SCIENCE CHINA
Information Sciences

• **Supplementary File** •

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

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

[1]*Tsinghua University, Beijing* 100084*, China;*
[2]*University of Oklahoma, Norman, OK* 73019*, USA*

Appendix A Proof of Theorem 1

Denote by σ the Frobenius endomorphism of K:

$$\sigma(f(X)) = (f(X))^p, \forall f(X) \in K,$$

and by $\tau = \sigma^2$, a generator of the Galois group $\mathrm{Gal}(K/\mathbb{F}_{p^2})$. For arbitrary $f(X) \in K^*$, we have

$$\tau^i(f(X)) = (f(X))^{p^{2i}} = f(X + 2i),$$

for $i = 0, 1, \cdots, p-1$. Particularly, when f is monic and linear, the Frobenius relations are

$$(X + u)^{p^{2i}} = X + u + 2i. \tag{A1}$$

We define the *orbit* of an element $f \in K^*$ as

$$\mathbf{O}_f = \{\tau^i(f) \mid i = 0, 1, \cdots, p-1\}.$$

Given an orbit $\mathbf{O}_f$, we call f a *representative* of the orbit. For any $f' \in \mathbf{O}_f$, we define the *relative distance* from f' to f as the smallest integer t such that $f'(X) = \tau^t(f(X))$.

It is easy to verify that $\mathbf{O}_{X+\theta g} = \{X + \theta g + \alpha \mid \alpha \in \mathbb{F}_p\}$. Let $\mathcal{B}_1$ be the set of all monic linear elements of K^*, and we have

$$\mathcal{B}_1 = \dot{\cup}_{\theta \in \mathbb{F}_p} \mathbf{O}_{X+\theta g}$$

where $\dot{\cup}$ is the union of disjoint sets. For arbitrary $X + u' \in \mathbf{O}_{X+u}$ where $u, u' \in \mathbb{F}_{p^2}$, we can compute the relative distance $dist = h(u' - u)$ where $h(\alpha) = \frac{\alpha}{2} \bmod p$ for $\alpha \in \mathbb{F}_p$ and $h(\alpha) = 0, 1, \cdots, p-1$.

According to [3, 4, 5], we can write the representatives of these degenerate transformations in $\mathrm{PGL}_2(\mathbb{F}_{p^2})/\mathrm{PGL}_2(\mathbb{F}_p)$ as

$$\left\{ \begin{pmatrix} a & g \\ 0 & 1 \end{pmatrix} | a \in \mathbb{F}_{p^2}^* \right\} \bigcup \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} | a \in \mathbb{F}_{p^2}^* \setminus \mathbb{F}_p^* \right\}.$$

Thus we can obtain the following two corresponding linear systems respectively:

$$\log((a^p - a)X + a^p + g^p - g) = \sum_{\alpha \in \mathbb{F}_p} \log(aX + g + \alpha), \forall a \in \mathbb{F}_{q^2}, \tag{**I**}$$

$$\log((a^p - a)X + a^p) = \sum_{\alpha \in \mathbb{F}_p} \log(aX + \alpha), \forall a \in \mathbb{F}_{q^2}. \tag{**II**}$$

we have the following lemma for these two linear systems.

Lemma 1. In the Artin-Schreier extension, the linear system of all degenerate relations can be obtained by operating the Möbius transformations of $\left\{ \begin{pmatrix} g + \beta & 0 \\ 0 & 1 \end{pmatrix} \mid \beta \in \mathbb{F}_p \right\}$ and the Frobenius endomorphism over the identity

$$x^p - x = \prod_{\alpha \in \mathbb{F}_p} (x + \alpha).$$

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

Proof. Note that $\left\{\begin{pmatrix} g+\beta & 0 \\ 0 & 1 \end{pmatrix} \mid \beta \in \mathbb{F}_p\right\}$ is a set of representatives of $\left\{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} | a \in \mathbb{F}^*_{p^2} \setminus \mathbb{F}^*_p\right\}$. All we need is to prove that the linear systems (**I**) and **(II)** defined above are equivalent.

