Tatra Mt. Math. Publ. **25** (2002), 11–22

Tatra Mountains
Mathematical Publications

SECRET- AND PUBLIC-KEY CRYPTOSYSTEMS FROM GROUP FACTORIZATIONS

Spyros S. Magliveras

ABSTRACT. Many known cryptosystems, symmetric or asymmetric, have been based on properties of large abelian groups. Here we discuss cryptosystems based on non-abelian, in fact non-solvable groups. A symmetric key cryptosystem based on *logarithmic signatures* for finite permutation groups was proposed by the author in [S. S. Magliveras: *A cryptosystem from logarithmic signatures of finite groups*, In Proceedings of the 29'th Midwest Symposium on Circuits and Systems, Elsevier Publishing Company, (1986), pp. 972–975], and its algebraic properties were studied in [S. S. Magliveras, N. D. Memon: *The Algebraic Properties of Cryptosystem PGM*, J. of Cryptology, **5** (1992), 167-183]. Moreover, two possible approaches to the construction of new public key cryptosystems using *group factorizations* were described in [S. S. Magliveras, Tran Van Trung and D. R. Stinson: *New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups*, to appear in the J. Cryptology]. We discuss the above systems, issues related to them, and provide some insight into a question posed by M. I. González Vasco and R. Steinwaldt.

1. Introduction

We are at a moment in history when *security* of information and communications has become paramount as political, social and economic infrastructures world-wide depend on it. At the dawn of the 21st century only a few known public key cryptosystems remain unbroken. Among them are RSA, ElGamal over a finite field $\mathbb{F}_q$ or an elliptic curve, NTRU, GGH, McEliece, and this list is for all practical purposes rather complete. Most of these systems rely on the perceived difficulty of certain problems in particular large finite abelian groups. But abelian groups, including integral lattices, have well understood structures. This makes cryptosystems based on abelian groups more susceptible to crypt-

2000 Mathematics Subject Classification: 94A60, 20B40, 20F99.
Keywords: PGM, trap-door one-way functions, group factorizations, public key cryptosystems, finite groups.

This material is based upon work supported by the National Science Foundation under Grant No. 9610138.

analysis. In this paper we explore the possibility of building cryptosystems on non-abelian, in fact non-solvable groups.

In this paper we describe how, in principle, we can use group factorizations to build symmetric cryptosystems, one way functions and explore the possibility of two new public key cryptosystems. When the underlying groups are permutation groups, composition of two permutations can be done in one machine cycle in specially designed hardware, and therefore the new systems are potentially fast. A permutation group environment would be particularly useful in applications involving video encryption, in which images are scrambled by applying streaming pseudo-random permutations to rows and columns of a digital image. There is a fundamental difference between the known systems and the ones we propose. While the former are based on large cyclic groups, our systems are based on large non-solvable groups of much higher structural complexity than that of a cyclic group.

We wish to warn the reader that our asymmetric systems are currently hypothetical, in the sense that we do not have efficient algorithms to generate efficiently parameters for secure versions of the proposed systems. Some impediments for constructing secure instances of our systems have been discussed by the authors of [12] and their observations need to be considered carefully. However, we still hope that the techniques introduced in this paper may eventually lead to the realization of new, practical building blocks for cryptographers.

2. Preliminaries

We define the *degree* of an abstract finite group G to be the degree of the smallest faithful permutation representation of G. On the other hand, for permutation groups the *degree* n has the usual meaning, that is, the degree of G is the number n of points permuted by the elements of G. We denote by $G^{[\mathbb{Z}]}$ the collection of all finite sequences in G, and view the elements of $G^{[\mathbb{Z}]}$ as single-row matrices with entries in G. Under ordinary tensor product of matrices, $G^{[\mathbb{Z}]}$ is a monoid. The following example illustrates the operation,

$$[x_1, x_2, x_3] \otimes [y_1, y_2] = [x_1y_1, x_1y_2, x_2y_1, x_2y_2, x_3y_1, x_3y_2]\,.$$

We simplify notation and write $X\cdot Y$ or XY for $X\otimes Y$. If $X = [x_1, x_2, \ldots, x_r] \in G^{[\mathbb{Z}]}$, the *length* r of X is denoted by $|X|$, and $\overline{X}$ denotes the element $\sum_{i=1}^{r} x_i$ in the group ring $\mathbb{Z}G$. It follows that $\overline{XY} = \overline{X}\,\overline{Y}$ and $|X\,Y| = |X|\,|Y|$, for any $X, Y \in G^{[\mathbb{Z}]}$.

