SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

May 2017, Vol. 60 052106:1–052106:11
doi: 10.1007/s11432-015-5479-3

Minimum length key in MST cryptosystems

Haibo HONG[1], Licheng WANG[2], Haseeb AHMAD[2], Yixian YANG[2] & Zhiguo QU[3]*

[1]*School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou* 310018*, China;*
[2]*Information Security Center, State Key Laboratory of Networking and Switching Technology,*
Beijing University of Posts and Telecommunications, Beijing 100876*, China;*
[3]*Jiangsu Engineering Center of Network Monitoring,*
Nanjing University of Information Science & Technology, Nanjing 210044*, China*

Received October 22, 2015; accepted December 8, 2015; published online September 13, 2016

Abstract As a special factorization category of finite groups, logarithmic signature (LS) is used as the main component of cryptographic keys that operate within secret key cryptosystems such as PGM and public key cryptosystems like MST_1, MST_2 and MST_3. An LS with the shortest length is called a minimal logarithmic signature (MLS) that constitutes of the smallest sized blocks and offers the lowest complexity, and is therefore desirable for cryptographic constructions. However, the existence of MLSs for finite groups should be firstly taken into an account. The MLS conjecture states that every finite simple group has an MLS. If it holds, then by the consequence of Jordan-Hölder Theorem, every finite group would have an MLS. In fact, many cryptographers and mathematicians are keen for solving this problem. Some effective work has already been done in search of MLSs for finite groups. Recently, we have made some progress towards searching a minimal length key for MST cryptosystems and presented a theoretical proof of MLS conjecture.

Keywords MLS conjecture, finite groups, (minimal) logarithmic signature, minimum length key, MST cryptosystems

Citation Hong H B, Wang L C, Ahmad H, et al. Minimum length key in MST cryptosystems. Sci China Inf Sci, 2017, 60(5): 052106, doi: 10.1007/s11432-015-5479-3

1 Introduction

Currently, most asymmetric cryptographic primitives are based on the perceived intractable problems in number theory. Prominent hard problems consist of large integers factoring problem (IFP); the discrete logarithm problem (DLP) over a finite field F_q or an elliptic curve, etc. While, because of Shor's and other quantum algorithms [1, 2] for integer factoring and solving the DLP, the known public key systems will be insecure, when quantum computers would become practical. Therefore, it is an imminent work to search for more complex mathematical platforms and to design effective cryptographic schemes, which can resist against quantum attacks. In this context, cryptographers began to pay more attention towards non-commutative cryptography. Being different from commutative cryptography based on number theory, non-commutative cryptography is based on non-commutative algebraic structures. Also, non-commutative cryptography takes the advantage of intractable problems in quantum computing,

*Corresponding author (email: qzghhh@126.com) combinatorial group theory and computational complexity theory to construct cryptographic platforms. This extension has a profound background and rich connotation. First, from the viewpoint of the platforms, non-commutative cryptography extends the research territory of cryptography. A large number of non-commutative algebraic structures are waiting to be explored for building new public key cryptosystems. Non-commutative cryptography concerns with combinatorial group theory, algebraic representation theory, topology, category theory, etc. Second, due to the ability of resisting quantum attacks, non-commutative cryptography is expected to achieve a higher strength. Because of the hard restrictions on bounds within non-commutative algebraic structures, the difficulty of several kinds of mathematical problems has increased significantly [3]. Especially, from the viewpoint of typical framework of quantum algorithm—Hidden Subgroup Problem (HSP), we have already know that how to design efficient quantum algorithms for solving HSP problem in any abelian group; but up to now we are still unable to construct even a single efficient algorithm for dealing HSP problems in non-abelian groups [4].

In the developmental era of public key cryptography, research on the underlying intractable hypothesis of mathematical problems while being used within non-commutative cryptography, has always got priority among priorities. Therefore, from 1980's, some experts began to apply difficult problems from group theory into cryptography. In 1984, Wagner et al. [5] designed a public key cryptosystem based on undecidable word problem in groups and semigroups. In 2000, Ko et al. [6] developed braid group cryptography based on the intractable assumption of conjugate search problem in braid group. In 2004, Eick and Kahrobaei [7] devised a new cryptosystem based on the polycyclic group. In 2005, Shpilrain and Ushakov [8] put forward a new public key cryptosystem by using Thomsen group. Recently, Kahrobaei et al. [9] designed a key exchange protocol based on the intractable assumption of discrete logarithm problem in the group ring matrix.. At the same time, a type of cryptosystems based on the intractable assumption in non-abelian group—group factorization problem (GFP) has gradually become a typical representative of non-commutative cryptography and achieved rapid development in recent thirty years. In 1986, Magliveras [10] constructed a symmetric cryptosystem—PGM by using a special factorization basis in finite permutation groups—logarithmic signature (LS). Then, in the literatures [11–14], algebraic properties of PGM were discussed in detail. In 2002, Magliveras et al. [15] designed a trapdoor permutation function and two public key cryptosystems MST_1 and MST_2 by using LS in finite non-abelian groups. In 2009, Magliveras et al. [16] devised a new public key cryptographic system—MST_3 based on random covers and LS in finite non-abelian groups. Meanwhile, Magliveras et al proposed a practical platform—Suzuki 2-group for the first time [17] and devised MST cryptosystems into practice. However, a lot of research has already been done to attack on MST cryptosystems effectively. In 2008, Magliveras et al. [18] provided a comprehensive analysis of MST_3 cryptosystem and stated that transitive LS is not suitable for MST_3 cryptosystem. In 2009, Blackburn et al. [19] pointed out that amalgamated LS is also not a reasonable choice for MST cryptosystems. In 2010, Vasco et al. [20] gave a more profound analysis of MST_3 and showed that the intractability assumption GFP doesn't always hold for random cover of group G. Also they discussed that MST_3 cryptosystem can't achieve (OW-CPA) in chosen plaintext attack model as well as not (IND-CCA2) secure against adaptive chosen ciphertext attacks. Therefore, in 2010, Svaba et al. [21] constructed a more secure cryptosystem $eMST_3$ by adding a secret homomorphic map. Moreover, they analyzed all of the published references about attacking MST cryptosystems and developed a set of weak key test tool for $eMST_3$ cryptosystem. They also claimed that they can exclude bad LSs by replacing this tool. In 2014, to the best of our knowledge, we presented the first digital signature scheme based on logarithmic signatures and random covers [22].

