A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm

Palash Sarkar, Shashank Singh

Indian Statistical Institute
INRIA, France

Asiacrypt 2016

Finite Field $\mathbb{F}_Q$, $Q = p^n$

Sub-exponential expression:

$$L_Q(a, c) = O\left(\exp\left((c + o(1))(\log Q)^a (\log \log Q)^{1-a}\right)\right)$$

Classification:

- Small characteristic: if $a \leq 1/3$.
- Medium characteristic: if $1/3 < a < 2/3$.
- Boundary case: if $a = 2/3$.
- Large characteristic: if $a > 2/3$.

Recent Progress on DLP over Finite Fields

Small characteristic case:

- Development of the Function Field Sieve (FFS) algorithm has led to a quasi-polynomial time algorithm.

Medium characteristic case:

- Recent interest in the Number Field Sieve (NFS) algorithm.

NFS for DLP Over $\mathbb{F}_Q$

- $f(x)$ and $g(x)$ are polynomials over $\mathbb{Z}$ having a common irreducible factor $\varphi(x)$ of degree n over $\mathbb{F}_p$.
- $\alpha, \beta \in \mathbb{C}$ are roots of $f(x)$ and $g(x)$; $m \in \mathbb{F}_{p^n}$ is a root of $\varphi(x)$.

$$\begin{tikzcd}
 & \mathbb{Z}[x] \arrow[dl, "\alpha \mapsfrom x"'] \arrow[dr, "x \mapsto \beta"] & \\
\mathbb{Z}(\alpha) \arrow[dr, "\alpha \mapsto m"'] & & \mathbb{Z}(\beta) \arrow[dl, "m \mapsfrom \beta"] \\
 & \mathbb{F}_p(m) &
\end{tikzcd}$$

Figure : The basic principle of NFS.

Factor Basis

Number fields: $\mathbb{K}_1 = \mathbb{Q}[x]/(f)$ and $\mathbb{K}_2 = \mathbb{Q}[x]/(g)$;

$\mathcal{O}_1$ and $\mathcal{O}_2$ are the ring of integers of $\mathbb{K}_1$ and $\mathbb{K}_2$ respectively.

Factor basis: prime ideals of $\mathcal{O}_1$ and $\mathcal{O}_2$ whose norms are at most some pre-specified bound B.

Size of the factor basis: $B^{1+o(1)}$.

Relation Collection

Polynomials $\phi(x) \in \mathbb{Z}[x]$ of degrees at most $t-1$ are considered.

If the principal ideals $\phi(\alpha)\mathcal{O}_1$ and $\phi(\beta)\mathcal{O}_2$ are both smooth over the factor basis, then a relation among the factor basis elements is obtained.

- Formally, a linear relation between the discrete logs of certain elements of $\mathbb{F}_{p^n}$ is obtained.
- Such discrete logs are called virtual logarithms.

A little more than B relations are collected.

Polynomial Selection and Sizes of Norms

- Norm of $\phi(\alpha)\mathcal{O}_1$ is $\mathrm{Res}(f, \phi)$.
- For ensuring smoothness of $\phi(\alpha)\mathcal{O}_1$ it is sufficient that $\mathrm{Res}(f, \phi)$ is B-smooth; similarly, for $g(x)$.

$$
\begin{aligned}
|\mathrm{Res}(f, \phi)| &= O\left((\|f\|_\infty)^{t-1} E^{2(\deg f)/t} \right) \\
|\mathrm{Res}(g, \phi)| &= O\left((\|g\|_\infty)^{t-1} E^{2(\deg g)/t} \right),
\end{aligned}
$$

- E is such that $\|\phi\|_\infty \approx E^{2/t}$ and so E^2 sieving polynomials ϕ are considered.
- The lower the norms, the easier it becomes to find a relation.
- The norms are determined by $\|f\|_\infty$, $\|g\|_\infty$, $\deg f$ and $\deg g$.

Asymptotic Complexity

Asymptotic run time of NFS:

- Medium prime case: $L_Q(1/3, (96/9)^{1/3})$.
  - Obtained using the Conjugation method.
- Boundary case: $L_Q(1/3, (48/9)^{1/3})$ for $c_p = 12^{1/3}$.
  - Obtained using the Conjugation method.
  - More complete analysis using the SS method.
- Large prime case: $L_Q(1/3, (64/9)^{1/3})$.
  - Obtained using the GJL method.

