2018 Czechoslovak Mathematical Journal 10 pp
Online first

THE DISCRETE LOGARITHM PROBLEM OVER PRIME FIELDS: THE SAFE PRIME CASE. THE SMART ATTACK, NON-CANONICAL LIFTS AND LOGARITHMIC DERIVATIVES

Hejmadi Gopalakrishna Gadiyar, Ramanathan Padma, Vellore

Received March 20, 2017. First published February 2, 2018.

Abstract. We connect the discrete logarithm problem over prime fields in the safe prime case to the logarithmic derivative.

Keywords: discrete logarithm; Hensel lift; group extension

MSC 2010: 11A07, 11T71, 11Y16, 14G50, 68Q25, 94A60

1. Introduction

Let a_0 be a primitive root of a prime number $p > 2$. We know that for every $b_0 \in \{1, 2, \ldots, p-1\}$ there exists a unique integer n_p modulo $p-1$ satisfying

$$a_0^{n_p} \equiv b_0 \pmod p. \tag{1.1}$$

n_p is called the discrete logarithm or index of b_0 to the base a_0 modulo p. Given a_0 and b_0 modulo p, finding n_p modulo $(p-1)$ is called the discrete logarithm problem (DLP) over the prime field F_p. The DLP is believed to be computationally difficult if p is a randomly chosen large prime. There are various algorithms to compute the DLP like the baby step—giant step method, Pollard's ϱ-method, Pohlig-Hellman attack and the index calculus method. The Pohlig-Hellman algorithm works in polynomial time if all the prime factors of $p-1$ are 'small'. The other algorithms are exponential or sub-exponential time algorithms, see [6], [15]. There are no known polynomial time algorithms to compute the discrete logarithm for a large prime p. The computational intractability of the DLP is the basis of the famous Diffie-Hellman key exchange protocol which is the first public key cryptographic algorithm, see [5]. Variants of

DOI: 10.21136/CMJ.2018.0128-17

this protocol are used in the Internet security standards provided by IEEE P1363, RFC 2631, ANSI X9.42, NIST etc.

The DLP can be generalized to the multiplicative group of a finite field, elliptic curves and hyperelliptic curves over a finite field. An elliptic curve E modulo a prime p is called anomalous if the number of points on E modulo p is equal to the modulus p. These curves should not be used for cryptographic purpose as there is a linear time algorithm to compute the discrete logarithm on such curves and this was done almost simultaneously by Smart in [21], Semaev in [19], Satoh and Araki in [18]. There are two steps in their attack: The first step is to lift the elliptic curve discrete logarithm problem (ECDLP) modulo p^2 and the second step is to take the p-adic elliptic logarithm.

The aim of this paper is to generalize their argument to the DLP over a prime field. There are two tools we use in which the first is the Teichmüller lifting which we explain now. By Fermat's little theorem we have

$$x_0^p \equiv x_0 \pmod{p} \tag{1.2}$$

for any integer $x_0 \in \{0, 1, 2, \ldots, p-1\}$. We can write this as

$$x_0^p \equiv x_0 + x_1 p \pmod{p^2}. \tag{1.3}$$

Here $x_0 + x_1 p$ is the Teichmüller expansion of x_0 modulo p^2. When $\gcd(x_0, p) = 1$, then

$$(x_0 + x_1 p)^{p-1} \equiv 1 \pmod{p^2}, \tag{1.4}$$

by Euler's theorem of congruences. As $x_1 = (x_0^p - x_0)/p \pmod{p}$, and $x_0^p \pmod{p^2}$ can be computed in polynomial time using the repeated square and multiply algorithm, see [11], one can compute x_1 in polynomial time.

Similarly $x_0^{p^2} \equiv x_0 + x_1 p + x_2 p^2 \pmod{p^3}$ is the Teichmüller expansion of x_0 modulo p^3 and $(x_0 + x_1 p + x_2 p^2)^{p-1} \equiv 1 \pmod{p^3}$ when $\gcd(x_0, p) = 1$. Thus one gets the Teichmüller representative $T(x_0)$ of x_0 as a p-adic integer which is represented by

$$T(x_0) = \lim_{k \to \infty} x_0^{p^k}. \tag{1.5}$$

Note that

$$T(x_0)^{p-1} = 1 \tag{1.6}$$

for any $x_0 \not\equiv 0 \pmod{p}$.

