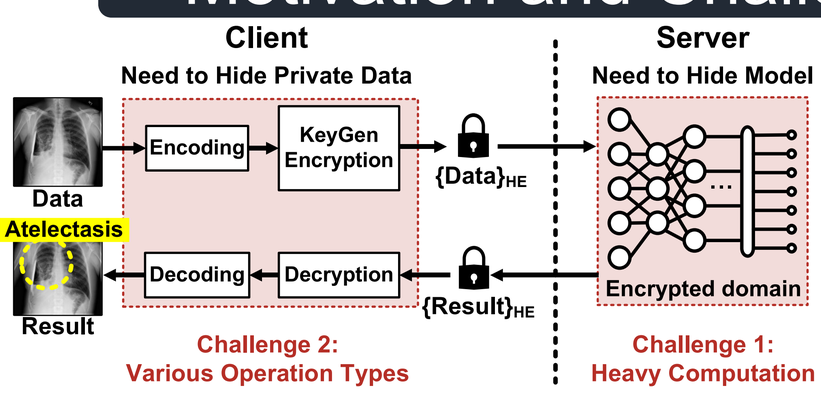
IDEC Chip Design Contest

A 28nm Reconfigurable Security Processor with Unified MAC Array for Private Inference

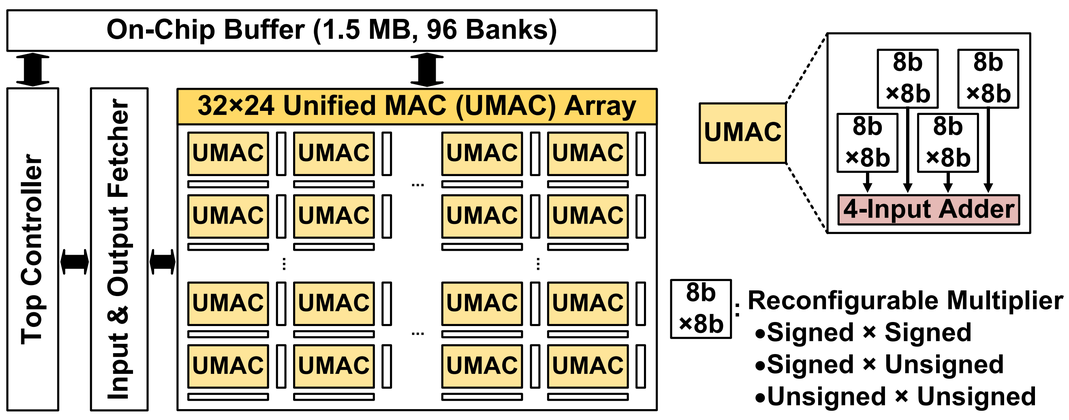
Suheun Moon*[1], Sangouk Jeon*[1], Sangsu Jeong [1], Jonghun Kim[2], Hyunjin Park[2], Yoonmyung Lee[2], Dongsuk Jeon [1], [1] Seoul National University, [2]Sungkyunkwan University

Motivation and Challenges



▶ Privacy-Preserving neural network inference protocol using HE

Overall Architecture

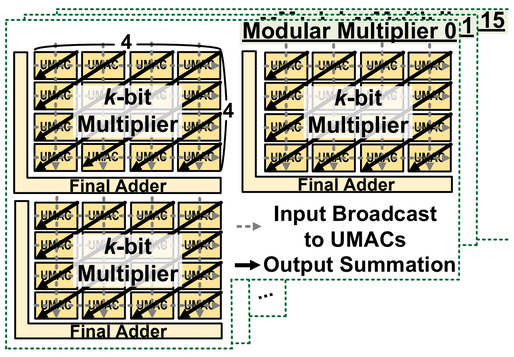


Unified MAC Architecture

▶ Array-Level UMAC Configuration

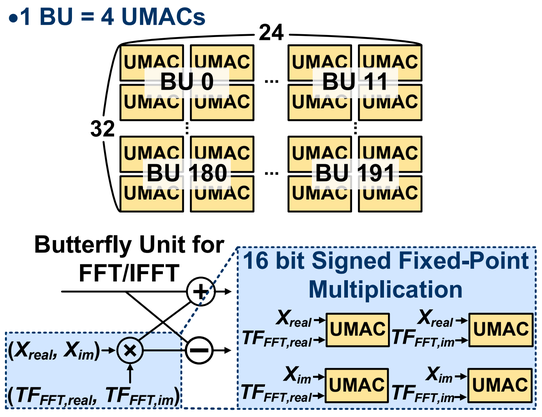
NTT/INTT Mode

- Configured as 16 MMs
- 1 Barrett MM = 48 UMACs



FFT/IFFT Mode

- Configured as 192 BUs
- 1 BU = 4 UMACs

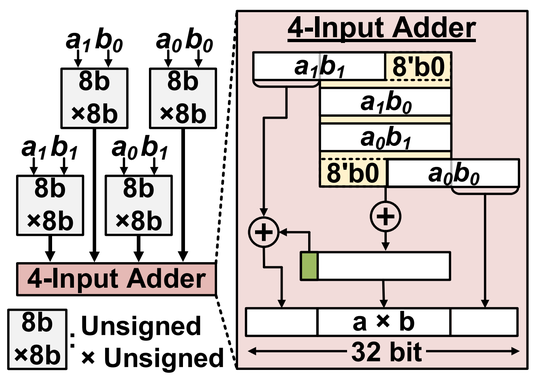


▶ Unit-Level UMAC Configuration

NTT/INTT Mode

16-bit Unsigned Multiplication ($a \times b$)

