Discrete logarithms for finite groups

Lee C. Klingler, Spyros S. Magliveras, Fred Richman

Department of Mathematical Sciences, Florida Atlantic University

777 Glades Road, Boca Raton, FL 33431, U.S.A.

{klingler,spyros,richman}@fau.edu

Michal Sramka

Department of Computer Science, University of Calgary

2500 University Drive NW, Calgary AB T2N 1N4, Canada

msramka@ucalgary.ca

August 31, 2008

Abstract

We present group-theoretic and cryptographic properties of a generalization of the traditional discrete logarithm problem (DLP) from cyclic to arbitrary finite groups. Questions related to properties which contribute to cryptographic security are investigated, such as distributional, coverage and complexity properties. We show that the distribution of elements in a certain multiset tends to be uniform. In particular we consider the family of finite non-abelian groups $\mathrm{PSL}_2(\mathbb{F}_p)$, p a prime, as possible candidates in the design of new cryptographic primitives, based on our new discrete logarithm.

AMS Subject Classification 94A60, 20G40.

Key words. Discrete logarithm, non-abelian groups, presentations, linear groups, uniformity, short relations.

1 Introduction

Let G be a finite cyclic group of order n, written multiplicatively, and let α be a generator of G. If $\beta \in G$, the *discrete logarithm* of β with respect to α is the element $x \in \mathbb{Z}_n$ such that $\beta = \alpha^x$. The *discrete logarithm problem* (DLP) for G is to determine x when G, α and β are given.

For the DLP to be useful in the construction of cryptographic primitives it is necessary that the problem be *intractable*, in other words that there should be no polynomial-time algorithm for solving it. The computational intractability of the discrete logarithm problem is not a group theoretic property – it depends on the particular representation of the cyclic group G. For example, when G is the multiplicative group of a finite field, $\mathbb{F}_q$, the problem is generally considered intractable. On the other hand, if G is the additive group of integers modulo n, the problem clearly has a polynomial-time solution based on the extended Euclidean algorithm for computing multiplicative inverses in the ring of integers modulo n. Another cryptographically desirable property of the DLP is that if x is a uniform random variable with values in $\mathbb{Z}_n$, then α^x is uniformly distributed in the cyclic group G.

Several factors motivate our extending the DLP from cyclic to non-cyclic and non-abelian groups: (i) the desire for a formal extension of the DLP from cyclic to arbitrary finite groups; (ii) P. Shor's algorithm [13] for quantum computers, which efficiently solves the traditional DLP; (iii) a search for problems not currently solvable in sub-exponential time.

The use of particular representations of finite abelian groups is very common in present day cryptography. Examples are subgroups of the multiplicative group of a finite field, or subgroups of an elliptic/hyperelliptic curve over a finite field. There are three standard methods of specifying a general, not necessarily abelian, finite carrier group G in the context of cryptography: (i) by permutations, (ii) by matrices over a ring, (iii) by a finite presentation. In cases (i) & (ii) a group G is usually specified by a set of generators, and a problem of interest is the following *factorization problem:* Given an element $y \in G$, write y as a word in the generators. The problem is not very difficult in the case of permutation groups, where one first uses the Schreier-Sims algorithm to obtain a *base* and a *strong generating set* [4] and then replaces the strong generators by words in the original generators given. In case (ii) the problem is generally considered intractable [4]. In case (iii) group elements are already words in the generators, and the relevant question is generally *undecidable.* Of course the word problem is decidable for a finite group, but depending on the presentation, could still be intractable. In case (iii) if the group has a faithful permutation representation of small degree (i.e. a subgroup H of relatively small index containing no proper normal subgroups of G, then an application of the Todd-Coxeter *coset enumeration* procedure with respect to H produces a faithful permutation representation of G, and the methods of (i) can be used to solve the word problem.

In what follows we assume that G is a finite group. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ be an ordered t-tuple of elements of G such that $G = \langle \alpha_1, \ldots, \alpha_t \rangle$, and denote

the order of α_i by n_i. Define the multiset

$$\mathcal{S}_k(\boldsymbol{\alpha}) \;=\; \left\{ \prod_{i=1}^{k} (\alpha_1^{x_{i,1}} \cdots \alpha_t^{x_{i,t}}) \;\middle|\; x_{i,j} \in \mathbb{Z}_{n_j} \right\},$$

and for $g \in G$, denote by $\mu_{\alpha,k}(g)$ the multiplicity of g in $\mathcal{S}_k(\boldsymbol{\alpha})$. Further, define the set

$$\hat{\mathcal{S}}_k(\boldsymbol{\alpha}) \;=\; \{g \in G \mid g \in \mathcal{S}_k(\boldsymbol{\alpha})\}.$$

Since $G = \langle \alpha_1, \ldots, \alpha_t \rangle$, there is a smallest positive integer k_0 such that for each $k \geq k_0$, $G \subseteq \mathcal{S}_k(\boldsymbol{\alpha})$. The integer k_0 is called the *depth* of G relative to $\boldsymbol{\alpha}$. If $k \geq k_0$ we also say that $\mathcal{S}_k(\boldsymbol{\alpha})$ and $\hat{\mathcal{S}}_k(\boldsymbol{\alpha})$ *cover* G. Clearly $|G| \leq (\prod_{i=1}^{t} n_i)^{k_0}$.

Definition. Given an element $y \in G$, the *generalized discrete logarithm problem (GDLP)* for y with respect to $\boldsymbol{\alpha}$ is: Find a positive integer k and a kt-tuple of non-negative integers $\mathbf{x} = (x_{1,1}, \ldots, x_{1,t}, \ldots, x_{k,1}, \ldots, x_{k,t})$ such that

$$y = \prod_{i=1}^{k} \alpha_1^{x_{i,1}} \cdots \alpha_t^{x_{i,t}}. \tag{1}$$

We formally write the product on the right-hand side of (1) as $\boldsymbol{\alpha}^{\mathbf{x}}$. The kt-tuples $\mathbf{x}$ for which (1) holds will be called the *generalized discrete logarithms* of y with respect to α.

If k is the smallest positive integer for which $y \in \mathcal{S}_k(\boldsymbol{\alpha})$, the lexicographically smallest kt-tuple $(x_{1,1}, \ldots, x_{1,t}, \ldots, x_{k,1}, \ldots, x_{k,t})$ among all the kt-tuples of non-negative integers satisfying equation (1) is called the *discrete logarithm* of y *with respect to* $\boldsymbol{\alpha}$. Moreover, the problem of determining the discrete logarithm of $y \in G$ with respect to $\boldsymbol{\alpha}$ is referred to as the *discrete logarithm problem (DLP) with respect to* $\boldsymbol{\alpha}$.