One can also get the Teichmüller expansions using Hensel lifting with the polynomial $f(x) = x^{p-1} - 1$. We will obtain the Teichmüller expansion modulo p^2 as follows. Note that $f'(x) = (p-1)x^{p-2}$ and hence $f'(x_0) \equiv -x_0^{-1} \pmod{p}$, and by Fermat's little theorem $f(x_0) \equiv x_0^{p-1} - 1 \equiv 0 \pmod{p}$ and thus the Hensel lifting $x_0 - f(x_0)/f'(x_0)$ of x_0 gives precisely $x_0 + x_1 p \pmod{p^2}$.

The second tool is the Iwasawa logarithm which is defined as follows. For a p-adic integer $x = x_0 + x_1 p + x_2 p^2 + \ldots$ with $\gcd(x_0, p) = 1$, the Iwasawa logarithm of x is denoted by $\operatorname{Log} x$ and is defined as $(p-1)^{-1} \log x^{p-1}$. Note that the Iwasawa logarithm of the Teichmüller representative satisfies $\operatorname{Log} T(x) = 0$. See [17], [23] and [22] for these two topics.

In [8] the authors lifted the DLP (1.1) modulo p^2. This is got by raising both sides of (1.1) to the power p:

$$a_0^{n_p p} \equiv b_0^p \pmod{p^2}, \tag{1.7}$$

which can be written with the notation used in (1.3) as

$$(a_0 + a_1 p)^{n_p} \equiv b_0 + b_1 p \pmod{p^2}. \tag{1.8}$$

Finding the Iwasawa logarithm of both sides of this equation modulo p^2 is the same as raising both sides by $p-1$. Unfortunately both sides become 1 modulo p^2 by (1.4) and we could not find n_p but a formula

$$n_p \equiv \frac{(b_1 - \beta_{n_p})/b_0}{a_1/a_0} \pmod{p} \tag{1.9}$$

was obtained where β_{n_p} is the carry

$$a_0^{n_p} \equiv b_0 + \beta_{n_p} p \pmod{p^2}. \tag{1.10}$$

Kontsevich in [12] and Riesel in [16] point out that the difficulty arises because the problem is stated modulo p and the solution is needed modulo $p-1$. Hence we go to the discrete logarithm problem modulo the composite modulus $p(p-1)$. In this connection, see Bach [1].

In this paper we consider primes p of the form $2q+1$ where q is a prime number. Prime p is called a safe prime as it is believed that the discrete logarithm problem is computationally difficult in this case when p is 'large'. In order to explain our attack, a few lemmas are required which we state and prove in Section 2 and give the main idea in Section 3.

2. Lemmas

We need some definitions and notation before we prove our lemmas. In [14] Lerch defined the Fermat quotient for a composite modulus. Let x be such that $\gcd(x,n)=1$. Then $q(x)$ defined by

$$x^{\varphi(n)} \equiv 1 + q(x)n \pmod{n^2} \tag{2.1}$$

is called the Fermat quotient of x modulo n. We replace Euler's φ-function by Carmichael's λ function. The $\lambda(n)$ is defined as follows (see [4], [3]): $\lambda(1)=1$, $\lambda(2)=1$, $\lambda(4)=2$ and

$$\lambda(n) = \begin{cases} \varphi(P^r) & \text{if } n = P^r, \\ 2^{r-2} & \text{if } n = 2^r,\ r \geqslant 3, \\ \operatorname{lcm}(\lambda(p_1^{r_1}), \lambda(p_2^{r_2}), \ldots, \lambda(p_k^{r_k})) & \text{if } n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}, \end{cases} \tag{2.2}$$

where $P > 2$, $p_1, \ldots, p_k$ are primes.