Let G be a finite group. Suppose that $\alpha = [A_1, A_2, \ldots, A_s]$ is a sequence of $A_i \in G^{[\mathbb{Z}]}$, such that $\sum_{i=1}^{s} |A_i|$ is bounded by a polynomial in the degree of G.

Moreover, let

$$\overline{A_1} \cdot \overline{A_2} \cdots \overline{A_s} = \sum_{g \in G} a_g g\,, \;\; a_g \in \mathbb{Z}\,. \tag{2.1}$$

Then, we say that α is

i) a *cover* for G if for all $g \in G$, $a_g > 0$;

ii) a *pseudo logarithmic signature* for G, if $\prod_{i=1}^{s} |A_i| = |G|$;

iii) a *logarithmic signature* for G, if for all $g \in G$, $a_g = 1$;

iv) an $[s,r]$-mesh for G, if

  a) $\alpha = [A_1, \ldots, A_s]$ is a cover with $|A_i| = r$ for $1 \le i \le s$, and

  b) the probability distribution $\left\{\frac{a_g}{r^s} \colon g \in G\right\}$ is approximately uniform.

It is clear from the definition that if $\alpha = [A_1, \ldots, A_s]$ is a logarithmic signature for G, then, each element $y \in G$ can be expressed uniquely as a product of the form

$$y = q_1 \cdot q_2 \cdot \ldots \cdot q_{s-1} \cdot q_s \tag{2.2}$$

for $q_i \in A_i$. For general covers, however, the factorization in (2.2) is not unique, and the problem of finding a factorization for a given $y \in G$ is in general intractable.

Let $\alpha = [A_1, \ldots, A_s]$ be a logarithmic signature for G with $r_i = |A_i|$, then, the A_i are called the *blocks* of α and the vector of block lengths $(r_1, \ldots, r_s)$ the *type* of α. We define the *length* of α to be the integer $\ell = \sum_{i=1}^{s} r_i$. We say that α is *nontrivial* if $s \ge 2$ and $r_i \ge 2$ for $1 \le i \le s$; otherwise α is said to be *trivial.* A logarithmic signature is called *tame* if the factorization in equation (2.2) can be achieved in time polynomial in the degree n of G and *supertame* if the factorization can be achieved in time $O(n^2)$. The existence of supertame logarithmic signatures is discussed in [8]. A logarithmic signature is called *wild* if it is not tame. We denote by $\mathcal{C}$, and Λ the respective collections of *covers* and *logarithmic signatures* for G. In some occasions, we represent a logarithmic signature $\alpha = [A_1, \ldots, A_s]$ of type $(r_1, \ldots, r_s)$ by an $s \times r$ matrix

$$\alpha = (a_{i,j}) \tag{2.3}$$

where $r = \max\{r_i\}$, $a_{i,j} = A_i(j)$ is the jth element of A_i, for $1 \le j \le r_i$, and $a_{i,j} = 0$ for $j > r_i$.

If $\alpha = [A_1, \ldots, A_s]$ is a logarithmic signature for a group G, then the sequence $A_1 \otimes \cdots \otimes A_s$ contains each element of G exactly once. Thus, α induces a bijection $\breve{\alpha} \colon \mathbb{Z}_{|G|} \to G$.

Proofs for the following propositions are given in [9].

Proposition 2.1. *In the class $\mathcal{G}$ of finite groups there are instances (G, α), $\alpha \in \mathcal{C}$, where the factorization in (2.2) is equivalent to solving the discrete logarithm problem in G.*

Proposition 2.2. *Suppose that α is a logarithmic signature of a finite group G, then, $\breve{\alpha}$ is always efficiently computable. However, $\breve{\alpha}^{-1}$ is efficiently computable if and only if α is tame.*

The following statement follows naturally:

Proposition 2.3. *Let G be a finite group, α a wild logarithmic signature and β a tame logarithmic signature for G, then the mapping $\breve{\alpha}\breve{\beta}^{-1} : \mathbb{Z}_{|G|} \to \mathbb{Z}_{|G|}$ is a one-way permutation.*

Abusing language somewhat we use the phrase "α can be inverted" to mean that $\breve{\alpha}$ can be inverted efficiently, i.e., that the factorization in (2.2) is achievable in polynomial time.

