SCIENCE CHINA
Information Sciences

• LETTER •

September 2019, Vol. 62 199501:1–199501:3
https://doi.org/10.1007/s11432-017-9700-7

A faster method to compute primitive elements and discrete logarithms of factor base in Artin-Schreier extensions

Dianyan XIAO[1*] & Qi CHENG[2]

[1]*Institute for Advanced Study, Tsinghua University, Beijing* 100084, *China;*
[2]*School of Computer Science, University of Oklahoma, Norman* OK 73019, *USA*

Received 30 August 2018/Revised 12 October 2018/Accepted 21 November 2018/Published online 30 July 2019

Citation Xiao D Y, Cheng Q. A faster method to compute primitive elements and discrete logarithms of factor base in Artin-Schreier extensions. Sci China Inf Sci, 2019, 62(9): 199501, https://doi.org/10.1007/s11432-017-9700-7

Dear editor,

The discrete logarithm problem is a classical problem in mathematics and widely used in cryptography [1–4]. The pre-computation of discrete logarithms of factor base is a crucial and extremely expensive step in many algorithms solving discrete logarithms. In finite fields of small characteristics, one can use the Möbius transformations and the Frobenius endomorphism to generate relations between elements of factor base [5]. To improve the efficiency, it is interesting to find a subset of transformations sufficient to recover the discrete logarithms of factor base, especially in special fields. In this study, we focus on the Artin-Schreier extension $K = \mathbb{F}_{p^2}[x]/(x^p - x - 1)$ for prime p. We prove that the linear system of degenerate relations derived from transformations in the Borel set is not sufficient to compute the logarithms of factor base. We use a subset of non-degenerate relations to recover the logarithms of factor base, which reduces the heuristic complexity from $O(p^6)$ [6] to $\tilde{O}(p^\omega)$ where $\omega \leqslant 2.38$ is the matrix multiplication exponent over a ring. Our algorithm does not depend on the heuristic of smooth numbers, and it will find a primitive element of multiplicative group K^*. We base the correctness of our algorithm on a heuristic which has been verified for finite fields of size within 10000 bits.

Preliminaries. The Artin-Schreier extension is modeled as $K = \mathbb{F}_{p^2}[x]/(x^p - x - 1)$, where $\mathbb{F}_{p^2}$ is a quadratic extension of prime field $\mathbb{F}_p$. Denote by $\eta \in \mathbb{F}_p$ a quadratic non-residue of $\mathbb{F}_p$ and by $g \in \mathbb{F}_{p^2}$ a square root of η. It is noted that $g^p = -g$ since the minimal polynomial of g is $x^2 - \eta$. Also, for any $u \in \mathbb{F}_{p^2}$, we can represent u as $u = u_1 + u_2 g$ where $u_1, u_2 \in \mathbb{F}_p$ are unique. It is easy to find such a pair (η, g) and express all elements of $\mathbb{F}_{p^2}$ in the form $u_1 + u_2 g$ with $u_1, u_2 \in \mathbb{F}_p$. We denote by ζ a $(p+1)$-th primitive root of unity in $\mathbb{F}_{p^2}$, and by $\zeta_\alpha \in \mathbb{F}_{p^2}$ an arbitrary $(p+1)$-th root of $\alpha \in \mathbb{F}_p^*$. The complexity of algorithms is estimated by the number of arithmetic operations in $\mathbb{Z}/(p^{2p} - 1)\mathbb{Z}$, or rings of similar sizes.

Assume that ρ is a primitive generator of the multiplicative group K^*. For arbitrary $u \in \mathbb{F}_{p^2}^*$, we have

$$u^{p^2-1} = 1 \Rightarrow \left(1 + p^2 + \cdots + p^{2(p-1)}\right) | \log_\rho u.$$

Exploiting the Pohlig-Hellman technique [7], we can obtain the logarithms of elements in K^* by solving the problem in $\mathbb{F}_{p^2}^*$ and $K^*/\mathbb{F}_{p^2}^*$ separately. Because the logarithms of elements in $\mathbb{F}_{p^2}^*$ are quite easy to calculate, we focus on the problem in the subgroup $K^*/\mathbb{F}_{p^2}^*$ and set $\log u = 0$ for any $u \in \mathbb{F}_{p^2}^*$ in the rest of the study. We note that the logarithms of elements in $K^*/\mathbb{F}_{p^2}^*$ lie in $\mathbb{Z}/N\mathbb{Z}$ where $N = 1 + p^2 + \cdots + p^{2(p-1)}$.

