Weak Discrete Logarithms in Non-Abelian Groups

Ivana Ilić, Spyros S. Magliveras
Department of Mathematical Sciences,
Florida Atlantic University
777 Glades Road, Boca Raton, FL 33431, U.S.A.
iilic@fau.edu, spyros@fau.edu

Abstract

The intractability of the traditional discrete logarithm problem (DLP) forms the basis for the design of numerous cryptographic primitives. In [2] M. Sramka et al. generalize the DLP to arbitrary finite groups. One of the reasons mentioned for this generalization is P. Shor's quantum algorithm [4] which solves efficiently the traditional DLP. The DLP for a non-abelian group is based on a particular representation of the group and a choice of generators. In this paper we show that care must be taken to ensure that the representation and generators indeed yield an intractable DLP. We show that in $PSL(2,p) = \langle \alpha, \beta \rangle$ the generalized discrete logarithm problem with respect to (α, β) is easy to solve for a specific representation and choice of generators α and β. As a consequence, such representation of $PSL(2,p)$ and generators should not be used to design cryptographic primitives.

1 Introduction

When cryptographic primitives are built based on the discrete logarithm problem (DLP), it is required that the DLP be computationally intractable. The intractability of the discrete logarithm problem depends on the group representation. For example, in $\mathbb{Z}_n$, the additive group of integers modulo n, the discrete logarithm problem is easy to solve. Namely, for a given element β in $\mathbb{Z}_n$ and generator α of $\mathbb{Z}_n$, it is easy to find the non-negative integer x such that $x\alpha = \beta$. Since $gcd(n, \alpha) = 1$, the multiplicative inverse of α can be computed by means of the Extended Euclidean algorithm and hence the discrete logarithm revealed.

JCMCC **74** (2010), pp. 3-11

In [2] the authors generalize the discrete logarithm from cyclic to any finite group. We assume that the generalized DLP is defined as in [2] and examine its tractability in the projective special linear group $PSL(2,p)$, where p is an odd prime. We show that in $PSL(2,p) = \langle \alpha, \beta \rangle$ the generalized DLP with respect to (α, β) is easy to solve for a specific group representation and specific choice of generators α and β.

As a consequence we have that such group representation of $PSL(2,p)$ together with particular generators should not be used in the design of cryptographic primitives whose security relies on the intractability of the DLP.

2 Preliminaries

Let G be a finite cyclic group generated by element α, and let β be an element from group G. The traditional discrete logarithm problem is to find the non-negative integer x such that $\alpha^x = \beta$.

As defined in [2], the generalized discrete logarithm problem (GDLP) for an arbitrary finite group is as follows: Let G be a finite group generated by $\alpha_1, \ldots, \alpha_t$. Given $\beta \in G$, determine a positive integer k and a (kt)-tuple of non-negative integers $(x_{11}, \ldots, x_{1t}, \ldots, x_{k1}, \ldots, x_{kt})$ such that

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

The (kt)-tuples $(x_{11}, \ldots, x_{1t}, \ldots, x_{k1}, \ldots, x_{kt})$ for which equation (1) holds are called the *generalized discrete logarithms* of β with respect to $(\alpha_1, \ldots, \alpha_t)$.

If

$$S_k = \left\{ \prod_{i=1}^{k} (\alpha_1^{x_{i1}} \ldots \alpha_t^{x_{it}}) \mid x_{ij} \in \mathbb{Z}_{n_j} \right\} \tag{2}$$

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 $(\alpha_1, \ldots, \alpha_t)$.

Given a field $\mathbb{F}_q$, of q elements, and a fixed natural number n, the group of all $n \times n$ nonsingular matrices with respect to the operation of matrix multiplication is known as the *general linear group* of degree n over $\mathbb{F}_q$ and is denoted by $GL(n,q)$. It is easy to see that $|GL(n,q)| = \prod_{i=0}^{n-1}(q^n - q^i)$. The set of all matrices in $GL(n,q)$ of determinant 1 forms a subgroup of $GL(n,q)$, the *special linear group*, denoted by $SL(n,q)$. $SL(n,q)$ is

the kernel of the homomorphism $det : GL(n,q) \rightarrow \mathbb{F}_q^*$, and therefore $|SL(n,q)| = |GL(n,q)|/(q-1)$. The center $Z(GL(n,q))$, of $GL(n,q)$, consists of all *scalar* matrices $\{\lambda I \mid \lambda \in \mathbb{F}_q^*\}$, thus the center of $SL(n,q)$ consists of all matrices $\{\lambda I \mid \lambda^n = 1\}$. The *projective special linear group* of degree n over $\mathbb{F}_q$, is the quotient group $PSL(n,q) = SL(n,q)/Z(SL(n,q))$. Here, we deal with the case $n = 2$, where q is odd, hence $|PSL(2,q)| = (q^2-1)q/2$.