Definition 2.1. Two logarithmic signatures α, β of G are said to be *equivalent* if $\breve{\alpha} = \breve{\beta}$.

3. Classes and transformations

We now discuss briefly *classes* of logarithmic signatures and basic *transformations* on logarithmic signatures for a group G. When we discuss matters involving computational complexity, we further assume that G is a permutation group of degree n.

Let γ: $1 = G_0 < G_1 < \cdots < G_{s-1} < G_s = G$ be a chain of subgroups of G, and A_i an ordered, complete set of right coset representatives of G_{i-1} in G_i. It is clear that $[A_1, A_2, \ldots, A_s]$ forms a logarithmic signature for G. Such a logarithmic signature is called *exact-transversal* with respect to γ. The following proposition is an easy corollary of a theorem by F u r s t, H o p c r o f t, and L u k s, [3]. For the proof see [8].

Proposition 3.1. *Let G be a finite permutation group of degree n, and α an exact-transversal logarithmic signature of length polynomial in n. Then, α is tame.*

We denote the set of all exact-transversal logarithmic signatures of G by $\mathcal{E}$.

Proposition 3.2. *Let G be a finite permutation group of degree n, and suppose that $\alpha = [A_1, A_2, \ldots, A_s]$ is a pseudo logarithmic signature for G. Then, there is a polynomial time algorithm which decides whether $\alpha \in \mathcal{E}$.*

Proof. For $k = 1, \dots, s$ let $V_k = \langle A_1 \cup \dots \cup A_k \rangle$. We first check that $V_1 = A_1$, i.e., that A_1 is a subgroup. This takes polynomial time by using [3], or simply testing closure. Now, suppose we have verified in polynomial time that $|V_k| = |V_{k-1}| \cdot |A_k|$. Using the Schreier-Sims [11] or similar algorithm we build "strong generators" for V_{k+1} using $A_1 \cup \dots \cup A_k \cup A_{k+1}$ as the initial generating set and verify that $|V_{k+1}| = |V_k| \cdot |A_{k+1}|$. Both s and the time taken in the kth step are bounded by a polynomial in n . □

Different types of transformations on logarithmic signatures have been considered in [8] and [10]. Here, we consider just two. The first type, called the *shuffle* or *monomial shuffle*, derives new logarithmic signatures from a given exact-transversal by changing the coset representatives, and permuting the elements within each block. The second type of transformation can be described as follows: Suppose that $\alpha = [A_1, A_2, \dots, A_s] \in \Lambda$. Let $g_0, g_1, \dots, g_s \in G$, and consider the sequence $\beta = [B_1, B_2, \dots, B_s]$, where $B_i = g_{i-1}^{-1} A_i g_i$. It is easy to see that β is a logarithmic signature for G. When $g_0 = g_s = 1$ we say that β is a *sandwich* of α. When $g_0 = 1$, β is said to be a *right translation* of α by g_s. If $g_s = 1$, then β is called a left translation of α by g_0. The following proposition is proved in [8].

Proposition 3.3. *Let α and β be two logarithmic signatures of G, both of type $(r_1, r_2, \dots, r_s)$. Then, α and β are equivalent if and only if one is a sandwich of the other.*

A logarithmic signature α for G is called *transversal* if and only if it is the sandwich of an exact-transversal logarithmic signature for G. We denote the set of all transversal logarithmic signatures of G by $\mathcal{T}$.

The following proposition was also proved in [9] and asserts that we can decide in polynomial time whether a given logarithmic signature is transversal or not. In the proof we present an algorithm for accomplishing the task. Recall that the order of a permutation group of degree n, generated by a polynomial in n number of generators can be computed in time polynomial in n [3].

