先进密码算法硬件加速

高迎雪

gyingxue@njupt.edu.cn

南京邮电大学

集成电路科学与工程学院

2026年5月7日

目录

研究背景：量子计算机及攻击算法对公钥密码体系的严峻挑战

➢ 量子计算机?

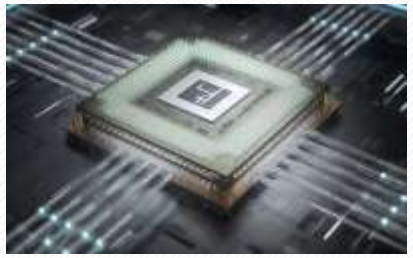
- 量子计算机是一种以量子比特为信息处理单元，有望实现**颠覆性算力突破**的新型计算机。

➢ 量子计算机发展

- 谷歌研究团队在最新论文中表明，随着量子错误纠正技术的迭代，破解 ECDSA-256所需的**量子资源已较此前预期降低 20 倍**；
- 量子计算初创企业 Oraatomic 表示采用中性原子架构的量子计算机仅需约 1 万个可重构量子比特，即可完成对 RSA-2048 的破解 。

➢ 量子攻击算法（Shor算法-1994年，Grover算法-1996年）

- 一旦实用化的量子计算机问世，Shor算法便能以多项式时间复杂度，解决在经典计算机上需要指数级时间的问题，使现有**公钥密码体系**不堪一击。



谷歌Willow芯片

祖冲之三号

九章

2025物理诺奖：宏观尺度观测量子隧穿效应，系**超导量子计算领域的重要开端。**

研究背景：公钥密码体系

公钥密码体系应用领域


国防军事


交通高铁


金融领域


智能驾驶


互联网通信

当前：经典公钥密码算法

RSA	ECC	SM系列
特点：兼容性好，应用广泛，效率较慢	**特点**：适合资源受限环境，效率较快	**特点**：国家标准，效率较快
场景：数据加密、数字签名、密钥交换	**场景**：移动设备、公钥证书、TLS	**场景**：SM2用于公钥加密/签名

迁移

未来：后量子密码（PQC)算法

- KYBER
- Dilithium
- FALCON
- SPHINCS+

- 基于新的数学困难问题
- 抗量子计算攻击
- 多样化的算法类型
- 性能与利用率的研究

研究背景：PQC发展进程

➢ 美国后量子密码进程

- 美国率先在**政府战略部署**，**NIST标准化进程**和**工业迁移应用**角度进行布局。

量子安全生态及NIST、IETF相关参与方布局

2022年5月4日，拜登总统签署了**国家安全备忘录**，要求美国国家标准技术研究院（NIST）牵头PQC算法的开发与标准化。

2024年8月13日，NIST正式发布三项**PQC标准**：FIPS 203（ML-KEM）、FIPS 204（ML-DSA）及FIPS 205（SLH-DSA）。

2024年11月12日，**谷歌** Chrome 131版本正式支持在TLS 1.3协议中使用混合后量子密钥交换算法。

2025年3月17日，**Cloudflare**宣布为所有CDN用户免费提供混合PQC算法的HTTPS加密服务。

2025年4月8日，**OpenSSL** 3.5.0原生支持三项PQC标准。

2025年6月6日，特朗普总统**签署行政令**，要求2025年12月1日前公布PQC产品目录，各联邦政府机构必须尽快启动PQC迁移。

2025年8月，**美国政府网站、国务院网站及多项政务服务系统**、互联网关键基础设施已陆续启用后量子密码HTTPS加密。

军事安全：美军方非常重视后量子密码的研究，美国家安全局已研究出两种后量子加密方案：NewHope（基于格）和Circuit ORAM（基于多线性映射）。NewHope可以在未来遭受量子破解攻击下确保军方通信安全；Circuit ORAM未来为云存储在遭受量子攻击时提供安全保护。

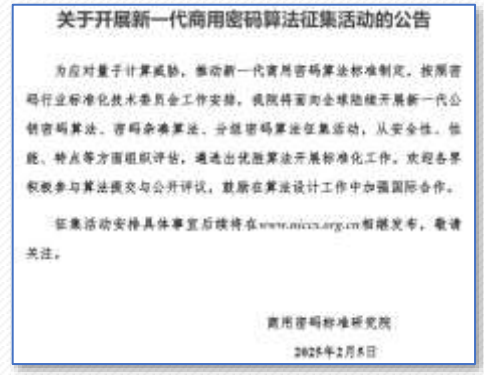
研究背景：PQC发展进程

➢ 我国后量子密码进程

- **2018年6月**，中国密码学会组织了全国密码算法设计竞赛
- **2023年11月**，信通院《后量子密码应用研究报告》
- **2024年6月**，西电广研院《后量子密码迁移白皮书》
- **2024年**，三未信安与江南科友《抗量子密码技术与应用白皮书》
- **2024年12月**，商用密码标准研究院成立
- **2025年2月**，商用密码标准研究院发布公告，在全球范围内公开征集新一代商用密码算法。保证**安全性**，**多样性**，**实用性**和**一体化**等目标。