With our assumptions on p and q, $\varphi(p^2q^2) = 2pq^2\varphi(q)$ and $\lambda(p^2q^2) = pq\varphi(q)$. In other words the order of the group of units modulo p^2q^2 is $\varphi(p^2q^2)$ whereas $\lambda(p^2q^2)$ is the order of the largest cyclic group modulo p^2q^2. Hence we define $Q(x)$ by the congruence

$$x^{\lambda(p^2q^2)} \equiv x^{pq\varphi(q)} \equiv 1 + Q(x)p^2q^2 \pmod{p^3q^3}. \tag{2.3}$$

Lemma 1. *Let a_0 be a primitive root of p and q. Let $\gcd(b_0,q)=1$. Then the congruence $a_0^{n_p} \equiv b_0 \pmod p$ can be extended to*

$$a_0^n \equiv b_0 \pmod{pq} \tag{2.4}$$

if and only if the Legendre symbols satisfy

$$\left(\frac{b_0}{p}\right) = \left(\frac{b_0}{q}\right). \tag{2.5}$$

P r o o f. $a_0^n \equiv b_0 \pmod{pq}$ if and only if

$$a_0^n \equiv a_0^{n_p} \equiv b_0 \pmod p \quad \text{and}$$
$$a_0^n \equiv a_0^{n_q} \equiv b_0 \pmod q.$$

This happens if and only if

$$n \equiv n_p \pmod{p-1} \quad \text{and} \tag{2.6}$$
$$n \equiv n_q \pmod{q-1}. \tag{2.7}$$

This is possible if and only if

$$2 = \gcd(p-1, q-1) \mid n_p - n_q, \tag{2.8}$$

where we have used the Chinese remainder theorem when the moduli are not relatively prime, see [13]. That is

$$n_p \equiv n_q \pmod 2. \tag{2.9}$$

In other words b_0 is a quadratic residue or nonresidue modulo p and q simultaneously. That is $\left(\frac{b_0}{p}\right) = \left(\frac{b_0}{q}\right)$. □

Lemma 2. *Let $a_0^n \equiv b_0 \pmod{pq}$. Then the Teichmüller lifts of a_0 and b_0 modulo p^2q^2 are $a_0 + a_1 pq$ and $b_0 + b_1 pq$ modulo p^2q^2, respectively, and satisfy*

$$(a_0 + a_1 pq)^n \equiv b_0 + b_1 pq \pmod{p^2q^2}, \tag{2.10}$$

where

$$a_1 = -\frac{Q(a_0)a_0}{\varphi(q)} \pmod{pq} \quad \text{and} \quad b_1 = -\frac{Q(b_0)b_0}{\varphi(q)} \pmod{pq}. \tag{2.11}$$

Proof. We want a_1 and b_1 to satisfy (2.11). Using the carry notation

$$a_0^n \equiv b_0 + \beta_n pq \pmod{p^2q^2} \tag{2.12}$$

in (2.10) and expanding using the binomial theorem we get the equation

$$\beta_n + n\frac{b_0}{a_0}a_1 \equiv b_1 \pmod{pq}. \tag{2.13}$$

Taking the power $pq\varphi(q)$ on both sides of (2.12) yields

$$a_0^{npq\varphi(q)} \equiv (b_0 + \beta_n pq)^{pq\varphi(q)} \pmod{p^3q^3} \tag{2.14}$$

and using (2.3) we get

$$nQ(a_0) \equiv Q(b_0) + \frac{\beta_n}{b_0}\varphi(q) \pmod{pq}. \tag{2.15}$$

Comparing (2.13) and (2.15) gives the desired values of a_1 and b_1. □

Remarks.

(1) Note that a_1, b_1 and the Legendre symbols in (2.5) can be computed in polynomial time.

(2) The order of $(a_0 + a_1pq)$ is $q\varphi(q)$ modulo p^2q^2.

(3) We are given b_0 mod p. If (2.5) fails for the given b_0 then we can do one of the following:

(i) We can check the same for $b_0 + kp$ for $k = 1, 2, 3, \ldots$ until the condition is satisfied or we can multiply b_0 by a_0^k for some k and check the condition. In the first case n_p does not change and in the second case n_p becomes $n_p + k$ modulo $p - 1$.

