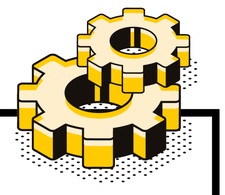
Homomorphic Evaluation of LWR-based PRFs and Application to Transciphering

Amit Deo Marc Joye Benoît Libert Benjamin R. Curtis Mayeul de Bellabre

FHE.org 2025 • Sofia, March 25, 2025



Main Ideas

- **Fast homomorphic** evaluation of Learning with Rounding PRF
- Methods utilize **native** TFHE operations; e.g., blind rotation
- Optimization 1: Securely tweak PRF definition for **negacyclicity**
- Optimization 2: Tweak parameters to save **∼ 40%** of PBS time
- Applications: Transciphering and blockchain games

Application: Transciphering

A client can send large amounts of data to the cloud using **transciphering**. The message M is encrypted and stored on the cloud **compactly** as

$$\left(x, M \oplus \mathrm{PRF}_{\boldsymbol{k}}(x)\right)$$

with a secret key $\boldsymbol{k}$. The cloud uses a homomorphically encrypted k to recover an FHE encryption of M, which **reduces transmission costs**

Technical Details

$$\mathbf{A} = H(x) \in \mathbb{Z}_q^{m \times n} \qquad \boldsymbol{k} \leftarrow \{0,1\}^n$$

Original PRF	Tweaked PRF
$\mathrm{PRF}_{\boldsymbol{k}}(x) = \left\lfloor \frac{p}{q} \mathbf{A} \cdot \boldsymbol{k} \right\rceil \bmod p$	$\mathrm{PRF}'_{\boldsymbol{k}}(x) = (-1)^{msb} \cdot \mathrm{PRF}_{\boldsymbol{k}}(x)$
Security directly from standard LWR with binary secret	Security via reduction from original PRF
"non-negacyclic"	"negacyclic"

Negacyclic functions requires a **single** PBS

↓

Original PRF requires **two** sequential PBSes and **tweaked** PRF requires **one** PBS (i.e., has PBS **depth 1**)

Experimental Results

We consider two parameter sets presented in the below table for our implementation

	n	n_{LWR}	N	q
`MESSAGE_1_CARRY_1`	702	409	512	2^{64}
`MESSAGE_2_CARRY_2`	742	445	2048	2^{64}

Single-threaded results: On `hpc7a.96xlarge`, the depth-1 construction with `1_1` parameters yields **∼ 1070 encrypted PRF bits/s**. The second result on an Apple MacBook yields ∼ 808 PRF bits/s

Parameter set	`MESSAGE_1_CARRY_1`	`MESSAGE_2_CARRY_2`
Plaintext bits	3	4
Latency (ms)	2.803 / 3.714	6.033 / 8.187
Throughput (bits/s)	**1070** / 808	829 / 611
Bootstrap Key	11.0 MB	23.9 MB
PRF Eval Key	**6.4 MB**	13.9 MB

Optimization improves the 2_2 parameter throughput to **961/981 bits/s** with PRF Eval key size 9 MB

ZAMA

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

Full paper: ePrint 2024/665