At present, while comparing with mainstream cryptosystems, MST cryptosystem suffers the overheads including larger public key (secret key) size, inefficient encryption (decryption) algorithm and up till now only enjoys a single known platform—Suzuki 2-group. Therefore, in order to improve the efficiency of MST cryptosystem, the need of the hour is to optimize the mathematical structures of LS and to obtain a minimal length key—called minimal logarithmic signature (MLS). However, the existence of MLSs must have to be solved first. This problem essentially involves the factorization of finite groups. From the viewpoint of cryptography and mathematics, it's meaningful to study this problem. With the great efforts of the cryptographers and mathematicians, a lot of finite groups have already been proved to have MLSs. Therefore, in 2010, Nikhil Singhi et al. proposed the MLS conjecture stating that every finite simple group has an MLS. If it holds, then by the Jordan – Hölder Theorem, every finite group would have an MLS. In recent years, many positive results related to MLSs for finite groups are being reported. In 2003, Vasco et al. [23] proved that all finite groups with order $\leqslant 175560$ have MLSs. In 2004, Holmes [24] constructed MLSs for some sporadic groups. In 2005, Lempken et al. [25] proved that with some exceptions, all finite groups with order no higher than 10^{10} have MLSs. In 2010 and 2011, Singhi et al [26, 27] constructed MLSs for some classical groups. Recently, according to the classification theorem of finite simple groups, we utilize the matrix groups, Lie groups, associative algebra and other mathematical methods to present the structures of MLSs for remaining four categories of finite simple groups [28–31], and prove the MLS conjecture.

2 Development and progress of research on minimum length key

2.1 Logarithmic signature and minimal logarithmic signature

The definition of logarithmic signature (LS) was first put foward by Magliveras in 1986 [10]. Here, the definition is different from traditional logarithmic signature in cryptography, it refers to a special group factorization basis. The GFP based on LS can be stated as follows: for a given LS, each element of the group must be given a unique presentation. So far, this problem is considered to be intractable [15, 16], and cryptographers took advantage of aforementioned intractable assumption for designing MST cryptosystems. At the same time, in order to reduce the block length and the size of public (secret) key, cryptographers are keen on optimizing the general logarithmic signature structure for obtaining the shortest length of the logarithmic signature-called minimal logarithmic signature (MLS). Hence, in 2003, Vasco [23] utilized the prime factorization of the orders of finite groups to present an accurate definition of MLS and also constructed MLSs for some finite groups. From then on, the existence of MLSs for finite groups gradually aroused the attention of cryptographers and mathematicians.

Definition 1 (LS [25])**.** 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 $\alpha_i = [\alpha_{i1}, \ldots, \alpha_{ir_i}]$ with $\alpha_{ij} \in G$, $(1 \leqslant j \leqslant r_i)$. Then α is called a logarithmic signature (LS) for G if each $g \in G$ is uniquely represented as a product

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

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

The sequences α_i are called the blocks of α, the length of α is defined to be $l(\alpha) = \sum_{i=1}^{s} r_i$. let $|G| = \prod_{j=1}^{k} p_j^{a_j}$ be the prime power decomposition of $|G|$ and $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_s]$ be an LS for G. From [32], we observe that $l(\alpha) \geqslant \sum_{j=1}^{k} a_j p_j$.

Definition 2 (MLS [25])**.** An LS α for a finite group G with $l(\alpha) = \sum_{j=1}^{k} a_j p_j$ is called an minimal logarithmic signature (MLS).

2.2 Development of proving MLS conjecture

The work on proving the existence of MLSs for finite groups was first started in 2003 [23]. Until now, this work has been going on more than ten years, cryptographers and mathematicians have introduced many different mathematical methods to prove the existence of MLSs for some simple groups. These methods can be roughly divided into five categories.

1. Vasco [23] utilized Sylow subgroups factorization of finite groups, Zappa-Szép product, projective geometry and some mathematical softwares to prove that every finite group with order $\leqslant 175560$ has an MLS.

In that article, Vasco et al. first put forward a general idea of constructing MLSs: for a given group permutation presentation $G|\Omega$ for G, $p \in \Omega$ and corresponding stabilizer G_p. Suppose $A = \{gG_p \mid g \in G\}$ is a left coset representation of G_p. If G_p and A both have MLSs, then G also has an MLS. More generally, when G is factorized into several disjoint parts, if each part has an MLS, implies that G also has an MLS . In the concrete operating process, the authors firstly combined the Sylow subgroups factorization of finite groups with mathematical softwares such as GAP and Magma for factorizing simple groups into some disjoint Sylow subgroups. Thus, they obtained MLSs for some simple groups including five types of sporadic groups (M_{11}, M_{12}, M_{22}, M_{23} and M_{24}). Then, they utilized projective geometry and group theory for factorizing simple groups into several disjoint subgroups and constructed corresponding MLSs for these simple groups. Comparing to Sylow subgroup factorization, this method is more general, but some simple groups can't be handled properly by using aforementioned methods. Therefore, the authors used Zappa-Szép product for factorizing such groups into a product of several subgroups and corresponding stabilizers, then obtained corresponding MLSs. Consequently, Vasco et al. attained MLSs for all finite groups with order $\leqslant 175560$.

2. Holmes [24] took advantage of group permutation presentation theory, chart of finite simple groups [33] and mathematical softwares to construct MLSs for some sporadic group.

In his article, based on the conclusion that every finite simple group is a normal subgroup of some finite group, Holmes reduced the construction of MLSs of finite groups into the structure of MLSs for finite simple groups. The author selected two subgroups A and B, divided group G into three parts by using group action and coset decomposition, where two parts are groups and third one is a set with prime cardinality that satisfies certain conditions. More generally, the authors further increased the number of the blocks and divided G into four parts, where only two parts are groups, the other two parts are sets with prime cardinality that satisfy certain conditions. Combining aforementioned two methods with the help of GAP, Holmes constructed corresponding MLSs for eight types of sporadic groups J_1, J_2, HS, M^cL, He, Co_3, Ru and Suz (the proof of Ru and Suz still need some hypotheses).

3. Lempken et al. [25] used double coset decomposition and chart of finite simple groups [33] to construct MLSs for finite groups with order $\leqslant 10^{10}$.