* Corresponding author (email: xiaody12@mails.tsinghua.edu.cn)

After operating the Möbius transformation $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_{p^2})$ to the identity $x^p - x = \prod_{\alpha\in\mathbb{F}_p}(x+\alpha)$, we obtain

$$\left(\frac{ax+b}{cx+d}\right)^p - \frac{ax+b}{cx+d} = \prod_{\alpha\in\mathbb{F}_p}\left(\frac{ax+b}{cx+d}+\alpha\right).$$

Let $X = x \bmod (x^p - x - 1)$, then

$$\begin{aligned} &AX^2 + BX + C \\ &\quad\equiv (cX+d)\prod_{\alpha\in\mathbb{F}_p}[(a+\alpha c)X + (b+\alpha d)], \end{aligned} \tag{1}$$

where $A = a^pc - ac^p$, $B = a^pc - ac^p + b^pc - bc^p + a^pd - ad^p$, and $C = a^pd - bc^p + b^pd - bd^p$. Apparently, transformations in the same coset of $\mathrm{PGL}_2(\mathbb{F}_{p^2})/\mathrm{PGL}_2(\mathbb{F}_p)$ derive equivalent relations. We call these relations with $a^pc - ac^p = 0$ degenerate and those with $a^pc - ac^p \neq 0$ non-degenerate.

The Frobenius endomorphism of K leads to the relations:

$$(X+\mu_1 g+\mu_2)^{p^i} = \begin{cases} X+\mu_1 g+\mu_2+i, & \text{if } 2 \mid i; \\ X-\mu_1 g+\mu_2+i, & \text{if } 2 \nmid i, \end{cases} \tag{2}$$

for arbitrary $\mu = \mu_1 + \mu_2 g \in \mathbb{F}_{p^2}$.

By taking logarithms on both sides of (1) and (2), we may obtain a linear system to recover the discrete logarithms of factor base.

The linear system of degenerate relations. The degenerate relations, where $a^qc - ac^q = 0$, are derived from transformations in the Borel subgroup

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a,b,d \in \mathbb{F}_{p^2},\ ad \neq 0 \right\}.$$

We claim that the linear system of relations generated by transformations in the Borel subgroup holds a kernel of dimension $\geqslant \frac{p-3}{4}$.

Theorem 1. Given $K = \mathbb{F}_{p^2}[x]/(x^p - x - 1)$, the linear system generated by the degenerated relations of (1) where $a^qc - ac^q = 0$ and the Frobenius relation (2) holds a kernel of dimension $\geqslant \frac{p-3}{4}$. That is, these relations generated by transformations in the Borel subgroup and the Frobenius endomorphism are not sufficient to recover the discrete logarithms of linear factor in subgroup $K^*/\mathbb{F}_{p^2}^*$.

The proof of Theorem 1 is given in Appendix A.

Remark 1. Theorem 1 shows that the case of Artin-Schreier extensions is quite different with that of Kummer case [8].

Computing the primitive root and the DLs of linear factor base. We apply the Möbius transformation with $a^{p+1} \neq c^{p+1}$ to the identity $x^{p+1} - 1 = \prod_{k=0}^{p}(x - \zeta^k)$, then we get that over K,

$$\begin{aligned} &X^2 + (1+t+t^p)X + t + t^{p+1} - s^{p+1} \\ &\quad = \prod_{k=0}^{p}(X + t - \zeta^k s), \end{aligned} \tag{3}$$

where

$$t = \frac{a^pb - c^pd}{a^{p+1} - c^{p+1}}, \quad s = \frac{ad - bc}{a^{p+1} - c^{p+1}}.$$

Actually, the relation is determined by (t, s^{p+1}) which goes though $\mathbb{F}_{p^2} \times \mathbb{F}_p$.

With consideration of the Frobenius endomorphism, it can be verified directly that the relation determined by (t, s^{p+1}) is equivalent to the one determined by $(t+\alpha, s^{p+1})$ for arbitrary $\alpha \in \mathbb{F}_p$. Therefore, we can obtain Lemma 1.

Lemma 1. In Artin-Schreier extension modeled above, the linear system with all non-degenerate relations can be obtained by operating the Möbius transformations of

$$\left\{ \begin{pmatrix} 1 & \beta g \\ 0 & \zeta_\alpha \end{pmatrix} \middle| \beta \in \mathbb{F}_p,\ \zeta_\alpha^{p+1} = \alpha \in \mathbb{F}_p^* \right\},$$

and the Frobenius endomorphism to x in the identity,

$$x^{p+1} - 1 = \prod_{k=0}^{p}(x + \zeta^k).$$

Remark 2. Lemma 1 describes the representative transformations that generate the linear algebra of non-degenerate relations. If we move to the identity factorization of $x^p - x$, then the representative set of transformations will be

$$\left\{ \begin{pmatrix} v & 1 \\ 1 & v \end{pmatrix} \begin{pmatrix} 1 & \beta g \\ 0 & \zeta_\alpha \end{pmatrix} \middle| \beta \in \mathbb{F}_p, \alpha \in \mathbb{F}_p^* \right\},$$

where $v(\neq \pm 1)$ is an arbitrary $(p+1)$-th root of 1.