3 Weak GDLP in $PSL(2,p)$ with respect to two specific generators

Consider the group $G = PSL(2,p)$ where p is an odd prime. Let α and β be any two non-commuting elements of order p in G, and let H and K be the subgroups of group G generated by α and β, respectively. In [5] the author shows that G is generated by α and β and that $G = HKHK$. Thus, the depth of G with respect to generators α and β is two.

For the purpose of further analysis we assume that the group G is represented by matrices of $SL(2,p)$, up to a factor $\pm I$, where I is the 2×2 identity matrix.

The matrices

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

are both of order p, non-commuting and generate G, i.e., $G = \langle A, B \rangle$. We show that the generalized discrete logarithm problem in G with respect to (A, B) can be solved efficiently.

Suppose that $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$, with $a, b, c, d \in \mathbb{F}_p$. Since the depth of G is two, M can be represented as $M = A^i B^j A^k B^\ell$ for some non-negative integers i, j, k, ℓ. Solving the generalized discrete logarithm problem means to find a tuple of non-negative integers (i, j, k, ℓ) such that $M = A^i B^j A^k B^\ell$.

Note that

$$A^i = \begin{bmatrix} 1 & i \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad B^j = \begin{bmatrix} 1 & 0 \\ j & 1 \end{bmatrix}. \tag{3}$$

Then,

$$A^i B^j A^k B^\ell = \begin{bmatrix} 1 & i \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ j & 1 \end{bmatrix} \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \ell & 1 \end{bmatrix}. \tag{4}$$

Hence,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1+ij+\ell((1+ij)k+i) & (1+ij)k+i \\ j+\ell(jk+1) & jk+1 \end{bmatrix}. \qquad (5)$$

By equating corresponding entries of the matrices, we obtain the following system of four equations with four unknowns i, j, k, ℓ in $\mathbb{F}_p = \mathbb{Z}_p$:

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

Indeed, the system of equations can be solved for i, j, k, ℓ using Gröbner basis computation. Let I be the ideal

$$\begin{aligned} I = \langle\, 1+\ell k+ij+ijk\ell+i\ell-a, \\ k+ijk+i-b, \\ j+jk\ell+\ell-c, \\ jk+1-d \,\rangle. \end{aligned}$$

A Gröbner basis GB for the ideal I is computed over the set of rational numbers:

$$\begin{aligned} GB = [\, \ell-jic+ja-c, \\ k+id-b, \\ jibc+ji-jab-a+bc+1, \\ jid-jb+d-1, \\ ad-bc-1 \,]. \end{aligned}$$

Therefore, solving the generalized discrete logarithm problem in the group $PSL(2,p)$ with respect to (A,B) is equivalent to solving the following system of equations in $i, j, k, \ell \in \mathbb{Z}_p$.

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

Generally, the system of equations has more than one solution. The following proposition provides a method for obtaining a solution when $M \in G$.

For the next proposition we continue to have $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, elements of $PSL(2,p)$.

Proposition 3.1 *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: The proof consists of directly verifying 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.

□

The example that follows illustrates the described method.

Example 3.1 *Consider the group $G = PSL(2,7)$ represented by means of matrices of $SL(2,7)$ modulo $\{\pm I\}$. Suppose M, A, $B \in G$ are as follows:*

$$M = \begin{bmatrix} 5 & 2 \\ 6 & 4 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Computing the generalized discrete logarithm of matrix M with respect to the generators A and B corresponds to determining the tuple of non-negative integers (i, j, k, ℓ) such that $A^i B^j A^k B^\ell = M$.

The system we encountered earlier becomes:

$$\begin{aligned} 1 + ij + \ell((1+ij)k + i) &= 5 \\ (1+ij)k + i &= 2 \\ j + \ell(jk+1) &= 6 \\ jk + 1 &= 4 \end{aligned}$$

Proposition 3.1 yields $(i, j, k, \ell) = (0, 5, 2, 2)$. Simple matrix multiplication in $\mathbb{Z}_7$ shows that indeed $A^0 B^5 A^2 B^2 = M$.

4 Weak GDLP in $PSL(2,p)$ with respect to any two generators of order p

Suppose now that C and D are any two non-commuting elements of order p in $G = PSL(2,p)$, and that A and B are the matrices defined in the previous section. We have that $G = \langle C, D \rangle$, moreover, by exploiting the fact that G acts doubly transitively by conjugation on the $(p+1)$ p–Sylow subgroups of G, we can efficiently solve the generalized discrete logarithm

problem with respect to the generating tuple (C, D). Thus, for any given $M \in G$ our goal is to determine non-negative integers i, j, k, ℓ such that:

$$M = C^i D^j C^k D^\ell.$$

Let Ω be the collection of all p-Sylow subgroups of G. Then $|\Omega| = p+1$ and if $P \in \Omega$, then $|P| = p$. G has a doubly transitive representation on Ω by conjugation. Thus, the normalizer of $P \in \Omega$, $N_G(P)$, is of order $p(p-1)/2$ and acts transitively on $\Omega \setminus \{P\}$.