(ii) We can take b_0^2 mod pq and consider the new discrete logarithm problem

$$a_0^n \equiv b_0^2 \pmod{pq}. \tag{2.16}$$

(iii) We can even relax the conditions in Lemma 1 as in our earlier preprint [7] as follows. Let $\gcd(a_0, q) = 1$ and $\gcd(b_0, q) = 1$. Let a_0 be a primitive root of p and let a_0 and b_0 satisfy $a_0^n \equiv b_0 \pmod{p}$. Then it is easy to see that

$$a_0^{n\varphi(q)} \equiv b_0^{\varphi(q)} \pmod{pq}. \tag{2.17}$$

3. Main idea: non-canonical lifts

From (1.1) and with the assumptions made in Lemma 1 we can go to the discrete logarithm problem

$$a_0^n \equiv b_0 \pmod{pq}. \tag{3.1}$$

Here a_0 generates a subgroup of order $q\varphi(q)$ modulo pq. From Lemma 2 we get

$$(a_0 + a_1pq)^n \equiv b_0 + b_1pq \pmod{p^2q^2}. \tag{3.2}$$

The order of the group generated by $a_0 + a_1pq$ modulo p^2q^2 is again $q\varphi(q)$. Also

$$(a_0 + a_1pq)^{q\varphi(q)} \equiv 1 \pmod{p^2q^3}. \tag{3.3}$$

Expanding (3.2) using the binomial theorem, we get

$$a_0^n + na_0^{n-1}a_1pq \equiv b_0 + b_1pq \pmod{p^2q^2}. \tag{3.4}$$

Writing

$$a_0^n \equiv b_0 + \beta_n pq \pmod{p^2q^2} \tag{3.5}$$

gives

$$\beta_n + n\frac{b_0}{a_0}a_1 \equiv b_1 \pmod{pq}. \tag{3.6}$$

Here β_n is the carry of a_0^n modulo p^2q^2; note that n and β_n are the two unknowns in the above linear congruence.

The summary of what we have done so far is that there are three problems when we try to solve the DLP modulo p:

(1) The problem is given modulo p and the solution is needed modulo $p-1$.
(2) The Iwasawa logarithm of the Teichmüller representative is 0.
(3) The binomial theorem on the Teichmüller expansion modulo p^2 gives 'carry'.

We overcome the first problem by going to a DLP modulo pq. The fact that we cannot get n arises from two possibilities being blocked as in the modulo p case. The analogue of the Teichmüller lift modulo p^2q^2 does not have a nonzero logarithm (see (3.3)) and if the binomial theorem is used, a carry occurs as in the case of mod p, see (3.6).

However, if we can construct a non-canonical lift modulo p^2q^2 then the problems dissolve. Thus solving the discrete logarithm problem is equivalent to the construction of a non-canonical lift.

Non-canonical lifts exist and can be written in the form

$$(a_0 + (a_1 + k)pq)^n \equiv b_0 + (b_1 + l)pq \pmod{p^2q^2}. \tag{3.7}$$

When $k = k_1p$ for some $k_1 \not\equiv 0 \bmod q$, then $l = l_1p$ for some $l_1 \bmod q$. In this case the order of the group is $q\varphi(q)$. For the other $k \not\equiv 0$ and l modulo pq the order of the group will be $pq\varphi(q)$. On expanding (3.7) using the binomial theorem, one gets

$$(a_0 + a_1pq)^n + n(a_0 + a_1pq)^{n-1}kpq \equiv (b_0 + b_1pq) + l\ pq \pmod{p^2q^2} \tag{3.8}$$

and using (3.2) we get

$$n \equiv \frac{l_1/b_0}{k_1/a_0} \pmod{q} \tag{3.9}$$

in the first case and

$$n \equiv \frac{l/b_0}{k/a_0} \pmod{pq} \tag{3.10}$$

in the second case.

If we use the notation da_0 for k_1 and db_0 for l_1 then

$$n \equiv \frac{db_0/b_0}{da_0/a_0} \pmod{q} \tag{3.11}$$

and if we use the notation da_0 for k and db_0 for l then

$$n \equiv \frac{db_0/b_0}{da_0/a_0} \pmod{pq}. \tag{3.12}$$

Thus n can be thought of as the logarithmic derivative. The non-canonical extensions (modulo p^2q^2) of the subgroup generated by $a_0 \pmod{pq}$ are labeled by da_0. As $p = 2q+1$, once we get $n \pmod{q}$, $n \pmod{p-1}$ would be either n or $n+q \pmod{p-1}$ which can be checked in polynomial time.