In their article, Lempken et al. introduced a new technology – double coset decomposition. They divided G into H, A and K, where $H, K \leqslant G$, A is the right (left) coset decomposition of $H(K)$. Using this structure, the authors presented MLSs for finite groups with order $\leqslant 10^{10}$ (except for eight special cases). In fact, the requirements for double coset decomposition are rather stringent, therefore, the method has certain limitations. For example, although McL can't have MLS by using double coset decomposition, Holmes [24] explicitly gave MLS for McL and corresponding construction process. Finally, the authors used the product of two subgroups factorization to present MLSs for some finite groups including A_6 and J_2.

4. Singhi et al. [26] employed Singer subgroups [34, 35] and Levi decomposition of parabolic subgroups to construct MLSs for some finite groups.

In their article, the authors introduced some relevant concepts of algebraic group theory and took advantage of Levi decomposition of parabolic subgroups to construct corresponding MLSs for $GL_n(q)$, $SL_n(q)$ and $Sp_n(q)$. Then, utilized linear transformations of linear spaces to for obtaining corresponding MLSs. Meanwhile, the authors put forward the MLS conjecture stating that every finite simple group has an MLS.

5. Singhi et al. [27] made further efforts to propose MLSs for some finite groups by using spread and semi-direct product decomposition.

In their article, the authors introduced spread theory [36,37] and employed semi-direct product decomposition for factorizing parabolic subgroups (stabilizers) of finite groups. They utilized the relationship between singular points of projective spaces and spreads for constructing corresponding cyclic subgroups (cyclic set) and proved that the existence of LSs for each small part, and then proved the existence of MLSs for G. The authors mainly constructed MLSs for $Sp_n(q)$ and $O^{\pm}_{2m}(q)$ $(q = 2^e)$, and then used canonical homomorphisms and the relationship between $O^{\pm}_{2m}(q)$ and $\Omega^{\pm}_{2m}(q)$ to construct corresponding MLSs for $PSp_n(q)$ and $\Omega^{\pm}_{2m}(q)$ $(q = 2^e)$. Actually, there exist some mature theories on permutation presentation of stabilizers that correspond to the classical groups and exceptional groups of Lie type. Therefore, we take advantage of stabilizers and linear transformations of finite simple groups to study MLSs for corresponding finite simple groups.

Table 1 Comparison of the related work

Reference	Technology	Result	Characteristic	Deficiency
Vasco [23]	Sylow subgroups decomposition of finite groups, projective geometry and mathematical softwares	Every group with order $\leqslant 175560$ has an MLS	Block number is not restricted, structure is clear	Each block must be a group, the requirements are stringent
Holmes [24]	Group permutation presentation theory, chart of finite simple groups and mathematical softwares	The existence of MLSs for some sporadic groups	Two blocks are groups, two blocks are sets with prime cardinality	Sets selection is complex, blocks are less in numbers
Lempken [25]	Double coset decomposition, subgroup product decomposition and chart of finite simple groups	Except for eight special cases, MLSs for finite groups with order $\leqslant 10^{10}$	Two blocks are groups, one block is a set with prime cardinality	Sets selection is complex, blocks are less in numbers
Singhi [26, 27]	Levi decomposition of parabolic subgroups and spreads	MLSs for some finite simple groups	Method is universal, suitable for classical groups and exceptional groups of Lie type	The structures of stabilizers and sharply transitive sets are complicated, blocks are less in numbers

Here, we summarize the aforementioned methods in Table 1.

According to the classification [33,38], finite simple groups can be divided into five categories as follows: cyclic groups of prime order, alternating groups A_n ($n \geqslant 5$), classical groups, 10 types of exceptional groups of Lie type and 26 types of sporadic groups. Until 2012, there were 4 unsolved problems on MLS conjecture: (1) the existence of MLSs for the commutator subgroup of projective orthogonal group $P\Omega_n(q)$ ($q = p^e$, p is an odd prime); (2) the existence of MLSs for the projective special unitary groups $PSU_n(q)$; (3) the existence of MLSs for 10 types of exceptional groups of Lie type; (4) the existence of MLSs for the remaining 13 sporadic groups.

3 Our work

From 2012, we have employed many mathematical methods such as the matrix groups, Lie groups and associative algebra to provide MLSs for the remaing simple groups. Consequently, we have contributed to prove MLS conjecture completely.

1. The existence of MLSs for a type of classical simple group $P\Omega_n(q)$ [30].

In 2011, Singhi et al. [27] presented MLSs for $Sp_{2m}(q)$ (isomorphic to $O_{2m+1}(q)$), $O^{\pm}_{2m}(q)$ and $\Omega^{\pm}_{2m}(q)$ ($q = 2^e$, e is an integer). But, in case when $q = p^e$ (p is an odd prime, e is an integer), the problem becomes more complicated. In this case, it's difficult to construct bilinear form and quadratic space of the orthogonal group $O_n(q)$. At the same time, according to the parity of n, the orthogonal group $O_n(q)$ (special orthogonal group $SO_n(q)$) can be divided into: $O^+_{2m}(q)$ ($SO^+_{2m}(q)$), $O^-_{2m}(q)$ ($SO^-_{2m}(q)$) and $O_{2m+1}(q)$ ($SO_{2m+1}(q)$).

We know that that there are corresponding permutations presentation related to subset of projective space that belongs to classical groups. At present, mathematicians have done effective work on permutation presentation of stabilizers. Therefore, our idea is to use the relationship between stabilizers of one-dimensional isotropic subspace of the orthogonal group $O_n(q)$ ($SO_n(q)$) and its parabolic subgroups and to combine the basic theory of spread, we divided the orthogonal group $O_n(q)$ ($SO_n(q)$) into some parts, then proved that each part has an MLS and therefore, $O_n(q)$ ($SO_n(q)$) also has an MLS. Finally, using the relationship between special orthogonal group $SO_n(q)$, the projective special orthogonal group $PSO_n(q)$ and projective commutator subgroup $P\Omega_n(q)$, we utilized a canonical homomorphism to prove the existence of MLSs for projective commutator subgroup $P\Omega_n(q)$. Our basic theory is presented as follows:

Lemma 1 ([26, 27])**.** Let $H \trianglelefteq G$, $A \subseteq G$ and η be the canonical homomorphism $\eta : G \to G/H$ such that $a, b \in A$, $a \neq b$ imply that $aH \neq bH$. Let $A' = \eta(A)$, and suppose that $[A_1, A_2, \ldots, A_k]$ is an LS for

