Cryptogr. Commun.
DOI 10.1007/s12095-015-0129-6

The existence of minimal logarithmic signatures for the sporadic Suzuki and simple Suzuki groups

A. R. Rahimipour[1] · A. R. Ashrafi[2] · A. Gholami[1]

Received: 12 July 2014 / Accepted: 11 March 2015

Abstract A logarithmic signature for a finite group G is a sequence $[A_1, \cdots, A_s]$ of subsets of G such that every element $g \in G$ can be uniquely written in the form $g = g_1 \cdots g_s$, where $g_i \in A_i$, $1 \leq i \leq s$. The aim of this paper is proving the existence of an MLS for the Suzuki simple groups $Sz(2^{2m+1})$, $m > 1$, when $2^{2m+1} + 2^{m+1} + 1$ or $2^{2m+1} - 2^{m+1} + 1$ are primes. The existence of an MLS for untwisted group $G_2(4)$ and the sporadic Suzuki group Suz are also proved. As a consequence of our results, we prove that the simple groups
$Sz(2^7)$ $Sz(2^{11})$ $Sz(2^{19})$ $Sz(2^{29})$ $Sz(2^{47})$ $Sz(2^{73})$ $Sz(2^{79})$
$Sz(2^{113})$ $Sz(2^{151})$ $Sz(2^{157})$ $Sz(2^{163})$ $Sz(2^{167})$ $Sz(2^{239})$ $Sz(2^{241})$
$Sz(2^{283})$ $Sz(2^{353})$ $Sz(2^{367})$ $Sz(2^{379})$.
have an MLS.

Keywords Logarithmic signature · Suzuki group · Sporadic group · Cryptosystem

Mathematics Subject Classification 20G40 · 05E15 · 11T71 · 20D06

A. R. Ashrafi holds a PhD degree at University of Kashan.
A. R. Rahimipour holds a PhD degree at University of Qom.
A. Gholami holds a PhD degree at University of Qom.

✉ A. R. Ashrafi
ashrafi@kashanu.ac.ir

[1] Department of Mathematics, Faculty of Science, University of Qom, P.O. Box 37161–46611, Qom, I.R., Iran

[2] Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan 87317–51116, I.R., Iran

Published online: 11 April 2015

1 Introduction

Magliveras in a pioneering work in 1986 [13], defined a private-key cryptosystem called permutation group mappings, abbreviated by PGM. The system is constructed from a finite permutation group G of finite degree, so that each encryption transformation of the system is a permutation of the message space $Z_{|G|}$, which coincides with the cipher space. This cryptosystem is based on the prolific existence of certain kinds of factorisation sets, called logarithmic signatures, for finite permutation groups. The main algebraic properties of PGM was reported in [14]. After introducing PGM, the logarithmic signatures used for presenting some public key cryptosystems like MST_1, MST_2 and MST_3 [18, 20]. Factorizable logarithmic signatures for finite groups are the essential component of the cryptosystems MST_1 and MST_3. In a recent paper, Svaba et al. [26], considered the problem of finding efficient algorithms for factoring group elements with respect to a given class of logarithmic signatures. They concerned about the factorization algorithms with respect to transversal and fused transversal logarithmic signatures for finite abelian groups. The papers [15–17] and references therein are very useful for further information on this topic.

In order to apply logarithmic signatures in some practical cryptographic schemes effectively, the question of finding logarithmic signatures with shortest length arises naturally. This paper consider such objects into account. Before we proceed further, we present some algebraic notions.

All groups in this paper are assumed to be finite. The logarithmic signatures (LS's) of groups have several remarkable applications in cryptography and computational group theory. Here, a logarithmic signature for a group G is a sequence $\alpha = [A_1, \cdots, A_s]$ of subsets of G such that every element $g \in G$ can be uniquely written in the form $g = g_1 \cdots g_s$, where $g_i \in A_i$, $1 \le i \le s$. The number $\sum_{i=1}^{s} |A_i|$ is called the length of α and denoted by $l(\alpha)$.