The DLP relative to a given $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ is obviously well-defined. If $\mathbf{x}$ is a generalized discrete logarithm of y, and $1 = \boldsymbol{\alpha}^{\mathbf{x}'}$, then the catenations $\mathbf{x}, \mathbf{x}'$ and $\mathbf{x}', \mathbf{x}$ are also generalized discrete logarithms of y. Hence, by allowing k to increase, one can obtain infinitely many generalized discrete logarithms of $y \in G$. Understanding the GDLP with respect to $\boldsymbol{\alpha}$ corresponds to knowing the group theoretic relations of length at most $k_0 t$ among the generators $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ in the particular representation given. The task of understanding the GDLP for a given group G and $\boldsymbol{\alpha}$ leads to an exploration of numerous induced *presentations* of the group.

We explore cryptographic and group-theoretic characteristics that would be required in any secure application of the GDLP. In addition to determining the *depth* of a particular $t-$tuple of generators for a given group, we are also

interested in *distributional* properties. In particular, we are interested in the parameter

$$\lambda_k = \frac{\min_{g \in G} \mu_{\alpha,k}(g)}{\max_{g \in G} \mu_{\alpha,k}(g)}$$

A desirable property is that $\lim_{k \to \infty} \lambda_k = 1$, that ism group elements are distributed approximately uniformly in $\mathcal{S}_k(\boldsymbol{\alpha})$ when k is large. A good situation of course occurs when the convergence is fast.

In the sections that follow, we address (i) distributional properties for finite groups in general as $k \to \infty$, and (ii) distributional and coverage properties for the finite, non-abelian simple groups $\mathrm{PSL}_2(\mathbb{F}_p)$ where p is a prime. We suggest that, with some care, this family of groups can be used in cryptographic primitives based on the DLP we have defined for arbitrary finite groups.

The security of many present day cryptographic primitives relies on the *intractability* of the traditional discrete logarithm problem. A new proposal, like the present one, should demonstrate the intractability of attacking the new scheme, with complexity of a successful attack at least as high as the complexity of a successful attack on the traditional DLP. Finally, one should be able to argue that the proposed scheme offers a computationally efficient implementation, in terms of space requirements, and the time complexity for computing $y = \boldsymbol{\alpha}^{\mathbf{x}}$, for given $\boldsymbol{\alpha}$ and $\mathbf{x}$. We characterize these as *complexity* properties of the proposed scheme. We leave the question of how G and $\boldsymbol{\alpha}$ can be chosen to insure desirable complexity properties to a subsequent paper.

2 Distribution

Regarding the distribution of the elements of G, in the multiset $\mathcal{S}_k(\boldsymbol{\alpha})$, we have two results – two ways to achieve uniform distribution. In Section 2.1 we prove that the distribution approaches a uniform distribution as $k \to \infty$. On the other hand, in Section 2.2 we show that for the projective special linear group $\mathrm{PSL}_2(\mathbb{F}_p)$, where p is a prime, it is possible to achieve a uniform distribution with fixed k and $p \to \infty$ (Theorem 1).

2.1 For groups in general

Let G be a finite group and suppose that $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ generate G. In this section we show that the distribution of elements of the group G in the multiset $\mathcal{S}_k(\boldsymbol{\alpha})$ approaches a uniform distribution as $k \to \infty$.

Let $\mathbb{R}G$ denote the group algebra of the group G over the field $\mathbb{R}$ of real numbers. For each group element $g \in G$, let a_g denote the multiplicity of g

in the multiset $\mathcal{S}_1(\boldsymbol{\alpha})$, and let $\mathbf{a} = \sum_{g\in G} a_g g$ in the group algebra $\mathbb{R}G$. Note that, by the definition of multiplication in $\mathbb{R}G$, for each integer $k \geq 1$ and each element $g \in G$, the coefficient of g in the product $\mathbf{a}^k$ is precisely the multiplicity of g in the multiset $\mathcal{S}_k(\boldsymbol{\alpha})$. If $n_1, \ldots, n_t$ are the orders of the generators $\alpha_1, \ldots \alpha_t$, respectively, and we set $n = \prod_{i=1}^{t} n_i$, then $|\mathcal{S}_k(\boldsymbol{\alpha})| = n^k$ for each positive integer k. Thus, $n^{-k}\mathbf{a}^k$ has nonnegative coefficients which sum to 1. To prove Theorem 1, we show that $n^{-k}\mathbf{a}^k$ converges to the idempotent $|G|^{-1}\sum_{g\in G} g$ as $k \to \infty$.

For an element $\mathbf{b} = \sum_{g\in G} b_g g \in \mathbb{R}G$, we denote by M_b the maximum of the coefficients b_g, and by m_b the minimum of the coefficients b_g. Our main tool is the following elementary fact.

Lemma 1. *If $\mathbf{b} = \sum_{g\in G} b_g g$ and $\mathbf{c} = \sum_{g\in G} c_g g$ are elements of the group algebra $\mathbb{R}G$ such that $\sum_{g\in G} b_g = \sum_{g\in G} c_g = 1$, then*

$$M_{bc} - m_{bc} \leq (1 - m_b)(M_c - m_c)$$

Proof. For some permutation σ of the elements of the group G, we have

$$\begin{aligned} M_{bc} &= \sum_{g\in G} b_g c_{\sigma(g)} \\ &= \sum_{g\in G} (b_g - m_b) c_{\sigma(g)} + \sum_{g\in G} m_b c_{\sigma(g)} \\ &\leq \sum_{g\in G} (b_g - m_b) M_c + \sum_{g\in G} m_b c_{\sigma(g)} \\ &= (1 - m_b) M_c + m_b \end{aligned}$$

using the fact that $\sum_{g\in G} b_g = \sum_{g\in G} c_g = 1$. Similarly, for some permutation τ of the elements of the group G, we have

$$\begin{aligned} m_{bc} &= \sum_{g\in G} b_g c_{\tau(g)} \\ &= \sum_{g\in G} (b_g - m_b) c_{\tau(g)} + \sum_{g\in G} m_b c_{\tau(g)} \\ &\geq \sum_{g\in G} (b_g - m_b) m_c + \sum_{g\in G} m_b c_{\tau(g)} \\ &= (1 - m_b) m_c + m_b \end{aligned}$$

Subtracting the two inequalities proves the lemma. □

We are now ready to prove the main theorem of this section.