PQC研究报告与白皮书

商用密码算法征集公告


关于开展新一代商用密码算法征集活动的公告

为应对量子计算威胁，推动新一代商用密码算法标准制定，按照密码行业标准化技术委员会工作安排，我院将面向全球陆续开展新一代公钥密码算法、密码杂凑算法、分组密码算法征集活动，从安全性、性能、特点等方面组织评估，遴选出优胜算法开展标准化工作，欢迎各界积极参与算法提交与公开评议，鼓励在算法设计工作中加强国际合作。

征集活动安排具体事宜后续将在www.nicrs.org.cn相继发布，敬请关注。

商用密码标准研究院

2025年2月5日

研究背景：PQC算法侧发展趋势

➢ PQC算法

- **标准化**：NIST已选定以Kyber(ML-KEM)、Dilithium(ML-DSA)、Falcon(FN-DSA)、SPHINCS+(SLH-DSA)为核心标准，全球商用密码将向主流算法收敛。
- **高性能**：面向物联网、移动设备、云计算等场景，持续推动算法轻量化与高效设计。
- **高安全**：针对侧信道攻击、故障注入等新型威胁，持续优化算法实现安全性。
- **多样性**：保留多技术路线并存（格、哈希等），防止单一数学结构被攻破导致系统性风险。

密码家族	代表算法	优点	缺点
基于格	**Kyber**，**Falcon**，**Dilithium**，NTRU，Saber, FrodokEM, LAC	轻量，高效	数学结构单一
基于编码	Classic McEliece BIKE, **HQC**	历史悠久，安全性深入	公钥巨大
基于哈希	**SPHINCS+** XMSS, MSS	安全性成熟理论基础稳固	签名长、速度慢状态管理复杂
基于多变量	Rainbow, GeMSS	签名快、密钥短	多次出现重大破译
基于同源	SIKE	公钥非常小	潜在风险较高

研究背景：PQC算法介绍

- **以Kyber算法为例**
  - ① 多算子
  - ② 多交互
  - ③ 多阶段
  - ④ 多安全等级

密钥生成阶段

Algorithm 1: Key Generation Process

Input: Random seed rs.
Output: Public key pk, Secret key sk.

1 $(\rho, \alpha) = \text{SHA3\_512}(rs)$;
2 $\hat{A} = \text{Hash}_A(\rho)$;
3 $(s, e) = \text{Hash}_E(\alpha)$;
4 $\hat{s} = \text{NTT}(s)$;
5 $\hat{e} = \text{NTT}(e)$;
6 $\hat{t} = \hat{A} \cdot \hat{s} + \hat{e}$;
7 $pk = \text{Encode}(\hat{t} \mid\mid \rho)$;
8 $sk = \text{Encode}(\hat{s})$;
9 return (pk, sk);

加密阶段

Algorithm 2: Encryption Process

Input: Random seed rs, Public key pk, Message m.
Output: Ciphertext c.

1 $(\hat{t}, \rho) = \text{Decode}(pk)$;
2 $\hat{A}^T = \text{Hash}_A(\rho)$;
3 $(r, e_1, e_2) = \text{Hash}_E(rs)$;
4 $\hat{r} = \text{NTT}(r)$;
5 $u = \text{INTT}(\hat{A}^T \cdot \hat{r}) + e_1$;
6 $v = \text{INTT}(\hat{t}^T \cdot \hat{r}) + e_2 + \text{Decompress}(\text{Decode}(m))$;
7 $(c_1, c_2) = \text{Encode}(\text{Compress}(u, v))$;
8 $c = (c_1 \mid\mid c_2)$;
9 return c

解密阶段

Algorithm 3: D

Input: Secret key sk, Ciphertext c.
Output: Message m.