Suppose $\alpha = [A_1, \cdots, A_s]$ is an LS for a finite group G and $|G| = \prod_{i=1}^{s} p_i^{m_i}$ is the prime factorisation of $|G|$. It is clear that $l(\alpha)$ has an upper bound $|G|$. An observation by González Vasco and Steinwandt [5] shows that $l(\alpha) \ge \sum_{i=1}^{s} m_i p_i$. A logarithmic signature α is said to be minimal (MLS) if $l(\alpha) = \sum_{i=1}^{s} m_i p_i$. In the mentioned paper, the authors proved that the symmetric group S_n has MLS. The same result for alternating groups first reported by Magliveras [19].

It is a well-known conjecture that any finite group admits an MLS. González Vasco et al. [4, Proposition 3.1], proved that any finite solvable group has a logarithmic signature of minimal length. They also proved that if G is a finite group containing a normal subgroup K such that K and $\frac{G}{K}$ both have MLS, then G has an MLS. Suppose that G is a finite group of minimal order without MLS. If G has a proper non-trivial normal subgroup T then T and $\frac{G}{T}$ have MLS and so by the mentioned result of González Vasco et al., G has an MLS, a contradiction. So, if there is a finite group without an MLS, the smallest counterexample should be a simple group. Hence, the existence of MLS for any finite group can be reduced to the existence of MLS for finite simple groups.

González Vasco et al. [4] proved that an MLS exists for all groups of order less than 175,560, the order of Janko's first sporadic group. An MLS for a group G is called cyclic, if each A_i can be written as $A_i = \{x^i \mid 0 \le i \le |A_i| - 1\}$, for some $x \in G$. Singhi and Singhi [24], verified the conjecture for $PSL_n(q)$ and Singhi et al. [23], used a geometrical approach to prove the existence of a cyclic MLS for the classical simple groups $PSp_{2n}(q)$ and $\Omega^{-}_{2n}(q)$, $\Omega^{+}_{2n}(q)$, q is a power of 2. We also refer to two PhD thesis written by Nikhil Singhi [21] and Nidhi Singhi [22], for more information on this problem.

Lempken and van Trung [11], presented two important techniques for dealing with the conjecture:

(1) **Double Coset Decomposition** [11, Theorem 4.1]**:** Suppose G is a finite group and $H, K \leq G$ such that $H \cap gKg^{-1} = 1$, for all $g \in G$. Suppose $G = \cup_{i=1}^{n} Hg_iK$ is the double coset decomposition of G with respect to H and K. Moreover, we assume that H and K have an MLS. If $n = 1, 4$ or n is a prime number then G has a minimal logarithmic signature.

(2) **Non-disjoint factorisation**: Suppose $G = H \cdot K$, where H and K are subgroups of G with this property that $H \cap K \neq 1$. Then one can construct sometimes an MLS for G by gluing one of H and one of K.

They used the technique of double coset decomposition to prove existence of an MLS, for all groups of order smaller than 10^{10} other than the Tits group, $U_3(9)$, J_3, ${}^3D_4(2)$, $G_2(4)$, $U_3(13)$, $U_3(17)$ and McL. They also apply the standard disjoint subgroup factorisation to prove that the general and the projective general linear groups have an MLS. Holmes [7] proved the existence of an MLS for sporadic groups J_1, J_2, HS, McL, He and Co_3.

It is still an open question that whether all finite simple groups have an MLS. The aim of this paper is to prove the existence of an MLS for some new simple groups. In the end of this paper, a gap in the proof of a recently published paper [8] is reported. Our main result is:

Theorem. The following simple groups have MLS:

(1) The Suzuki group $Sz(q)$, when $q = 2^{2m+1}$, $r = 2^{m+1}$ and one of $q+r+1$ or $q-r+1$ is a prime number.

(2) The untwisted group $G_2(4)$ and the sporadic Suzuki group Suz.

Throughout this paper our notation is standard and can be taken from the famous book of Huppert [10].

2 Main results

The aim of this section is to prove our main theorem. As a consequence of our result, the existence of an MLS for the simple groups $Sz(2^7)$, $Sz(2^{11})$, $Sz(2^{19})$, $Sz(2^{29})$, $Sz(2^{47})$, $Sz(2^{73})$, $Sz(2^{79})$, $Sz(2^{113})$, $Sz(2^{151})$, $Sz(2^{157})$, $Sz(2^{163})$, $Sz(2^{167})$, $Sz(2^{239})$, $Sz(2^{241})$, $Sz(2^{283})$, $Sz(2^{353})$, $Sz(2^{367})$, $Sz(2^{379})$ and the sporadic group Suz are deduced.

