# Breaking the power-of-two barrier: noise estimation for BGV in NTT-friendly rings

Andrea Di Giusto[1] and Chiara Marcolla[2]

1 Eindhoven University of Technology, Eindhoven, the Netherlands 2 Technology Innovation Institute, Abu Dhabi, United Arab Emirates,

## Why non-power-of-two polynomial?

Let $\mathcal{R} = \mathbb{Z}[x]/\langle \Phi_m(x) \rangle$, where $\Phi_m(x)$ is the cyclotomic polynomial of degree $n = \phi(m)$.
Usually $m = 2^i$ ($n = m/2$ and $\Phi_m(x) = x^n + 1$) $\implies$ gaps in security estimates.
To fill the gaps, we explore the case $m = 2^i 3^j$:
Now $n = m/3$ and $\Phi_m(x) = x^n - x^{n/2} + 1$ $\implies$ the structure of $\mathcal{R}$ changes.

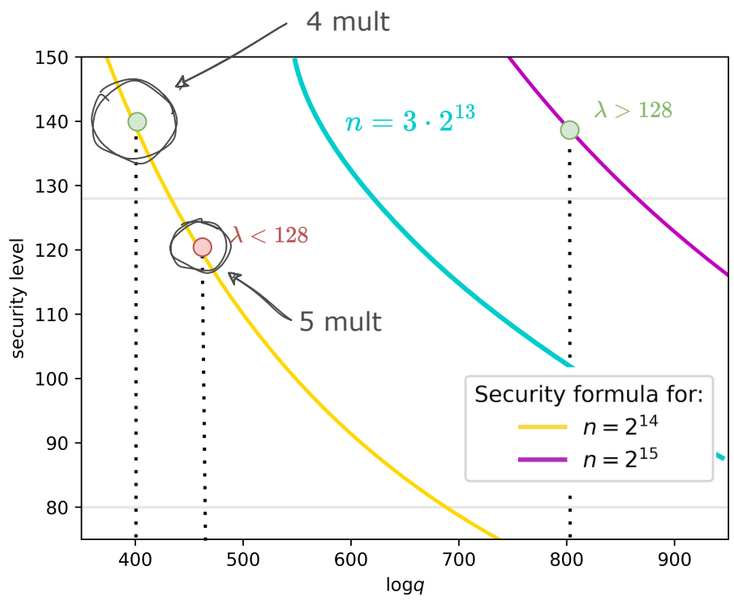
1. Every operation increases the error.
2. Security & Parameters problem:

   # operations ↑ $q$ ↑ $\lambda$ ↓

   # operations ↑ $q$ ↑ $\lambda$ = $n$ ↑
3. Decrease the polynomial degree $n$

   ⇩

   Decrease the length of ciphertexts.




| | M | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|
| $n = 2^{14}$ | $\log q$ | 379 | 461 | 542 | 624 | 707 | 789 | 870 |
| | $\lambda$ | 147 | 119 | 101 | 88 | 78 | 71 | 65 |
| $n = 2^{13} \cdot 3$ | $\log q$ | 352 | 425 | 499 | 572 | 645 | 719 | 793 |
| | $\lambda$ | 259 | 208 | 173 | 149 | 131 | 117 | 105 |
| $n = 2^{15}$ | $\log q$ | 392 | 476 | 560 | 645 | 730 | 815 | 899 |
| | $\lambda$ | 310 | 248 | 206 | 176 | 153 | 136 | 123 |
| $n = 2^{14} \cdot 3$ | $\log q$ | 364 | 439 | 513 | 588 | 671 | 748 | 824 |
| | $\lambda$ | 562 | 449 | 372 | 317 | 271 | 239 | 214 |

## Coefficient variance in random products

Ciphertexts are random polynomials $a(x) \in \mathcal{R}_q = \mathcal{R}/q\mathcal{R}$ having centered coefficients with variance $V_a$.

$$V_a \implies \text{norm estimation} \implies \text{error estimation.}$$

**Noise estimation** through homomorphic operations: we use the canonical norm with the estimate $\|a\|^{can} \leq 6\sqrt{nV_a}$ to keep track of the noise growth.
**Issue**: Bound $V_c$ when $c(x) = a(x)b(x) \in \mathcal{R}$, $a(x), b(x)$ random.