Proposition 3.4. *Let G be a finite permutation group of degree n, and suppose that $\alpha = [A_1, A_2, \dots, A_s]$ is a logarithmic signature for G. Then, there is a polynomial time algorithm to determine whether α is transversal and, if so, determine an exact transversal β equivalent to α.*

Proof. We describe the algorithm for $s \geq 3$ and omit a proof of correctness. In the first step, replace $[A_1, A_2, A_3, \dots, A_s]$ by $[B_1, C_2, A_3, \dots, A_s]$ where $B_1 = A_1 x_1^{-1}$, $C_2 = x_1 A_2$ and $x_1 = A_1(1)$. The kth step, $k = 2, \dots, s-1$ replaces $[B_1, B_2, \dots, B_{k-1}, C_k, A_{k+1}, A_{k+2}, \dots, A_s]$ by $[B_1, B_2, \dots, B_{k-1}, B_k, C_{k+1}, A_{k+2}, \dots, A_s]$, where $B_k = C_k x_k^{-1}$, $C_{k+1} = x_k A_{k+1}$, and $x_k = C_k(1) \dots$ We finally test whether the resulting logarithmic signature $\beta = [B_1, B_2, \dots, B_{s-1}, C_s]$ is an exact transversal. If $\beta \in \mathcal{E}$ then $\alpha \in \mathcal{T}$ and the x_i provide the sandwiching transformation. If $\beta \notin \mathcal{E}$ then α is not transversal. If $s = 2$, we have a much easier task: replace $\alpha = [A_1, A_2]$ by $\beta = [B_1, C_2]$ where $B_1 = A_1 x_1^{-1}$, $C_2 = x_1 A_2$, $x_1 = A_1(1)$ and perform the final test as for the $s \geq 3$ case. $\square$

The process of obtaining $[B_1, B_2, \ldots, B_{s-1}, C_s]$ from $[A_1, A_2, \ldots, A_s]$ by appropriate sandwiching is called *normalization*. Normalization of a transversal logarithmic signature produces an equivalent exact transversal. The following is a consequence of Propositions (3.1) and (3.4).

Corollary 3.1. *Any transversal logarithmic signature of a finite permutation group G is tame.*

It follows that the class $\mathcal{W}$ of wild logarithmic signatures is a subclass of the class $\mathcal{NT}$ of *non-transversal* logarithmic signatures of G. There is another class of signatures which is farther from being transversal than logarithmic signatures in $\mathcal{NT}$. This is the class of *totally non-transversal* ($\mathcal{TNT}$) logarithmic signatures. A logarithmic signature α is said to be *totally-non-transversal* if each block of α is not a coset of a non-trivial subgroup of G. We adopt the cryptographic assumption that logarithmic signatures which are far from being transversal are difficult to invert, i.e., that logarithmic signatures in $\mathcal{TNT}$ are "wild-like". On the other hand, recent observations by the authors of [12] suggest that in building wild-like logarithmic signatures one needs to exercise much closer scrutiny so as to avoid possible pitfalls of weakened $\mathcal{TNT}$ logarithmic signatures which contain transversal-like segments. We believe that the problems discussed in [12] can be overcome, so that *strong* $\mathcal{TNT}$ signatures would be constructible. This however is the topic of future work.

Experimentation with relatively small groups shows that there are many more $\mathcal{TNT}$ logarithmic signatures, than transversal ones. Moreover, we know of no theoretical reasons why in general there should exist polynomial time algorithms to invert carefully chosen $\mathcal{TNT}$ logarithmic signatures. On the contrary, Proposition (2.1) supports our assumption.

We now identify the elements of G with the elements in $\mathbb{Z}_{|G|}$ by selecting a fixed supertame logarithmic signature η. Then $g \in G$ corresponds to $\eta^{-1}(g) \in \mathbb{Z}_{|G|}$. Once η has been selected, each logarithmic signature α gives rise to a computable permutation $\widehat{\alpha}$ of $\mathbb{Z}_{|G|}$ defined by $\widehat{\alpha} = \breve{\alpha}\breve{\eta}^{-1}$. If $\mathbb{F} \subset \Lambda$, we write $\widehat{\mathbb{F}} = \{\widehat{\alpha} \colon \alpha \in \mathbb{F}\}$.

