NATO Science for Peace and Security Series
D: Information and Communication Security - Vol. 29

Information Security, Coding Theory and Related Combinatorics

Information Coding and Combinatorics

Edited by
Dean Crnković
Vladimir Tonchev

IOS Press

NATO OTAN

This publication is supported by:

The NATO Science for Peace and Security Programme

Information Security, Coding Theory and Related Combinatorics

Information Coding and Combinatorics

Edited by

Dean Crnković
University of Rijeka, Rijeka, Croatia

and

Vladimir Tonchev
Michigan Technological University, Houghton, Michigan, USA

IOS Press

Amsterdam • Berlin • Tokyo • Washington, DC

Published in cooperation with NATO Emerging Security Challenges Division

Proceedings of the NATO Advanced Study Institute on Information Security and Related Combinatories
Opatija, Croatia
31 May - 11 June 2010

ISBN 978-1-60750-662-1 (print)
ISBN 978-1-60750-663-8 (online)
Library of Congress Control Number: 2010941318

Publisher
IOS Press BV
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

Distributor in the USA and Canada
IOS Press, Inc.
4502 Rachael Manor Drive
Fairfax, VA 22032
USA
fax: +1 703 323 3668
e-mail: iosbooks@iospress.com

PRINTED IN THE NETHERLANDS

INFORMATION SECURITY, CODING THEORY AND RELATED COMBINATORICS

NATO Science for Peace and Security Series

This Series presents the results of scientific meetings supported under the NATO Programme: Science for Peace and Security (SPS).

The NATO SPS Programme supports meetings in the following Key Priority areas: (1) Defence Against Terrorism; (2) Countering other Threats to Security and (3) NATO, Partner and Mediterranean Dialogue Country Priorities. The types of meeting supported are generally "Advanced Study Institutes" and "Advanced Research Workshops". The NATO SPS Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO's "Partner" or "Mediterranean Dialogue" countries. The observations and recommendations made at the meetings, as well as the contents of the volumes in the Series, reflect those of participants and contributors only; they should not necessarily be regarded as reflecting NATO views or policy.

Advanced Study Institutes (ASI) are high-level tutorial courses to convey the latest developments in a subject to an advanced-level audience.

Advanced Research Workshops (ARW) are expert meetings where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for future action.

Following a transformation of the programme in 2006 the Series has been re-named and re-organised. Recent volumes on topics not related to security, which result from meetings supported under the programme earlier, may be found in the NATO Science Series.

The Series is published by IOS Press, Amsterdam, and Springer Science and Business Media, Dordrecht, in conjunction with the NATO Emerging Security Challenges Division.

Sub-Series

A.	Chemistry and Biology	Springer Science and Business Media
B.	Physics and Biophysics	Springer Science and Business Media
C.	Environmental Security	Springer Science and Business Media
D.	Information and Communication Security	IOS Press
E.	Human and Societal Dynamics	IOS Press

http://www.nato.int/science
http://www.springer.com
http://www.iospress.nl

Sub-Series D: Information and Communication Security – Vol. 29

ISSN 1874-6268 (print)
ISSN 1879-8292 (online)

Information Security, Coding Theory and Related Combinatorics
D. Crnković and V. Tonchev (Eds.)
IOS Press, 2011

Preface

This book contains papers based on lectures presented at the NATO Advanced Study Institute "Information Security and Related Combinatorics", held in the beautiful town of Opatija at the Adriatic Coast of Croatia from May 31 to June 11, 2010. On behalf of all participants, we would like to thank the NATO Science for Peace and Security Programme for providing funds for the conference, as well as the local sponsors, which included the Ministry of Science and Education of the Republic of Croatia, the Croatian Academy of Sciences and Arts, the Primorsko-goranska County, the University of Rijeka and its Mathematics Department, the Foundation of the University of Rijeka, the Society of Mathematicians and Physicists, the Login Co., the Opatija Tourist Board, the City of Opatija, the City of Rijeka, and Brodokomerc.nova.