Table 2 MLSs for $O_n(q)$ and $SO_n(q)$

	$A = \langle a \rangle$	$B' = \{hC \mid h \in B\}$ with $C \leqslant B = \langle b \rangle$, $\lvert C \rvert = q-1$	$G_w = P : Q$ with $Q = GL_1(q) \times Y$	
	a	b	$\lvert P \rvert$	Y
$O_n(q)$	$x_1^{q^m-1}$ for $x_1 \in GL_{2m}(q)$	$\begin{pmatrix} D_1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (D_1^t)^{-1} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ for $D_1 \in GL_{2m-2}(q)$	q^{2m-2}	$O^-_{2m-2}(q)$
	$x_2^{q^{m-1}-1}$ for $x_2 \in GL_{2m}(q)$	$\begin{pmatrix} D_2 & 0 \\ 0 & (D_2^t)^{-1} \end{pmatrix}$ for $D_2 \in GL_{2m}(q)$	q^{2m-2}	$O^+_{2m-2}(q)$
	$x_3^{q^m-1}$ for $x_3 \in GL_{2m+1}(q)$	$\begin{pmatrix} D_3 & 0 & 0 \\ 0 & (D_3^t)^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$ for $D_3 \in GL_{2m}(q)$	q^{2m-1}	$O_{2m-1}(q)$
$SO_n(q)$	$x_1^{*q^m-1}$ for $x_1^* \in O^-_{2m}(q)$	$\begin{pmatrix} D_1^* & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & D_1^{*t} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ for $D_1^* \in O_{m-1}(q)$	q^{2m-2}	$SO^-_{2m-2}(q)$
	$x_2^{*q^{m-1}-1}$ for $x_2^* \in O^+_{2m}(q)$	$\begin{pmatrix} D_2^* & 0 \\ 0 & D_2^{*t} \end{pmatrix}$ for $D_2^* \in O_m(q)$	q^{2m-2}	$SO^+_{2m-2}(q)$
	$x_3^{*q^m-1}$ for $x_3^* \in O_{2m+1}(q)$	$\begin{pmatrix} D_3^* & 0 & 0 \\ 0 & D_3^{*t} & 0 \\ 0 & 0 & 1 \end{pmatrix}$ for $D_3^* \in O_m(q)$	q^{2m-1}	$SO_{2m-1}(q)$

A. Let $B_i = \eta(A_i) \subseteq G/H$ for $1 \leqslant i \leqslant k$. Then $[B_1, B_2, \ldots, B_k]$ is an LS for A'.

Lemma 2 ([26, 27])**.** Suppose that $G|L$ is a transitive permutation group action such that G is a subgroup of $GL(V)$ and $L \subseteq P(V)$ is a Singhi subset. Let S be an r-partial spread in V, which can be viewed as the projective partitions of L. Let $W \in S$, $w \in P(W)$ and G_w be the stabilizer of w in G. Suppose there are sets A, $B \subseteq G$ such that

(i) A acts sharply transitive on S with respect to W under the action of G on the set of all r-dimensional subspaces of V;

(ii) B acts sharply transitive on $L \cap P(W)$ with respect to w under the action of G on $P(W)$.

Then, $[A, B, G_w]$ is an LS for G.

Finally, we presented new constructions of MLSs for the orthogonal group $O_n(q)$, the special orthogonal group $SO_n(q)$, the projective special orthogonal group $PSO_n(q)$, the commutator subgroup $\Omega_n(q)$ and one type of classical groups [30]—projective commutator subgroup $P\Omega_n(q)$ with q as a power of odd primes. For $O_n(q)$ and $SO_n(q)$, the proposed MLSs have the similar structure $[A, B', G_w]$, where $A = \langle a \rangle$, and $B' = \{hC \mid h \in B\}$, $C \leqslant B$, $B = \langle b \rangle$, while $G_w = P : Q$ is a semi-direct product of a p-group P and a direct product $Q = GL_1(q) \times Y$ (Table 2). We employed two canonical homomorphisms $\eta : SO_n(q) \rightarrow PSO_n(q)$ and $\theta : \Omega_n(q) \rightarrow P\Omega_n(q)$ for proving the existence of MLSs for $PSO_n(q)$ and $P\Omega_n(q)$, respectively.

2. The existence of MLSs for the projective special unitary group $PSU_n(q)$ [29].

Being different from the orthogonal group $O_n(q)$, the structure of unitary group $U_n(q)$ depends on conjugate-symmetric sesquilinear form and Hermitian space. Being similar to other classical groups, permutation presentations related to stabilizers and parabolic subgroups of permutation presentation that belong to unitary group are very clear. Therefore, being similar to the case in $O_n(q)$, our main idea is described as follows: using the relationship between stabilizers of one-dimensional isotropic subspace of the unitary group $U_n(q)$ ($SU_n(q)$) and its parabolic subgroups and combining the basic theory of spread, we divided the unitary group $U_n(q)$ ($SU_n(q)$) into some parts, then proved that each part has an MLS and $U_n(q)$ ($SU_n(q)$) has an MLS. Finally, using the relationship between $U_n(q)$ ($SU_n(q)$) and $PU_n(q)$ ($PSU_n(q)$), we utilized canonical homomorphism to prove the existence of MLSs for $PU_n(q)$ ($PSU_n(q)$).

Finally, we constructed MLSs for unitary group $U_n(q)$, special unitary group $SU_n(q)$ and projective unitary group $PU_n(q)$, as well as also for a type of simple groups—projective special unitary group $PSU_n(q)$ [29]. For $U_n(q)$ and $SU_n(q)$, the proposed MLSs have the similar structure $[A', B', G_w]$, where $A' = \{gH \mid g \in A\}$, $H \leqslant A$, $A = \langle a \rangle$, and $B' = \{hD \mid h \in B\}$, $D \leqslant B$, $B = \langle b \rangle$, while $G_w = P : Q$ is a semi-direct product of a p-group P and a direct product $Q = GL_1(q^2) \times Y$ (Table 3). Then, we employed two canonical homomorphisms $\eta_1 : U_n(q) \rightarrow PU_n(q)$ and $\eta_2 : SU_n(q) \rightarrow PSU_n(q)$ to construct the MLSs for $PU_n(q)$ and $PSU_n(q)$. The corresponding MLSs are $[\eta_1(A'), \eta_1(B'), \eta_1(G_w)]$ and