4. Symmetric key systems based on logarithmic signatures

A family of secret-key cryptosystems was proposed in [7] which briefly works as follows. For a given large finite group G let α and β be randomly selected transversal logarithmic signatures for G. Consider the transformation $E_{(\alpha,\beta)} = \widehat{\alpha}\widehat{\beta}^{-1}\colon \mathbb{Z}_{|G|} \to \mathbb{Z}_{|G|}$ which is efficiently computable in both directions since both α and β are tame. The encryption transformation is $E_{(\alpha,\beta)} = \widehat{\alpha}\widehat{\beta}^{-1}$, and the corresponding decryption mapping is $D_{(\alpha,\beta)} = \widehat{\beta}\widehat{\alpha}^{-1}$ $(= E_{(\beta,\alpha)})$. The reader will find more information about this symmetric system in [8, 1]. The following theorem is proved in [8]:

Theorem 4.1. *If G is a finite non-hamiltonian group with $|G|$ different from q, $(1+q^2)$, $(1+q^3)$, $\frac{(q^n-1)}{(q-1)}$, $2^{n-1}(2^n \pm 1)$, 11, 12, 15, 22, 23, 24, 176, 276 where q is a prime power and n a positive integer, then the group $\langle\widehat{\mathcal{T}}\rangle$ generated by $\widehat{\mathcal{T}}$ is the full symmetric group $\mathcal{S}_{|G|}$.*

Theorem (4.1) is rather technical, but has important consequences. Essentially, the theorem says that *almost always* the giant group $\mathcal{S}_{|G|}$ is generated by $\widehat{\mathcal{T}} = \widehat{\mathcal{E}}$, i.e., by the collection of permutations induced by exact-transversal logarithmic signatures. Thus, any permutation $\sigma \in \mathcal{S}_{|G|}$ can be written as the composition of permutations $\widehat{\theta}_i$ induced by transversal logarithmic signatures. Note, moreover, that the conclusion of the theorem is independent of the choice of $\eta \in \mathcal{T}$. This follows from the simple observation that for $\theta \in \mathcal{T}$, $\alpha \in \Lambda$, $\breve{\alpha}\breve{\theta}^{-1} = \breve{\alpha}\breve{\eta}^{-1}\breve{\eta}\breve{\theta}^{-1} = \widehat{\alpha}\widehat{\theta}^{-1}$.

Incidentally, experimentation in groups of small order shows that the conclusion of Theorem (4.1) is true even when its hypotheses fail to hold.

5. First potential public key system MST_1

Suppose now that α is a wild, and β a tame logarithmic signature for a finite permutation group G. By Proposition (2.3), $\sigma = \widehat{\alpha}\widehat{\beta}^{-1} = \breve{\alpha}\breve{\theta}^{-1}$ is a one-way permutation in $\mathcal{S}_{|G|}$. Then, by Theorem (4.1), σ can be written as the product of a finite (hopefully small) number of elements in $\widehat{\mathcal{E}} = \widehat{\mathcal{T}}$ and their inverses. Because the mappings induced from transversal logarithmic signatures can be inverted efficiently, such factorizations, if they could be efficiently computed, could be used as trap-doors for a public key cryptosystem.

Suppose that a factorization of σ as the composition of elements of $\widehat{\mathcal{T}}$ is known only by Alice. Then, Alice can efficiently invert σ but no one else can. Now, given the one-way permutation σ above, the problem of factoring σ as the composition of transversal $\widehat{\theta}_i$ is in general hard, otherwise if we had a general, efficient algorithm for factoring σ, we would in principle be able to solve DLP. This is the basis for cryptosystem MST_1 we shall now discuss.