2.1 MLSs for some Suzuki groups

Following Suzuki [25], a group G is called a $ZT-$group if G acts on a set Ω in such a way that, (1) G is a doubly transitive group on $1 + N$ symbols, (2) the identity is the only element which leaves three distinct symbols invariant, (3) G contains no normal subgroup of order $1 + N$, and (4) N is even. Suzuki proved that for each prime power $q = 2^{2m+1}$, there is a unique $ZT-$group $Sz(q)$ of order $q^2(q-1)(q^2+1)$ which is called later the Suzuki group. This group is simple, when $q > 2$. Suppose that $r = 2^{m+1}$, a is a symbol on which G acts and $H = G_a$. By [25], it follows from the conditions (1) and (2) that H is a Frobenius group on $\Omega \setminus \{a\}$. Apply a well-known result of Frobenius to deduce that H contains a regular normal subgroup Q of order N such that every non-identity element of Q leaves only the symbol a invariant. Suppose $b \in \Omega \setminus \{a\}$ and $K = H_b$. Suppose $x \in N_G(K)$ is an involution. Then it is well-known that the Suzuki group are containing two elements y and z such that y is an involution and $xyx = z^{-1}xz$, and three cyclic subgroups A_0, A_1 and A_2 of orders $q-1$, $q+r+1$ and $q-r+1$, respectively.

The Suzuki groups can be defined as a subgroup of $GL(4,q)$. To do this, we assume that $K = GF(q)$. Define:

$$S(a,b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & a^r & 1 & 0 \\ a^{r+2}+ab+b^r & a^{r+1}+b & a & 1 \end{pmatrix}; M(k) = \begin{pmatrix} k^{1+2^m} & 0 & 0 & 0 \\ 0 & k^{2^m} & 0 & 0 \\ 0 & 0 & k^{-2^m} & 0 \\ 0 & 0 & 0 & k^{-1-2^m} \end{pmatrix},$$

where $a, b, k \in K$ and $k \neq 0$. Consider $S(q)$ and $K(q)$ to be the subgroups generated by all $S(a,b)$ and $M(k)$, respectively. Suppose

$$T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then by [25], the Suzuki group $Sz(q)$ has the following properties:

(1) The Suzuki group $Sz(q)$ can be generated by $S(q)$, $K(q)$ and T.

Table 1 Some Values of m such that $2^{2m+1} - 2^{m+1} + 1$ or $2^{2m+1} + 2^{m+1} + 1$ is a Prime Number

m		$2^{2m+1} + 2^{m+1} + 1$		$2^{2m+1} - 2^{m+1} + 1$
1	⋆	$2^3 + 2^2 + 1 = 13$	⋆	$2^3 - 2^2 + 1 = 5$
2		$2^5 + 2^3 + 1 = 41$	⋆	$2^5 - 2^3 + 1 = 25$
3		$2^7 + 2^4 + 1 = 145$	⋆	$2^7 - 2^4 + 1 = 113$
5	⋆	$2^{11} + 2^6 + 1 = 2113$		$2^{11} - 2^6 + 1 = 1985$
9	⋆	$2^{19} + 2^{10} + 1 = 525313$		$2^{19} - 2^{10} + 1 = 523265$
14	⋆	$2^{29} + 2^{15} + 1 = 536903681$		$2^{29} - 2^{15} + 1 = 536838145$
23		$2^{47} + 2^{24} + 1 = 140737505132545$	⋆	$2^{47} - 2^{24} + 1 = 140737471578113$
36		$2^{73} + 2^{37} + 1$	⋆	$2^{73} - 2^{37} + 1$
39		$2^{79} + 2^{40} + 1$	⋆	$2^{79} - 2^{40} + 1$
56		$2^{113} + 2^{57} + 1$	⋆	$2^{113} - 2^{57} + 1$
75		$2^{151} + 2^{76} + 1$	⋆	$2^{151} - 2^{76} + 1$
78	⋆	$2^{157} + 2^{79} + 1$		$2^{157} - 2^{79} + 1$
81	⋆	$2^{163} + 2^{82} + 1$		$2^{163} - 2^{82} + 1$
83		$2^{167} + 2^{84} + 1$	⋆	$2^{167} - 2^{84} + 1$
119		$2^{239} + 2^{120} + 1$	⋆	$2^{239} - 2^{120} + 1$
120		$2^{141} + 2^{121} + 1$	⋆	$2^{241} - 2^{121} + 1$
141	⋆	$2^{283} + 2^{142} + 1$		$2^{283} - 2^{142} + 1$
176		$2^{353} + 2^{177} + 1$	⋆	$2^{353} - 2^{177} + 1$
183		$2^{367} + 2^{184} + 1$	⋆	$2^{367} - 2^{184} + 1$
189	⋆	$2^{379} + 2^{190} + 1$		$2^{379} - 2^{190} + 1$