Table 3 MLSs for $U_n(q)$ and $SU_n(q)$

	$A' = \{gH \mid g \in A\}$ $H \leqslant A = \langle a\rangle$, $\lvert H\rvert = q+1$	$B' = \{hD \mid h \in B\}$ with $D \leqslant B = \langle b\rangle$,$\lvert D\rvert = q-1$	$Gw = P : Q$ $Q = GL_1(q^2) \times Y$	
	a	b	$\lvert P\rvert$	Y
$U_n(q)$	$x^{q^{2m+1}-1}$, $x \in GL_{2m+1}(q^2)$	$\begin{pmatrix} C & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (\overline{C}^t)^{-1} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $C \in GL_m(q^2)$	q^{4m-1}	$U_{2m-1}(q)$
	$x^{q^{2m-1}-1}$, $x \in GL_{2m-1}(q^2)$	$\begin{pmatrix} C' & 0 \\ 0 & (\overline{C'}^t)^{-1} \end{pmatrix}$, $C' \in GL_m(q^2)$	q^{4m-3}	$U_{2m-2}(q)$
$SU_n(q)$	$x^{q^{2m+1}-1}$, $x \in SU_{2m+1}(q)$	$\begin{pmatrix} C'' & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \overline{C''}^t & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $C'' \in U_m(q)$	q^{4m-1}	$SU_{2m-1}(q)$
	$x^{q^{2m-1}-1}$, $x \in SU_{2m-1}(q)$	$\begin{pmatrix} C''' & 0 \\ 0 & \overline{C'''}^t \end{pmatrix}$, $C''' \in U_m(q)$	q^{4m-3}	$SU_{2m-2}(q)$

$[\eta_2(A'), \eta_2(B'), \eta_2(G_w)]$, respectively.

3. The existence of MLSs for 10 types of exceptional groups of Lie type [28].

From the viewpoint of Lie algebra, exceptional groups of Lie type can be divided into three different types [38]. The first type consists of five families of Chevalley (untwisted) groups $G_2(q)$, $F_4(q)$, $E_6(q)$, $E_7(q)$ and $E_8(q)$ with q as a power of a prime. Next are the Steinberg-Tits-Hertzig twisted groups ${}^3D_4(q)$ and ${}^2E_6(q)$ for any finite field F_q with q a power of a prime. Finally, there are three families of Suzuki and Ree groups ${}^2B_2(2^{2n+1})$, ${}^2G_2(3^{2n+1})$ and ${}^2F_4(2^{2n+1})$. Comparing with classical groups, the structures of exceptional groups of Lie type are more complex. However, being similar to classical groups, there are corresponding permutation presentations in subset (one-dimensional isotropic subspace) of projective spaces related to exceptional groups that belongs to Lie type and the structures of stabilizers of the permutation representations are very clear. Therefore, we combined stabilizers of one-dimensional isotropic subspaces of exceptional groups of Lie type with the linear transformations of corresponding algebraic systems (Octonion algebras, Albert algebras, Lie algebras) to construct MLSs for [28] all 10 families of exceptional groups of Lie type.

For each of exceptional group of Lie type, the corresponding MLS has the similar structure: $[A, T_1, T_2, G_w]$ or $[A, T, G_w]$, where G_w is the stabilizer of the corresponding exceptional groups of Lie type G; T_1, T_2 are the cyclic maximal torus of G; T is the sharp cyclic torus of G; A is a product of some cyclic subgroups of G (Table 4). Meanwhile, we proved the existence hypothesis of MLSs for Ru and Suz, indirectly presented the proof for the existence of MLSs for the two types of sporadic groups.

4. The existence of MLSs for 13 types of sporadic groups [31].

From the viewpoint of group theory, we observe that the sporadic groups are divided into four classes, three consecutive levels plus the Pariahs. The levels are Mathieu's (M_{11}, M_{12}, M_{22}, M_{23} and M_{24}), Leech's (Co_1, Co_2, Co_3, HS, McL, J_2, Suz) and Monster's (M, B, Fi_{22}, Fi_{23}, Fi_{24}', HN, Th, He), plus 6 Pariah groups (Ru, $O'N$, Ly, J_1, J_3, J_4). So, there are 26 sporadic groups. Until now, the existence of MLSs for 13 families of sporadic groups have been proved. These sporadic groups are listed as follows: M_{12}, M_{22}, M_{23}, M_{24}, Co_3, HS, McL, J_1, J_2, Suz, Ru (we proved the existence hypothesis of MLSs for Ru and Suz) and He. Hence, we only need to consider the remaining 13 types of sporadic groups. Comparing with the aforementioned finite simple groups, the orders of sporadic groups are much larger and the structures are much more complicated. Thus, we should take the advantage of some new technologies in order to deal with this problem. Here, our idea is to take the collective advantage while combining with stabilizers of corresponding sporadic groups, group action theory and Sylow theorem, we divided every sporadic group into several disjoint parts and proved that each part has an MLS, then proved that whole group has an MLS by splicing technology. Our basic theory is presented as follows:

Lemma 3 ([26, 27]). If $G(G|X)$ contains cyclic subgroups (sets) $A_1, \ldots, A_n$ and G_w such that