1 $(u, v) = \text{Decompress}(\text{Decode}(c))$;
2 $\hat{s} = \text{Decode}(sk)$;
3 $m = \text{Encode}(\text{Compress}(v - \text{INTT}(\hat{s} \cdot \text{NTT}(u))))$;
4 return m;

安全等级	度	模数	密文长度（字节）	公钥长度（字节）	私钥长度（字节）
1	256	3329	768	800	1632
3	256	3329	1088	1184	2400
5	256	3329	1568	1568	3168

研究背景：PQC硬件加速挑战

➢ 架构设计挑战

□ 效率挑战

- 1）多样算数结构；2）昂贵执行操作；3）复杂数据交互；

□ 灵活性挑战

- 1）多算子；2）多阶段；3）多安全级别；

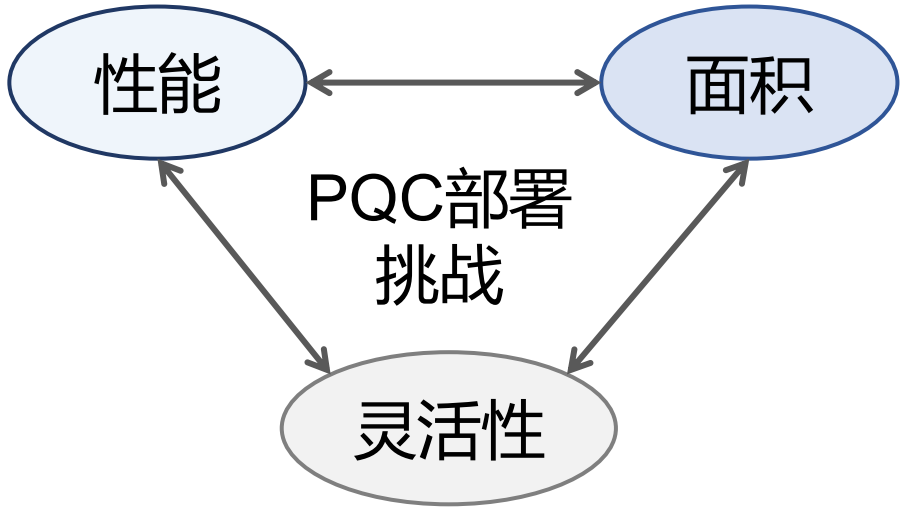
➢ 迁移场景挑战

□ 网络终端

- 低延迟，低能效
- 实时应用

□ 云服务器

- 高能效，高吞吐
- 高传输服务器



后量子密码算法

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

KYBER
Dilithium
FALCON
SPHINCS+

部署

硬件平台

研究背景：PQC硬件加速工作概述

PQC算法

基于格　基于编码　基于多变量　基于哈希　基于超奇异同源

算子实现

核心算子提取 → 核心算子实现优化

硬件单元优化

算子加速

NTT加速器　Schoolbook加速器　Matrix-Vector加速器　……

SHA加速器　Karatsuba加速器

架构集成优化

PQC架构

效率：全固化式硬件架构

灵活性：可重配置硬件架构

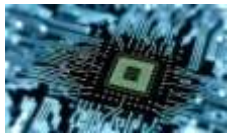
灵活性：基于RISC-V硬件架构

硬件平台

CPU 

GPU  

FPGA 

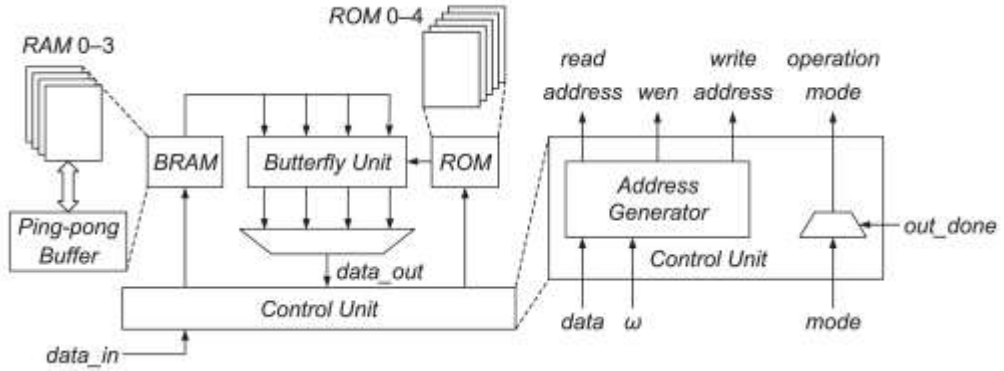
ASIC 

针对PQC硬件架构开展硬件定制化研究

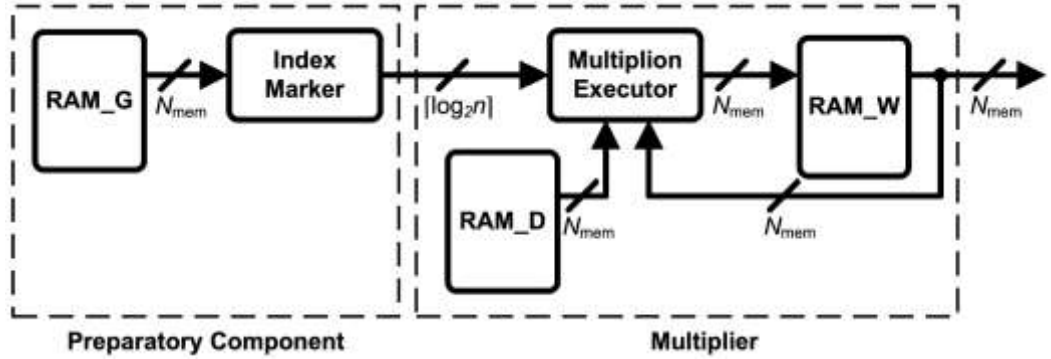
研究背景：PQC硬件加速工作概述

技术路线	实现方式	性能	灵活性	代表性工作	典型平台
全固化式硬件架构	为特定PQC算法深度定制，功能模块以专用硬件逻辑固化实现	计算效率与吞吐率高，能效最优	差，电路固化后无法修改，难以适应算法迭代	[**TC' 23**] High-Speed Hardware; [**J. Inf. Intell.' 24**] A lightweight;	ASIC和FPGA
基于RISC-V硬件架构	基于通用RISC-V核心，通过扩展指令集或协处理器接口进行加速	性能通常低于全固化设计，处于均衡水平	高，指令集可扩展、软件可编程，能快速适配新算法	[**TCHES' 19**] Sapphire; [**CHES' 24**] Optimized Hardware; [**Cryptol. ePrint' 25**] HORCRUX;	支持扩展的RISC-V SoC
可重配置硬件架构	为PQC算法定制硬件单元，并从多层面（如逻辑、数据通路）探究重配置性	性能介于RISC-V架构与全固化架构之间	可通过重配置硬件逻辑来适应算法变化，是灵活性与效率的折衷方案	[**TCAD' 23**] Reconfigurable; [**TVLSI' 24**] An Area-Efficient;	FPGA

