgroups of $K = A_7$ we see that $X \leq M$ with $M = S_5$ a maximal subgroup of K. Let $C \leq M$ be any subgroup of order 3. Then the pair (X, C) provides an MLS α_M for M by the MDCD: precisely $\alpha_M = \alpha_X \cup \{1, h\} \cup \alpha_C$, in which α_C is an MLS for C. Now let $N \leq K$ be a subgroup of order 7. Using the MDCD with the pair (M, N) we obtain an MLS α_K of the form: $\alpha_K = \alpha_M \cup \{1, k_1, k_2\} \cup \alpha_N$, where α_N is an MLS for N. Thus

$$\alpha_K = \alpha_X \cup \{1, h\} \cup \alpha_C \cup \{1, k_1, k_2\} \cup \alpha_N.$$

By gluing α_H and α_K together we obtain the following MLS for G:

$$\alpha_G = \alpha_A \cup \{1, g\} \cup \alpha_X \cup \{1, h\} \cup \alpha_C \cup \{1, k_1, k_2\} \cup \alpha_N.$$

8.3 $G = J_2$

It is shown in [Liebeck et al. 90] that $G = A.B$ with $A = U_3(3)$ and $B = A_5 \times D_{10}$ both maximal subgroups of G, where $|A \cap B| = 6$. Let $C := A \cap B$. We state that C is a cyclic group of order 6. This can be seen as follows. G contains two classes of 6A and 6B elements, for which the square of an 6A element is of type 3A and the square of an 6B element is of type 3B. Now as any 3-element in the factor A_5 of B is of type 3A (see [Conway et al. 85, page 42]), we see that a 6-element of B is of type 6A. Further, an inspection of the permutation characters of $A = U_3(3)$ shows that A contains only 6A-elements. By conjugation, we conclude that $C = A \cap B$ contains a 6A-element, and therefore is cyclic. As a consequence, an involution in the factor D_{10} of B is of type 2A, whereas the involutions in the factor A_5 of B are of type 2B [Conway et al. 85].

Next we construct two appropriate MLS for B and A, so that they can be glued to form an MLS for G.

We take a pair of subgroup (H, K) for B satisfying the condition of Theorem 4.1 as follows: $H = 5^2$, a Sylow 5-subgroup and $K = C$. Then, with the double coset method, we obtain an MLS

$$\alpha_B = \alpha_H \cup \{1, x_1, x_2, x_3\} \cup \alpha_C,$$

where α_H, respectively α_C, are MLS for H, respectively C.

By conjugation we can assume that $C = A \cap B$ is contained in a maximal subgroup $M = 3^{1+2}.8$ of A. Let $L := 3^{1+2}.2 \trianglelefteq M$. We first construct an MLS for M having α_C as a block. Note that if α_L is any MLS for L, then it is easy to see that α_L can be extended to an MLS α_M for M as $M/L \cong 4$, (or see Lemma 2.4). Thus we have

$$\alpha_M = \alpha_L \cup \{1, y_1, y_2, y_3\}.$$

Further, $C \leq L$ and an 3-element of C is of type 3A. Let $D = 3B$ be a subgroup of order 3 in L. Then using the pair (C, D) for the double coset method, we obtain an MLS α_L for L of the form

$$\alpha_L = \alpha_C \cup \{1, u_1, u_2\} \cup \alpha_D.$$

Thus

$$\alpha_M = \alpha_C \cup \{1, u_1, u_2\} \cup \alpha_D \cup \{1, y_1, y_2, y_3\}.$$

Further, using the double coset method with a pair (M, N), where $N = 7$ is any Sylow 7-subgroup of H, we obtain an MLS α_A for A:

$$\alpha_A = \alpha_M \cup \{1, g_1, g_2, g_3\} \cup \alpha_N.$$

Hence

$$\alpha_A = \alpha_C \cup \{1, u_1, u_2\} \cup \alpha_D \cup \{1, y_1, y_2, y_3\} \cup \{1, g_1, g_2, g_3\} \cup \alpha_N.$$