(i) $|G| = |A_1| \cdots |A_n| \cdot |G_w|$,

(ii) A_i has an MLS for all i,

(iii) G_w has an MLS,

Table 4 MLSs for exceptional groups of Lie type

G	A	T or T_1, T_2	G_w
$G_2(q)$	$A=\langle a\rangle$ $a=x^{q-1}$, $x\in G_2(q)$	$\|T_1\|=q^2+q+1$ $\|T_2\|=q^2-q+1$	$G_w=q^{2+1+2}:GL_2(q)$
${}^2G_2(q)$	$A=\langle a\rangle$ $a=x^{q-1}$, $x\in {}^2G_2(q)$	$\|T_1\|=q+\sqrt{3q}+1$ $\|T_1\|=q-\sqrt{3q}+1$	$G_w=q^{1+1+1}:C_{q-1}$
${}^3D_4(q)$	$A=A_1A_2$, $A_i=\langle a_i\rangle$, $1\leqslant i\leqslant 2$ $a_1=x^{q^2-1}$, $a_2=x^{q^3-1}$ for $x\in {}^3D_4(q)$	$\|T\|=q^4-q^2+1$	$G_w=q^{2+3+6}:SL_2(q)\cdot C_{q^2-1}$
${}^2B_2(q)$	$\|A\|=1$	$\|T_1\|=q+\sqrt{2q}+1$ $\|T_2\|=q-\sqrt{2q}+1$	$G_w=q^{1+1}\cdot C_{q-1}$
$F_4(q)$	$A=A_1A_2A_3A_4$, $A_i=\langle a_i\rangle$, $1\leqslant i\leqslant 4$ $a_1=x_1^{q-1}$, $a_2=x_2^{q^2-1}$, $a_3=x_3^{q^3-1}$, $a_4=x_4^{q^4-1}$	$\|T\|=q^4-q^2+1$	$G_w=q^{7+8}:2\cdot\Omega_7(q).C_{q-1}$ for q odd, $G_w=(q^6\times q^{1+8})Sp_6(q).C_{q-1}$ for q even
${}^2F_4(q)$	$A=A_1A_2A_3$, $A_i=\langle a_i\rangle$, $1\leqslant i\leqslant 3$ $a_1=x_1^{q-1}$, $a_2=x_2^{q^2-1}$, $a_3=x_3^{q^3-1}$	$\|T_1\|=q^2+\sqrt{2q^3}+q+\sqrt{2q}+1$ $\|T_2\|=q^2-\sqrt{2q^3}+q-\sqrt{2q}+1$	$G_w=q^1\cdot q^4\cdot q^1\cdot q^4:({}^2B_2(q)$ $\times C_{q-1})$
$E_6(q)$	$A=A_1A_2$, $A_i=\langle a_i\rangle$, $1\leqslant i\leqslant 2$ $a_1=x_1^{q-1}$, $a_2=x_2^{q^4-1}$	$\|T\|=q^6+q^3+1$	$G_w=q^{16}:(\Omega_{10}^{+}(q)\times C_{q-1})$
${}^2E_6(q)$	$A=A_1A_2A_3$, $A_i=\langle a_i\rangle$, $1\leqslant i\leqslant 3$ $a_1=x_1^{q-1}$, $a_2=x_2^{(q^3-1)(q+1)}$, $a_3=x_3^{q^6-1}$	$\|T_1\|=q^6-q^3+1$, $\|T_2\|=(q^4+1)(q^2-1)$	$G_w=q^{21}:(SU_6(q)\times C_{q-1})$
$E_7(q)$	$A=A_1A_2A_3$, $A_i=\langle a_i\rangle$, $1\leqslant i\leqslant 3$ $a_1=x_1^{q-1}$, $a_2=x_2^{q^5-1}$, $a_3=x_3^{q^9-1}$	$\|T\|=q^7+1$ for q even $\|T\|=(q^7+1)/2$ for q odd	$G_w=q^{27}:(E_6(q)\times C_{q-1})$ for q even $G_w=q^{27}:2\cdot(E_6(q)\times C_{(q-1)/2})\cdot 2$ for q odd
$E_8(q)$	$A=A_1A_2A_3A_4$, $A_i=\langle a_i\rangle$, $1\leqslant i\leqslant 4$ $a_1=x_1^{q^6-1}$, $a_2=x_2^{q^{10}-1}$, $a_3=x_3^{q^{12}-1}$, $a_4=x_4^{\|T\|(q-1)}$	$\|T\|=q^8-q^7+q^5-q^4+q^3-q+1$ for q even $\|T\|=(q^8-q^7+q^5-q^4+q^3-q+1)/2$ for q odd	$G_w=q^1\cdot q^{56}:(E_7(q)\times C_{q-1})$ for q even $G_w=q^1\cdot q^{56}:2\cdot(E_7(q)\times C_{(q-1)/2})\cdot 2$ for q odd

(iv) $G=A_1\cdots A_n\cdot G_w$ ($H=A_1\cdots A_n$, G is a sharply transitive set on X with respect to $w\in X$), then $[A_1,A_2,\ldots,A_n,G_w]$ is an LS for G and G has an MLS.

Then, we presented the constructions of MLSs for remaining 13 types of sporadic groups [31], For each kind of sporadic groups, the proposed MLS has the similar structures $[H,G_w]$, where G_w is the stabilizer of corresponding sporadic groups G; H is a product of some appropriate subgroups of G (Table 5).

Finally, utilizing some of the mathematical methods such as the matrix groups, Lie groups and associative algebras, we proposed the constructions of MLSs for the remaining four categories of finite simple groups. Until now, we get the conclusion that all finite simple group has an MLS.

Further discussion of related problems. Recently, Ashrafi et al. [39] also presented the structures of MLSs for some Suzuki simple groups and the projective special unitary groups. Following the lines of Lempken [25], Ashrafi et al. took the advantage of double coset decomposition technique to discuss MLSs for several kinds of Suzuki simple groups and the projective special unitary groups, and also presented that there are many simple groups, which can't be handled by this method. At the same time, the authors also pointed out some possible bugs in our paper [28]. By inspection and analysis, we found that there are some obscure contents in our paper. Therefore, it is necessary to further explain our basic theory and concrete process of constructing MLSs.

First of all, the most ideal conclusion of LSs for group G is that G can be factorized into $[A_1,A_2,\ldots,A_n]$, where $A_i\leqslant G$ ($1\leqslant i\leqslant n$). The corresponding results are presented as follows:

Lemma 4 ([24])**.** If $G(G|X)$ contains subgroups (sets) $A_1,\ldots,A_n$ such that