⋆denotes prime numbers

Table 2 Generators of the Subgroup P_{32}

1	$bxby^3x^2by^2b^{-1}x^3yxa$
2	$yxz^2b^{-1}ywz$
3	$by^2b^{-1}xy(xbx)^2(zw)^2bz^2b$
4	$zb^{-2}xy^2a(b^{-1}y)^4x^2yb^{-1}$
5	$xy^3b^{-1}xyxz^3w$

(2) The subgroup $S(q)$ is a 2−Sylow subgroup of $Sz(q)$ of order q^2.
(3) The subgroup $K(q)$ is cyclic of order $q-1$ and $S(q)\cap K(q)=1$.
(4) If $H(q)=N_{Sz(q)}(S(q))$ then $H(q)=S(q):K(q)$, where $A:B$ denotes a semidirect product of A by B.
(5) $Sz(q)$ are having two cyclic subgroups U_1 and U_2 of orders $q-r+1$ and $q+r+1$, respectively.

We notice that from these properties of Suzuki groups, it is immediately proved that $|Sz(q)|=q^2(q-1)(q+r+1)(q-r+1)$.

We are now ready to prove if $q-r+1$ or $q+r+1$ are prime then the Suzuki group $Sz(q)$ has an MLS. To do this, we first prove that $(q+r+1,q-r+1)=1$ and $(q^2(q-1),q\pm r+1)=1$. To do this, we assume that $a=(q+r+1,q-r+1)$, $b=(q^2(q-1),q\pm r+1)$ and $c=(q-1,q\pm r+1)$. Since a is an odd integer dividing $2r$, $a=1$. But, c is an odd integer that divides $(q+r+1)(q-r+1)-(q-1)(q+1)=2$. Thus, $c=1$ and $(q-1,q\pm r+1)=(q\pm r-1,q^2)=1$. So $(q^2(q-1),q\pm r+1)=1$.

Next we show that for each $g\in Sz(q)$, $U_1^g\cap H(q)=U_2^g\cap H(q)=1$, and that the subgroups U_1,U_2 and $H(q)$ have MLS. To prove, we notice that by (4), $|H(q)|=q^2(q-1)$ and $(|H(q)|,|U_1|)=(|H(q)|,|U_2|)=1$. On the other hand, by [4, Proposition 3.1], every solvable group has an MLS and so the subgroups U_1 and U_2 have MLS. On the other hand, by [7, Condition 2.1], if a group G has a normal subgroup K such that $\frac{G}{K}\cong H$ and H and K both have minimal logarithmic signature, then G has a minimal logarithmic signature. Again by (4), $H(q)$ is a split extension of a solvable group by a cyclic group that implies that $H(q)$ has an MLS.

Finally, by double coset decomposition, we can assume that $|Sz(q)|=\cup_{i=1}^{m_1}H(q)g_iU_1=\cup_{j=1}^{m_2}H(q)h_jU_2$. Thus, $q^2(q-1)(q-r+1)(q+r+1)=Sz(q)=m_1|H(q)||U_1|=m_2|H(q)||U_2|$. This implies that $m_1=q+r+1$ and $m_2=q-r+1$. We now apply double coset decomposition to deduce that the Suzuki group $Sz(q)$, $q+r+1$ or $q-r+1$ is prime, has an MLS. This completes the first part of our main theorem.