According to Lemma 1, the linear system of non-degenerate relations is

$$\begin{aligned} &\log(X^2 + X + \beta g - \beta^2 g^2 - \alpha) \\ &\quad = \sum_{k=0}^{p} \log(X + \beta g + \zeta^k \zeta_\alpha) \end{aligned} \tag{4}$$

with $\beta \in \mathbb{F}_p$. Since we attempt to find relations between discrete logarithms of linear factors, it is required that the polynomial at LHS is reducible. Let

$$X^2 + X + \beta g - \beta^2 g^2 - \alpha = (X + \mu g + \nu + 1)(X - \mu g - \nu)$$

for $\mu, \nu \in \mathbb{F}_p$, then we get

$$\begin{cases} \beta = -\mu(2\nu + 1), \\ \alpha = \mu^2 g^2 - \beta^2 g^2 + \nu^2 + \nu. \end{cases}$$

We only require p linear independent relations to recover the discrete logarithms of linear factor that are not conjugate, and then compute the remaining logarithms through the Frobenius relations. The point is how to select p pairs of (μ_i, ν_i) or (β_i, α_i) for $i = 0, \ldots, p-1$ such that their corresponding relations constitute a linear system with 1-dimensional kernel.

We set $\nu = 1$, μ runs over $\mathbb{F}_p$, and multiply p at both sides of (4). We obtain that

$$\begin{aligned}&\log(X + \mu g) + \log(X - \mu g + 3)\\ &= \sum_{k=0}^{p} \log(X + 3\mu g + 1 + \zeta^k \zeta_{\hat{\alpha}}),\end{aligned} \tag{5}$$

where $\hat{\alpha} = -8\mu^2 g^2 + 2$. We can use (2) to reduce the number of variables to p.

It can be verified numerically that for those $p < 599$, the kernel of linear system (5) is 1-dimensional over $\mathbb{Z}/N'\mathbb{Z}$ where N' is the composite of large factors. Therefore, we make Heuristic 1.

Heuristic 1.

$$\dim(\ker \text{System (5)}) = 1 \quad \text{over } \mathbb{Z}/N'\mathbb{Z},$$

with $N' \mid N$ and N' is free of factors $\leqslant p^2$.

Exploiting Pohlig-Hellman technique, we can construct a method to recover the linear factor discrete logarithms under Heuristic 1.

The experimental evidence of Heuristic 1 is given in Appendix B.

Proposition 1. Assume that Heuristic 1 holds. There exists an algorithm with cost $\tilde{O}(p^\omega)$ that computes the discrete logarithms of linear factors modulo N, and a primitive element of $K^*/\mathbb{F}_{p^2}^*$. Here $\omega \leqslant 2.38$ is the exponent parameter of fast matrix multiplication over rings.

The proof of Proposition 1 is given in Appendix C.

Conclusion and Future work. We focus on the pre-computation of discrete logarithms over Artin-Schreier extensions: the factor base logarithms. We developed an efficient algorithm to compute the discrete logarithms of linear factor base together with a primitive element, based on a convincing heuristic.

There are still a few problems we have not work out. Our heuristic seems solid from the experimental aspect. However, a theoretical proof would be more encouraging if one can exploit the special structures of the linear algebra in our algorithm. Another issue is that whether there exist more efficient techniques for the descent phase, which would perfect the whole algorithm for discrete logarithm problems over Artin-Schreier extension. We leave it to the future work.

Acknowledgements This work was partially supported by National Key Research and Development Program of China (Grant No. 2017YFA0303903), National Natural Science Foundation of China (Grant No. 61502269), and National Science Foundation of the United States (Grant No. CCF-1409294).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inform Theory, 1976, 22: 644–654
2 ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. In: Proceedings of Workshop on the Theory and Application of Cryptographic Techniques, 1984
3 Koblitz N. Elliptic curve cryptosystems. Math Comput, 1987, 48: 203–209
4 Wang L L, Chen K F, Long Y, et al. An efficient pairing-free certificateless signature scheme for resource-limited systems. Sci China Inf Sci, 2017, 60: 119102
5 Joux A. A new index calculus algorithm with complexity $L(1/4+o(1))$ in small characteristic. In: Proceedings of International Conference on Selected Areas in Cryptography, 2013
6 Joux A, Pierrot C. Improving the polynomial time precomputation of Frobenius representation discrete logarithm algorithms – simplified setting for small characteristic finite fields. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2014
7 Pohlig S, Hellman M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Trans Inform Theory, 1978, 24: 106–110
8 Xiao D Y, Zhuang J C, Cheng Q. Factor base discrete logarithms in Kummer extensions. Finite Fields Theiry Appl, 2018, 53: 205–225