We observe that the subset $\left\{\begin{pmatrix} \alpha' & g \\ 0 & 1 \end{pmatrix} | \alpha' \in \mathbb{F}^*_p\right\}$ of $\left\{\begin{pmatrix} a & g \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_{p^2}\right\}$ produces trivial relations:

$$\log(\alpha' + g^p - g) = \log \alpha' + \sum_{\alpha \in \mathbb{F}_p} \log(X + \frac{g}{\alpha'} + \alpha) \text{ for } \alpha' \in \mathbb{F}^*_{p^2}.$$

By using relation (A1), we can obtain that the addition at RHS is

$$\sum_{\alpha \in \mathbb{F}_p} \log(X + \frac{g}{\alpha'} + \alpha) = (1 + p^2 + \cdots + p^{2(p-1)}) \log(X + \frac{g}{\alpha'}) = N \log(X + \frac{g}{\alpha'}) = 0 (\mathrm{mod} N),$$

and $\log(\alpha' + g^p - g) = 0$ since $\alpha' + g^p - g \in \mathbb{F}^*_{p^2}$.

Let us compare the remaining relations of the linear system (**I**) generated by $\left\{\begin{pmatrix} a & g \\ 0 & 1 \end{pmatrix} | a \in \mathbb{F}^*_{p^2} \setminus \mathbb{F}^*_p\right\}$

$$\log(X + \frac{a^p}{a^p - a} + \frac{g^p - g}{a^p - a}) = \sum_{\alpha \in \mathbb{F}_p} \log(X + \frac{g + \alpha}{a}) \tag{I'}$$

and the linear system (**II**). We notice that for arbitrary $a = a_1 + a_2 g \in \mathbb{F}^*_{p^2}/\mathbb{F}^*_p$ with $a_2 \neq 0$,

$$\log\left(X + \frac{a^p}{a^p - a} + \frac{g^p - g}{a^p - a}\right) = p^{2h(1/a_2)} \log\left(X + \frac{a^p}{a^p - a}\right).$$

On the other hand, there exists a bijection $\alpha = \alpha'' - \frac{a_1}{a_2}$ in $\mathbb{F}_p$, which indicates that

$$\log\left(X + \frac{g + \alpha''}{a}\right) = p^{2h(1/a_2)} \left(X + \frac{\alpha}{a}\right).$$

Then we state that (**I'**) and (**II**) are equivalent under the Frobenius endomorphism, which implies our conclusion. Q.E.D.

We apply the transformations in set $\left\{\begin{pmatrix} 1 & 0 \\ 0 & g+\beta \end{pmatrix} | \beta \in \mathbb{F}_p\right\}$ and obtain these effectual relations

$$\log(X + \frac{g + \beta}{g - g^p}) = \sum_{\alpha \in \mathbb{F}_p} \log(X + \alpha g + \alpha\beta),\ \beta = 0, 1, \cdots, p-1.$$

Without loss of generality, we may take $\beta = 2\theta\eta$ with θ runs over $\mathbb{F}_p$. It turns out that the system can be represented as

$$\log(X + \theta g + \frac{1}{2}) = \sum_{\alpha \in \mathbb{F}_p} \log(X + \alpha g + 2\eta\alpha\theta),\ \theta \in \mathbb{F}_p.$$

Deploying the Frobenius endomorphism as illustrated in Equation (A1), we have

$$p^\lambda \log(X + \theta g) = \sum_{\alpha \in \mathbb{F}_p} p^{2\eta\alpha\theta} \log(X + \alpha g),$$

where $\lambda = \frac{p(2+(-1)^{\frac{p-1}{2}})+1}{2}$. We denote by $\mathbf{M} = ((p^{2\eta})^{ij})$, $\mathbf{D} = p^\lambda \mathbf{I}_p \in (\mathbb{Z}/N\mathbb{Z})^{p \times p}$. Then the linear system (**II**) can be represented as $\mathbf{M} - \mathbf{D}$.

In fact, the linear system $\mathbf{M} - \mathbf{D}$ is not sufficient to compute the discrete logarithms of linear elements of $K/\mathbb{F}^*_{p^2}$. We will exhibit a result on the eigenvalues of matrix M, which explains the reason of the insufficiency.