The Advanced Study Institute had fourteen lecturers: K.T. Arasu (USA), C. Colbourn (USA), F. Fuji-Hara (Japan). W. Haemers (The Netherlands), M. Jimbo (Japan), J.D. Key (USA), H. Kharaghani (Canada), C. Lam (Canada), S. Magliveras, (USA), J. Moori (South Africa), T. Shaska (USA), L. Storme (Belgium), V.D. Tonchev (USA), R. Wilson (USA), and was attended by over 60 graduate students and junior scientists from Albania, Armenia, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Germany, Italy, Macedonia, The Netherlands, Russia, Turkey, and USA.

The unifying theme of the conference was combinatorial mathematics used in applications related to information security, cryptography, and coding theory.

The book will be of interest to mathematicians, computer scientists and engineers working in the area of digital communications, as well as to researchers and graduate students who are willing to learn more about the applications of combinatorial mathematics to problems arising in communications and information security. The majority of papers are surveys on topics that are subject to current research and are written in a tutorial text book style that makes this volume a good source as an additional text for a course in discrete mathematics or applied combinatorics. The book can be used in graduate courses of applied combinatorics with a focus on coding theory and cryptography.

Dean Crnković and Vladimir Tonchev

Contents

Information Security, Coding Theory and Related Combinatorics
D. Crnković and V. Tonchev (Eds.)
IOS Press, 2011

doi:10.3233/978-1-60750-663-8-1

Crypto applications of combinatorial group theory

Ivana Ilić and Spyros S. Magliveras
CCIS, Department of Math. Sciences, Florida Atlantic University, Boca Raton, FL 33431, USA
e-mail: iilic@fau.edu, spyros@fau.edu

Abstract. The design of a large number of cryptographic primitives is based on the intractability of the traditional discrete logarithm problem (tDLP). However, the well known quantum algorithm of P. Shor [9] solves the tDLP in polynomial time, thus rendering all cryptographic schemes based on tDLP ineffective, should quantum computers become a practical reality. In [5] M. Sramka et al. generalize the DLP to arbitrary finite groups. The DLP for a non-abelian group is based on a particular representation of a chosen family of groups, and a choice of a class of generators for these groups. In this paper we show that for $PSL(2,p) = \langle \alpha, \beta \rangle$, p an odd prime, certain choices of generators (α, β) must be avoided to insure that the resulting generalized DLP is indeed intractable. For other types of generating pairs we suggest possible cryptanalytic attacks, reducing the new problem to the earlier case. We note however that the probability of success is asymptotic to $\frac{1}{p}$ as $p \to \infty$. The second part of the paper summarizes our successful attack of the $SL(2,2^n)$ based Tillich Zémor cryptographic hash function [2], and show how to construct collisions between palindromic strings of length $2n+2$.

2000 Mathematics Subject Classification: 68P25, 94A60.
Keywords. Discrete logarithm, finite groups, intractability, representations and presentations of groups, $PSL(2,p)$, public key cryptosystems, Tillich-Zémor hash function.

Introduction

In a recent quote, P. Nguyen states "Due to Shor's algorithms for computing prime factorizations and discrete logarithms on quantum computers, most of present day public key cryptosystems must be considered insecure , if sufficiently large quantum computers became available. ... One interesting line of research in this direction is the use of computational problems in non-abelian groups ... " [6]. In this article we discuss recent results on the generalized discrete logarithm problem (GDLP) in the family of non-abelian simple groups $PSL(2,p)$, p an odd prime. In particular we examine these groups in their representations as matrices over $GF(p)$, and investigate weak generator choices for the generalized DLP problem. In the second part of the paper we summarize the interest-

ing approach in [2] which culminated with the demise of the well known Tillich-Zémor cryptographic hash function [13].

1. Preliminaries

The authors of [5] generalize the discrete logarithm problem from finite cyclic groups to arbitrary finite groups. We restate the definition. Let G be a finite group generated by $\alpha_1, \ldots, \alpha_t$, i.e., $G = \langle \alpha_1, \ldots, \alpha_t \rangle$. Denote by $\alpha = (\alpha_1, \ldots, \alpha_t)$, the ordered tuple of generators of the group G. As defined in [5], for a given $\beta \in G$, the generalized discrete logarithm problem (GDLP) of β with respect to α is to determine a positive integer k and a (kt)-tuple of non-negative integers $x = (x_{11}, \ldots, x_{1t}, \ldots, x_{k1}, \ldots, x_{kt})$ such that

$$\beta = \prod_{i=1}^{k} (\alpha_1^{x_{i1}} \ldots \alpha_t^{x_{it}}) .$$

We can write this formally as $\beta = \alpha^x$. The (kt)-tuples $(x_{11}, \ldots, x_{1t}, \ldots, x_{k1}, \ldots, x_{kt})$ are called the generalized discrete logarithms of β with the respect to $\alpha = (\alpha_1, \ldots, \alpha_t)$.