Theorem 1. *If $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ generates the finite group G, then the elements of G in the multiset $\mathcal{S}_k(\boldsymbol{\alpha})$ approach a uniform distribution as $k \to \infty$.*

Proof. As above, let $\mathbf{a} = \sum_{g \in G} a_g g$, and note that the coefficient of each group element in the sum $\mathbf{a}^k$ counts the multiplicity of that group element in $\mathcal{S}_k(\boldsymbol{\alpha})$. Thus, if n is the product of the orders of the generators $\alpha_1, \ldots, \alpha_t$, then for each positive integer k, the group algebra element $n^{-k}\mathbf{a}^k$ has nonnegative coefficients which sum to 1. Moreover, since $\alpha_1, \ldots, \alpha_t$ generate the group G, there is some positive integer r such that every element of the group G occurs at least once in the multiset $\mathcal{S}_r(\boldsymbol{\alpha})$; that is, the group algebra element $n^{-r}\mathbf{a}^r$ has strictly positive coefficients which sum to 1.

If we set $\mathbf{b} = n^{-r}\mathbf{a}^r$ and $\mathbf{c} = \mathbf{b}^k$ for arbitrary positive integer k, then by Lemma 1 we get $M_{b^{k+1}} - m_{b^{k+1}} \leq (1 - m_b)(M_{b^k} - m_{b^k})$, so that by induction, $M_{b^{k+1}} - m_{b^{k+1}} \leq (1 - m_b)^k (M_b - m_b)$. Since all of the coefficients in $\mathbf{b}$ are positive and sum to 1, we note that $0 \leq 1 - m_b < 1$, which forces $M_{b^{k+1}} - m_{b^{k+1}} \to 0$ as $k \to \infty$. Thus, $\mathbf{a}^{rk} = \mathbf{b}^k \to |G|^{-1} \sum_{g \in G} g$ as $k \to \infty$, completing the proof. □

2.2 For $\mathrm{PSL}_2(\mathbb{F}_p)$

Having shown in the last section that the elements of a finite group G approach a uniform distribution in the multiset $\mathcal{S}_k(\boldsymbol{\alpha})$ as $k \to \infty$, provided only that $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ generate G, in this section we provide sharper results for a particular class of finite simple groups, the projective special linear group $\mathrm{PSL}_2(\mathbb{F}_p)$, in case p is prime. For fixed prime $p \geq 3$ and integer $k \geq 3$, and for arbitrary non-commuting elements α, β of order p in $\mathrm{PSL}_2(\mathbb{F}_p)$, we give a bound on the ratios of distributions of group elements in $\mathcal{S}_k(\alpha, \beta)$, in terms of k and p (Theorem 2). As a consequence, it follows that, for fixed $k \geq 3$, the distributions approach a uniform distribution as $p \to \infty$ (Corollary 1).

We begin by recalling some notation and facts about the projective special linear group.

Let $p > 2$ be a rational prime, and let $\mathbb{F}_p$ denote the prime field for p. Recall that the special linear group $\mathrm{SL}_2(\mathbb{F}_p)$ can be viewed as the multiplicative group of all 2×2 matrices of determinant 1, over the field $\mathbb{F}_p$. The center of $\mathrm{SL}_2(\mathbb{F}_p)$ is the subgroup $Z(\mathrm{SL}_2(\mathbb{F}_p)) = \{\pm I_2\}$, where I_2 denotes the 2×2 identity matrix, and the projective special linear group is the quotient $\mathrm{PSL}_2(\mathbb{F}_p) = \mathrm{SL}_2(\mathbb{F}_p)/Z(\mathrm{SL}_2(\mathbb{F}_p)) = \mathrm{SL}_2(\mathbb{F}_p)/\{\pm I_2\}$. One easily computes that $\mathrm{SL}_2(\mathbb{F}_p)$ has order $p(p^2-1)$, so that $\mathrm{PSL}_2(\mathbb{F}_p)$ has order $p(p^2-1)/2$. Thus, each Sylow p-subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$ has order p.

We shall find it convenient to work in the group $\mathrm{SL}_2(\mathbb{F}_p)$, so that we can compute using 2×2 matrices over $\mathbb{F}_p$, and then reduce modulo $\{\pm I_2\}$. In

$\mathrm{SL}_2(\mathbb{F}_p)$, let

$$a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad b = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

For the remainder of this section, we fix $\alpha = \bar{a}$ and $\beta = \bar{b}$, the images of the matrices a and b, respectively, in $\mathrm{PSL}_2(\mathbb{F}_p)$. We fix also the subgroups $H = \langle \pm a \rangle$ and $K = \langle \pm b \rangle$ in $\mathrm{SL}_2(\mathbb{F}_p)$, and we denote by $\bar{H} = \langle \alpha \rangle$ and $\bar{K} = \langle \beta \rangle$ their images in $\mathrm{PSL}_2(\mathbb{F}_p)$, so that $\bar{H}$ and $\bar{K}$ are distinct Sylow p-subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$.

We note the following well-known fact, whose proof (which includes liberal use of the Sylow theorems) we include for completeness.

Lemma 2. *Let X be the collection of all Sylow p-subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$. Then $|X| = p + 1$, and the action of $\mathrm{PSL}_2(\mathbb{F}_p)$ on X by conjugation is doubly transitive.*

Proof. As noted above, $\bar{H} \neq \bar{K}$ are Sylow p-subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$, so that $|X| > 1$. Since $|X| \equiv 1 \mod p$, to prove that $|X| = p + 1$ it suffices to show that $|X| \leq p+1$. Note that the diagonal matrices in $\mathrm{SL}_2(\mathbb{F}_p)$ form a subgroup of order $p - 1$, and the diagonal matrices are in the normalizer N of H in $\mathrm{SL}_2(\mathbb{F}_p)$. Reducing modulo $\{\pm I_2\}$, it follows that the normalizer $\bar{N}$ of $\bar{H}$ in $\mathrm{PSL}_2(\mathbb{F}_p)$ contains a subgroup of order $(p-1)/2$. That is, $|\bar{N}| \geq p(p-1)/2$, so that $|X| = |\mathrm{PSL}_2(\mathbb{F}_p)|/|\bar{N}| \leq p + 1$, as desired.