Now gluing α_A and α_B together gives an MLS α_G for G with

$$\alpha_G = \alpha_H \cup \{1, x_1, x_2, x_3\} \cup \alpha_C \cup \{1, u_1, u_2\} \cup \alpha_D \cup \{1, y_1, y_2, y_3\} \cup \{1, g_1, g_2, g_3\} \cup \alpha_N.$$

9. CONCLUSIONS

We have introduced a simple, however, very effective method of double coset decomposition to deal with the question of the existence of minimal logarithmic signatures for finite groups, and have shown that this method allows construction of minimal logarithmic signatures for almost all groups of order $\leq 10^{10}$ as well as for certain infinite families of projective special linear groups. Further, we have discussed a method of constructing minimal logarithmic signatures for groups of the form $G = A.B$ with subgroups A and B and $A \cap B \neq 1$, by means of constructing appropriate minimal logarithmic signatures for A and B and then "gluing" them together. It turns out that even here the method of double coset decomposition plays a crucial role. The fundamental question whether any finite group has a minimal logarithmic signature is, to our knowledge, still far from being answered. This question is, of course, not only significant regarding cryptographic purposes but also interesting from the group-theoretic point of view, and it is worth further investigations.

ADDITIONAL NOTE

During the refereeing process of this paper the attention of the authors was drawn to the preprint "On Minimal Factorisations of Sporadic Groups" by P. E. Holmes, where the existence problem of minimal factorisation of the sporadic groups J_1, J_2, HS, M^cL, He, and Co_3 is solved using methods similar to the ones presented here.

REFERENCES

[Bosma et al. 97] W. Bosma, J. Cannon, and C. Playoust. "The Magma Algebra System I. The User Language." *Journal of Symbolic Computation* 24 (1997), 235–265.

[Conway et al. 85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *ATLAS of Finite Groups*. Oxford: Clarendon Press, 1985. Reprinted 2003.

[González Vasco and Steinwandt 02] M. I. González Vasco and R. Steinwandt. "Obstacles in Two Public Key Cryptosystems Based on Group Factorizations." In *Cryptology*, edited by K. Nemega and O. Grošek, Tatra Mountains Math. Pub. 25, pp. 23–37. Bratislava: Mathematical Institute of Slovak Academy of Sciences, 2002.

[González Vasco et al. 03] M. I. González Vasco, M. Rötteler, and R. Steinwandt. "On Minimal Length Factorizations of Finite Groups." *Experimental Mathematics* 12 (2003), 1–12.

[Holt and Rowley 93] D. F. Holt and P. Rowley. "On Products of Sylow Subgoups in Finite Groups." *Archiv der Mathematik* 60 (1993), 105–107.

[Liebeck et al. 90] M. W. Liebeck, C. E. Praeger, and J. Saxl. "The Maximal Factorizations of the Finite Simple Groups and Their Automorphism Groups." *Memoirs of the American Mathematical Society* 86:432 (1990), 1–151.

[Magliveras 86] Spyros S. Magliveras. "A Cryptosystem from Logarithmic Signatures of Finite Groups." In *Proceedings of the 29th Midwest Symposium on Circuits and Systems*, pp. 972–975. Amsterdam: Elsevier Publishing Company, 1986.

[Magliveras 02] Spyros S. Magliveras. "Secret and Public-Key Cryptosystems from Group Factorizations." In *Cryptology*, edited by K. Nemega and O. Grošek, Tatra Mountains Math. Pub. 25, pp. 11–22. Bratislava: Mathematical Institute of Slovak Academy of Sciences, 2002.

[Magliveras et al. 02] 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.

Wolfgang Lempken, Institute for Experimental Mathematics, University of Duisburg-Essen, Ellernstrasse 29,
45326 Essen, Germany (lempken@exp-math.uni-essen.de)

Tran van Trung, Institute for Experimental Mathematics, University of Duisburg-Essen, Ellernstrasse 29,
45326 Essen, Germany (trung@exp-math.uni-essen.de)

Received June 28, 2004; accepted October 25, 2004.