Tower Number Field Sieve Algorithm

Let $n = \eta\kappa$ and $q = p^\eta$.

Tower field representation: $\mathbb{F}_{p^n} = \mathbb{F}_{q^\kappa}$.

Main idea for TNFS:

- Suppose $p = L_Q(a, c_p)$ with $1/3 < a < 2/3$ and $q = L_Q(2/3, c_p)$.
- The boundary case complexity is achieved for the medium prime case.

exTNFS: variant of TNFS proposed by Kim-Barbulescu (2016).

Setting of exTNFS

Choose $h(z)$ such that:

- $\deg h = \eta$; $\|h\|_\infty$ is small; $h(z)$ is irreducible over $\mathbb{F}_p$.

Define

$$\mathbb{F}_{p^\eta} = \mathbb{F}_p[z]/(h) \text{ and } R = \mathbb{Z}[z]/(h).$$

Choose $f(x)$ and $g(x)$ in $Z[x]$ such that:

- Both are irreducible over R and over $\mathbb{F}_{p^\eta}$.
- $\varphi(x) = \gcd(f(x), g(x))$ is of degree κ and is irreducible over $\mathbb{F}_{p^\eta}$.

$$\mathbb{F}_{p^n} = \mathbb{F}_{p^\eta}[x]/(\varphi) = (R/pR)[x]/(\varphi).$$

Kim-Barbulescu (2016)

- Requires $\varphi(x)$ over $\mathbb{F}_p$ having degree κ to be irreducible over $\mathbb{F}_{p^\eta}$.
- This condition requires $\gcd(\eta, \kappa) = 1$.
- Applies to composite non prime-power n such as $n = 6, 12, 15, 18, 21, \ldots$
- Cannot be applied to composite prime power n such as $n = 4, 8, 9, 16, \ldots$

Medium prime case: complexity $L_Q(1/3, (48/9)^{1/3})$.

- Previously known complexity $L_Q(1/3, (96/9)^{1/3})$.

A New Polynomial Selection Method

Input:

- p;
- $n = \eta\kappa$;
- d a factor of κ;
- $r \geq k = \kappa/d$;
- $\lambda \in \{1, \eta\}$.

Random trials to find suitable $f(x), g(x)$ and $\varphi(x)$.

- $f(x)$ and $g(x)$ are in $R[x]$ and are irreducible over R.
- $\varphi(x) \in \mathbb{F}_{p^\eta}[x]$; has degree κ and is irreducible over $\mathbb{F}_{p^\eta}$.

Using LLL: Notation

Given $\mathfrak{a}(x) \in R[x]$ of degree k and positive integer $r \geq k$, we define

- a matrix $M_{\mathfrak{a},r}$ and a polynomial $\mathrm{LLL}(M_{\mathfrak{a},r})$.

Suppose

$$\mathfrak{a}(x) \quad = \quad x^k + \mathfrak{a}_{k-1}(z)x^{k-1} + \cdots + \mathfrak{a}_1(z)x + \mathfrak{a}_0(z)$$

where each $\mathfrak{a}_i$ has degree less than $\lambda \in \{1, \eta\}$.

Write

$$\begin{aligned} \mathfrak{a}_i &= (\mathfrak{a}_{i,0}, \ldots, \mathfrak{a}_{i,\lambda-1}); \\ \mathfrak{a} &= (\mathfrak{a}_{0,0}, \ldots, \mathfrak{a}_{0,\lambda-1}, \ldots, \mathfrak{a}_{k-1,0}, \ldots, \mathfrak{a}_{k-1,\lambda-1}). \end{aligned}$$

The Matrix $M_{\mathfrak{a},r}$

$$\begin{bmatrix} \mathrm{diag}_{\lambda k}(p) & & & & & \\ \mathfrak{a} & 1 & & & & \\ \mathbf{0}_{\lambda-1,1+\lambda k} & \mathrm{diag}_{\lambda-1}(p) & & & & \\ & \mathrm{shift}_{\lambda}(\mathfrak{a}) & 1 & & & \\ & \mathbf{0}_{\lambda-1,1+\lambda(k+1)} & \mathrm{diag}_{\lambda-1}(p) & & & \\ & & \mathrm{shift}_{2\lambda}(\mathfrak{a}) & 1 & & \\ & & \ddots & \ddots & & \\ & & & \mathbf{0}_{\lambda-1,1+\lambda(r-1)} & \mathrm{diag}_{\lambda-1}(p) & \\ & & & \mathrm{shift}_{(r-k)\lambda}(\mathfrak{a}) & & 1 \end{bmatrix}_{(r\lambda+1)\times(r\lambda+1)}$$

Determinant of $M_{\mathfrak{a},r}$ is $p^{r(\lambda-1)+k}$.