Set $G = \mathrm{PSL}_2(\mathbb{F}_p)$, and fix $P \in X$. Since G acts transitively on X, the action is doubly transitive if and only if the stabilizer G_P acts transitively on $X \setminus \{P\}$. Because $|P| = p$, the orbits of P acting on $X \setminus \{P\}$ can only have length 1 or p. For $Q \in X \setminus \{P\}$, the stabilizer G_Q is the normalizer of Q in G, so that G_Q contains unique Sylow p-subgroup Q, and hence $P \not\subseteq G_Q$. That is, the orbit of Q in the action of P on $X \setminus \{P\}$ must have length p, from which it follows that G_P acts transitively on $X \setminus \{P\}$. □

We observe that, since $\mathcal{S}_k(\alpha, \beta)$ depends only on the subgroups $\langle \alpha \rangle$ and $\langle \beta \rangle$, it follows from Lemma 2 that the limiting distribution of elements of $\mathrm{PSL}_2(\mathbb{F}_p)$ in $\mathcal{S}_k(\alpha, \beta)$ is independent of our choice of non-commuting elements α and β of order p.

Our strategy is to partition $\mathrm{PSL}_2(\mathbb{F}_p)$ into five subsets according to the action of right-multiplication by the subgroups $\bar{H}$ and $\bar{K}$, and, for each of these subsets, compute the multiplicity of group elements of $\mathrm{PSL}_2(\mathbb{F}_p)$ after

right-multiplication. We begin by defining the following subsets of $\mathrm{SL}_2(\mathbb{F}_p)$.

$$\begin{aligned} A &= \left\{ \left[\begin{array}{cc} i & j \\ 0 & i^{-1} \end{array} \right] \;\middle|\; i,j \in \mathbb{F}_p;\ i \neq 0, \pm 1 \right\} \\ B &= \left\{ \left[\begin{array}{cc} i & -k^{-1} \\ k & 0 \end{array} \right] \;\middle|\; i,k \in \mathbb{F}_p;\ k \neq 0 \right\} \\ C &= \left\{ \pm \left[\begin{array}{cc} 1+jk & j \\ k & 1 \end{array} \right] \;\middle|\; j,k \in \mathbb{F}_p;\ k \neq 0 \right\} \\ D &= \left\{ \left[\begin{array}{cc} i & k^{-1}(il-1) \\ k & l \end{array} \right] \;\middle|\; i,k,l \in \mathbb{F}_p;\ k \neq 0;\ l \neq 0, \pm 1 \right\} \end{aligned} \tag{2}$$

Clearly $\mathrm{SL}_2(\mathbb{F}_p)$ equals the disjoint union $H \cup A \cup B \cup C \cup D$. Moreover, if we let $\bar{A}$, $\bar{B}$, $\bar{C}$, and $\bar{D}$ denote the images of A, B, C, and D, respectively, in $\mathrm{PSL}_2(\mathbb{F}_p)$, then since H, A, B, C, and D are closed under multiplication by $\{\pm I_2\}$, it follows that $\mathrm{PSL}_2(\mathbb{F}_p)$ equals the disjoint union $\bar{H} \cup \bar{A} \cup \bar{B} \cup \bar{C} \cup \bar{D}$.

We collect in the following two lemmas the main technical computations needed for the proof of the main theorem.

Lemma 3. *As multisets:*

(i) $\bar{H}\bar{H} = \bar{H}$*, where each element has multiplicity* p*.*

(ii) $\bar{A}\bar{H} = \bar{A}$*, where each element has multiplicity* p*.*

(iii) $\bar{B}\bar{H} = \bar{B} \cup \bar{C} \cup \bar{D}$*, where each element has multiplicity* 1*.*

(iv) $\bar{C}\bar{H} = \bar{B} \cup \bar{C} \cup \bar{D}$*, where each element has multiplicity* 2*.*

(v) $\bar{D}\bar{H} = \bar{B} \cup \bar{C} \cup \bar{D}$*, where each element has multiplicity* $p-3$*.*

Proof. We give the details of the proof of (v); the other cases are similar but mostly easier. We first compute the product DH and count the multiplicity of its elements as a multiset. Multiplying the expression for D in (2) by H, we obtain a product of the form

$$\left[\begin{array}{cc} i & k^{-1}(il-1) \\ k & l \end{array} \right] \left(\pm \left[\begin{array}{cc} 1 & m \\ 0 & 1 \end{array} \right] \right) = \pm \left[\begin{array}{cc} i & im + k^{-1}(il-1) \\ k & km + l \end{array} \right] \tag{3}$$

where $i,k,l,m \in \mathbb{F}_p$ are such that $k \neq 0$ and $l \neq 0, \pm 1$. The fact that $k \neq 0$ forces the matrix in (3) to be in $B \cup C \cup D$. Moreover, an arbitrary matrix in $B \cup C \cup D$ has the form

$$\left[\begin{array}{cc} r & t^{-1}(ru-1) \\ t & u \end{array} \right] \tag{4}$$

where $r, t, u \in \mathbb{F}_p$ are such that $t \neq 0$.

For the plus sign in (3), we can obtain the matrix in (4) in $p-3$ ways, by choosing $i = r$, choosing $k = t$, and, for each of the $p-3$ possible values of l, choosing $m = k^{-1}(u-l)$. Similarly, for the minus sign in (3), we can also obtain the matrix in (4) in $p-3$ ways, by choosing $i = -r$, choosing $k = -t$, and, for each of the $p-3$ possible values of l, choosing $m = k^{-1}(-u-l)$. Thus, the multiset DH consists of the elements of the set $B \cup C \cup D$, each with multiplicity $2(p-3)$.