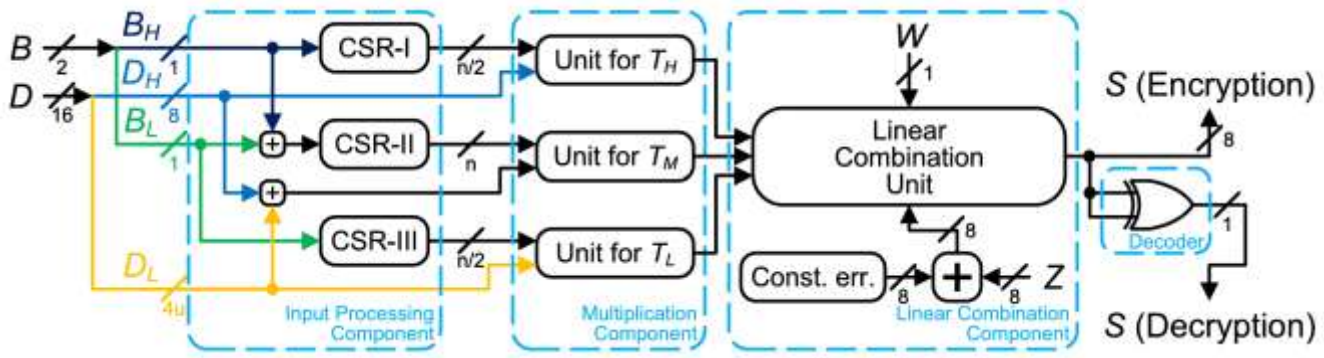
研究背景：PQC算子硬件加速工作举例



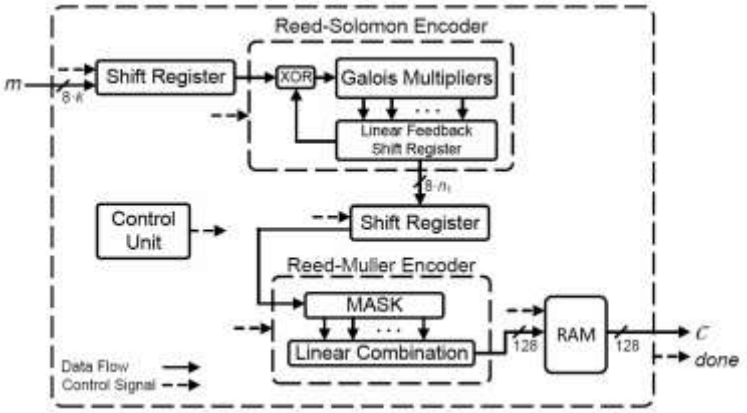
[ICAS' 24] NTT算子优化



[TVLSI' 23] 稀疏多项式乘法算子优化

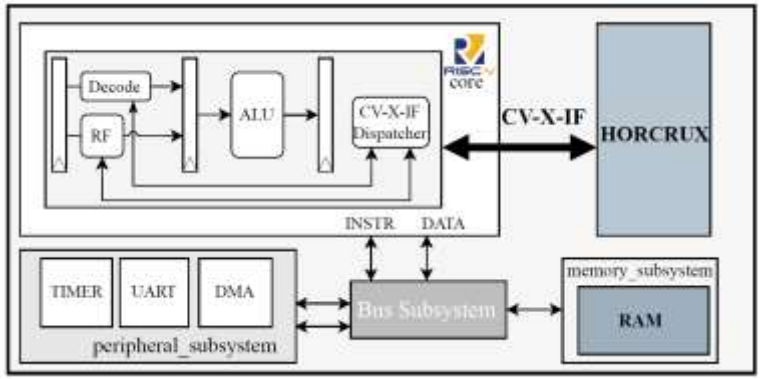


[TRETS' 24] Karatsuba算子优化



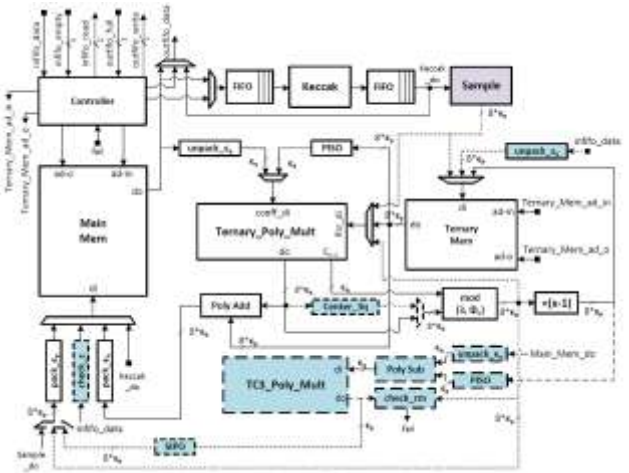
[CAL' 24] 编解码算子优化

研究背景：PQC算法硬件加速工作举例

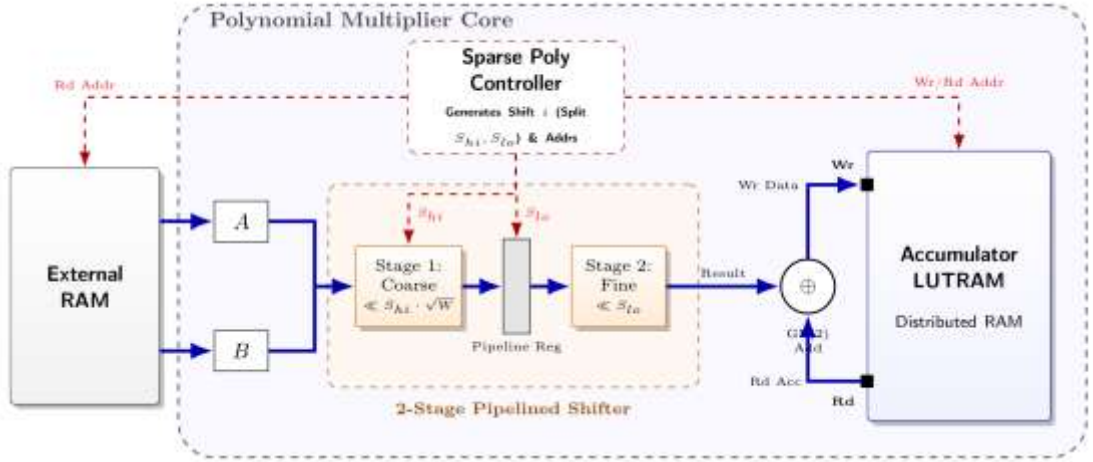


Class	Instruction
KECCAK	rol32_h
	rol32_l
	bcop32
COMPRESS	compress1
	compress2
	compress3
	compress4
REDUCTION	KEM-fast-reduce
	KEM-reduce16
	DSA-fast-reduce
	DSA-reduce32
CBD	cbd3_1, cbd3_2, cbd3_3, cbd3_4
	cbd2_1, cbd2_2, cbd2_3, cbd2_4 cbd2_5, cbd2_6, cbd2_7, cbd2_8
	rej_uniform
GF	karats_1, karats_2 karats_3, karats_4
	gf_carryless_mul_1, gf_carryless_mul_2 gf_carryless_mul_3, gf_carryless_mul_4