Our system is described as follows: User "Alice" is given a pair of logarithmic signatures (α, β) where α is in $\mathcal{TNT}$, and β is transversal. Alice is also given the factorization of $\sigma = \widehat{\alpha}\widehat{\beta}^{-1}$ as the composition $\sigma = \widehat{\theta}_1 \cdots \widehat{\theta}_k$ where the θ_i are exact-transversal, and where k is a small integer ≥ 2. Alice publishes (α, β) and G as her public key, but keeps $\theta_1, \ldots, \theta_k$ as her secret key. Since the θ_i are transversal, Alice can efficiently compute $\widehat{\theta}_i^{-1}$, and therefore can compute efficiently σ^{-1}. The message and cipher space are $\mathbb{Z}_{|G|}$. To send a message $m \in \mathbb{Z}_{|G|}$ to Alice, Bob encrypts m as $c = \sigma(m) = [\widehat{\alpha}\widehat{\beta}^{-1}](m)$ and transmits c to Alice. Upon receiving c, Alice decrypts c by computing $\widehat{\theta}_k^{-1}(\widehat{\theta}_{k-1}^{-1}(\ldots(\widehat{\theta}_1^{-1}(c))\ldots) = m$.

A procedure for building a trapdoor of the above type is discussed in [9]. Although experimentation shows that the probability of finding a trap-door of the above type is positive, the procedure discussed in [9] is not efficient. At the present time, we do not know whether the trapdoors indicated in the proposed scheme can be constructed efficiently.

To ensure security, the order of G should indeed be exponential in the degree of G, but this will not be sufficient. We are presently studying the possible contexts in which MST_1 can be practical. Of course transformations σ that have relatively small cycles as elements of $\mathcal{S}_{|G|}$ must be avoided since such σ would be vulnerable to birthday-type or cycling attacks.

6. Second potential public key system MST_2

We now turn our attention to a system based on $[s, r]$-meshes for a group G. Recall that an $[s, r]$-mesh is a uniform cover for G. These meshes are constructed by probabilistic methods. We measure the *degree of uniformity* of a mesh by applying the standard statistical uniformity measures to the probability distribution $\{P_g \colon g \in G\}$, where $P_g = \frac{a_g}{r^s}$ (for example an appropriate Kolmogorov-Smirnov statistic). In general it will be difficult to test the uniformity of $\{P_g\}$ for a particular proposed mesh. However, a test can be carried out to determine whether the dynamically produced (run-time) estimates for $\{\frac{a_g}{r^s}\}$ represent the conjugacy classes of G at the correct ratios, a necessary condition.

Experimentation with matrices $(a_{i,j})$ constructed by sampling random elements $a_{i,j}$ in arbitrary groups shows that $[s, r]$-meshes proliferate. In practice, we may select all the $a_{i,j}$ from a given conjugacy class of G.

Suppose now that $\alpha = (a_{i,j})$ is a random $[s, r]$-mesh covering a finite group G. Our cryptographic hypothesis is that, if $g \in G$, then finding a factorization

$$g = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s} \tag{6.4}$$

is, in general, an intractable problem. Let H be a second group and $f\colon G \to H$ an epimorphism, i.e., a homomorphism of G onto H. Then $\beta = (b_{i,j})$, where $b_{i,j} = f(a_{i,j})$, is an $[s,r]$-mesh for H. In general, the surjections $\breve{\alpha}\colon \mathbb{Z}_{r^s} \to G$ and $\breve{\beta}\colon \mathbb{Z}_{r^s} \to H$ are not bijections, but are efficiently computable.

We are now ready to describe our second public key cryptosystem in the context of $[s,r]$-meshes for groups.

6.1 The Second system MST$_2$

Alice chooses large groups G and H, an epimorphism $f\colon G \to H$, and generates a random $[s,r]$-mesh $\alpha = (a_{i,j})$ for G. Alice computes $\beta = f(\alpha) = (b_{i,j}) = \big(f(a_{i,j})\big)$. She makes the pair (α, β) public, but keeps f secret. If Bob wants to send a message $x \in H$ to Alice, he:

i) Chooses a random integer $R \in \mathbb{Z}_{r^s}$.

ii) Computes $y_1 = \breve{\alpha}(R)$, $y_2 = \breve{\beta}(R)$, $y_3 = xy_2$, and

iii) sends $y = (y_1, y_3)$ to Alice.

Upon receiving (y_1, y_3), Alice computes $y_2 = \breve{\beta}(R) = f\big(\breve{\alpha}(R)\big) = f(y_1)$, and from $xy_2 = y_3$ obtains the message $x = y_3 y_2^{-1}$.

