

Rump Session 2016

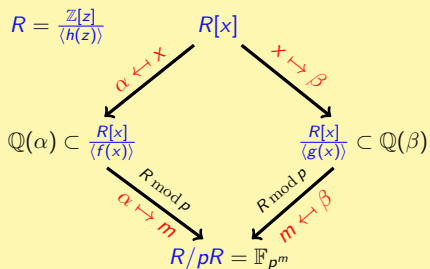


Tower Number Field Sieve Variant of a Recent Polynomial Selection Method

Palash Sarkar; Shashank Singh

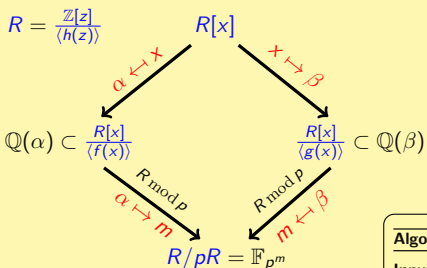
Indian Statistical Institute

The Tower Number Field Sieve + SS Polynomial Selection



Barbulescu et al.
(Asiacrypt 2015)

The Tower Number Field Sieve + SS Polynomial Selection



Barbulescu et al.
(Asiacrypt 2015)

Sarkar-Singh
Polynomial
Selection
Algorithm
(Eurocrypt 2016)

Algorithm: \mathcal{A} : A new method of polynomial selection for NFS.

Input: p, n, d (a factor of n) and $r \geq n/d$.

Output: $f(x), g(x)$ and $\varphi(x)$.

Let $k = n/d$;

repeat

Randomly choose a monic irr $A_1(x)$ with small coeff.: $\deg A_1 = r + 1 \pmod p$, $A_1(x)$ has an irr factor $A_2(x)$ of deg k .

Choose monic $C_0(x)$ and $C_1(x)$: $\deg C_0 = d$ and $\deg C_1 < d$.

Define

$$f(x) = \text{Res}_y(A_1(y), C_0(x) + y C_1(x));$$

$$\varphi(x) = \text{Res}_y(A_2(y), C_0(x) + y C_1(x)) \bmod p;$$

$$\psi(x) = \text{LLL}(M_{A_2, r});$$

$$g(x) = \text{Res}_y(\psi(y), C_0(x) + y C_1(x)).$$

until $f(x)$ and $g(x)$ are irr over \mathbb{Z} and $\varphi(x)$ is irr over \mathbb{F}_p ;

return $f(x), g(x)$ and $\varphi(x)$.



Taechan Kim and Razvan Barbulescu, *Extended Tower Number Field Sieve: A New Complexity for Medium Prime Case* - Cryptology ePrint Archive: Report 2015/1027

Setup (\mathbb{F}_Q):

$$Q = p^n, \text{ where } n = \eta \times \kappa \text{ and } \gcd(\eta, \kappa) = 1$$

- Complexity of NFS for non-prime field is better for boundary case i.e., $p = L_Q(2/3, c_p)$.
- Idea is to leverage the boundary case complexity by increasing p .



Polynomial Selection for TNFS



Palash Sarkar and Shashank Singh, *Tower Number Field Sieve Variant of a Recent Polynomial Selection Method*. - Cryptology ePrint Archive: Report 2016/401

- Polynomial Selection method subsumes GJL method.
- Polynomial Selection method generalises Conjugation method.
- It gives the new trade-offs which not covered by GJL and Conjugation method.



Algorithm: \mathcal{B} : Polynomial selection for TNFS.

Input: p , $n = \eta\kappa$, d (a factor of κ) and $r \geq \kappa/d$.

Output: $h(x)$, $f(x)$, $g(x)$ and $\varphi(x)$.

Let $k = \kappa/d$; Randomly choose $h(z)$ of deg η with small coeffs and irreducible modulo p . Let $R = \mathbb{Z}[z]/\langle h(z) \rangle$.

repeat

Randomly choose a monic irr $A_1(x)$ with small coeff.: deg $A_1 = r + 1$;
mod p , $A_1(x)$ has an irr factor $A_2(x)$ of deg k .