Denote by

$$S_k = \left\{ \prod_{i=1}^{k} (\alpha_1^{x_{i1}} \ldots \alpha_t^{x_{it}}) \mid x_{ij} \in \mathbb{Z}_{n_j} \right\}$$

where n_j denotes the order of element α_j. Then, the smallest positive integer k_0 such that for all $k \geq k_0$ $G \subseteq S_k$ is called the *depth* of group G with respect to $(\alpha_1, \ldots, \alpha_t)$. There could be more than one generalized discrete logarithm of β with respect to α. Actually, there will be infinitely many generalized discrete logarithms: if x is a generalized discrete logarithm of β with respect to α and if $\alpha^{x'} = 1$, then, the catenations $x||x'$ and $x'||x$ are also generalized discrete logarithms of β with respect to α.

The generalization of the discrete logarithm problem to finite groups has potential applications in cryptography. To be able to construct secure cryptographic primitives based on the generalized discrete logarithm problem in finite groups, care must be taken to ensure that the groups along with their representations and choice of generators have an intractable generalized discrete logarithm problem.

The traditional discrete logarithm problem is generally considered computationally intractable. However, there exist groups and their representations in which the problem can be solved efficiently. For example, in $\mathbb{Z}_n$, the additive group of integers modulo n, the discrete logarithm can be easily computed. For a given element β in $\mathbb{Z}_n$ and generator α of $\mathbb{Z}_n$, it is easy to find a non-negative integer x such that $x\alpha = \beta$. Since α is a generator, $gcd(n, \alpha) = 1$, and the multiplicative inverse in the ring $(\mathbb{Z}_n, +, \cdot)$ of α can be computed by the extended Euclidean algorithm. In general, one may speak of a tractable/intractable GDLP problem for a given infinite family of pairs $\{(G_\ell, A_\ell)\}_{\ell \in \mathcal{L}}$ indexed by $\mathcal{L}$, where the G_ℓ are groups in a common representation ρ, and A_ℓ a particular set of generators for G_ℓ.

The generalized discrete logarithm problem may be tractable for some groups and generators in representation ρ. We examined the groups $PSL(2,p)$ as potential candidates for cryptographic applications, but our results show that when $PSL(2,p)$ is represented by matrices, the generalized discrete logarithm problem with respect to several types of generating sets does not provide the required strength.

As is customary, we denote by $\mathbb{Z}$ the ring of integers. We also denote by $\mathbb{Z}^+$ the positive integers, and by $\mathbb{Z}^0$ the non-negative integers.

2. Generalized discrete logarithm problem in $PSL(2,p)$

Suppose that for an odd prime p the group $G = PSL(2,p)$ is represented by matrices of $SL(2,p)$, up to a factor $\pm I$, where I is the 2×2 identity matrix. Suppose further that G is generated by two elements, i.e., $G = \langle A, B\rangle$. We have examined the tractability of the generalized discrete logarithm problem in this setup with respect to different generating pairs of elements (A, B). The results of our research show that the hardness of computation of the generalized discrete logarithm problem will depend not only on the group representation, but also on the choice of generators. To perform a detailed analysis on whether the generalized discrete logarithm can be computed efficiently, we considered the following cases: 1) group G is generated by special elements: $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, and $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$; 2) group G is generated by two elements both of order p; 3) group G is generated by two elements, one of which is of order p; 4) group G is generated by two elements none of which is of order p. We have analyzed the first two cases in [4]. Suppose that $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, with $a, b, c, d \in \mathbb{F}_p$, the field of order p.

The matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

are both of order p, non-commuting and generate G, i.e., $G = \langle A, B\rangle$. Moreover, the authors of [5] show that the depth of group G with the respect to the (A, B) is two, so that the element $M \in G$ can be written as $M = A^i B^j A^k B^\ell$. We have

$$A^i B^j A^k B^\ell = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \ell & 1 \end{pmatrix}.$$

Hence,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 + ij + \ell\,((1+ij)\,k + i) & (1+ij)\,k + i \\ j + \ell\,(jk+1) & jk+1 \end{pmatrix}.$$

By equating corresponding entries in the previous equality we obtain the system of equations

$$\begin{aligned} 1 + ij + \ell\left((1+ij)\,k + i\right) &= a \\ (1+ij)\,k + i &= b \\ j + \ell\,(jk+1) &= c \\ jk + 1 &= d \end{aligned}$$

which can be solved for i, j, k, ℓ by computing Gröbner basis of the ideal $I = \langle\, 1 + \ell k + ij + ijk\ell + i\ell - a, k + ijk + i - b, j + jk\ell + \ell - c, jk + 1 - d \,\rangle$. A Gröbner basis for the above ideal is computed over the set of rational numbers: $[\, \ell - jic + ja - c, k + id - b, jibc + ji - jab - a + bc + 1, jid - jb + d - 1, ad - bc - 1 \,]$, which yields the following system of equations: in $i, j, k, \ell \in \mathbb{Z}_p$.

$$\begin{aligned} \ell - jic + ja - c &= 0 \\ k + id - b &= 0 \\ jid - jb + d - 1 &= 0 \end{aligned}$$

whose solutions in i, j, k, l represent the generalized discrete logarithms of M with respect to (A, B). The solutions are given by the following proposition:

Proposition 2.1 *Let A, B and M be as above. Then, there exists a non-negative integer $n < p$ such that $nd - b \neq 0$ over $\mathbb{Z}_p$, and such that the 4-tuple (i, j, k, ℓ) with $i = n$, $j = (1-d)(nd-b)^{-1}$, $k = b - nd$, $\ell = (1-d)(nc-a)(nd-b)^{-1} + c$ provides a solution to $M = A^i B^j A^k B^\ell$.*

Proof. It can be directly verified that the given values for i, j, k, ℓ satisfy the above system of equations. The existence of n is ensured since $M \in PSL(2, p)$ and hence b and d can not simultaneously be equal to zero. □

We have shown that the generalized discrete logarithm problem can be solved efficiently in $PSL(2, p)$ with respect to the special given generators (A, B) as defined above. Further, as in [4], we construct an algorithm for computing the generalized discrete logarithm problem in $PSL(2, p)$ with respect to any two generators of order p. Assume that C, D are two non-commuting elements of order p in $PSL(2, p)$. Then, since any two non-commuting elements of order p from $PSL(2, p)$ generate the whole group, it follows that $PSL(2, p) = \langle C, D \rangle$. To determine non-negative integers i, j, k, ℓ such that: $M = C^i D^j C^k D^\ell$, we look for an element $g \in G$ which satisfies $C = g^{-1} A^s g$ and $D = g^{-1} B^t g$, for some non-negative integers $s, t < p$ and where A and B are the matrices defined above.

Then,

$$\begin{aligned} M &= C^i D^j C^k D^\ell \\ &= (g^{-1}A^s g)^i (g^{-1}B^t g)^j (g^{-1}A^s g)^k (g^{-1}B^t g)^\ell \\ &= (g^{-1}A^{si} g)(g^{-1}B^{tj} g)(g^{-1}A^{sk} g)(g^{-1}B^{t\ell} g) \\ &= g^{-1}A^{si}B^{tj}A^{sk}B^{t\ell} g \end{aligned}$$

Denote by $x = si$, $y = tj$, $v = sk$ and $w = t\ell$. Then, $gMg^{-1} = A^x B^y A^v B^w$. Let $M_1 = gMg^{-1}$. Obviously, $M_1 \in G$ and $M_1 = A^x B^y A^v B^w$. We have transformed the generalized discrete logarithm problem of $PSL(2,p)$ with respect to (C,D) to the generalized discrete logarithm problem of $PSL(2,p)$ with respect to (A,B) which we are able to solve as described earlier.