6.2 Security of MST$_2$

There are two types of attacks we can imagine against MST$_2$. The first would be to determine a random number R from an intercepted $y = (y_1, y_3)$, so that $y_1 = \breve{\alpha}(R)$. Note that in general R is not unique, but finding any R' such that $y_1 = \breve{\alpha}(R) = \breve{\alpha}(R')$ constitutes breaking the system. Finding an R such that $y_1 = \breve{\alpha}(R)$, amounts to being able to factorize y_1 with respect to α, and determine pointers $(j_1, j_2, \ldots, j_s)$ for which

$$y_1 = a_{1,j_1} a_{2,j_2} \cdots a_{s,j_s} \,.$$

As discussed earlier, this attack is considered infeasible if parameters are chosen appropriately.

A second possible attack is to infer any homomorphism $f' \in \mathrm{HOM}(G,H)$ such that $\beta = f'(\alpha)$. Finding such an f' would constitute breaking Alice's key.

The security of MST$_2$ is based on the fact that if G is an arbitrary finite group and if $\{g_i\}$ is a collection of elements of G, then in general, computing the intersection of centralizers in G of the g_i is hard.

For example, we note that the ElGamal system [2] is a special case of MST$_2$, where the ambient space is a large cyclic group. Whether we can find a practical and efficient implementation of MST$_2$ for large non-abelian groups is still an open question.

Consider the instance of the system where $G = H$ is a large, non-abelian group, and where $f\colon G \to G$ is conjugation by an element $g \in G$. Thus, Alice has chosen an $[s,r]$-mesh $(a_{i,j})$ for G, and a secret element $g \in G$, and computes the second mesh $\beta = (b_{i,j})$ by $b_{i,j} = a_{i,j}^g$. She publishes the two meshes $\alpha = (a_{i,j})$ and $\beta = (b_{i,j})$, but keeps g secret. Here, finding any element $g' \in G$ such that $b_{i,j} = a_{i,j}^{g'}$ would constitute breaking Alice's key.

Assume that finding respective elements $u_{i,j} \in G$ such that $a_{i,j}^{u_{i,j}} = b_{i,j}$ is easy. Now, from elementary group theory we know that if $x, y, z \in G$ such that $z = x^y$, then $\{w \in G\colon x^w = z\} = C_G(x)y$, where $C_G(x)$ is the centralizer of x in G. So, the set of all elements which conjugate x onto z is a right coset of the centralizer of x in G. Thus to make the second attack work, the cryptanalyst needs to compute an element in

$$\Theta = \bigcap_{i,j} C_G(a_{i,j})u_{i,j}\,. \tag{6.5}$$

This problem is polynomially equivalent to finding the intersection

$$\Theta = \bigcap_{i,j} C_G(a_{i,j})\,. \tag{6.6}$$

which is generally known to be hard [5], [6]. On the other hand, for certain choices of the group G, the problem can be solved in polynomial time. For example, in the special case where the group G is the symmetric group S_n in its natural representation on n points, the resulting system MST_2 is not secure. Determining environments and parameter choices for which MST_2 is feasible is clearly an interesting problem.

7. On a question of Vasco and Steinwaldt

In [12] M. I. González Vasco and R. Steinwaldt show that if a group G has order $|G| = \prod_{j=1}^{t} p_j^{a_j}$, p_j prime, then a lower bound for the length of a logarithmic signature for G is

$$\ell(G) = \sum_{j=1}^{t} a_j p_j\,.$$

They show furthermore that the bound is attainable for solvable group and the symmetric groups $\mathcal{S}_n$. Here we note that as a direct consequence of the Jordan–Hölder theorem, the low bound would be achievable by any finite group, if it were achievable for all finite *simple* groups. We conjecture that the bound *is* achievable by all finite simple groups. We offer proofs for a couple of classes of finite simple groups. Suppose that G is a finite group, with subgroups H and K such that $H \cap K = 1$ and $G = H \cdot K$. Suppose, moreover, that H and K attain their respective bounds $\ell(H)$ and $\ell(K)$, then, clearly G attains its bound $\ell(G)$.