In the end of this section, we first record in Table 1 some values of m, $1\le m\le 200$, such that at least one of $2^{2m+1}-2^{m+1}+1$ or $2^{2m+1}+2^{m+1}+1$ is a prime number. Then we use these information and our result for to find 18 new Suzuki groups with an MLS. Notice that the existence of an MLS for $Sz(2^3)$ in [4] and for $Sz(2^5)$ in [11] were presented. Our calculations are recorded in Table 3.

Table 3 The Existence of MLS for some New Suzuki Groups

$Sz(2^3)$ [4]	$Sz(2^5)$ [11]	$Sz(2^7)$	$Sz(2^{11})$	$Sz(2^{19})$
$Sz(2^{29})$	$Sz(2^{47})$	$Sz(2^{73})$	$Sz(2^{79})$	$Sz(2^{113})$
$Sz(2^{151})$	$Sz(2^{157})$	$Sz(2^{163})$	$Sz(2^{167})$	$Sz(2^{239})$
$Sz(2^{241})$	$Sz(2^{283})$	$Sz(2^{353})$	$Sz(2^{367})$	$Sz(2^{379})$

Table 4 Elements of Set A_{13}

1	$Id(G_2(4))$
2	$bx(xy)^2b^{-1}x^2y^3xa(bx)^2$
3	$(bz)^2b^{-1}(y^2b^{-1}x)^2xbyx^2a$
4	$zb^2y^3xyb^{-1}xz^2(bx)^2zb^{-2}x$
5	$xz^2(bx)^2zw(bx)^3by^2a$
6	$yw^3b^{-1}(wbzw)^2w$
7	$yxz^2w^2b^2yx^2(yb^{-1})^2y^2a$
8	$z^2wb^2ya(b^{-1}y)^3wb^2yx^2$
9	$(bx)^2y(xb)^2x^2y^3b^{-1}xz^3$
10	$yx^4(z^2wbz)^2zw$
11	$by^3b^{-1}(xb)^2x(zbzw)^2$
12	$xya(bx)^2zb^{-1}(yb^{-1}x)^2xby^2b^{-1}$
13	$x^2zw(bx)^2y^6x^2$

2.2 MLSs for untwisted group $G_2(4)$ and the Sopradic group Suz

Our calculations given this section are done with the aid of GAP [27] and ATLAS of Finite Group Representations - Version 3 [1]. The aim of this section is to prove the existence of MLS for untwisted group $G_2(4)$ and the sporadic group Suz.

We first consider the untwisted group $G_2(4)$ of order $251596800 = 2^{12}\cdot 3^3\cdot 5^2\cdot 7\cdot 13$. The group $G_2(4)$ is primitive and its point group stabilizers are maximal subgroups [3, Corollary 1.5.A]. Choose $H = G_1$, the stabilizer of point 1 which is a maximal subgroup isomorphic of the Janko group J_2. This maximal subgroup has a transversal T of size 416 and so $G_2(4) = H \cdot T$. We are looking for a subgroup P_{32} and a subset A_{13} such that $T = P_{32} \cdot A_{13}$. Consider the permutation representation $G_2(4) = \langle a, b\rangle$ on these 416 points, see [1]. Set $x = ab$, $y = ab^{-1}$, $z = ba$ and $w = b^{-1}a$. The elements of a generating set for P_{32} are recorded in Table 2.

In Table 4, the elements of A_{13} are recorded. By [3, Theorem 1.4.A], if G is a group acting on a set Ω, $x, y \in G$ and $\alpha \in \Omega$, then $\alpha^x = \alpha^y$ if and only if $G_\alpha x = G_\alpha y$. Hence the set T is a right transversal of H if each $t \in T$ maps point 1 to distinct points. Now a simple calculation by GAP shows that $G_2(4) = HP_{32}A_{13}$, since 416 elements of T map point 1 to 416 distinct points. By Holmes [7], H has an MLS and since P_{32} is a 2−group, it has an MLS. On the other hand, the number of elements of A_{13} is prime and so $G_2(4)$ has an MLS.