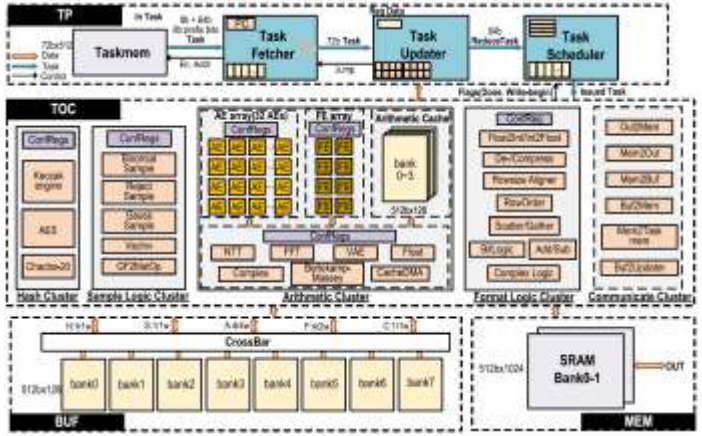
[Cryptol' 25] RISC-V指令集架构



[TC' 23] 全固化式电路设计



[Cryptol' 26] 可配置硬件设计



[ISSCC' 24] PQC系统实现

目录

PQC硬件加速 — 从算子到架构的多层次优化

➢ 研究遵循“**通用→专用→通用**”研究路线，从**算子、电路和架构**三个方面展开，旨在构建高效灵活的PQC硬件架构

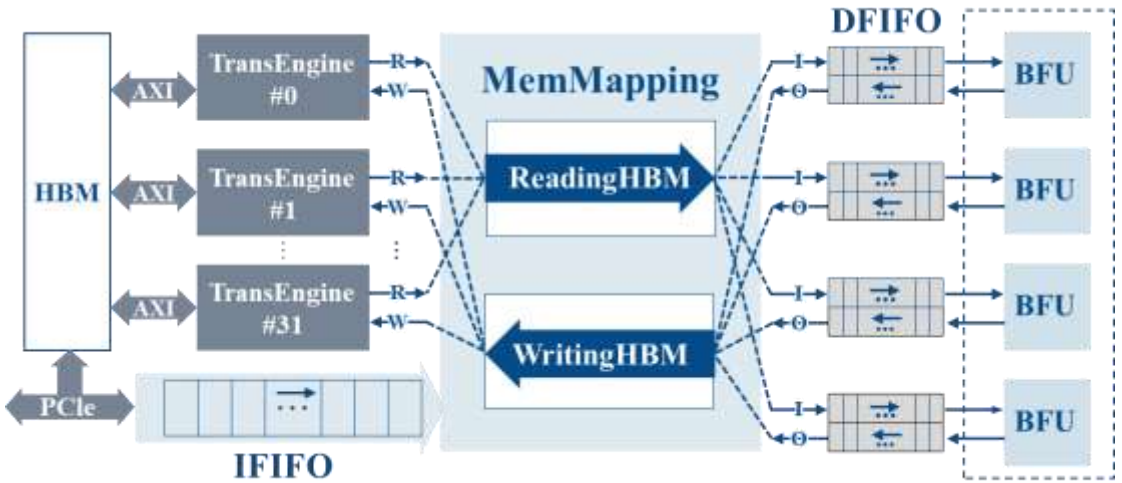
层级	关注点	实现概述	优化目标	硬件平台
算子层	PQC算子优化	针对PQC中核心算子，探究算法-硬件设计	单次执行延迟、面积、复杂度	FPGA、存内计算
电路层	PQC电路优化	针对PQC中算法，进行电路优化	延迟、面积、频率	
架构层	PQC架构优化	针对PQC中算法，进行架构设计与映射调度	吞吐、灵活性、通用可编程性	