PROPOSITION 7.1. *Let G be a finite group which is isomorphic to the alternating group $\mathcal{A}_n$. Then G attains its bound $\ell(G)$.*

Proof. We proceed by induction on n. The statement is trivially true for $n = 1, 2$ and 3. Consider $G = \mathcal{A}_n$ in its natural representation on n points. Then $G = H \cdot G_1$, where $G_1 \cong \mathcal{A}_{n-1}$ is the stabilizer of point 1. By the induction hypothesis G_1 attains its bound. Now, if n is odd, then $\pi = (1, 2, \dots, n)$ is an even permutation and $H = \langle \pi \rangle$. If n is even, $n = 2m$, let $\sigma = (1, 2, \dots, m)(m+1, m+2, \dots, n)$ and $\tau = (1, m+1)(2, m+2) \cdots (m, n)$. Then, $H = \langle \sigma, \tau \rangle$. In either case H is solvable so it attains its lower bound $\ell(H)$. ☐

PROPOSITION 7.2. *Let G be a finite group which is isomorphic to the simple group $PSL_2(q)$. Then G attains its bound $\ell(G)$.*

Proof. Let $G \cong \mathrm{PSL}_2(q)$ be represented on the $q+1$ points of the projective line. Then, $G = H \cdot G_1$, where G_1 is the stabilizer of a point among the $q+1$. G_1 is an affine group of order $q(q-1)/2$ or $q(q-1)$ according to whether q is odd or even. In either case G_1 is solvable, so it attains its lower bound $\ell(G_1)$. If q is even, then H is cyclic of order $q+1$. If q is odd then H is dihedral of order $q+1$. In either case H is solvable so it attains its lower bound $\ell(H)$. ☐

We are rather confident that similar proofs will dispose of most and probably all finite simple group cases.

REFERENCES

[1] ČANDA, V.—TRAN VAN TRUNG—MAGLIVERAS, S.—HORVÁTH, T.: *Symmetric Block Ciphers Based on Group Bases*, Selected Areas in Cryptography, Lecture Notes Comput. Sci., Vol. 2012, Springer-Verlag, Berlin, 2001, pp. 89–105.

[2] ElGAMAL, T.: *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inform. Theory **31** (1985), 469–472.

[3] FURST, M.—HOPCROFT, J. E.—LUKS, E.: *Polynomial-time algorithms for permutation groups*, in: Proceedings of the 21'st IEEE Symposium on Foundations of Computation of Computer Science, 1980, pp. 36–41.

[4] FAN, H.: *Group Factorizations and Cryptography*, M. Sc. Thesis, Department of Computer Science and Engineering, University of Nebraska—Lincoln, 1999, pp. 1–58.

[5] LUKS, E.: *Isomorphism of graphs of bounded valence can be tested in polynomial time*, J. Comput. System Sci. **25** (1982), 42–65.

[6] LUKS, E.: *Computing the composition factors of a permutation group in polynomial time*, Combinatorica **7** (1987), 87–99.

[7] MAGLIVERAS, S. S.: *A cryptosystem from logarithmic signatures of finite groups*, in: Proceedings of the 29'th Midwest Symposium on Circuits and Systems, Elsevier Publishing Company, Amsterdam, 1986, pp. 972–975.

[8] MAGLIVERAS, S. S.—MEMON, N. D.: *The algebraic properties of cryptosystem PGM*, J. Cryptology **5** (1992), 167–183.

[9] MAGLIVERAS, S. S.—TRAN VAN TRUNG—STINSON, D. R.: *New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups*, to appear in the J. Cryptology, 2002.

[10] QU, M.—VANSTONE, S. A.: *Factorizations of elementary abelian p-groups and their cryptographic significance*, J. Cryptology **7** (1994), 201–212.

[11] SIMS, C. C.: *Some group-theoretic algorithms*, Topics in Algebra (M. F. Newman, ed.), Lecture Notes in Math., Vol. 697, Springer-Verlag, Berlin, 1978, pp. 108–124.

[12] GONZÁLEZ VASCO, M. I.—STEINWALDT, R.: *Obstacles in two public key cryptosystems based on group factorizations*, Tatra Mt. Math. Publ. **25** (2002), 23–37.

Received March 17, 2002

Department of Mathematical Sciences
Florida Atlantic University
Boca Raton, Florida 33431
U. S. A.

E-mail: spyros@fau.edu