(i) $|G|=|A_1|\cdots|A_n|$,

Table 5 MLSs for 13 types of sporadic groups

G	H	G_w
Co_1	$H = ABCD$ $\lvert A\rvert = 3^6, \lvert B\rvert = 5^3, \lvert C\rvert = 7, \lvert D\rvert = 13$	$G_w = 2^{11} : M_{24}$
Co_2	$H = ABC$ $\lvert A\rvert = 3^4, \lvert B\rvert = 5^2, \lvert C\rvert = 23$	$G_w = 2^{10} : M_{22} : 2$
Fi_{22}	$H = ABCD$ $\lvert A\rvert = 2, \lvert B\rvert = 3^5, \lvert C\rvert = 5, \lvert D\rvert = 13$	$G_w = PSU_6(2)$
Fi_{23}	$H = ABC$ $\lvert A\rvert = 3^4, \lvert B\rvert = 17, \lvert C\rvert = 23$	$G_w = 2.Fi_{22}$
Fi'_{24}	$H = ABCD$ $\lvert A\rvert = 2^3, \lvert B\rvert = 3^3, \lvert C\rvert = 7^2, \lvert D\rvert = 29$	$G_w = Fi_{23}$
Th	$H = ABCDEF$ $\lvert A\rvert = 2^3, \lvert B\rvert = 3^5, \lvert C\rvert = 5^3, \lvert D\rvert = 7, \lvert E\rvert = 19, \lvert F\rvert = 31$	$G_w =^3 D_4(2) : 3$
HN	$H = ABCD$ $\lvert A\rvert = 2^6, \lvert B\rvert = 3, \lvert C\rvert = 5^5, \lvert D\rvert = 19$	$G_w = A_{12}$
B	$H = ABCDEF$ $\lvert A\rvert = 2^3, \lvert B\rvert = 3^4, \lvert C\rvert = 5^4, \lvert D\rvert = 23, \lvert E\rvert = 31, \lvert F\rvert = 47$	$G_w = 2.^2E_6(2) : 2$
M	$H = ABCDEFGH$ $\lvert A\rvert = 2^5, \lvert B\rvert = 3^7, \lvert C\rvert = 5^3, \lvert D\rvert = 11, \lvert E\rvert = 13^2, \lvert F\rvert = 41, \lvert G\rvert = 59, \lvert H\rvert = 71$	$G_w = 2.B$
$O'N$	$H = ABCD$ $\lvert A\rvert = 2^2, \lvert B\rvert = 3^2, \lvert C\rvert = 11, \lvert D\rvert = 31$	$G_w = PSL_3(7) : 2$
Ly	$H = ABCDE$ $\lvert A\rvert = 2^2, \lvert B\rvert = 3^4, \lvert C\rvert = 11, \lvert D\rvert = 37, \lvert E\rvert = 67$	$G_w = G_2(5)$
J_3	$H = ABCD$ $\lvert A\rvert = 2^2, \lvert B\rvert = 3^2, \lvert C\rvert = 17, \lvert D\rvert = 19$	$G_w = 3 \times (3 \times A_6) : 2$
J_4	$H = ABCDE$ $\lvert A\rvert = 11^2, \lvert B\rvert = 29, \lvert C\rvert = 31, \lvert D\rvert = 37, \lvert E\rvert = 43$	$G_w = 2^{11} : M_{24}$

(ii) A_i has an MLS for all i,

(iii) $G = A_1 \cdots A_n$,

then $[A_1, A_2, \ldots, A_n]$ is an LS for G and G has an MLS.

In particular, if $G = P_1 \cdots P_k$, P_i is a subgroup of p_i-Sylow, then $[P_1, P_2, \ldots, P_k]$ is an LS for G, where $p_1, \ldots, p_k$ is different factor of $|G|$ (Subsection 4.1 in [23]). When $n = 2$, the corresponding conclusions are given as follows [25]: if $A, B \leqslant G$, $G = AB$, $A \cap B = 1$, then $[A, B]$ is an LS for G.

Secondly, when $n \geqslant 3$, it's difficult to construct LS for G: on the one hand, the conditions of group factorization is more strict [25]; on the other hand, from the definition of LS (definition 1 in [28]) we observe that A_i needn't be the subgroup of G. Therefore, some experts presented more general results about LS by using algebraic group theory [26, 27].

Lemma 5 ([27])**.** Let $A \subseteq G$. Suppose $[A_1, A_2, \ldots, A_r]$ is an LS for A and for each A_i, $1 \leqslant i \leqslant r$, $[B_{i1}, \ldots, B_{ik_i}]$ is an LS for A_i. Then $\alpha = [B_{11}, \ldots, B_{1k_1}, \ldots, B_{r1}, \ldots, B_{rk_r}]$ is an LS for A.

Lemma 6 ([27])**.** Let $G|X$ be a transitive permutation group. Suppose $A \subseteq G$ is a sharply transitive set on X with respect to $x \in X$ and G_x is the stabilizer of x in G. Then, $[A, G_x]$ is an LS for G.

Therefore, combining the aforementioned facts with Lemmas 2 and 3, we obtain MLSs for all 10 types of exceptional group of Lie type. In fact, we utilize stabilizers of isotopic 1-subspaces and linear transformations in corresponding algebraic systems to construct MLSs for all ten families of exceptional groups of Lie type. Our method has universal meanings.

Finally, we employ Figure 1 for summarizing the proof history of MLS conjecture, in which node (1) is

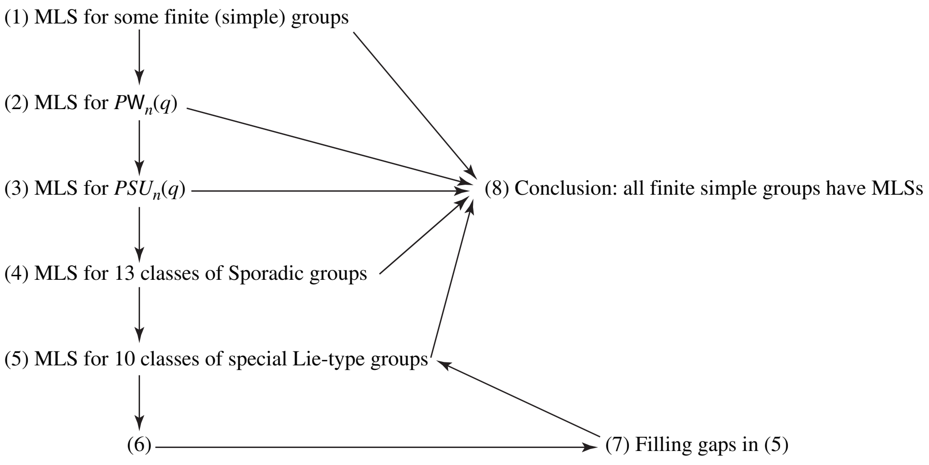
(1) MLS for some finite (simple) groups
(2) MLS for $PW_n(q)$
(3) MLS for $PSU_n(q)$
(4) MLS for 13 classes of Sporadic groups
(5) MLS for 10 classes of special Lie-type groups
(6)
(7) Filling gaps in (5)
(8) Conclusion: all finite simple groups have MLSs

Figure 1 Research on MLS conjecture.

mainly composed of Vasco [23], Holmes [24], Lempken [25] and Singhi [26,27], node (6) is the contribution of Ashrafi et al [39], nodes (2)–(5) are completed by [28–31], nodes (7) and (8) are presented in this paper.