To determine an element g for which the conditions $C = g^{-1}A^s g$ and $D = g^{-1}B^t g$ hold simultaneously, we write the system of equations: $gC = A^s g$ and $gD = B^t g$, for some non-negative integers $s, t < p$. Since, $g = \left(\begin{smallmatrix} g_1 & g_2 \\ g_3 & g_4 \end{smallmatrix}\right)$, we obtain a system of equations in $g_1, \ldots, g_4$ and s and t from which an element g is determined. The existence of such an element g is ensured since $PSL(2,p)$ acts doubly transitively by conjugation on its $(p+1)$ Sylow-p subgroups. Then, for any two pairs of p-Sylow subgroups, and hence for the particular pairs $(\langle A\rangle, \langle B\rangle)$ and $(\langle C\rangle, \langle D\rangle)$, there exists an element $g \in G$ such that $(\langle C\rangle, \langle D\rangle) = (\langle A\rangle^g, \langle B\rangle^g)$.

The third case in our analysis of hardness of the generalized discrete logarithm problem in $PSL(2,p)$, with respect to a pair of generators, is when one of the generators is of order p. Suppose now that $PSL(2,p) = \langle A, B\rangle$ where $|A| = p$. Note that the order of element B can only be divisor of the order of the group $p(p^2-1)/2$. Given an element $M \in PSL(2,p)$ our goal is to write M in terms of the generators (A,B). In the construction of a word in A and B that represents element M, we will use the result of the following proposition.

Proposition 2.2 *If $G = PSL(2,p) = \langle A, B\rangle$ where $|A| = p$, then $G = \langle A, A^B\rangle$, where $A^B = B^{-1}AB$.*

Proof. Every two non-commuting elements of order p from $PSL(2,p)$ generate the whole group. So we prove that elements A and A^B are non-commuting of order p. Conjugate elements have the same order, so $|A^B| = |A| = p$. Now, suppose that elements A and A^B commute. Then, A^B is in the centralizer of element A, i.e., $A^B \in C_G(A) = \langle A\rangle$. So, $A^B = A^i$ for some $i \in \{0, \ldots, p-1\}$. But then, B normalizes $\langle A\rangle$, hence, $\langle A\rangle$ is a proper normal subgroup of $\langle A, B\rangle$. But $PSL(2,p)$ is simple, thus $\langle A, B\rangle$ can not be all of $PSL(2,p)$, a contradiction to the fact that A and B generate G. □

The proposition that follows provides an upper bound for the depth of $PSL(2,p)$ with respect to two generators one of which is of order p and its proof provides an algorithm for constructing a word in generators A and B that represents a given element M.

Proposition 2.3 *Suppose that $G = PSL(2,p) = \langle A, B\rangle$, where $|A| = p$, with no further assumptions on $|B| = m$. Then, the depth of G with respect to the generating tuple (A,B) is less than or equal to four.*

Proof. Let $C = A^B = B^{-1}AB$. By Proposition (2.2) the group $PSL(2,p)$ is generated by elements A and C, both of order p. The generalized discrete logarithm problem can be solved efficiently in $PSL(2,p)$ represented by matrices, with respect to two generators of order p. By the method described earlier, the generalized discrete logarithm (i,j,k,ℓ) can be found such that $M = A^i C^j A^k C^\ell$. To represent the element M in terms of the generators A and B we write the following sequence of equalities.

$$\begin{aligned} M &= A^i C^j A^k C^\ell \\ &= A^i (B^{-1}AB)^j A^k (B^{-1}AB)^\ell \\ &= A^i B^{-1} A^j B A^k B^{-1} A^\ell B \\ &= A^i B^{m-1} A^j B A^k B^{m-1} A^\ell B \end{aligned}$$

Therefore, the generalized discrete logarithm of $M \in PSL(2,p)$ with respect to generating tuple (A,B), where $|A| = p$ and $|B| = m$ is $(i, m-1, j, 1, k, m-1, \ell, 1)$. It follows that every element M from $PSL(2,p) = \langle A,B\rangle$, where $|A| = p$ and $|B| = m$ can be represented as $M = A^{x_1}B^{y_1}A^{x_2}B^{y_2}A^{x_3}B^{y_3}A^{x_4}B^{y_4}$ for some integers $x_1, x_2, x_3, x_4 \in \{0, ..., p-1\}$ and $y_1, y_2, y_3, y_4 \in \{0, ..., m-1\}$. The proposition follows. □

The described method for writing element M as a word in generators A and B does not assure obtaining the shortest possible word that represents M in these generators.