PQC硬件加速是系统性工程，需在性能、面积与灵活性之间联合优化

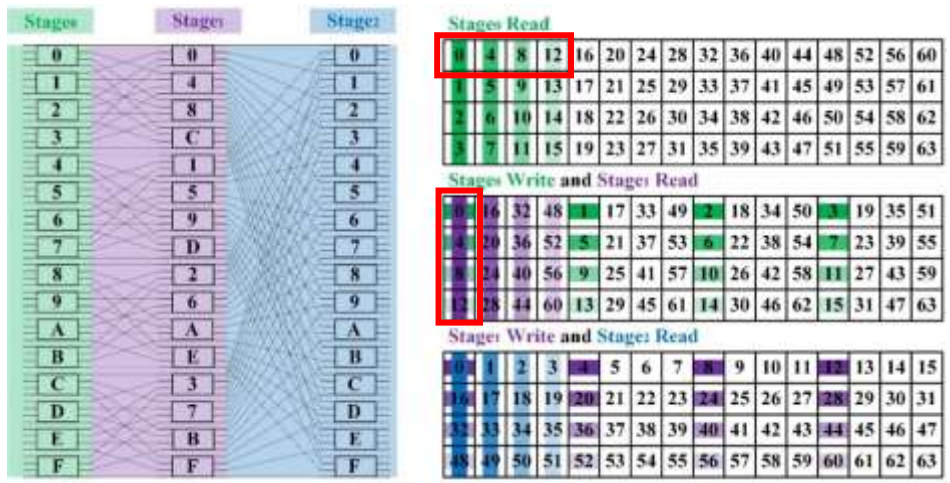
算子优化：高性能低开销NTT硬件加速器

- **背景**：多项式乘法是PQC算法中的**计算密集部分**，其开销高达总工作量的30%~80%。采用NTT可将计算复杂度从$O(n^2)$优化降至$O(n\log_n)$
- **挑战**：NTT算子硬件部署时会面临**数据依赖**和**流水线停顿**问题

整体架构



无冲突数据流

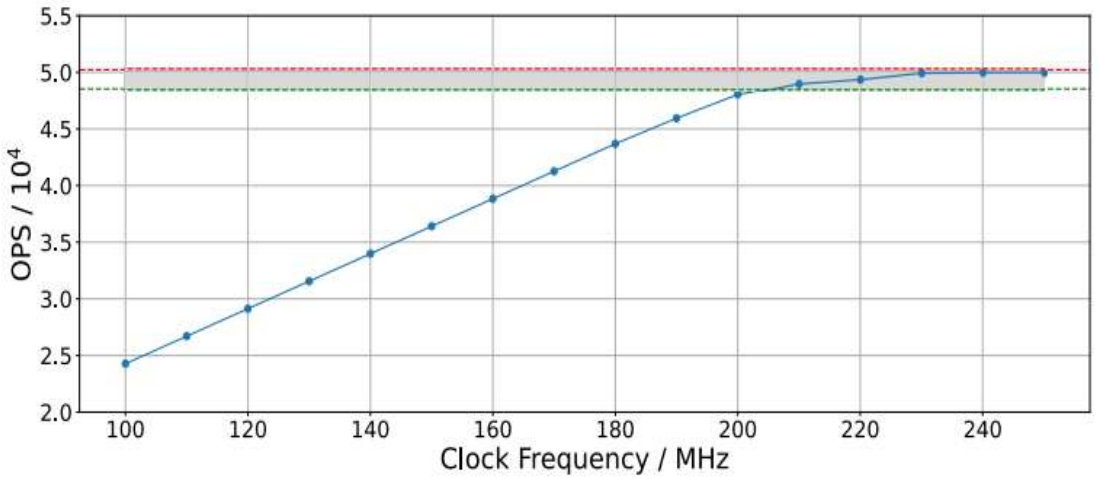


Zhaojun Lu, Weizong Yu, Peng Xu, Wei Wang, Jiliang Zhang*, Dengguo Feng, “An NTT/INTT Accelerator with Ultra-High Throughput and Area Efficiency for FHE”, in Proceedings of the 61st ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 2024, pp. 1-6.

算子优化：高性能低开销NTT硬件加速器

- **实验结果**：与Poseidon和TensorFHE这两项同期最先进工作相比，提出的NTT硬件加速器实现了**3~10倍**的**性能**提升，**5倍**的**面积效率**提升。

最大工作频率与性能测试



实验结果对比

Scheme	Platform	N	Conflict-Free	OPS	Area
2021 [12]	V100	2^{16}	✗	3,619	-
2023 [8]	A100	2^{16}	✗	4,705	-
2022 [15]	Virtex-7	2^{10}	✓	-	Medium
2022 [6]	UltraScale+	2^{12}	✓	-	Medium
2020 [16]	Stratix 10	2^{16}	✗	237	High
2023 [2]	U280	2^{16}	✗	941	High
2023 [20]	U280	2^{16}	✗	12,474	High
Ours	U55C	2^{16}	✓	**48,543**	**Low**

Zhaojun Lu, Weizong Yu, Peng Xu, Wei Wang, Jiliang Zhang*, Dengguo Feng, “An NTT/INTT Accelerator with Ultra-High Throughput and Area Efficiency for FHE”, in Proceedings of the 61st ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 2024, pp. 1-6.