- For $m = 2^i$, $V_c \leq nV_aV_b$ (diagonal covariance matrix).
- For $m = 2^i 3^j$ the covariance matrix is obtained using the NTT algorithm:

$$\mathsf{CovM}(\mathbf{c}) = \begin{pmatrix} \mathsf{Diag}(\alpha_0, \ldots, \alpha_{n/2-1}) & \mathsf{Diag}(\beta_0, \ldots, \beta_{n/2-1}) \\ \mathsf{Diag}(\beta_0, \ldots, \beta_{n/2-1}) & \mathsf{Diag}(\alpha_{n/2}, \ldots, \alpha_{n-1}) \end{pmatrix}$$

where

$$\alpha_k = \begin{cases} \left(\frac{3}{2}n - (k+1)\right) V_aV_b & \text{if } 0 \leq k < n/2 \\ \frac{3}{2}nV_aV_b & \text{if } n/2 \leq k < n \end{cases}$$
$$\beta_k = (k + 1 - n)V_aV_b \qquad 0 \leq k < n/2 \,.$$

and so $V_c \leq \frac{3}{2}nV_aV_b$ in our estimates.

## NTT-friendly rings

Let $\Psi$ be the CRT isomorphism

$$\begin{array}{ccc} \mathcal{R}_q & \to & \mathcal{R}_q^l \times \mathcal{R}_q^r \\ \sum_{i=0}^{n-1} f_i x^i & \to & \left(\sum_{i=0}^{n/2-1} f_i^l x^i, \sum_{i=0}^{n/2-1} f_i^r x^i\right) \end{array}$$

$m = 2^i$: with radix-2 butterfly NTT algorithm, the computation of polynomial products in $\mathcal{R}_q$ requires $O(n \log n)$ operations.

$$\Phi_m(x) = x^n + 1 = (x^{n/2} + \zeta_2)(x^{n/2} - \zeta_2)$$
$$\begin{pmatrix} f_i^l \\ f_i^r \end{pmatrix} = \begin{pmatrix} 1 & -\zeta_2 \\ 1 & \zeta_2 \end{pmatrix} \begin{pmatrix} f_i \\ f_{i+n/2} \end{pmatrix}$$

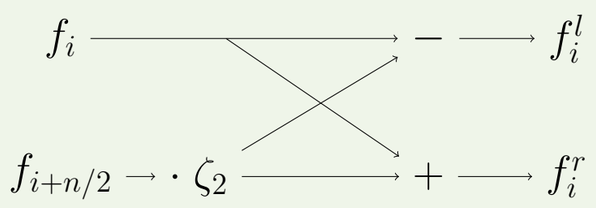



Figure 1: Cooley-Tukey radix-2 butterfly

$m = 2^i 3^j$: similar solution, with one extra addition (red arrow in the diagram) for each butterfly iteration in the first level.

$$\Phi_m(x) = x^n - x^{n/2} + 1 = (x^{n/2} - \zeta_6)(x^{n/2} - \zeta_6^5)$$
$$\begin{pmatrix} f_i^l \\ f_i^r \end{pmatrix} = \begin{pmatrix} 1 & \zeta_6 \\ 1 & 1 - \zeta_6 \end{pmatrix} \begin{pmatrix} f_i \\ f_{i+n/2} \end{pmatrix}$$

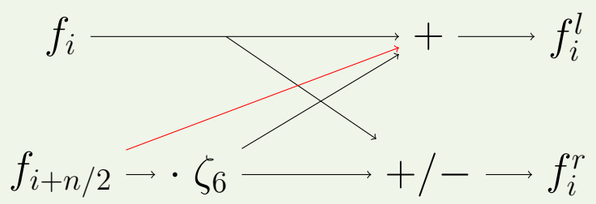
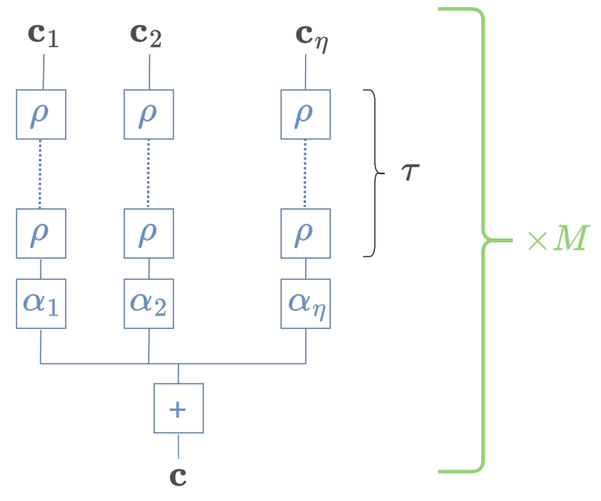



Figure 2: Alternative first-layer butterfly

The other layers are similar to the radix-2, so again $O(n \log n)$. **Extra additions are not costly**.

## Considering BGV...

BGV example with
$\eta = 9$ $\tau = 8$ $\alpha_i \neq 1$ $t = 64$ $\lambda_{\text{target}} \geq 128$




Notations

$M$ = # multiplications
$\eta$ = # summands
$\tau$ = # rotations
$\alpha$ = constant multiplication

## References

https://eprint.iacr.org/2023/783

Contact Information

- A. Di Giusto: a.di.giusto@tue.nl
- C. Marcolla: chiara.marcolla@tii.ae