Next, we take a look into a possible strategy for writing an element M of group $PSL(2,p)$ in terms of two generators none of which is of order p. Suppose that we have an efficient method for constructing an element of order p in terms of the generators A and B. In the following proposition we will use the notation $w_p(A,B)$ to represent a word in A and B which is of order p as an element of G.

Proposition 2.4 *If $G = PSL(2,p) = \langle A,B\rangle$ where the orders of A and B are relatively prime to p, and if $P = w_p(A,B)$, is a word in A and B, of order p as an element of G, then $G = \langle A,P\rangle$ or $G = \langle B,P\rangle$.*

Proof. Let N be the normalizer in G of $\langle P\rangle$, i.e. $N = N_G(\langle P\rangle)$. Then, at least one of the elements A, B is not in N. Otherwise if A, B were both in N, then $\langle A,B\rangle$ would be a subgroup of N, that is $G = \langle A,B\rangle \leq N$, and therefore we would have that $N = G$. This would imply that $\langle P\rangle$ is a non-trivial, proper, normal subgroup of G, contradicting the fact that G is simple. Without loss of generality, suppose that $A \notin N$. Then $\langle A,P\rangle = PSL(2,p)$, because the only proper subgroups of $PSL(2,p)$ containing $\langle P\rangle$ are subgroups of the normalizer of $\langle P\rangle$. Similarly, if $B \notin N$, it follows that $PSL(2,p) = \langle B,P\rangle$. □

If A, B and P are as in Proposition 2.4 we can solve efficiently the generalized discrete logarithm problem with respect to (A,P) since $PSL(2,p) = \langle A,P\rangle$ and $|P| = p$. Therefore, we can solve the generalized discrete logarithm problem with respect to (A,B). Given $M \in PSL(2,p) = \langle A,B\rangle$ and $P = w_p(A,B)$ as in the Proposition 2.4 we can write element M as a word in A, B as follows. Without loss of generality, assume that $A \notin N_G$. Conjugate element P by element A, i.e., compute $P^A = A^{-1}PA$. Based

on the Proposition 2.2, $PSL(2,p) = \langle P, P^A \rangle$. Based on the proof of the Proposition 2.3, if $|A| = s$, we have:

$$\begin{aligned} M &= P^i (P^A)^j P^k (P^A)^\ell \\ &= P^i A^{s-1} P^j A P^k A^{s-1} P^\ell A \\ &= w_p(A,B)^i A^{s-1} w_p(A,B)^j w_p(A,B) w_p(A,B)^k A^{s-1} w_p(A,B)^\ell A \end{aligned}$$

The direct consequence is that the depth of the $PSL(2,p)$ with respect to the generators both of order relatively prime to p, will depend on the word $P = w_p(A,B)$.

We examine a bit further possible attacks to the GDLP for $G = PSL(2,p)$ based on Proposition 2.4. A word of shortest possible length in A and B to produce an element of order p is AB or BA. We will consider the case where $|A| = |B| = d = (p-1)/2$ and $|AB| = p$. This condition occurs systematically in $PSL(2,p)$, however, unfortunately for the cryptanalyst, the probability of this occurrence goes to zero as $p \to \infty$.

We will need some well known facts about the group $PSL(2,q)$, $q = p^m$, p an odd prime, which we state below, without proof, as a proposition. In what follows ϕ stands for Euler's ϕ function.

Proposition 2.5 *Suppose that $G = PSL(2,q)$, $q = p^m$, p an odd prime. Then,*

(a) The Sylow-p subgroup of G is elementary abelian of order q,
(b) If $x \in G$ is of order d, then d divides $(q-1)/2$, or $d = p$, or d divides $(q+1)/2$,
(c) There is a single conjugacy class of subgroups of order $(q-1)/2$, and these are cyclic. Similarly, there is a single conjugacy class of subgroups of order $(q+1)/2$, and they are cyclic.
(d) If $x \in G$ is of order $d \neq 2$ dividing $(q \pm 1)/2$ then x belongs to one and only one cyclic subgroup of G of order $(q \pm 1)/2$.
(e) If $d \neq 2$ divides $(q \pm 1)/2$ there are $\frac{\phi(q \pm 1)}{2}$ conjugacy classes of element of order d in G.
(f) If $x \in G$ is of order $d|(q \pm 1)/2$, $d \neq 2$, then the centralizer $C_G(x)$ is $\langle x \rangle$, while the normalizer $N_G(\langle x \rangle)$ is dihedral of order $q \pm 1$.