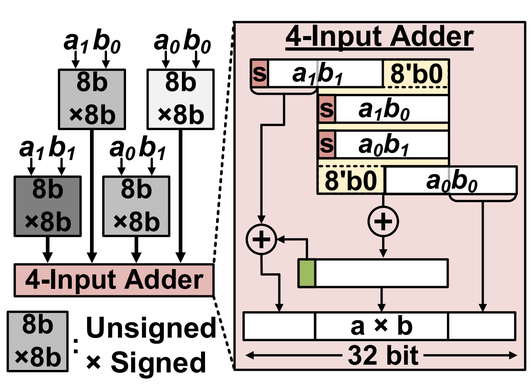
$a = (a_1 << 8) + a_0$, $b = (b_1 << 8) + a_0$



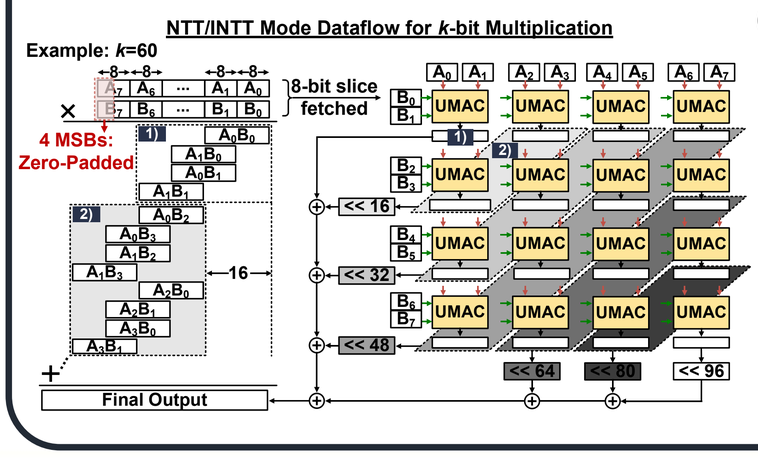
FFT/IFFT Mode

16-bit Signed Multiplication ($a \times b$)

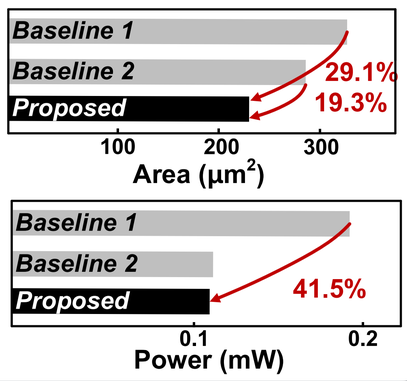
$a = (a_1<<8) + a_0$, $b = (b_1<<8) + b_0$,
(a_1 ,b_1): Signed / (a_0, b_0): Unsigned