Finally, to obtain (v), note that each element of the set $\bar{B} \cup \bar{C} \cup \bar{D}$ is counted twice in the set $B \cup C \cup D$ and hence $4(p-3)$ times in the multiset DH. But each element of the set $\bar{D}$ is counted twice in the set D, and each element of the set $\bar{H}$ is counted twice in the set H, so that each element of the multiset $\bar{D}\bar{H}$ is counted four times in the multiset DH. Thus, each element of the set $\bar{B} \cup \bar{C} \cup \bar{D}$ is counted $p-3$ times in the multiset $\bar{D}\bar{H}$. □

Lemma 4. *As multisets:*

(i) $\bar{H}\bar{K} = \bar{H} \cup \bar{C}$*, where each element has multiplicity* 1*.*

(ii) $\bar{A}\bar{K} = \bar{A} \cup \bar{D}$*, where each element has multiplicity* 1*.*

(iii) $\bar{B}\bar{K} = \bar{B}$*, where each element has multiplicity* p*.*

(iv) $\bar{C}\bar{K} = \bar{H} \cup \bar{C}$*, where each element has multiplicity* $p-1$*.*

(v) $\bar{D}\bar{K} = \bar{A} \cup \bar{D}$*, where each element has multiplicity* $p-1$*.*

Proof. In this case, we give the details of the proof of (iv) and leave the (similar) proofs of the remaining cases to the interested reader. As in the proof of Lemma 3, we first compute the product CK and count the multiplicity of its elements as a multiset. Multiplying the expression for C in (2) by K, we obtain a product of the form

$$\left(\pm \begin{bmatrix} 1+jk & j \\ k & 1 \end{bmatrix} \right) \left(\pm \begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix} \right) = \pm \begin{bmatrix} 1+j(k+m) & j \\ k+m & 1 \end{bmatrix} \tag{5}$$

where $j, k, m \in \mathbb{F}_p$ are such that $k \neq 0$. The fact that the $2,2$-entry is ± 1 forces the matrix in (5) to be in $H \cup C$. Moreover, an arbitrary matrix in $H \cup C$ has the form

$$\pm \begin{bmatrix} 1+st & s \\ t & 1 \end{bmatrix} \tag{6}$$

where $s, t \in \mathbb{F}_p$.

To obtain the matrix in (6) with the plus sign, we can choose the same sign for both factors on the left-hand side of (5); to obtain the minus sign,

we can choose one plus sign and one minus sign. Either way, we obtain the matrix in (6) by choosing $j = s$, and, for each of the $p-1$ possible values of k, choosing $m = t - k$. Thus, the multiset CK consists of the elements of the set $H \cup C$, each with multiplicity $2(p-1)$.

Finally, to obtain (iv), we argue as in the proof of Lemma 3. Each element of the set $\bar{H} \cup \bar{C}$ is counted twice in the set $H \cup C$ and hence $4(p-1)$ times in the multiset CK, while each element of the set $\bar{C}$ is counted twice in the set C, and each element of the set $\bar{K}$ is counted twice in the set K, so that each element of the multiset $\bar{C}\bar{K}$ is counted four times in the multiset CK. Therefore, each element of the set $\bar{H} \cup \bar{C}$ is counted $p-1$ times in the multiset $\bar{C}\bar{K}$. □

Lemmas 3 and 4 allow us to set up recurrence equations to compute the multiplicities of elements of $\mathrm{PSL}_2(\mathbb{F}_p)$ in the multiset $\mathcal{S}_k(\alpha, \beta)$. For $k \geq 1$, let h_k, a_k, b_k, c_k, and d_k denote the multiplicity of the elements of $\bar{H}$, $\bar{A}$, $\bar{B}$, $\bar{C}$, and $\bar{D}$, respectively, in the multiset $\mathcal{S}_k(\alpha, \beta)$. Since $\mathcal{S}_{k+1}(\alpha, \beta) = \mathcal{S}_k(\alpha, \beta)\bar{H}\bar{K}$, let h'_k, a'_k, b'_k, c'_k, and d'_k denote the multiplicity of the elements of $\bar{H}$, $\bar{A}$, $\bar{B}$, $\bar{C}$, and $\bar{D}$, respectively, in the multiset $\mathcal{S}_k(\alpha, \beta)\bar{H}$. (Of course, h_k, a_k, b_k, c_k, and d_k are all functions of p as well as of k, as are h'_k, a'_k, b'_k, c'_k, and d'_k.)

¿From Lemma 4 we obtain $\mathcal{S}_1(\alpha, \beta) = \bar{H}\bar{K} = \bar{H} \cup \bar{C}$, with each element of multiplicity 1, so that $h_1 = c_1 = 1$, and $a_1 = b_1 = d_1 = 0$. For $k \geq 1$, Lemma 3 then yields the equations

$$\begin{aligned} h'_k &= p h_k \\ a'_k &= p a_k \\ b'_k = c'_k = d'_k &= b_k + 2c_k + (p-3)d_k \end{aligned} \tag{7}$$

and Lemma 4 yields the equations

$$\begin{aligned} h_{k+1} = c_{k+1} &= h'_k + (p-1)c'_k \\ a_{k+1} = d_{k+1} &= a'_k + (p-1)d'_k \\ b_{k+1} &= p b'_k \end{aligned} \tag{8}$$

Finally, substituting equations (7) into equations (8) yields the equations

$$\begin{aligned} h_{k+1} = c_{k+1} &= p h_k + (p-1)(b_k + 2c_k + (p-3)d_k) \\ &= (3p-2)h_k + (p^2 - 4p + 3)a_k + (p-1)b_k \\ a_{k+1} = d_{k+1} &= p a_k + (p-1)(b_k + 2c_k + (p-3)d_k) \\ &= (2p-2)h_k + (p^2 - 3p + 3)a_k + (p-1)b_k \\ b_{k+1} &= p(b_k + 2c_k + (p-3)d_k) \\ &= 2p h_k + (p^2 - 3p)a_k + p b_k \end{aligned} \tag{9}$$

for all integers $k \geq 1$.

We are now ready to prove the main result of this section.

Theorem 2. *For prime $p \geq 3$ and integer $k \geq 3$, if $\alpha, \beta \in \mathrm{PSL}_2(\mathbb{F}_p)$ are non-commuting elements of order p, and if g and h are arbitrary elements of $\mathrm{PSL}_2(\mathbb{F}_p)$ of multiplicities r and s, respectively, in $\mathcal{S}_k(\alpha, \beta)$, then*

$$\left|\frac{r}{s} - 1\right| < \frac{1}{2p^{k-3}}$$

Proof. Each of r and s is one of the numbers h_k, a_k, or b_k, so it suffices to show, for each pair of these quantities, that their ratio is sufficiently close to 1. We begin by establishing a few identities and inequalities.