Choose monic $C_0(x)$ and $C_1(x)$: deg $C_0 = d$ and deg $C_1 < d$.

Define

$$f(x) = \text{Res}_y (A_1(y), C_0(x) + y C_1(x));$$

$$\varphi(x) = \text{Res}_y (A_2(y), C_0(x) + y C_1(x)) \text{ mod } p;$$

$$\psi(x) = \text{LLL}(M_{A_2, r});$$

$$g(x) = \text{Res}_y (\psi(y), C_0(x) + y C_1(x)).$$

until $f(x)$ and $g(x)$ are irr over R and $\varphi(x)$ is irr over $\mathbb{F}_{p^\eta}[z]/\langle h(z) \rangle$;

return $h(x)$, $f(x)$, $g(x)$ and $\varphi(x)$.

Example

Let p is a 201-bit prime given below.

$$p = 1606938044258990275541962092341162602522202993782792835301611$$

and $n = 6$. Let $(\eta, \kappa) = (3, 2)$.



Example

Let p is a 201-bit prime given below.

$$p = 1606938044258990275541962092341162602522202993782792835301611$$

and $n = 6$. Let $(\eta, \kappa) = (3, 2)$.

Taking $d = \kappa$ and $r = 1$, we get the following polynomials.

$$h(x) = x^3 + x^2 + 15x + 7$$

$$f(x) = x^4 - x^3 - 2x^2 - 7x - 3$$

$$g(x) = 717175561486984577278242843019x^2 + 2189435313197775056442946543188x \\ + 2906610874684759633721189386207$$

Note that $\|g\|_{\infty} \approx 2^{101}$.



Example

Let p is a 201-bit prime given below.

$$p = 1606938044258990275541962092341162602522202993782792835301611$$

and $n = 6$. Let $(\eta, \kappa) = (3, 2)$.

Taking $d = \kappa$ and $r = 1$, we get the following polynomials.

If we take $d = \kappa$ and $r = 2$, we get the following set of polynomials.

$$h(x) = x^3 + x^2 + 15x + 7$$

$$f(x) = x^6 - 4x^5 - 53x^4 - 147x^3 - 188x^2 - 157x - 92$$

$$g(x) = 15087279002722300985x^4 + 124616743720753879934x^3 + 451785460058994237397x^2 + 749764394939964245000x + 567202989572349792620$$

We have $\|g\|_{\infty} \approx 2^{69}$.



Asymptotic Analysis

Theorem

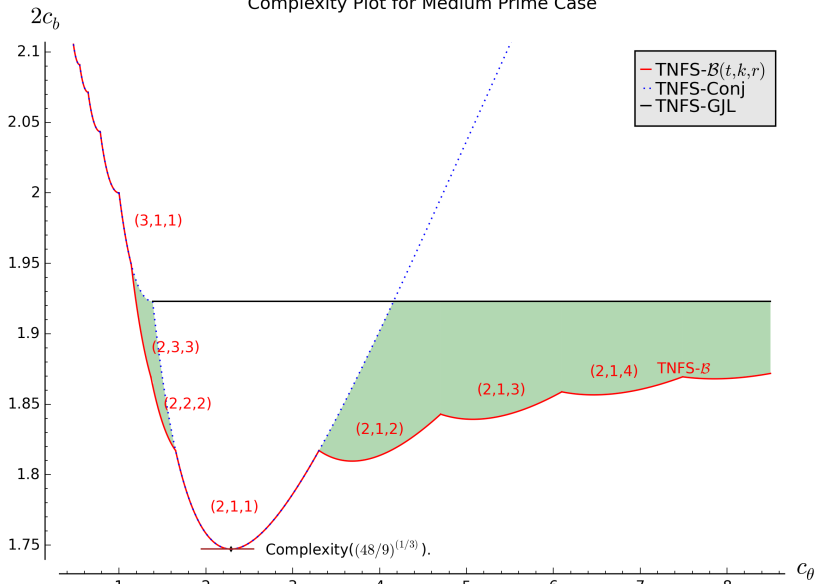
Let $n = \eta\kappa$; $\gcd(\eta, \kappa) = 1$; $\kappa = kd$; $r \geq k$; $t \geq 2$; $p = L_Q(a, c_p)$ with $1/3 < a < 2/3$ and $0 < c_p < 1$; and $\eta = c_\eta(\ln Q / \ln \ln Q)^{2/3-a}$. It is possible to ensure that the runtime of the NFS algorithm with polynomials chosen by Algorithm \mathcal{B} is $L_Q(1/3, 2c_b)$ where

$$c_b = \frac{2r+1}{3c_\theta kt} + \sqrt{\left(\frac{2r+1}{3c_\theta kt}\right)^2 + \frac{kc_\theta(t-1)}{3(r+1)}} \text{ and} \quad (2)$$