Note that we can get (3.9) and (3.10) by raising (3.7) to the powers $q\varphi(q)$ and $pq\varphi(q)$, respectively. In the second case we get

$$\big((a_0 + (a_1 + k)pq)^{pq\varphi(q)}\big)^n \equiv (b_0 + (b_1 + l)pq)^{pq\varphi(q)} \pmod{p^3q^3}, \tag{3.13}$$

which on expanding and using the notation in Section 2 gives

$$\begin{aligned} 1 + n\Big(q(a_0) + \frac{(a_1 + k)}{a_0}\varphi(q)\Big)p^2q^2 \\ \equiv 1 + \Big(q(b_0) + \frac{(b_1 + l)}{b_0}\varphi(q)\Big)p^2q^2 \pmod{p^3q^3}. \end{aligned} \tag{3.14}$$

Using the formula for a_1 and b_1 one gets (3.10). This way of getting n is analogous to the attack on anomalous elliptic curves by Smart in [21], Semaev in [19], Satoh and Araki in [18].

Remark. If we consider the DLP (2.17) given in Remark 5, then the formulae corresponding to (3.11) and (3.12) would be

$$n \equiv \frac{db_0}{da_0} \pmod{q} \tag{3.15}$$

and

$$n \equiv \frac{db_0/b_0^{\varphi(q)}}{da_0/a_0^{\varphi(q)}} \pmod{pq}. \tag{3.16}$$

We would like to comment that derivatives of numbers have been studied historically for a long time starting from Kummer, see [9], [24], Weil (expanded by Kawada) in [10] and more recently by Buium in [2]. Hence the problem which is standing in isolation being studied only by cryptologists gets connected to mainstream algebra and number theory.

4. Conclusion

When $p = 2q + 1$ where p and $q > 2$ are primes, the Euler function $\varphi(p^2q^2) = 2pq^2\varphi(q)$ and the Carmichael function $\lambda(p^2q^2) = pq\varphi(q)$ are not equal. Also $\lambda(p^2q^2) \mid \varphi(p^2q^2)$ and hence many non-canonical lifts exist. As is well known this would involve a suitable choice of the polynomial for lifting. Recall that the polynomials are $x^{p-1} - 1$ and $x^{pq\varphi(q)} - 1$ in the cases of Teichmüller lifting modulo p^2 and p^2q^2, respectively. This attack can be generalized to ECDLP over prime fields where q will be connected to the order of the group. See [20] for various ways of lifting the elliptic curve discrete logarithm problem.

Acknowledgement. We are grateful to the anonymous referee for giving valuable suggestions on how to reorganize the paper and improve the presentation of the ideas. We gratefully acknowledge Professor M. S. Rangachari for constant encouragement. We thank Dr. G. V. Ramanan (Sura Systems Private Limited) for some useful discussions. We would like to thank our friends Professors A. Lakshminarayan (IIT Madras), A. Sankaranarayanan (TIFR, Mumbai) and K. Srinivas (IMSc, Chennai) for making available innumerable papers and books. We dedicate this paper to the memory of two people who have influenced us personally: The late Dr. S. Ramanathan, musician and musicologist, emphasized the importance of classical scholarship and studying original sources. The second author is his daughter and the first author is his son-in-law. The other influence is the late K. R. Baliga who had served as a Joint Secretary in the Ministry of Defence, Government of India, who brought up the first author and emphasized the importance of national security as a motivation for academics.

References

[1] *E. Bach*: Discrete Logarithms and Factoring. University of California, Computer Science Division, Berkeley, 1984.

[2] *A. Buium*: Arithmetic analogues of derivations. J. Algebra *198* (1997), 290–299. zbl MR doi

[3] *P. J. Cameron, D. A. Preece*: Primitive Lambda-Roots. Available at `https://cameroncounts.files.wordpress.com/2014/01/plr1.pdf`, 2014.