Let $P, Q \in \Omega$ and let $g \in G$ such that $P^g = Q$, where $P^g = g^{-1}Pg$. There are in all $p(p-1)/2$ elements $g \in G$ carrying P to Q by conjugation, namely the elements of $N_G(P)g = gN_G(Q)$. 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

$$(\langle C\rangle, \langle D\rangle) = (\langle A\rangle^g, \langle B\rangle^g).$$

Then, C and D may be expressed as follows:

$$C = g^{-1}A^s g \quad D = g^{-1}B^t g$$

for some positive integers $s, t < p$.

To determine an element $g \in G$ such that $\langle A\rangle^g = \langle C\rangle$ and $\langle B\rangle^g = \langle D\rangle$, we proceed as follows. We determine an element $g_1 \in G$ such that $\langle A\rangle^{g_1} = \langle C\rangle$. Then $\langle B\rangle^{g_1} = \langle B_1\rangle$. Now, $N_G(\langle C\rangle)$, acts transitively on $\Omega \setminus \{\langle C\rangle\}$. Therefore, there exists an element $g_2 \in N_G(\langle C\rangle)$, such that $\langle B_1\rangle^{g_2} = \langle D\rangle$. Then, for $g = g_1 g_2$

$$\langle A\rangle^g = (\langle A\rangle^{g_1})^{g_2} = \langle C\rangle^{g_2} = \langle C\rangle, \text{ and}$$

$$\langle B\rangle^g = (\langle B\rangle^{g_1})^{g_2} = \langle B_1\rangle^{g_2} = \langle D\rangle.$$

Note that the element g_2 can be chosen among the p elements of $\langle C\rangle$, i.e., from the centralizer of $\langle C\rangle$, as $\Omega \setminus \{\langle C\rangle\}$ is a single orbit of length p.

If we assume that the element $g \in G$ such that $gCg^{-1} \in \langle A\rangle$ and $gDg^{-1} \in \langle B\rangle$ has been found, then for some positive integers s and t, $A^s = gCg^{-1}$ and $B^t = gDg^{-1}$. On the other hand $A^s = \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}$ and $B^t = \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix}$. Therefore, s is the $(1,2)$ entry of the matrix gCg^{-1} and t is the $(2,1)$ entry of the matrix gDg^{-1}.

Assume that we have computed element g. We may write:

$$M = C^i D^j C^k D^\ell$$

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

Let $x = si$, $y = tj$, $v = sk$ and $w = t\ell$. Then, $M = g^{-1}A^x B^y A^v B^w g$ and hence $gMg^{-1} = A^x B^y A^v B^w$. Denote by $M_1 = gMg^{-1}$. Obviously, $M_1 \in G$ and $M_1 = A^x B^y A^v B^w$. Thus, we have transformed the generalized discrete logarithm problem of $PSL(2,p)$ with respect to C and D to the generalized discrete logarithm problem of $PSL(2,p)$ with respect to A and B which we were able to solve in the previous section. Therefore, since every nonzero element in $\mathbb{Z}_p$ has an inverse, we are able to compute integers i, j, k and ℓ from $i = xs^{-1}$, $j = yt^{-1}$, $k = vs^{-1}$, $\ell = wt^{-1}$ where all operations are performed modulo p.

Note that it can not happen that s or t is equal to zero, due to the fact that $C = g^{-1}A^s g$ and $D = g^{-1}B^t g$. If say $s = 0$, then A^s is the identity matrix and therefore C would also be the identity matrix, which leads to the contradiction that C is matrix of order p. Similarly, $t \neq 0$.

The following example illustrates the algorithm we just described. Computations are performed using the Magma algebra system [1].

Example 4.1 *Suppose that group $G = PSL(2,7)$ is represented by matrices in $SL(2,7)$ up to a factor of $\pm I$. Non-commuting matrices C, D of order $p = 7$ in G are given, as well as $M \in G$:*

$$M = \begin{bmatrix} 3 & 5 \\ 2 & 6 \end{bmatrix} \quad C = \begin{bmatrix} 5 & 1 \\ 5 & 4 \end{bmatrix} \quad D = \begin{bmatrix} 2 & 5 \\ 4 & 0 \end{bmatrix}.$$

Our goal is to compute the generalized discrete logarithm of M with respect to (C,D) i.e., to find nonnegative integers i,j,k,ℓ such that $M = C^i D^j C^k D^\ell$.