Lemma 2. With $\mathbf{M} = (m_{i,j})_{p \times p} \in (\mathbb{Z}/N\mathbb{Z})^{p \times p}$ defined as $m_{i,j} = p^{2\eta ij \bmod 2p}$ $(i, j = 0, 1, \cdots, p-1)$, where $\eta \in \mathbb{F}_p$ is a quadratic non-residue of $\mathbb{F}_p$, the characteristic polynomial of $\mathbf{M}$ is of the form:

$$e(t) = (t - r_1)^{e_1} (t - r_2)^{e_2} (t - r_3)^{e_3} (t - r_4)^{e_4},$$

where

$$r_i^4 = p^2 \bmod N \quad \text{and} \quad e_i \geqslant \frac{p-3}{4}$$

for $i = 1, 2, 3, 4$.

Proof. We state that $p^{2\eta}$ is a p-th primitive root of unity over $\mathbb{Z}/N\mathbb{Z}$, because $(p^{2\eta})^p = 1 \bmod N$ and p is a prime. Also, p is a quadratic residue over $\mathbb{Z}/N\mathbb{Z}$ due to $\gcd(p, N) = 1$ and the Jacobi symbol $\left(\frac{p}{N}\right) = 1$. Then $\frac{1}{\sqrt{p}}\mathbf{M}$ turns into a Number Theoretic Transform(or general Discrete Fourier Transform). Therefore we can obtain the character polynomial of $\mathbf{M}$, which indicates our conclusion. Q.E.D.

It is easy to verify that p^λ is an eigenvalue of $\mathbf{M}$. Now we draw a conclusion that $\mathbf{M} - \mathbf{D}$ holds a kernel of dimension at least $\frac{p-3}{4}$.

Appendix B Experimental evidence of Heuristic

We will provide experimental verification for Heuristic 1 in our article. Provided an odd prime p, we generate the quadratic extension $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(f(x))$, with h the generator of $\mathbb{F}_{p^2}$. Then we select proper quadratic non-residue η and corresponding g. Constructing matrix $\mathbf{M}_r, \mathbf{M}_r$ as illustrated in the article, we verified that for all those p such that $\log_2 N \leqslant 11,035$

$$\det(\mathbf{M}_r - \mathbf{M}_l) = 0 \bmod N', \quad \text{GCD}\left(\frac{\det(\mathbf{M}_r - \mathbf{M}_l)}{N'}, N'\right) = 1$$

where $N = |K^*/(\mathbb{F}_{p^2}^*)| = \frac{p^{2p}-1}{p^2-1}$ as defined in the article, and $N'|N$ is the product of all N's factors that are free of primes less than $p^2 - 1$. Details can be referred in the following table.