The Polynomial $\mathrm{LLL}(M_{\mathfrak{a},r})$

Apply the LLL algorithm to $M_{\mathfrak{a},r}$ and write the first row as:

$$[\mathfrak{b}_{0,0}, \ldots, \mathfrak{b}_{0,\lambda-1}, \mathfrak{b}_{1,0}, \ldots, \mathfrak{b}_{1,\lambda-1}, \ldots, \mathfrak{b}_{r-1,0}, \ldots, \mathfrak{b}_{r-1,\lambda-1}, \mathfrak{b}_r].$$

This represents a polynomial $\mathfrak{b}(x) \in R[x]$ of degree r where

$$\begin{aligned}
\mathfrak{b}(x) &= \mathfrak{b}_0(z) + \mathfrak{b}_1(z)x + \cdots + \mathfrak{b}_{r-1}(z)x^{r-1} + \mathfrak{b}_r x^r; \\
\mathfrak{b}_i(z) &= \mathfrak{b}_{i,0} + \mathfrak{b}_{i,1}z + \cdots + \mathfrak{b}_{i,\lambda-1}z^{\lambda-1}; \\
\|\mathfrak{b}\|_\infty &= Q^{\varepsilon/n} \text{ with } \varepsilon = \frac{r(\lambda-1)+k}{r\lambda+1}.
\end{aligned}$$

The polynomial $\mathfrak{b}(x)$ is written as $\mathrm{LLL}(M_{\mathfrak{a},r})$.

Random Trials: Step 1

Choose a monic polynomial $A_1(x) \in R[x]$ such that:

- $\deg A_1 = r + 1$;
- $A_1(x)$ is irreducible over R;
- $A_1(x)$ has coefficient polynomials of size $O(\ln p)$;
- over $\mathbb{F}_{p^\eta}$, $A_1(x)$ has an irreducible factor $A_2(x)$ of degree k such that all coefficient polynomials of $A_2(x)$ have degrees at most $\lambda - 1$.

Random Trials: Step 2

Choose monic polynomials $C_0(x)$ and $C_1(x)$ with small integer coefficients such that $\deg C_1 < \deg C_0 = d$.

Define:

$$\begin{aligned}
f(x) &= \mathrm{Res}_y\left(A_1(y), C_0(x) + y\,C_1(x)\right);\\
\varphi(x) &= \mathrm{Res}_y\left(A_2(y), C_0(x) + y\,C_1(x)\right) \bmod p;\\
\psi(x) &= \mathrm{LLL}(M_{A_2,r});\\
g(x) &= \mathrm{Res}_y\left(\psi(y), C_0(x) + y\,C_1(x)\right).
\end{aligned}$$

Degrees and Norms

- $\deg(f) = d(r+1)$; $\deg(g) = rd$ and $\deg(\varphi) = \kappa$;
- over $\mathbb{F}_{p^\eta}$, both $f(x)$ and $g(x)$ have $\varphi(x)$ as a factor;
- $\|f\|_\infty = O(\ln(p))$ and $\|g\|_\infty = O(Q^{\varepsilon/n})$.

For a sieving polynomial ϕ

$$\begin{aligned} N(f,\phi) &= E^{2d(r+1)/t} \times L_Q(2/3, o(1)); \\ N(g,\phi) &= E^{2dr/t} \times Q^{(t-1)\varepsilon/\kappa} \times L_Q(2/3, o(1)). \end{aligned}$$

Relation to Previous Works

Case $\eta = 1$: reduces to NFS.

- λ must be 1; yields Algorithm-$\mathcal{A}$ (EC 2016).

Case $\eta > 1$ and $\lambda = 1$: $\varphi(x) \in \mathbb{F}_p$; $\deg \varphi = \kappa$;

- irreducibility of $\varphi(x)$ over $\mathbb{F}_{p^\eta}$ requires $\gcd(\eta, \kappa) = 1$.
- Kim-Barbulescu (Crypto 2016) exTNFS methods are special cases:
  $d = 1$, $k = \kappa$ yields exTNFS-GJL method; $d = \kappa$, $r = k = 1$ yields exTNFS-Conjugation.

