Extended External Products of Ciphertexts with Automorphisms and Applications

Olivier Bernard   Marc Joye

FHE.org 2025 ▪ Sofia, March 25, 2025

Key Contributions

Advancements in **automorphism-based** bootstrapping: closing the gap between binary and **Gaussian keys**

- Novel **traversal blind rotation algorithm** optimizing the number of key switches
- Introduction of an **automorphism-parametrized** external product **removing** automorphism **key switches**

Combined ⇝ **Aut-Parametrized Blind Rotation**: **efficient tradeoffs** between key sizes and efficiency/noise

- **46% reduction** in key switches with **similar key material** as LLW⁺ (TCHES 2024)
- **over 99%** reduction in key switches with **moderate** (9×) **increase** in key material

Theoretical framework aligning with experimental results

Aut-Parametrized External Product

- New **GGSW-like** ciphertext **format** (GGSW iff $\psi = \mathrm{id}$)

$$\mathrm{GLWE}_{\mathfrak{z}}^{\circledast,\psi}(\bar{\mu}) := \left\{\mathrm{GLWE}_{\mathfrak{z}}^{\nabla}(-\psi(\mathfrak{z}_1)\cdot\bar{\mu}), \dots, \mathrm{GLWE}_{\mathfrak{z}}^{\nabla}(-\psi(\mathfrak{z}_k)\cdot\bar{\mu}), \mathrm{GLWE}_{\mathfrak{z}}^{\nabla}(\bar{\mu})\right\}$$

for Gagdet ciphertexts $\mathrm{GLWE}_{\mathfrak{z}}^{\nabla}(\mu) \leftarrow \left(\mathrm{GLWE}_{\mathfrak{z}}(g_i\cdot\mu)\right)_{1\le i\le \ell}$

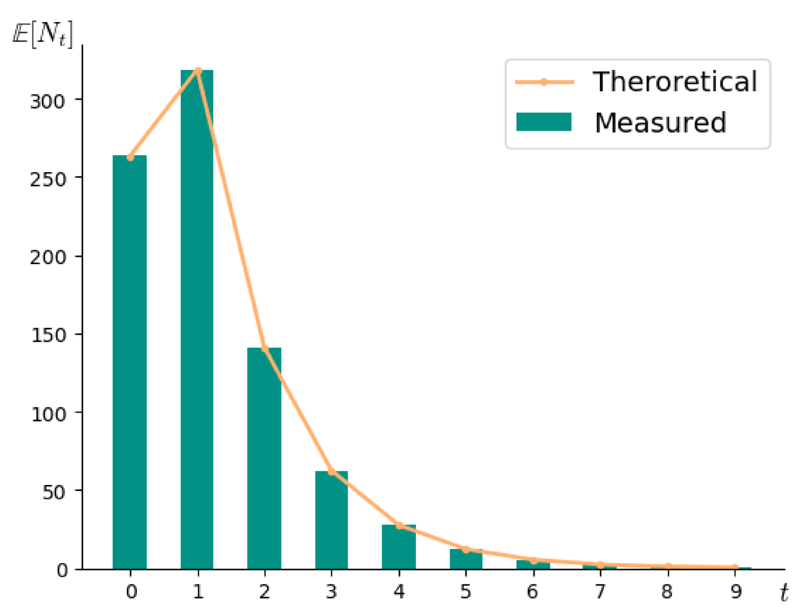
- **Automorphism-parametrized** external product

$$\mathrm{GLWE}_{sk}(\mu) \circledast_{\psi} \mathrm{GLWE}_{sk}^{\circledast,\psi}(\bar{\mu}) := \psi\left(\mathrm{GLWE}_{sk}(\mu)\right) \circledast \mathrm{GLWE}_{sk}^{\circledast,\psi}(\bar{\mu}) \rightsquigarrow \mathbf{GLWE}_{sk}\left(\psi(\mu)\cdot\bar{\mu}\right)$$

- **No automorphism key switch!**
- **Same noise** as classical external product ($\psi = \mathrm{id}$)
- Also applicable to **NTRU/NGS** or **any** `Enc/Enc`$^{\circledast}$

Theoretical Analysis

- **Average** number of **gaps** of size t:



- **Average** number of **aut. key switches** in $\mathcal{S}$-parametrized Blind Rotation for $\mathcal{S} = \{\tau_{\pm 1}, \tau_{\pm g}, \dots, \tau_{\pm g^{K}}\}$:

$$\mathbb{E}\left[\kappa_{\infty}^{\mathcal{S}\text{-}AUT}\right] \approx \left(1 + \frac{N}{2}\left(1 - \mathrm{e}^{-2n/N}\right)\right)\cdot \mathrm{e}^{-K\cdot 2n/N}$$