Table B1 Instances verified for $\log_2 N \leqslant 11,035$

p	K	f	η	g	p	K	f	η	g
3	$\mathbb{F}_{3^6}$	x^2+2x+2	2	$h+1$	263	$\mathbb{F}_{263^{526}}$	$x^2+261x+5$	5	$14h+249$
5	$\mathbb{F}_{5^{10}}$	x^2+4x+2	2	$4h+3$	269	$\mathbb{F}_{269^{538}}$	$x^2+268x+2$	2	$242h+148$
7	$\mathbb{F}_{7^{14}}$	x^2+6x+3	3	$2h+6$	271	$\mathbb{F}_{271^{542}}$	$x^2+269x+6$	6	$18h+253$
11	$\mathbb{F}_{11^{22}}$	x^2+7x+2	2	$10h+2$	277	$\mathbb{F}_{277^{554}}$	$x^2+274x+5$	5	$132h+79$
13	$\mathbb{F}_{13^{26}}$	$x^2+12x+2$	2	$7h+3$	281	$\mathbb{F}_{281^{562}}$	$x^2+280x+3$	3	$98h+232$
17	$\mathbb{F}_{17^{34}}$	$x^2+16x+3$	3	$11h+3$	283	$\mathbb{F}_{283^{566}}$	$x^2+282x+3$	3	$99h+92$
19	$\mathbb{F}_{19^{38}}$	$x^2+18x+2$	2	$8h+15$	293	$\mathbb{F}_{293^{586}}$	$x^2+292x+2$	2	$141h+76$
23	$\mathbb{F}_{23^{46}}$	$x^2+21x+5$	5	$19h+4$	307	$\mathbb{F}_{307^{614}}$	$x^2+306x+5$	5	$165h+71$
29	$\mathbb{F}_{29^{58}}$	$x^2+24x+2$	2	$3h+7$	311	$\mathbb{F}_{311^{622}}$	$x^2+310x+17$	17	$114h+254$
31	$\mathbb{F}_{31^{62}}$	$x^2+29x+3$	3	$13h+18$	313	$\mathbb{F}_{313^{626}}$	$x^2+310x+10$	10	$177h+204$
37	$\mathbb{F}_{37^{74}}$	$x^2+33x+2$	2	$36h+2$	317	$\mathbb{F}_{317^{634}}$	$x^2+313x+2$	2	$h+315$
41	$\mathbb{F}_{41^{82}}$	$x^2+38x+6$	6	$8h+29$	331	$\mathbb{F}_{331^{662}}$	$x^2+326x+3$	3	$44h+221$
43	$\mathbb{F}_{43^{86}}$	$x^2+42x+3$	3	$9h+17$	337	$\mathbb{F}_{337^{674}}$	$x^2+332x+10$	10	$151h+128$
47	$\mathbb{F}_{47^{94}}$	$x^2+45x+5$	5	$9h+38$	347	$\mathbb{F}_{347^{694}}$	$x^2+343x+2$	2	$346h+2$
53	$\mathbb{F}_{53^{106}}$	$x^2+49x+2$	2	$52h+2$	349	$\mathbb{F}_{349^{698}}$	$x^2+348x+2$	2	$277h+36$
59	$\mathbb{F}_{59^{118}}$	$x^2+58x+2$	2	$10h+54$	353	$\mathbb{F}_{353^{706}}$	$x^2+348x+3$	3	$61h+24$
61	$\mathbb{F}_{61^{122}}$	$x^2+60x+2$	2	$5h+28$	359	$\mathbb{F}_{359^{718}}$	$x^2+358x+7$	7	$15h+172$
67	$\mathbb{F}_{67^{134}}$	$x^2+63x+2$	2	$h+65$	367	$\mathbb{F}_{367^{734}}$	$x^2+366x+6$	6	$215h+76$
71	$\mathbb{F}_{71^{142}}$	$x^2+69x+7$	7	$49h+22$	373	$\mathbb{F}_{373^{746}}$	$x^2+369x+2$	2	$372h+2$
73	$\mathbb{F}_{73^{146}}$	$x^2+70x+5$	5	$29h+66$	379	$\mathbb{F}_{379^{758}}$	$x^2+374x+2$	2	$166h+343$
79	$\mathbb{F}_{79^{158}}$	$x^2+78x+3$	3	$11h+34$	383	$\mathbb{F}_{383^{766}}$	$x^2+382x+5$	5	$89h+147$
83	$\mathbb{F}_{83^{166}}$	$x^2+82x+2$	2	$53h+15$	389	$\mathbb{F}_{389^{778}}$	$x^2+379x+2$	2	$310h+6$
89	$\mathbb{F}_{89^{178}}$	$x^2+82x+3$	3	$52h+85$	397	$\mathbb{F}_{397^{794}}$	$x^2+392x+5$	5	$2h+392$
97	$\mathbb{F}_{97^{194}}$	$x^2+96x+5$	5	$27h+35$	401	$\mathbb{F}_{401^{802}}$	$x^2+396x+3$	3	$97h+359$
101	$\mathbb{F}_{101^{202}}$	$x^2+97x+2$	2	$100h+2$	409	$\mathbb{F}_{409^{818}}$	$x^2+404x+21$	21	$69h+32$
103	$\mathbb{F}_{103^{206}}$	$x^2+102x+5$	5	$8h+99$	419	$\mathbb{F}_{419^{838}}$	$x^2+418x+2$	2	$134h+352$
107	$\mathbb{F}_{107^{214}}$	$x^2+103x+2$	2	$106h+2$	421	$\mathbb{F}_{421^{842}}$	$x^2+417x+2$	2	$420h+2$
109	$\mathbb{F}_{109^{218}}$	$x^2+108x+6$	6	$31h+39$	431	$\mathbb{F}_{431^{862}}$	$x^2+430x+7$	7	$198h+332$
113	$\mathbb{F}_{113^{226}}$	$x^2+101x+3$	3	$80h+85$	433	$\mathbb{F}_{433^{866}}$	$x^2+432x+5$	5	$54h+406$
127	$\mathbb{F}_{127^{254}}$	$x^2+126x+3$	3	$99h+14$	439	$\mathbb{F}_{439^{878}}$	$x^2+436x+15$	15	$288h+7$
131	$\mathbb{F}_{131^{262}}$	$x^2+127x+2$	2	$h+129$	443	$\mathbb{F}_{443^{886}}$	$x^2+437x+2$	2	$384h+177$
137	$\mathbb{F}_{137^{274}}$	$x^2+131x+3$	3	$84h+22$	449	$\mathbb{F}_{449^{898}}$	$x^2+444x+3$	3	$211h+146$
139	$\mathbb{F}_{139^{278}}$	$x^2+138x+2$	2	$37h+51$	457	$\mathbb{F}_{457^{914}}$	$x^2+454x+13$	13	$319h+207$
149	$\mathbb{F}_{149^{298}}$	$x^2+145x+2$	2	$148h+2$	461	$\mathbb{F}_{461^{922}}$	$x^2+460x+2$	2	$187h+137$
151	$\mathbb{F}_{151^{302}}$	$x^2+149x+6$	6	$28h+123$	463	$\mathbb{F}_{463^{926}}$	$x^2+461x+3$	3	$34h+429$
157	$\mathbb{F}_{157^{314}}$	$x^2+152x+5$	5	$2h+152$	467	$\mathbb{F}_{467^{934}}$	$x^2+463x+2$	2	$h+465$
163	$\mathbb{F}_{163^{326}}$	$x^2+159x+2$	2	$h+161$	479	$\mathbb{F}_{479^{958}}$	$x^2+474x+13$	13	$235h+131$