New Case: $\lambda = \eta > 1$: $\varphi(x)$ is in $\mathbb{F}_{p^n} \setminus \mathbb{F}_p$.

- The condition $\gcd(\eta, \kappa) = 1$ is not necessary for the irreducibility of $\varphi(x)$.

Medium Prime Case: Asymptotic Complexity

Theorem

Let $n = \eta\kappa$; $\kappa = kd$; $r \geq k$; $t \geq 2$; $p = L_Q(a, c_p)$ *with* $1/3 < a \leq 2/3$; $\eta = c_\eta(\ln Q / \ln\ln Q)^{2/3-a}$; $c_\theta = c_p c_\eta$. *Runtime of the TNFS algorithm with polynomials chosen by Algorithm* $\mathcal{C}$ *is* $L_Q(1/3, 2c_b)$ *where*

$$c_b = \frac{2(2r+1)}{6c_\theta kt} + \sqrt{\left(\frac{2r+1}{3c_\theta kt}\right)^2 + \frac{(t-1)c_\theta\varepsilon}{3}}.$$

Medium Prime Case: Asymptotic Complexity

Minimise c_b with respect to c_θ: minimum achieved for $t = 2$.

Case $\lambda = 1$: minimum value is

$$\left(\frac{32(2r+1)}{9(r+1)}\right)^{1/3}$$

which takes the minimum value of $(48/9)^{1/3}$ for $r = 1$.

- Either $\eta = 1$, $a = 2/3$ (boundary case), or, $\eta > 1$, $1/3 < a < 2/3$ (medium prime case).
- $\lambda = 1$ implies that the condition $\gcd(\eta, \kappa) = 1$ is required.
- The minimum complexity is not achieved for all values of c_θ.

Medium Prime Case: Asymptotic Complexity

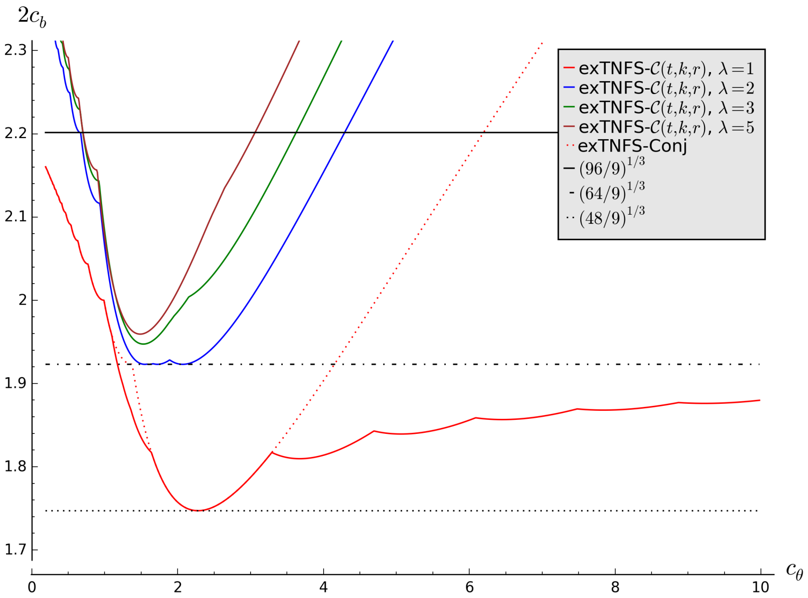
Minimise c_b with respect to c_θ: minimum achieved for $t = 2$.

Case $\lambda = \eta > 1$: minimum attained for $r = k = \kappa$ and the minimum value is

$$\left(\frac{32(2n+\eta)}{9(n+1)}\right)^{1/3}.$$

- $\eta = 2$: minimum is $(64/9)^{1/3} \approx 1.92$ for all $n = 2^i$.
- $\eta = 3$, $n = 9$: minimum is $(112/15)^{1/3} \approx 1.95$.
- $\eta = 5$, $n = 25$: minimum is $(880/117)^{1/3} \approx 1.96$.

Asymptotic Complexity Plots



Medium Prime Case: Continuing Story

- Jeong and Kim (2016): achieved complexity $(48/9)^{1/3}$ for all composite n.
- Sarkar and Singh (2016): a general polynomial selection method; concrete analysis.
- ...

Thank you for your kind attention!