4 Conclusion

We have completed the proof of MLS conjecture in theory. It can bring many implementation platforms to MST cryptosystems, effectively reducing the key size of public(private) key and improving the speed of encryption (decryption). Therefore, in the future, MST cryptosystems will have a wide application prospect. In addition, the problem of MLS conjecture relies on group factorization problems in finite groups and it is deeply related with algebraic and geometric structures in finite groups. It is meaningful for people to understand the structures of finite groups in a better way, for the development of algebraic, and computational group theory.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61502048, 61370194, 61373131) and NSFC A3 Foresight Program (Grant No. 61411146001). This work was also partially supported by PAPD and CICAEET.

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Shor P. Polynomial time algorithms for prime factorization and discrete logarithms on quantum computers. SIAM J Comput, 1997, 26: 1484–1509
2 Proos J, Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Inf Comput, 2003, 3: 317–344
3 Blaser M. Noncommutativity makes determinants hard. Electr Coll Comp Complex Report. No. 142. 2012
4 Rotteler M. Quantum algorithms: a survey of some recent results. Inf Forsch Entw, 2006, 21: 3–20
5 Wagner N, Magyarik M. A public-key cryptosystem based on the word problem. In: Proceedings of CRYPTO'84 on Advances in Cryptology. Berlin: Springer, 1985. 19–36
6 Ko K, Lee S, Cheon J, et al. New public-key cryptosystem using braid groups. In: Proceedings of 20th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, 2000. 166–183
7 Eick B, Kahrobaei D. Polycyclic groups: a new platform for cryptology. arXiv:math/0411077
8 Shpilrain V, Ushakov A. Thompson's group and public key cryptography. In: Proceedings of 3rd International Conference on Applied Cryptography and Network Security, New York, 2005. 151–164
9 Kahrobaei D, Koupparis C, Shpilrain V. Public key exchange using matrices over group rings. Groups Complexity Cryptol, 2013, 5: 97–115
10 Magliveras S S. A cryptosystem from logarithmic signatures of finite groups. In: Proceedings of 29th Midwest Symposium on Circuits and Systems. Amsterdam: Elsevier Publishing Company, 1986. 972–975
11 Magliveras S S, Memon N D. Properties of cryptosystem PGM. In: Proceedings of 9th Annual International Cryptology Conference, Santa Barbara, 1989. 447–460

12 Magliveras S S, Memon N D. Complexity tests for cryptosystem PGM. Congr Numer, 1990, 79: 61–68

13 Magliveras S S, Memon N D. Algebraic properties of cryptosystem PGM. J Cryptol, 1992, 5: 167–183

14 Caranti A, Volta D F. The round functions of cryptosystem PGM generate the symmetric group. Des Codes Cryptogr, 2006, 38: 147–155

15 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, 2002, 15: 285–297

16 Lempken W, Magliveras S S, van Trung T, et al. A public key cryptosystem based on non-abelian finite groups. J Cryptol, 2009, 22: 62–74

17 Higman G. Suzuki 2-groups. Ill J Math, 1963, 7: 79–96

18 Magliveras S S, Svaba P, van Trung T, et al. On the security of a realization of cryptosystem MST_3. Tatra Mt Math Publ, 2008, 41: 1–13

19 Blackburn S R, Cid C, Mullan C. Cryptanalysis of the MST_3 public key cryptosystem. J Math Crypt, 2009, 3: 321–338

20 González Vasco M I, Pérez del Pozo A L, Duarte P T. A note on the security of MST_3. Des Codes Cryptogr, 2010, 55: 189–200

21 Svaba P, van Trung T. Public key cryptosystem MST3: cryptanalysis and realization. J Math Cryptol, 2010, 4: 271–315

22 Hong H B, Li J, Wang L C, et al. A digital signature scheme based on MST_3 cryptosystem. Math Probl Eng, 2014, 2014: 630421

23 González Vasco M I, Rötteler M, Steinwandt R. On minimal length factorizations of finite groups. Exp Math, 2003, 12: 1–12

24 Holmes P E. On minimal factorisations of sporadic groups. Exp Math, 2004, 13: 435–440

25 Lempken W, van Trung T. On minimal logarithmic signatures of finite groups. Exp Math, 2005, 14: 257–269

26 Singhi N, Singhi N, Magliveras S S. Minimal logarithmic signatures for finite groups of Lie type. Des Codes Cryptogr, 2010, 55: 243–260

27 Singhi N, Singhi N. Minimal logarithmic signatures for classical groups. Des Codes Cryptogr, 2011, 60: 183–195

28 Hong H B, Wang L C, Yang Y X, et al. All exceptional groups of Lie type have minimal logarithmic signatures. Appl Algebr Eng Commun Comput, 2014, 25: 287–296

29 Hong H B, Wang L C, Yang Y X. Minimal logarithmic signatures for the unitary group $U_n(q)$. Des Codes Cryptogr, 2015, 77: 179–191

30 Hong H B, Wang L C, Ahmad H, et al. Minimal logarithmic signatures for a type of classical groups. arXiv:1507.01163

31 Hong H B, Wang L C, Ahmad H, et al. Minimal logarithmic signatures for sporadic groups. arXiv:1507.01162

32 González Vasco M I, Steinwandt R. Obstacles in two public key cryptosystems based on group factorizations. Tatra Mt Math Publ, 2002, 25: 23–37

33 Conway J, Curtis R, Norton S, et al. Atlas of Finite Groups. Oxford: Clarendon Press, 1985

34 Cossidente A, de Resmini M J. Remarks on singer cyclic groups and their normalizers. Des Codes Cryptogr, 2004, 32: 97–102

35 Hestenes M D. Singer groups. Can J Math, 1970, 22: 492–513

36 Thas J A. Ovoids and spreads of finite classical polar spaces. Geom Dedic, 1981, 10: 135–143

37 Kantor W M. Spreads, translation planes and Kerdock sets. I. SIAM J Algebr Discret Meth, 1982, 3: 151–165

38 Wilson R A. The Finite Simple Groups. London: Springer-Verlag, 2009

39 Rahimipour A R, Ashrafi A R, Gholami A. The existence of minimal logarithmic signatures for some Suzuki and simple unitary. Cryptogr Commun, 2015, 7: 535–542