p	K	f	η	g	p	K	f	η	g
167	$\mathbb{F}_{167^{334}}$	$x^2+166x+5$	5	$150h+92$	487	$\mathbb{F}_{487^{974}}$	$x^2+485x+3$	3	$27h+460$
173	$\mathbb{F}_{173^{346}}$	$x^2+169x+2$	2	$h+171$	491	$\mathbb{F}_{491^{982}}$	$x^2+487x+2$	2	$490h+2$
179	$\mathbb{F}_{179^{358}}$	$x^2+172x+2$	2	$137h+147$	499	$\mathbb{F}_{499^{998}}$	$x^2+493x+7$	7	$420h+237$
181	$\mathbb{F}_{181^{362}}$	$x^2+177x+2$	2	$180h+2$	503	$\mathbb{F}_{499^{1006}}$	$x^2+498x+5$	5	$2h+498$
191	$\mathbb{F}_{191^{382}}$	$x^2+190x+19$	19	$72h+155$	509	$\mathbb{F}_{509^{1018}}$	$x^2+508x+2$	2	$157h+176$
193	$\mathbb{F}_{193^{386}}$	$x^2+192x+5$	5	$18h+184$	521	$\mathbb{F}_{521^{1042}}$	$x^2+515x+3$	3	$136h+113$
197	$\mathbb{F}_{197^{394}}$	$x^2+192x+2$	2	$55h+158$	523	$\mathbb{F}_{523^{1046}}$	$x^2+522x+2$	2	$359h+82$
199	$\mathbb{F}_{199^{398}}$	$x^2+193x+3$	3	$10h+169$	541	$\mathbb{F}_{541^{1082}}$	$x^2+537x+2$	2	$h+539$
211	$\mathbb{F}_{211^{422}}$	$x^2+207x+2$	2	$h+209$	547	$\mathbb{F}_{547^{1094}}$	$x^2+543x+2$	2	$h+545$
223	$\mathbb{F}_{223^{446}}$	$x^2+221x+3$	3	$188h+35$	557	$\mathbb{F}_{557^{1114}}$	$x^2+553x+2$	2	$h+555$
227	$\mathbb{F}_{227^{454}}$	$x^2+220x+2$	2	$203h+84$	563	$\mathbb{F}_{563^{1126}}$	$x^2+559x+2$	2	$h+561$
229	$\mathbb{F}_{229^{458}}$	$x^2+228x+6$	6	$26h+216$	569	$\mathbb{F}_{569^{1138}}$	$x^2+568x+3$	3	$550h+294$
233	$\mathbb{F}_{233^{466}}$	$x^2+232x+3$	3	$91h+71$	571	$\mathbb{F}_{571^{1142}}$	$x^2+570x+3$	3	$538h+302$
239	$\mathbb{F}_{239^{478}}$	$x^2+237x+7$	7	$26h+213$	577	$\mathbb{F}_{577^{1154}}$	$x^2+572x+5$	5	$2h+572$
241	$\mathbb{F}_{241^{482}}$	$x^2+238x+7$	7	$10h+226$	587	$\mathbb{F}_{587^{1174}}$	$x^2+583x+2$	2	$586h+2$
251	$\mathbb{F}_{251^{502}}$	$x^2+242x+6$	6	$236h+193$	593	$\mathbb{F}_{593^{1186}}$	$x^2+592x+3$	3	$64h+561$
257	$\mathbb{F}_{257^{514}}$	$x^2+251x+3$	3	$227h+90$	599	$\mathbb{F}_{599^{1198}}$	$x^2+598x+7$	7	$494h+352$