We will now examine the very special case where $G = PSL(2,p)$ is generated by two elements of order $(p-1)/2$. Similar results can be derived for the other possible cases. In what follows, Let X be the set of all elements of order $d = (p-1)/2$ in G. We will consider the action of G by conjugation on $X \times X$. Note that all pairs (A,B) in a $G-$orbit on $X \times X$ share almost all critical properties of interest to our problem, as conjugation by an element $g \in G$ induces an automorphism of G. For example if (A,B) generate G so does $(A,B)^g = (A^g, B^g)$, for $g \in G$. Similarly, the order of AB is the same as the order of $A^g B^g = (AB)^g$, etc. Thus it suffices to examine one representative from each orbit of G on $X \times X$.

Since G acts transitively by conjugation on the cyclic subgroups of order $(p-1)/2$, without loss of generality, we will select one such subgroup, say C and one fixed generator $x \in C$, so that $C = \langle x \rangle$. Now, $C_G(x) = \{y \in G \mid xy = yx\} = \langle x \rangle = C$. We have the following consequences of Proposition 2.5:

Proposition 2.6 *If G and X are as above, and $d = (p-1)/2$, then:*

(a) $|X| = \phi(d)p(p+1)/2$,

(b) Let x be any fixed element of X. In the action of $C = C_G(x)$ on X by conjugation there are exactly $\phi(d)$ orbits of length 1, and $v = (\phi(d)p(p+1) - 2)/2d$ orbits of length d.

(c) Of the v orbits O_i of length d exactly $2\phi(d) - 2$ are such that if $y \in O_i$ then $|xy| = p$.

Proof. (a) Since each of the $\phi(d)/2$ conjugacy classes of elements of order d has $|G|/d = p(p+1)$ elements, it follows that $|X| = [\phi(d)p(p+1)]/2$.

(b) $C = C_G(x) = \langle x \rangle$ has exactly $\phi(d)$ elements y of order d in it, and since these elements commute with x, the orbit $y^C = \{y\}$ and has length 1. If $y \in X \setminus C$ then $K = C_G(y) = \langle y \rangle$, and $K \cap C = \{1\}$, hence the orbit y^C has exactly $|C|$ elements. Thus, the number of orbits of length d is $[(\phi(d)p(p+1))/2 - \phi(d)]/d = [\phi(d)(p(p+1)-2]/2d$.

(c) We will only give an idea about the proof here. The result follows from calculations in the center of the group ring $\mathbb{Z}G$. In particular, if $\{K_i\}_{i=1}^{c}$ are the conjugacy classes of G, they form a basis for the center of $\mathbb{Z}G$ and $K_iK_j = \sum_{k=1}^{c} a_{ijk}K_k$, with the a_{ijk} computable from the character table of G. We have that X is the sum of the $\phi(d)/2$ classes $\{K_{\alpha_i}\}$ with elements of order d. Thus, in the group ring, the number of elements in xX of order p is the sum of the coefficients of the two classes K_{p_-} and K_{p_+} in $\frac{1}{|K_x|}K_x \sum_{i=1}^{\phi(d)/2} K_{\alpha_i} = \frac{1}{p(p+1)} \sum_{i=1}^{\phi(d)/2} K_x K_{\alpha_i}$. Since each $C-$orbit on $X \setminus C$ are of length d, we further divide by d for the number of $C-$orbits. □

We are now able to state a proposition which is not of much help to the cryptanalyst, but which lends evidence to the notion that strong generators may be possible for a GDLP based system.

Proposition 2.7 *Let $G = PSL(2,p)$ and let d, X and $x \in X$ be as above. If we select a second element $y \in X$ randomly, then the probability that the order of xy is p is $\frac{2(\phi(d)-1)(p-1)}{\phi(d)p(p+1)}$ which is of course asymptotic to $\frac{2}{p}$ as $p \to \infty$.*

Proof: Having fixed $x \in X$, by Proposition 2.6 the number of elements $y \in X$ such that $|xy| = p$ is $2(\phi(d) - 1)d$. Since $|X| = \frac{\phi(d)}{2} \cdot \frac{|G|}{d}$ we have:

$$Pr\{|xy| = p\} = \frac{2(\phi(d)-1)d}{\frac{\phi(d)}{2} \cdot p(p+1)} = \frac{4(\phi(d)-1)d}{\phi(d)p(p+1)} = \frac{2(\phi(d)-1)(p-1)}{\phi(d)p(p+1)} \rightsquigarrow \frac{2}{p}$$

hence the result. □

It is clear of course that if $(A, B) \in X \times X$ with $|AB| = p$, then $\langle A, B \rangle = G$.