▶ NTT/INTT mode Detail

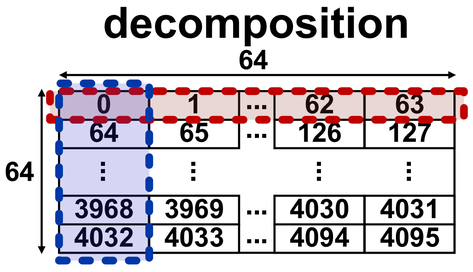


▶ Reconfigurable Adder Comparison



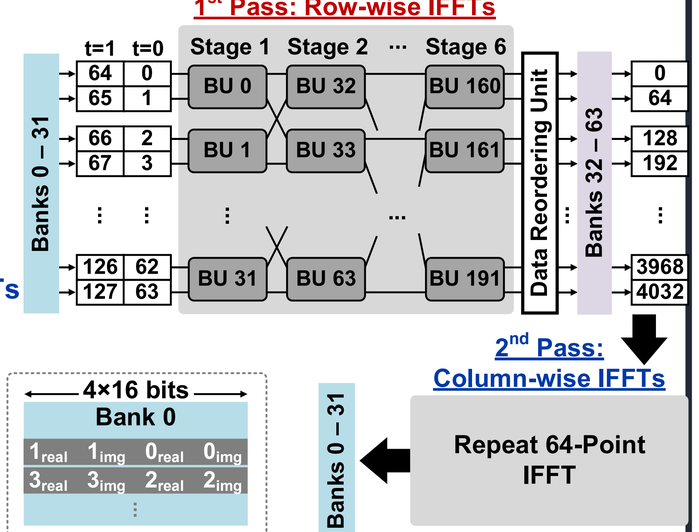
FFT/IFFT Mode Detail

▶ FFT/IFFT decomposition



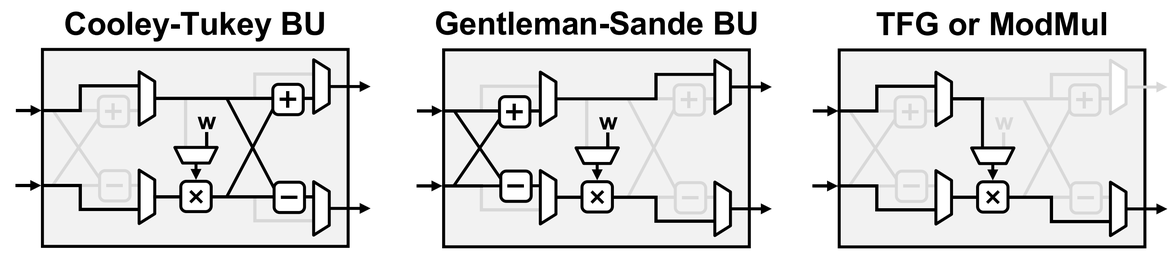
Large-scale FFT/IFFT is efficiently computed by row-column decomposition

▶ FFT/IFFT dataflow

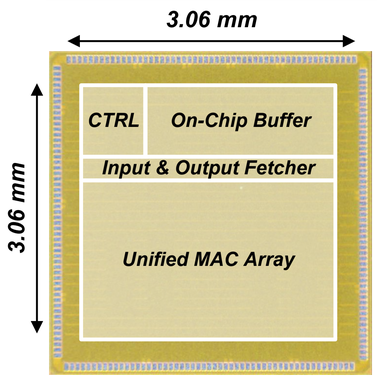


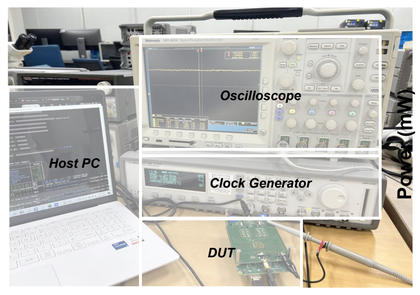
Reconfigurable Butterfly Unit

- ⊠ : Barrett ModMul
- ⊞⊟ : ModAdd/Sub

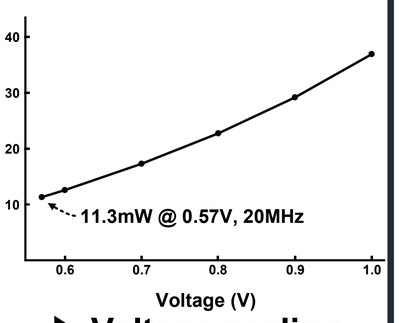


Die photography and Measurement





▶ Measurement setup using Opal kelly board



▶ Voltage scaling graph

Result & Conclusion

	This Work	CICC'19 [1]	ESSERC'23 [2]	TCAS-II'24 [3]	ISSCC'25 [4]
Technology	28nm FD-SOI	55nm	28nm	40nm (Synthesized)	28nm
Application	HE	HE	HE	HE	HE
Area (mm²)	9.36	3.13	1.69	3.22	5.4
Frequency (MHz)	20 – 110	0.01 – 60	0.5 – 157	210	125 – 625
Voltage (V)	0.57 – 1.00	0.28 – 1.20	0.64 – 1.10	–	0.70 – 1.10
Supported Operation	En/Decoding, En/Decryption, KeyGen (sk, pk)	En/Decryption, KeyGen (sk, pk)	En/Decryption	En/Decoding, En/Decryption	En/Decryption, KeyGen (sk, pk) Evaluation
Power (mW)	11.3 – 169.6	4.5	12.6	–	138 – 1185
HE Parameter ($\log_2 Q$, N)	(1292, 65536)	(34, 16)	(109, 4096)	(162, 8192)	(96, 4096)
Norm. NTT Energy* (pJ)	0.13	5.53	0.48	–	0.16
Norm. Encryption Energy* (pJ)	0.73	23.26	1.93	–	0.86

* Normalized Energy = (Total Energy) / ($\log_2 Q \times N \log N$)

▶ Highly reconfigurable architecture, minimizing hardware overhead

▶ The processor achieves a normalized NTT energy and encryption energy of 0.13 pJ and 0.73 pJ, outperforming state-of-the-art HE processors by 18.8% and 15.1%, respectively

[1] "A 55nm50nj/encode 13nj/decode homomorphic encryption crypto-engine for iotnodes to enable secure computation on encrypted data," CICC, 2019
[2] "A10.33 μj/encryption homomorphic encryption engine in 28nm cmos with4096-degree 109-bit polynomials for resource-constrained iot clients,", ESSERC, 2023
[3] "Acompact and efficient hardware accelerator for rns-ckks en/decoding anden/decryption," TCAS-II, 2024
[4] 17.2 a 28nm4.05μj/encryption 8.72khmul/s reconfigurable multi-scheme fully homo-morphic encryption processor for encrypted client-server computing," ISSCC, 2025