Aut-Parametrized Blind Rotation

Input: $\boldsymbol{c} \leftarrow (a_1, \dots, a_n, b) \in (\mathbb{Z}/2N\mathbb{Z})^{n+1}$, $a_i \in (\mathbb{Z}/2N\mathbb{Z})^{\times}$; $\upsilon \in \mathcal{R}_q$

Data: A set $\mathcal{S}$ of **admissible automorphisms**

- **Extended** bootstrapping keys $\mathrm{GLWE}_{\mathfrak{z}}^{\circledast,\psi}(x^{s_i})$, $\psi \in \mathcal{S}$ $(1 \le i \le n)$
- Automorphism keys $ak^{\mathcal{S}\text{-}AUT}$ for a **window size** w

Output: $\boldsymbol{c} \leftarrow \mathrm{GLWE}_{\mathfrak{z}}(x^{-\mu}\cdot\upsilon) \in \mathcal{R}_q^{k+1}$ with $\mu = b - \sum_{i=1}^{n} a_i s_i$

Initialization: $ACC \leftarrow (0, \dots, 0, x^{-b}\cdot\upsilon(x))$,
for $t = N/2 - 1$ **down to** 0 **such that** $I_t^{+} \cup I_t^{-} \neq \varnothing$ **do**
  for $\epsilon \in \{\epsilon_{first}, -\epsilon_{first}\}$ **such that** $I_t^{\epsilon} \neq \varnothing$ **do**
    // New **jumping strategy**
    Total jump is $\sigma\cdot g^{\delta} = \epsilon_{old}\cdot g^{t_{old}}/(\epsilon\cdot g^{t})$
    Find $(\delta_*, \epsilon_*) \in \mathcal{S}_*$ **alphabetically closest** to (δ, σ)
    Apply τ_v for $v = \sigma\cdot g^{\delta}/(\epsilon_*\cdot g^{\delta_*})$ with **steps of size** $\le w$
    // **First** external product **parametrized by** $\psi = \tau_{\epsilon_*\cdot g^{\delta_*}} \in \mathcal{S}$
    $ACC \leftarrow ACC \circledast_{\psi} bsk_{\psi}^{\mathcal{S}\text{-}AUT}[I_t^{\epsilon}[0]]$
    // Compute all remaining external products for I_t^{ϵ}
    for $i \in I_t^{\epsilon} \setminus \{I_t^{\epsilon}[0]\}$ **do**
      $ACC \leftarrow ACC \circledast bsk_{\mathrm{id}}^{\mathcal{S}\text{-}AUT}[i]$

Finalization: Apply τ_u for $u = \epsilon_{old}\cdot g^{t_{old}}$ with steps of size $\le w$
return ACC

Performance Measurements

Parameters: $n = 834$, $N = 2048$ and $k = 1$ $(\mathrm{e}^{2n/N} \approx 2.25)$

Method	w_{opt}	Keys (#GLWE$^{\nabla}$)	#(KS)	
[LMK⁺23]	20	$2n + 21$	688.5	
[LLW⁺24]	10	$\mathbf{4n + 10}$	**571.4**	
New $\mathcal{S}$-Parametrized Algorithms				
$\mathcal{S} = \{\boldsymbol{\tau_{\pm 1}}\}$	10	$\mathbf{3n + 11}$	**571.9**	
$\mathcal{S} = \{\mathbf{id}, \boldsymbol{\tau_g}\}$	±9	$\mathbf{3n + 19}$	**495.5**	
$\mathcal{S} = \{\mathbf{id}, \boldsymbol{\tau_{\pm g}}\}$	9	$\mathbf{4n + 10}$	**368.7**	$\times\frac{1}{2.25}$
$\mathcal{S} = \{\tau_{\pm 1}, \tau_{\pm g}\}$	9	$5n + 10$	254.0	
$\mathcal{S} = \{\tau_{\pm 1}, \tau_{\pm g}, \tau_{\pm g^2}\}$	8	$7n + 9$	112.5	$\times\frac{1}{2.25}$
⋮	⋮	⋮	⋮	$\times\frac{1}{59}$
$\mathcal{S} = \{\boldsymbol{\tau_{\pm g^k}} \mid 0 \le k \le 8\}$	2	$\mathbf{19n + 3}$	**1.9**	

ZAMA

Resources
zama.ai/blog
github.com/zama-ai

Read our full paper on **ePrint 2025/163**