Since $h_1 - a_1 = 1$, using (9) and induction we obtain

$$h_k - a_k = p(h_{k-1} - a_{k-1}) = p^{k-1} \tag{10}$$

for each $k \geq 2$. Moreover, since $h_1 = c_1 = 1$ and $a_1 = b_1 = d_1 = 0$, from equations (9) we obtain the values

$$\begin{array}{l} h_2 = c_2 = 3p - 2 \\ a_2 = d_2 = 2p - 2 \\ b_2 = 2p \end{array} \tag{11}$$

Thus, $b_2 - a_2 = 2$, so that, by (9), (10), and induction, we obtain

$$\begin{array}{rcl} b_k - a_k & = & 2(h_{k-1} - a_{k-1}) + b_{k-1} - a_{k-1} \\ & = & 2p^{k-2} + 2(\frac{p^{k-2}-1}{p-1}) = 2(\frac{p^{k-1}-1}{p-1}) \end{array} \tag{12}$$

for each $k \geq 2$. From (10) and (12) we see that $h_k \geq a_k$ and $b_k \geq a_k$ for each $k \geq 1$, and hence using (9) we compute that

$$a_{k+1} \geq (2p-2)a_k + (p^2 - 3p + 3)a_k + (p-1)a_k = p^2 a_k$$

for each $k \geq 1$. Therefore, by (11) and induction, we get

$$a_k \geq p^{2k-4} a_2 = 2(p-1)p^{2k-4} \tag{13}$$

for each $k \geq 2$.

First we note that, by (10) and (13), and since $p \geq 3$,

$$0 < \frac{h_k - a_k}{a_k} \leq \frac{p^{k-1}}{2(p-1)p^{2k-4}} = \frac{1}{2(p-1)p^{k-3}} \leq \frac{1}{4p^{k-3}}$$

for each $k \geq 3$, so that

$$0 < \frac{h_k}{a_k} - 1 \leq \frac{1}{4p^{k-3}} \tag{14}$$

proving the theorem for the ratio h_k/a_k. Similarly, by (12) and (13),

$$0 < \frac{b_k - a_k}{a_k} \leq \frac{2(p^{k-1}-1)}{2(p-1)^2 p^{2k-4}} = \frac{1 - \frac{1}{p^{k-1}}}{(p-1)^2 p^{k-3}} \leq \frac{1}{4p^{k-3}}$$

for each $k \geq 3$, so that

$$0 < \frac{b_k}{a_k} - 1 \leq \frac{1}{4p^{k-3}} \tag{15}$$

proving the theorem for the ratio b_k/a_k.

Next we note that, if $0 < x - 1 \leq \epsilon$, then $0 > 1/x - 1 \geq -\epsilon(1+\epsilon)^{-1}$, and hence $|1/x - 1| \leq \epsilon$. This fact, together with equations (14) and (15), yield

$$\left|\frac{a_k}{h_k} - 1\right| \leq \frac{1}{4p^{k-3}} \quad \text{and} \quad \left|\frac{a_k}{b_k} - 1\right| \leq \frac{1}{4p^{k-3}} \tag{16}$$

establishing the theorem for the ratios a_k/h_k and a_k/b_k as well.

Finally, we note that, by equations (12), (14), and (16),

$$\begin{aligned} \left|\frac{h_k}{b_k} - 1\right| &= \left|\frac{h_k}{a_k}\frac{a_k}{b_k} - \frac{a_k}{b_k} + \frac{a_k}{b_k} - 1\right| \\ &\leq \frac{a_k}{b_k}\left|\frac{h_k}{a_k} - 1\right| + \left|\frac{a_k}{b_k} - 1\right| < \frac{1}{2p^{k-3}} \end{aligned}$$

A similar computation establishes the theorem for the ratio b_k/h_k. □

For $k = 3$, we can improve the bound in Theorem 2 and establish the following necessary and sufficient condition for convergence to a uniform distribution as $p \to \infty$.

Corollary 1. *For prime $p \geq 3$ and positive integer k, if $\alpha, \beta \in \mathrm{PSL}_2(\mathbb{F}_p)$ are non-commuting elements of order p, then the distribution of the elements of $\mathrm{PSL}_2(\mathbb{F}_p)$ in $\mathcal{S}_k(\alpha, \beta)$ approaches a uniform distribution as $p \to \infty$ if and only if $k \geq 3$.*

Proof. Since $h_1 = c_1 = 1$ and $a_1 = b_1 = d_1 = 0$, certainly a uniform distribution is not possible for $k = 1$. Moreover, from equations (11) we see, for example, that the limiting ratio of multiplicity of elements of $\bar{H} \cup \bar{C}$ to the multiplicity of elements of $\bar{A} \cup \bar{D}$ in $\mathcal{S}_2(\alpha, \beta)$ is $\frac{3}{2}$ as $p \to \infty$, so that the limiting distribution is also not uniform for $k = 2$.

On the other hand, by Theorem 2, the limiting distribution as $p \to \infty$ is uniform if $k \geq 4$, so the only case left to establish is $k = 3$. We sharpen the bound given in Theorem 2 in this case.

Substituting the values (11) into equations (9) yields the values

$$h_3 = c_3 = (3p-2)(3p-2) + (p^2-4p+3)(2p-2) + (p-1)2p = 2p^3 + p^2 - 2$$
$$a_3 = d_3 = (2p-2)(3p-2) + (p^2-3p+3)(2p-2) + (p-1)2p = 2p^3 - 2$$
$$b_3 = 2p(3p-2) + (p^2-3p)(2p-2) + p2p = 2p^3 + 2p$$

Therefore, we easily compute that

$$0 < \frac{h_3}{a_3} - 1 = \frac{h_3 - a_3}{a_3} = \frac{p^2}{2p^3 - 2} < \frac{1}{p}$$

and

$$0 < \frac{b_3}{a_3} - 1 = \frac{b_3 - a_3}{a_3} = \frac{2p-2}{2p^3-2} = \frac{1}{p^2+p+1} < \frac{1}{p}$$

from which the desired limits follow exactly as in the proof of Theorem 2. □

3 Coverage

Suppose that G is generated by $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$, and its depth with respect to $\boldsymbol{\alpha}$ is k_0. Then, for all $k \geq k_0$, $\mathcal{S}_k(\boldsymbol{\alpha})$ covers G, and by Theorem 1 the distribution of elements in $\mathcal{S}_k(\boldsymbol{\alpha})$ tends to uniform as $k \to \infty$. We note that the problem of determining k_0 is closely related to the problem of determining the diameter of a finite group for a given generating set, i.e., finding the maximum among the minimum word lengths of words over the generating set for every $g \in G$. The problem of determining the diameter is known to be NP-hard [2]. However, the problem of determining the depth k_0 remains open. For the groups $\mathrm{PSL}_2(\mathbb{F}_p)$, p a prime, we are able to state the following:

Theorem 3. *For p an odd prime, let α, β be two non-commuting elements of order p in $G = \mathrm{PSL}_2(\mathbb{F}_p)$. Then $G = \langle \alpha, \beta \rangle$, and the depth of G with respect to α, β is 2.*

Proof. $|\mathcal{S}_1(\alpha, \beta)| = p^2 < |G|$, so $\hat{\mathcal{S}}_1(\alpha, \beta) \neq G$. However, for $k = 2$, from (11) we have $h_2 = c_2 = 3p-2$, $a_2 = d_2 = 2p-2$, and $b_2 = 2p$. Thus all elements of $\mathrm{PSL}_2(\mathbb{F}_p)$ have non-zero multiplicity in $\mathcal{S}_2(\alpha, \beta)$, and so $\mathrm{PSL}_2(\mathbb{F}_p) = \hat{\mathcal{S}}_2(\alpha, \beta)$. □

4 Complexity

In this section for $G = \langle \alpha_1, \ldots, \alpha_t \rangle$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$, we discuss the complexity of the DLP/GDLP relative to $\boldsymbol{\alpha}$. We present an assumption (Hypothesis 1) which ultimately allows us to design provably secure

cryptographic primitives. Unless otherwise noted, complexity statements are assumed to be based on the size of a specified security parameter. Obviously, the security of cryptographic primitives based on the DLP relative to $\boldsymbol{\alpha}$ depends on the intractability of the problem of factorization of a given group element as a word in the prescribed generators α_i. We list the ways known to us to factorize an element of a finite group G:

i) Factoring an element $\beta \in G$ over a generating set $\alpha_1, \ldots, \alpha_r$ is equivalent to computing preimages of the homomorphism $\psi : F_r \to G$, where F_r is the free group of rank r and ψ maps generators of F_r to $\{\alpha_1, \ldots, \alpha_r\}$. The problem is generally intractable except for special representations, such as permutation representations.

ii) Alternatively, factoring an element of G over a pre-defined set of elements $\alpha_1, \ldots, \alpha_t$, is equivalent to factorization with respect to logarithmic signatures or covers [9, 10]. Factoring with respect to logarithmic signatures or covers is considered intractable except for special instances in permutation groups.

iii) A group G is said to be *polycyclic* if it has a normal series of subgroups $1 = G_1 \lhd G_2 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$ with each G_i/G_{i-1} cyclic. Polycyclic groups have what are known as *consistent polycyclic presentations*. Moreover, in connection with these presentations, an efficient algorithm, called the *collection algorithm*, can be used to solve the factorization problem with respect to the polycyclic generating set [4].

iv) The Stabilizer Chain method [8], is known to efficiently factorize elements in permutation groups over a generating set, but there are many examples of matrix groups of moderately small dimension where we cannot find a suitable chain. This method does not guarantee finding the word of minimal length either. In fact, the well known Schreier-Sims algorithm for this task, described in [8], produces words of exponentially growing length. How to avoid the exponential growth in permutation groups in some situations is discussed in [1].

v) The method described in [14] can be easily and naturally generalized to groups with more than two generators. The problem with this method is that it requires subgroup membership tests and a single solution to the traditional DLP in cyclic groups. Also, the running time of this method is exponential in the size of the input.

An important observation is that the traditional DLP for cyclic groups is a special case of our DLP for arbitrary finite groups. In particular, if $G = \langle \alpha_1 \rangle$ is a finite cyclic group, then $\mathcal{S}_1(\alpha_1) = \hat{\mathcal{S}}_1(\alpha_1) = G$, and so the definition of the

traditional DLP and our definition of the DLP relative to (α_1) coincide. An immediate consequence is that for some groups the computational complexity of solving the DLP and the GDLP relative to $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ is at least as high as the computational complexity of solving the traditional DLP. There are instances where a finite cyclic group with an intractable DLP is embedded in a non-solvable finite matrix group with an intractable DLP.

It turns out however that I. Ilic [5], has recently proved that for $G = \mathrm{PSL}_2(\mathbb{F}_p)$, p a prime, there are instances $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$, $G = \langle \alpha_1, \alpha_2 \rangle$, where the corresponding DLP with respect to $\boldsymbol{\alpha}$ has a polynomial-time solution. This is analogous to the DLP based on the cyclic, additive $\mathbb{Z}_n$. However, for $G = \mathrm{PSL}_2(\mathbb{F}_p)$, the predominance of cases $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$ lead to an intractable DLP.

Based on the above discussion, we assert that the DLP relative to $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ is generally intractable. It may be possible, therefore, to design secure cryptographic primitives based on the more general DLP. Of course, specific examples can be constructed where the DLP would have efficient solutions. In this sense, the security of the DLP relative to some $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ is strongly related to the underlying groups G and their representation.

We finish this section with a security assumption based on the discussed group theoretic facts, its cryptographic application, and an example.

Hypothesis 1. *There is an infinite collection of finite groups $\{G_i\}_{i \in I}$ and a common representation of each G_i, and there is a sequence of elements $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ in G_i, such that every probabilistic algorithm running in time polynomial in the size of the order of G_i that can solve the GDLP relative to $\boldsymbol{\alpha}$ (i.e., which solves equation (1) with $y \in G$ chosen uniformly at random) succeeds with negligible probability.*

Since a solution to the DLP relative to $\boldsymbol{\alpha}$ also gives a solution to the GDLP relative to $\boldsymbol{\alpha}$, but not conversely, it follows that the acceptance of Hypothesis 1 also provides the existence of an infinite collection of finite groups $\{G_i\}_{i \in I}$ under a common representation where the DLP relative to $\boldsymbol{\alpha}$ over each G_i is intractable.

Based on this hypothesis, it is possible to construct a collection of one-way functions (in the sense of the definition in [3]). Such a construction was given in [14] and it was argued that it can be used for designing a secure *signature scheme*, that is, secure against an existential forgery under a chosen message attack [12] or a secure *pseudo-random number generator* whose output sequence is indistinguishable from a truly random sequence [6].