We use the matrices $A, B \in G$ which were defined in the previous section. First we find element $g_1 \in G$ such that $\langle A \rangle^{g_1} = \langle C \rangle$. Note that there are in all $p(p-1)/2 = 21$ elements $g_1 \in G$ such that $\langle A \rangle^{g_1} = \langle C \rangle$. These are the elements in $N_G(\langle A \rangle)g_1 = g_1 N_G(\langle C \rangle)$. One of them is $g_1 = \begin{bmatrix} 6 & 1 \\ 2 & 4 \end{bmatrix}$. Next we compute $B_1 = g_1^{-1} B g_1 = \begin{bmatrix} 2 & 6 \\ 1 & 0 \end{bmatrix}$. Element $g_2 = \begin{bmatrix} 2 & 5 \\ 5 & 6 \end{bmatrix}$ from $N_G(\langle C \rangle)$ is such that $\langle B_1 \rangle^{g_2} = \langle D \rangle$. Then, for $g = g_1 g_2 = \begin{bmatrix} 3 & 1 \\ 3 & 6 \end{bmatrix}$ the following holds: $\langle A \rangle^g = \langle C \rangle$ and $\langle B \rangle^g = \langle D \rangle$. Integer s corresponds to

the (1,2) entry in matrix $gCg^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ while integer t corresponds to the (2,1) entry in the matrix $gDg^{-1} = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$. Therefore, $s = 1$ and $t = 2$. So $s^{-1} = 1$ and $t^{-1} = 4$ in arithmetic modulo 7. Finally, $M_1 = gMg^{-1} = \begin{bmatrix} 3 & 3 \\ 1 & 6 \end{bmatrix}$.

We have transformed the generalized discrete logarithm problem to the canonical factorization $PSL(2,7) = \langle A \rangle \langle B \rangle \langle A \rangle \langle B \rangle$. Namely, we now look for integers x, y, v, w such that $M_1 = A^x B^y A^v B^w$. By using proposition 3.1 we obtain $(x, y, v, w) \in \{(0,4,3,3), (1,3,4,2), (2,1,5,0), (3,2,6,1), (5,5,1,4), (6,6,2,5)\}$ and the corresponding generalized discrete logarithms of M with respect to (C, D) are elements of the set $\{(0,2,3,5), (1,5,4,1), (2,4,5,0), (3,1,6,4), (5,6,1,2), (6,3,2,6)\}$.

An element $g \in G = PSL(2,p)$ such that $\langle C \rangle = \langle A \rangle^g$ and $\langle D \rangle = \langle B \rangle^g$ can also be computed by another method. 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 $s, t < p$. Equivalently, we require that $g \in G$ satisfies the following equations: $gC = A^s g$ and $gD = B^t g$, for some non-negative integers $s, t < p$. Since $g = \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix} \in G$, we obtain a system of equations in $g_1, \ldots, g_4$ and s and t from which an element g is determined.

5 Conclusions

We have discussed the tractability of the generalized discrete logarithm problem in the finite non-abelian group $PSL(2,p)$, represented by matrices of $SL(2,p)$ modulo $\{\pm I\}$, with respect to two generators of order p, and have showed that the GDLP is tractable in this setup. Obviously, this group representation together with the mentioned generators is not a good candidate for the design of cryptographic primitives. However, $PSL(2,p)$ can be generated by elements of order different from p. For example, by two elements of order $(p+1)/2$, or $(p-1)/2$. We conjecture that there are such instances where GDLP is intractable.

Acknowledgement

The authors would like to thank Rainer Steinwandt for his valuable comments and suggestions during this research.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. *The Magma algebra system. I. The user language.* J. Symbolic Comput., **24**(3-4)(1997), 235–265.

[2] Lee C. Klingler, Spyros S. Magliveras, Fred Richman, Michal Sramka. *Discrete logarithms for finite groups.* Computing **85**(2009), 3–19.

[3] Alfred Menezes, Paul C. van Oorschot, Scott A. Vanstone. *Handbook of Applied Cryptography* (CRC Press, Boca Raton, New York, London, Tokyo, 1996.)

[4] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM J. on Computing, **26**(5)(1997), 1484–1509.

[5] Michal Sramka, *New Results in Group Theoretic Cryptology*, Ph.D. Dissertatioon (Florida Atlantic University, Boca Raton, 2006.)

[6] Douglas R. Stinson, *Cryptography: Theory and Practice*, 2nd ed, (CRC Press, New York, 2002.)

[7] Michio Suzuki, *Group Theory I* (Springer-Verlag, New York, 1982.)