We now consider the sporadic group Suz of order $448345497600 = 2^{13}\cdot 3^7\cdot 5^2\cdot 7\cdot 11\cdot 13$. In [7], it is proved that if $G_2(4)$ has an MLS then Suz has an MLS. So, by above argument Suz has MLS.

3 Concluding remarks

In this paper the problem of existence of a minimal logarithmic signature is considered into account. It is proved that under some conditions the Suzuki group $Sz(q)$ has minimal logarithmic signature. We also proved that the untwisted group $G_2(4)$ has also MLS. As a consequence, it is firstly proved that the simple groups $Sz(2^7)$, $Sz(2^{11})$, $Sz(2^{19})$, $Sz(2^{29})$, $Sz(2^{47})$, $Sz(2^{73})$, $Sz(2^{79})$, $Sz(2^{113})$, $Sz(2^{151})$, $Sz(2^{157})$, $Sz(2^{163})$, $Sz(2^{167})$, $Sz(2^{239})$,

$Sz(2^{241})$, $Sz(2^{283})$, $Sz(2^{353})$, $Sz(2^{367})$, $Sz(2^{379})$ and the sporadic group Suz have MLS. We believed our method can be applied for some other classes of simple groups that there is enough information on their subgroup lattice. An example of such simple groups are simple unitary groups $PSU_3(2^n)$, where $n > 1$ and 2^n+1 or $2^{2n}-2^n+1$ are primes. The structure of maximal subgroups of $PSU_3(q)$ are given in [6, 12]. So, by a similar argument as the case of simple Suzuki groups $Sz(q)$, we can prove that the simple unitary groups $PSU_3(2^n)$ under above conditions have MLS. It is merit to mention here that the existence of MLSs for the unitary group $U_n(q)$ and the projective special unitary group $PSU_n(q)$ are proved in a recent paper by Hong et al. [9].

In the end of this paper we would like to report a gap in the proof of some results in a recently published paper [8]. Notice that it is possible that $H \cap K = 1$ and $|G| = |H||K|$, but $G \neq HK$. So, $[H, K]$ is not an LS. On the other hand, if H and K are subgroups of G such that $G = HK$ and $H \cap K = 1$ then $[H, K]$ is an LS for G. In [8, Theorem 4], the authors first used a result in [2] to prove that there are two maximum cyclic tori T_1 and T_2 of orders $q+\sqrt{2q}+1$ and $q-\sqrt{2q}+1$, respectively. Then they considered the stabilizer subgroup G_w and claimed that $[T_1, T_2, G_w]$ is an LS for $Sz(q)$. To apply the mentioned result we have to prove that $[T_1T_2$ is a subgroup of $Sz(q)$ and $T_1T_2 \cap G_w = 1]$ or $[T_2G_w$ is a subgroup of $Sz(q)$ and $T_1 \cap T_2G_w = 1]$. But the structure of subgroups of Suzuki groups given by Suzuki in [25] shows that T_1T_2 and T_2G_w are not subgroups of $Sz(q)$. This shows that the problem of existence of an MLS for $Sz(q)$, in general, is still open. In the same manner, they claimed that all exceptional groups of Lie type have minimal logarithmic signatures. Hence the problem of existence an MLS for the exceptional groups of Lie type is still open.

Acknowledgments The authors are indebted to the referees for their suggestions and helpful remarks leaded us to rearrange the paper. The research of the first and second authors are partially supported by INSF under grant number 93010006.