[4] *R. D. Carmichael*: The Theory of Numbers. Wiley & Sons, New York, 1914. zbl

[5] *W. Diffie, M. E. Hellman*: New directions in cryptography. IEEE Trans. Inf. Theory *22* (1976), 644–654. zbl MR doi

[6] *S. Goldwasser*: New directions in cryptography: twenty some years later (or cryptography and complexity theory: a match made in heaven). Proc. of the 38th Annual IEEE Symposium on Foundations of Computer Science, Foundations of Computer Science. 1997, pp. 314–324. doi

[7] *H. Gopalakrishna Gadiyar, R. Padma*: The discrete logarithm problem over prime fields can be transformed to a linear multivariable Chinese remainder theorem. Available at ArXiv: 1608.07032v1 [math.NT] (2016).

[8] *H. Gopalkrishna Gadiyar, K. M. S Sangeeta Maini, R. Padma*: Cryptography, connections, cocycles and crystals: a p-adic exploration of the discrete logarithm problem. Progress in Cryptology—INDOCRYPT 2004, 5th International Conf. on Cryptology in India, Chennai, 2004, (A. Canteaut et al., eds.). Lecture Notes in Comput. Sci. 3348 Springer, Berlin, 2004, pp. 305–314. zbl MR doi
[9] *D. Hilbert*: The Theory of Algebraic Number Fields. Springer, Berlin, 1998. zbl MR doi
[10] *Y. Kawada*: On the derivations in number fields. Ann. Math. (2) *54* (1951), 302–314. zbl MR doi
[11] *N. Koblitz*: A Course in Number Theory and Cryptography. Graduate Texts in Mathematics 114, Springer, New York, 1994. zbl MR doi
[12] *M. Kontsevich*: The $1\frac{1}{2}$-logarithm. Appendix to: On poly(ana)logs. I [Compositio Math. *130* (2002), 161–210] by P. Elbaz-Vincent and H. Gangl. Compositio Math. *130* (2002), 211–214. MR
[13] *R. Kumanduri, C. Romero*: Number Theory with Computer Applications. Prentice Hall, Upper Saddle River, 1998. zbl
[14] *M. Lerch*: Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$. Math. Ann. *60* (1905), 471–490. (In German.) zbl MR doi
[15] *K. S. McCurley*: The discrete logarithm problem. Cryptology and Computational Number Theory. Lect. Notes AMS Short Course 1989, Proc. Symp. Appl. Math. 42, 1990, pp. 49–74. zbl MR doi
[16] *H. Riesel*: Some soluble cases of the discrete logarithm problem. BIT *28* (1988), 839–851. zbl MR doi
[17] *A. M. Robert*: A Course in p-adic Analysis. Graduate Texts in Mathematics 198, Springer, New York, 2000. zbl MR doi
[18] *T. Satoh, K. Araki*: Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Comment. Math. Univ. St. Pauli *47* (1998), 81–92. zbl MR
[19] *I. A. Semaev*: Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. Math. Comput. *67* (1998), 353–356. zbl MR doi
[20] *J. H. Silverman*: Lifting and elliptic curve discrete logarithms. Selected Areas in Cryptography. Proc. of 15th International Workshop on Selected Areas in Cryptography, Sackville, 2008, Lecture Notes in Computer Science 5381 (R. M. Avanzi et al., eds.). Springer, Berlin, 2009, pp. 82–102. zbl doi
[21] *N. P. Smart*: The discrete logarithm problem on elliptic curves of trace one. J. Cryptology *12* (1999), 193–196. zbl MR doi
[22] *O. Teichmüller*: Diskret bewertete perfekte Körper mit unvollkommenem Restklassenkörper. J. Reine Angew. Math. *176* (1936), 141–152. (In German.) zbl MR doi
[23] *O. Teichmüller*: Über die Struktur diskret bewerteter perfekter Körper. Nachr. Ges. Wiss. Göttingen, math.-phys. Kl., FG 1, Neue Folge *1* (1936), 151–161. (In German.) zbl
[24] *L. C. Washington*: Introduction to Cyclotomic Fields. Graduate Texts in Mathematics 83, Springer, New York, 1997. zbl MR doi

Authors' address: Hejmadi Gopalakrishna Gadiyar, Ramanathan Padma, Department of Mathematics, School of Advanced Sciences, Vellore Institute of Technology, Near Katpadi Road, Vellore 632014, Tamil Nadu, India, e-mail: `gadiyar@vit.ac.in`, `rpadma@vit.ac.in`.