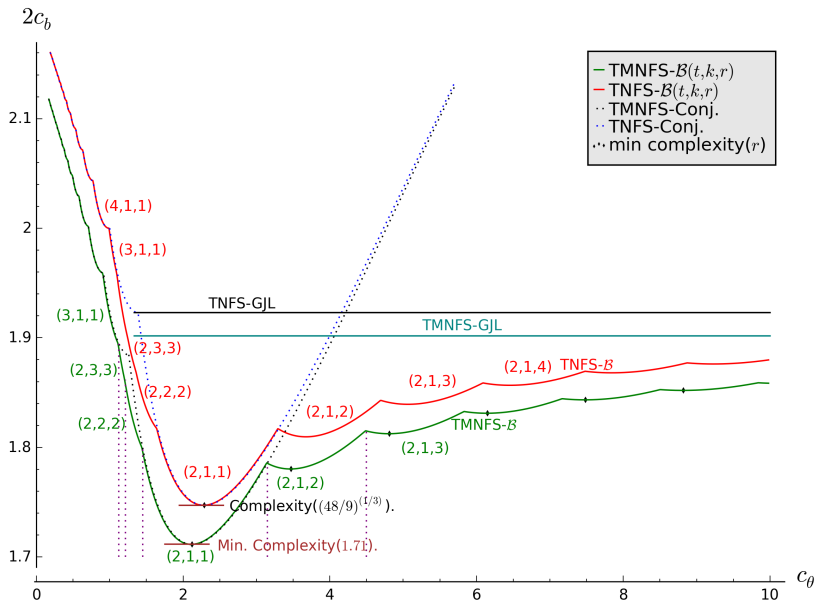
$$c_\theta = c_p c_\eta. \quad (3)$$



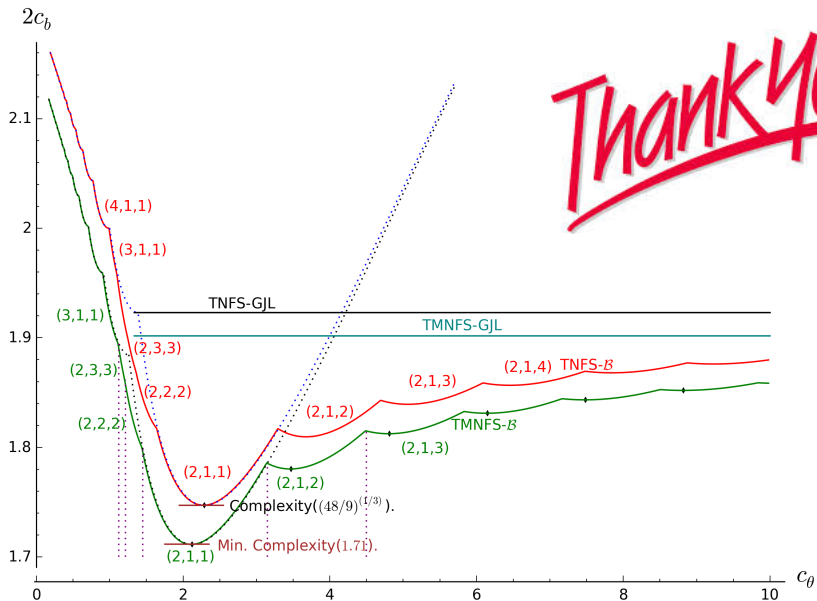
Complexity Plot for Medium Prime Case



MTNFS and TNFS Combined Plot



MTNFS and TNFS Combined Plot



Thank You!