References

1. Abbott, R., Bray, J., Linton, S., Nickerson, S., Norton, S., Parker, R., Suleiman, I., Tripp, J., Walsh, P., Wilson, R.: ATLAS of Finite Group Representations – Version 3, (http://brauer.maths.qmul.ac.uk/Atlas/v3/)
2. Babai, L., Pàlfy, P.P., Saxl, J.: On the number of p regular elements in finite simple groups. LMS J. Comput. Math. **12**, 82–119 (2009)
3. Dixon, J.D., Mortimer, B.: Permutation Groups, Graduate Texts in Mathematics, vol. 163. Springer-Verlag, New York (1996)
4. González Vasco, M.I., Rötteler, M., Steinwandt, R.: On minimal length factorizations of finite groups. Exp. Math. **12**(1), 1–12 (2003)
5. González Vasco, M.I., Steinwandt, R.: Obstacles in two public key cryptosystems based on group factorizations. Tatra Mt. Math. Publ. **25**, 23–37 (2002)
6. Hartley, R.W.: Determination of the ternary collineation groups whose coefficients lie in the $GF(2^n)$. Ann. Math. **27**, 140–158 (1926)
7. Holmes, P.E.: On minimal factorisations of sporadic groups. Exp. Math. **13**(4), 435–440 (2004)
8. Hong, H., Wang, L., Yang, Y., Ahmad, H.: All exceptional groups of Lie type have minimal logarithmic signatures. Appl. Aalgebra Eng. Commun. Comput. doi:10.1007/s00200-014-0226-3
9. Hong, H., Wang, L., Yang, Y.: Minimal logarithmic signatures for the unitary group $U_n(q)$. Des. Codes Cryptogr. doi:10.1007/s10623-014-9996-7
10. Huppert, B.: Endliche Gruppen I. Springer-Verlag, Berlin (1967)
11. Lempken, W., van Trung, T.: On minimal logarithmic signatures of finite groups. Exp. Math. **14**(3), 257–269 (2005)

12. Liu, W.: Finite linear spaces admitting a projective group $PSU(3, q)$ with q even. Linear Algebra Appl **374**, 291–305 (2003)
13. Magliveras, S.S.: A cryptosystem from logarithmic signatures of finite groups, In Proceedings of the 29th Midwest Symposium on Circuits and Systems, pp. 972–975. Elsevier Publishing Company, Amsterdam (1986)
14. Magliveras, S.S., Memon, N.D.: Algebraic properties of cryptosystem PGM. J. Cryptol. **5**, 167–183 (1992)
15. Magliveras, S.S., Memon, N.D.: Properties of cryptosystem PGM, in Advances in Cryptology Crypto '89, Lecture Notes in Computer Science, vol. 435, pp. 447–460. Springer-Verlag, Berlin (1989)
16. Magliveras, S.S., Memon, N.D.: Complexity tests for cryptosystem PGM. Congr. Numer. **79**, 61–68 (1990)
17. Magliveras, S.S., Oberg, B.A., Surkan, A.J.: A new random number generator from permutation groups. Rend. Sem. Mat. Fis. Milano **54**, 203–223 (1985)
18. Magliveras, S.S., Stinson, D.R., van Trung, T.: New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. J. Cryptol. **15**, 167–183 (2002)
19. Magliveras, S.S.: Secret- and Public-key Cryptosystems from Group Factorizations. In: Nemoga, K., Grošek, O. (eds.): Bratislava: Mathematical Institute,Slovak Academy of Sciences, vol. 25, p. 2002. Tatra Mountains Mathematical Publications
20. Lempken, W., van Trung, T., Magliveras, S.S., Wei, W.: A public key cryptosystem based on non-abelian finite groups. J. Cryptol. **22**, 62–74 (2009)
21. Singhi, N.: The Existence of Minimal Logarithmic Signatures for Classical Groups, PhD Thesis,Florida Atlantic University (2011)
22. Singhi, N.: On the Minimal Logarithmic Signature Conjecture, PhD Thesis, Florida Atlantic University (2011)
23. Singhi, N., Singhi, N.: Minimal logarithmic signatures for classical groups. Des. Codes Cryptogr. **60**(2), 183–195 (2011)
24. Singhi, N., Singhi, N., Magliveras, S.: Minimal logarithmic signatures for finite groups of Lie type. Des. Codes Cryptogr. **55**(2-3), 243–260 (2010)
25. Suzuki, M.: On a class of doubly transitive groups. Annals Math **75**(1), 105–145 (1962)
26. Svaba, P., van Trung, T., Wolf, P.: Logarithmic signatures for abelian groups and their factorization. Tatra Mt. Math. Publ. **57**, 21–33 (2013)
27. The GAP Team: GAP – Groups, Algorithms, and Programming, Version 4.5.5, 2012, (http://www.gap-system.org)