3. Relations

By solving the generalized discrete logarithm problem for a finite group with respect to a given set of generators we are factorizing group elements in terms of the generators. By equating two different factorizations of the same group element, we obtain a *relation*. This observation holds in any finite group as we discuss in the next section.

Let G be a finite group generated by $\alpha_1, \ldots, \alpha_t$, i.e., $G = \langle \alpha_1, \ldots, \alpha_t \rangle$. Denote by $\alpha = (\alpha_1, \ldots, \alpha_t)$ the ordered tuple of generators of the group G. For a given $\beta \in G$, assume that

$$\beta = \prod_{i=1}^{k} (\alpha_1^{x_{i1}} \ldots \alpha_t^{x_{it}})$$

i.e., $\beta = \alpha^x$, where $x = (x_{11}, \ldots, x_{1t}, \ldots, x_{k1}, \ldots, x_{kt})$. Recall that $x = (x_{11}, \ldots, x_{1t}, \ldots, x_{k1}, \ldots, x_{kt})$, the generalized discrete logarithm with respect to the generators $\alpha = (\alpha_1, \ldots, \alpha_t)$, is not unique, in fact there will exist infinitely many distinct $y = (y_{11}, \ldots, y_{1t}, \ldots, y_{s1}, \ldots, y_{st})$ such that $\beta = \alpha^y = \prod_{i=1}^{s} \alpha_1^{y_{i1}} \ldots \alpha_t^{y_{it}}$. For any such y we have:

$$\prod_{i=1}^{k} \alpha_1^{x_{i1}} \ldots \alpha_t^{x_{it}} = \prod_{i=1}^{s} \alpha_1^{y_{i1}} \ldots \alpha_t^{y_{it}}.$$

In this way we obtain non-trivial relations among the generators. Further, by collecting different relations we may obtain a *presentation* of the group : $G = \langle X|R \rangle$, where X is the set of generators, and R a set of relations of the above type, sufficiently many to completely determine the group.

Relations of particular interest in cryptography are those which represent the identity element of the group, that is of the form $1_G =$ *a word in the generators*. Moreover, in a finite group G we can always convert a presentation of the form $G = \langle X|R \rangle$, into one of the form $G = \langle X|R' \rangle$, where R' is a set of relations of the type: $\prod_{i=1}^{k} \alpha_1^{x_{i1}} \ldots \alpha_t^{x_{it}} = 1_G$.

The *length* of word $w = \prod_{i=1}^{k} \alpha_1^{x_{i1}} \ldots \alpha_t^{x_{it}}$ in the symbols $\alpha_1, \ldots, \alpha_t$, where the x_{ij} are non-negative integers, is defined to be the integer $|w| = \sum_{i=1}^{k} \sum_{j=1}^{t} x_{ij}$. Moreover, if w_1 and w_2 are words in the symbols $\alpha_1, \ldots, \alpha_t$ and $\rho : w_1 = w_2$ is a relation, the *length* of the relation is defined to be the integer $|\rho| := |w_1| + |w_2|$.

If G is a finite group generated by $\alpha_1, \ldots, \alpha_t$, a relation ρ in the $\alpha_1, \ldots, \alpha_t$ is said to be *short* if $|\rho| = O(\log(|G|))$, otherwise ρ is said to be *long*. Relations of importance to cryptographic hash functions of the Tillich-Zémor type are those which are short.

We turn to our group of interest, $PSL(2, p)$, and examine the length of some relations there.

Let $G = PSL(2, p)$, and consider the elements $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ in G. The matrices A and B are both of order p, non-commuting and thus generate $PSL(2, p)$. As we have seen earlier, the depth of $PSL(2, p)$ with respect to the generating tuple (A, B)