Appendix C Proof of Proposition 1

We denote by $\mathbf{M}_l$ the linear combinations of $\log(X+\theta g)$ at LHS and by $\mathbf{M}_r$ those at RHS. Let $\mathbf{D}=\mathbf{S}(\mathbf{M}_r-\mathbf{M}_l)\mathbf{T}$ is the Smith Normal Form of $\mathbf{M}_r-\mathbf{M}_l$, and $\mathbf{S},\mathbf{T}$ are corresponding transformation matrices. With Heuristic 1, we can obtain the form $\mathbf{D}=\mathrm{diag}(d_0,d_1,\cdots,d_{p-1})$ where $d_{p-1}=cN'$. Therefore, we can obtain that the last column of $\mathbf{T}$ is the ratio vector of $(\log X,\log(X+g),\cdots,\log(X+(p-1)g)$. Let $\mathbf{e}=(e_0,e_1,\cdots,e_{p-1})$ be the last row of $\mathbf{T}^{-1}$, then we have

$$r\left(e_0\log X+e_1\log(X+g)+\cdots+e_{p-1}\log(X+(p-1)g)\right)=1,$$

for some ratio r. For the reversibility of $\sum_{i=0}^{p}e_i\log(X+ig)$, we obtain a primitive element of $K^*/\mathbb{F}_{p^2}^*$:

Computing the Smith Normal Form would need $\tilde{O}(p^\omega)$ operations referring to [2], where $\omega\leqslant 2.38$[1] is the exponent parameter of fast matrix multiplication.

Utilizing the Pohlig-Hellman algorithm with results in $\mathbb{Z}/q\mathbb{Z}$, we obtain the logarithms of linear factor in $\mathbb{Z}/N\mathbb{Z}$ and a primitive element of $K^*/\mathbb{F}_{p^2}^*$. Q.E.D.

References

1 Don Coppersmith and Shmuel Winograd. Matrix multiplication via arithmetic progressions. *Journal of symbolic computation*, 9(3):251–280, 1990.

2 A. Storjohann. Near optimal algorithms for computing Smith Normal Forms of integer matrices. In *ISSAC 1996*, pages 267–274, 1996.

3 Dianyan Xiao, Jincheng Zhuang, and Qi Cheng. Factor base discrete logarithms in kummer extensions. *Finite Fields and Their Applications*, 53:205–225, 2018.

4 Y. Zhu, J. Zhuang, C. Lv, and D. Lin. Classifying and generating exact coset representatives of $\mathrm{PGL}_2(\mathbb{F}_q)$ in $\mathrm{PGL}_2(\mathbb{F}_{q^2})$. *Finite Fields and Their Applications*, 42:118 – 127, 2016.

5 J. Zhuang and Q. Cheng. On generating coset representatives of $\mathrm{PGL}_2(\mathbb{F}_q)$ in $\mathrm{PGL}_2(\mathbb{F}_{q^2})$. In *Inscrypt 2015*, volume 9589, page 167. Springer, 2016.