To appear at S&P 2025

Accelerated Authenticated Matrix Triple Generation with Scalable Prime Fields via Optimized HE Packing

Hyunho Cha, Intak Hwang, Seonhong Min, Jinyeong Seo and Yongsoo Song
Seoul National University

서 울 대 학 교
SEOUL NATIONAL UNIVERSITY

Summary

✓ **Generalized BFV**

New packing method for BFV, which supports large prime field with small error growth.

✓ **Proof of Plaintext Knowledge for Genearlized BFV**

New PoPK Protocol for Generalized BFV without noise flooding, utilizing randomized encoding and Hint-MLWE problem.

✓ **Faster Matrix Multiplication Algorithm**

New ciphertext-ciphertext matrix multiplication algorithm, which is asymptotically better than prior works.

Generalized BFV

To create authenticated triple in SPDZ online phase, large plaintext modulus is needed to guarantee sufficient security for MACs. We devise a new packing method that supports large prime modulus but with significantly lower error and ciphertext modulus.

✓ **Standard BFV**

In the usual BFV scheme, plaintext space is

$$\mathbb{Z}[X]/(t, X^N+1) \simeq \mathbb{Z}_t^N$$

✓ **Generalized BFV**

In Generalized BFV scheme, plaintext space is

$$\mathbb{Z}[X]/(X^{N/r}-b, X^N+1) \cong \mathbb{Z}[X]/(b^r+1, X^{N/r}-b) \cong \mathbb{Z}_{t := b^r+1}^{N/r}$$

	Standard BFV	Generalized BFV
Plaintext Space	t	$t = b^r + 1$
# of Slots	N	N / r
Error Growth	$\approx \log t$	$\approx \log b$

Proof of Plaintext Knowledge

A Proof of Plaintext Knowledge (PoPK) protocol for Generalized BFV ciphertexts are needed to guarantee the well-formedness of ciphertexts. Prior works relied on *noise flooding*, which resulted in exponential soundness slack. In our work, we overcome this issue by using randomized packing.

✓ **Randomized Packing**

In the first phase, each party samples the packing from

$$D_{m+P\mathbb{Z}^N, \sigma P}$$

where P is the negacyclic matrix of $X^{N/r} - b$.

✓ **Hint-MLWE**

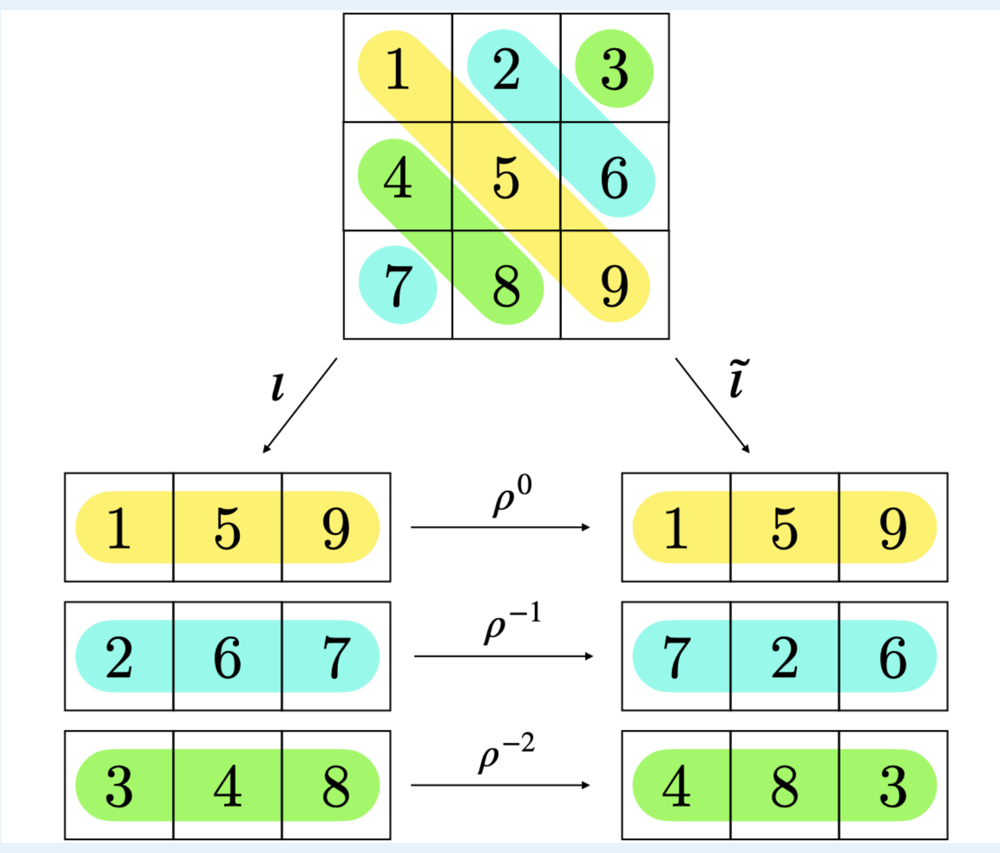
Once plaintext is randomized as Gaussian distribution, we can simulate the PoPK transcript via reduction to Hint-MLWE.

Matrix Multiplication Algorithm

Due to the recent rise of machine learning, creating matrix triples became important. We construct a new matrix multiplication algorithm, which requires only $O(N)$ key-switching.

✓ **Shifted Diagonal Packing**

Along with the usual diagonal packing used in Halevi-Shoup method, we introduce a new matrix packing called Shifted Diagonal Packing.



✓ **Faster Matrix Multiplication**

- multiply diagonally packed and shifted diagonally packed matrix
- Lazy Key-switching

	Jiang et al.	Halevi-Shoup	Ours
Decomp	$O(d^2)$	$O(d^2)$	$O(d^2)$
Inner Product	$O(d^3)$	$O(d^3)$	$O(d^2)$
Ring Arithmetic	$O(d^3)$	$O(d^3)$	$O(d^3)$
Depth	2	1	1
# Rotation key	$3d-3$	$d-1$	$d-1$

✓ **Batching**

Batching multiple matrices is also possible, achieving optimal packing rate for any power-of-two dimension matrix.

Experimental Results

✓ For 128-bit prime fields, our scheme reduces the key sizes by a factor at most 125, and reduces the runtime of matrix triple generation by a factor of at most 34.5x.

✓ Intel(R) Xeon(R) Platinum 8268 CPU @ 2.90 GHz and 378 GB RAM

		Ours (Param I)	Prev [CKR+20]	Improvement
d	128	0.99s	34.25s	34.5x
	256	6.84s	207.14s	30.28x
	512	48.62s	1459.63s	30.02x
Key size		1.45GB	27.4GB	18.9x