Finally, we mention one concrete and motivating example which supports our hypothesis, the hash function of J. P. Tillich and G. Zémor [17]. Let $f(x)$

be an irreducible polynomial of degree n over $\mathbb{F}_2$, and ρ a root of $f(x)$. The matrices

$$A = \begin{bmatrix} \rho & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} \rho & \rho+1 \\ 1 & 1 \end{bmatrix}$$

over $\mathbb{F}_{2^n}$ generate $G = \mathrm{SL}_2(\mathbb{F}_{2^n})$. Let $\pi : \{0,1\} \to \{A, B\}$ be given by $\pi(0) = A$ and $\pi(1) = B$. Then the Tillich-Zémor hash function from the set of all finite binary sequences to $\mathrm{SL}_2(\mathbb{F}_{2^n})$ is simply $s_1 s_2 \ldots s_t \mapsto \pi(s_1)\pi(s_2)\cdots\pi(s_t)$. Although there are some known attacks on the Tillich-Zémor hash function for some specific parameters and situations [16], it is still cryptographically secure for carefully chosen parameters. We note that if an element of $\mathrm{SL}_2(\mathbb{F}_{2^n})$ can be factored into a product of A's and B's, then we can find collisions of the Tillich-Zémor hash function. More precisely, the problem is to find *short relations* in A and B, where by "short" here we mean a relation of length $O(\log(|G|))$. It is easy to prove that short relations exist, but we have no efficient way of finding any one of them. Indeed, finding a short relation involves the same degree of difficulty as solving the GDLP relative to (A, B). Conversely, the ability to solve the GDLP relative to (A, B) allows us to find pre-images of the Tillich-Zémor hash function.

5 Conclusions

We have defined a natural generalization of the discrete logarithm problem from cyclic groups to arbitrary finite groups.

The security of the proposed DLP is based on the difficulty of the factorization problem in finite groups given by a set of generators in particular representations. Presently, no efficient classical or quantum algorithms are known for factoring elements in general matrix groups. The utility of the DLP is also based on the property that, as k gets large, the distribution of group elements in $\mathcal{S}_k(\boldsymbol{\alpha})$ tends to uniform. We have proposed that, for prime p, the family of groups $\mathrm{PSL}_2(\mathbb{F}_p)$ in their usual matrix representation might be an appropriate choice, if the generators are carefully chosen. We have further shown that, for non-commuting elements α and β of order p in $\mathrm{PSL}_2(\mathbb{F}_p)$ and for $k \geq 3$, the distribution of group elements in $\mathcal{S}_k(\alpha, \beta)$ tends to uniform as $p \to \infty$.

We mention also that there are a few other extensions and generalizations of the traditional DLP. The most recent ones include [7, 11, 15].

Finally, we list several open problems and areas for further study suggested by our results:

a) Can the DLP/GDLP with respect to $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ be used in

the direct design of encryption or signature primitives? Is there an appropriate algebra on the exponents? Can it be used for the construction of trapdoor one-way functions?

b) What is the real security (computational complexity) of the DLP/GDLP with respect to α? Are there any efficient methods or ways to factorize elements in concrete or abstract groups?

c) What other groups and representations will satisfy the assumptions in Hypothesis 1?

References

[1] Egner, S. and Pueschel, M.: Solving puzzles related to permutation groups. In *Proc. of the 1998 International Symposium on Symbolic and Algebraic Computation*, pp. 186–193. ACM Press, New York (1998).

[2] Even, S. and Goldreich, O.: Minimum-Length Generator Sequence Problem is NP-Hard. *J. Algorithms*, **2**(3), pp. 311–313 (1981).

[3] Goldreich, O.: Foundations of Cryptography. Cambridge University Press, Cambridge (2001).

[4] Holt, D.F., Eick, B., and O'Brien, E.A.: Handbook of Computational Group Theory. Chapman & Hall / CRC Press, Boca Raton (2005).

[5] Ilic, I.: Discrete logs in arbitrary finite groups. *Ph.D. research - unpublished*, Florida Atlantic University (2008).

[6] Impagliazzo, R., Levin, L.A. and Luby, M.: Pseudorandom Generation from One-Way Functions. In *Proc. of the 21st ACM Symposium on Theory of Computing*, pp. 12–24. ACM Press, New York (1989).

[7] Kashyap, S.K., Sharma, B.K., and Banerjee, A.: A Cryptosystem Based on DLP $\gamma \equiv \alpha^a \beta^b \pmod{p}$. *Intern. J. Network Security*, **3**(1), pp. 95–100 (2006).

[8] Leon, J.S.: On an algorithm for finding a base and a strong generating set for a group given by generating permutations. *Math. of Computation*, **35**, pp. 941–974 (1980).

[9] Magliveras, S.S., and Memon, N.D.: The Algebraic Properties of Cryptosystem PGM. *J. of Cryptology*, **5**, pp. 167–183 (1992).

[10] Magliveras, S.S., Tran, van Trung, and Stinson, D.R.: New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups. *J. Cryptology*, **15**, pp. 285–297 (2002).

[11] Mahalanobis, A.: The Diffie-Hellman key exchange protocol, and non-abelian nilpotent groups. *Israel J. Math.* **165**, pp. 161–187 (2008).

[12] Rompel, J.: One-way functions are necessary and sufficient for secure signatures. In *Proc. of the 22nd annual ACM Symposium on Theory of Computing*, pp. 387–394. ACM Press, New York (1990).

[13] Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. on Computing*, **26**(5), pp. 1484–1509 (1997).

[14] Sramka, M.: New Results in Group Theoretic Cryptology. Ph.D. thesis, Florida Atlantic University, Boca Raton, FL. (2006).

[15] Stickel, E.: A New Method for Exchanging Secret Keys. In *Proc. of the Third International Conference on Information Technology and Applications (ICITA'05)*, **2**, pp. 426–430 (2005).

[16] Steinwandt, R., Grassl, M., Geiselmann, W., and Beth, Th.: Weaknesses in the SL2(F2n) Hashing Scheme. In *Advances in Cryptology - CRYPTO 2000*, LNCS **1880**, pp. 287-299. Springer-Verlag (2000).

[17] Tillich, J.P., and Zémor, G.: Hashing with SL_2. In *Advances in Cryptology - CRYPTO '94*, LNCS **839**, pp. 40–49. Springer-Verlag (1994).