算子优化：基于MRAM的LPN密码存内计算加速器

LPN密码

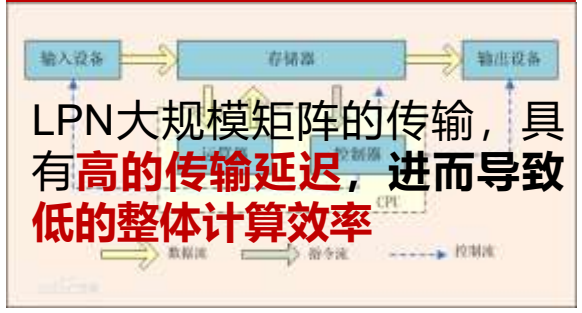
$$b_i = \left(\bigoplus_{j=1,\ldots,N} a_{ij} \wedge s_j\right) \oplus e_i$$

定义在布尔域上的格密码，**可直接由“与门”和“异或门”实现，计算过程简单**，广泛用于构建**多方安全计算与PQC算法**等。

数据规模大 | **计算简单**

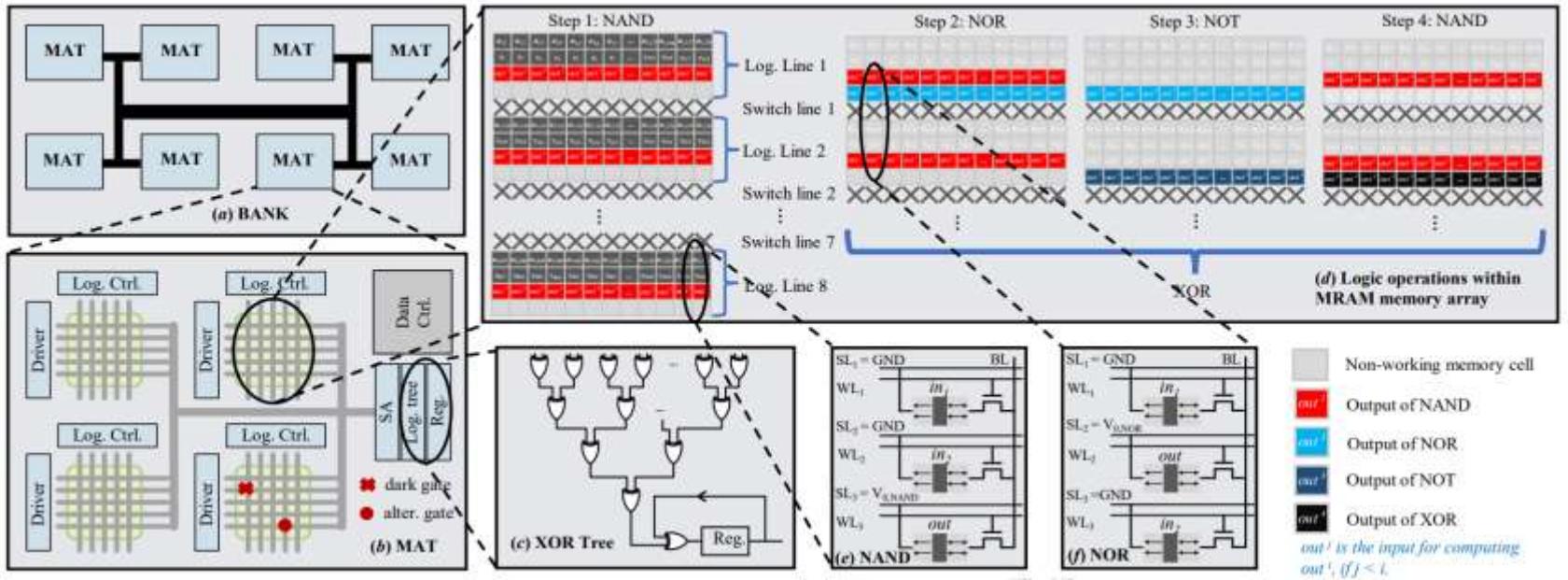
存储墙

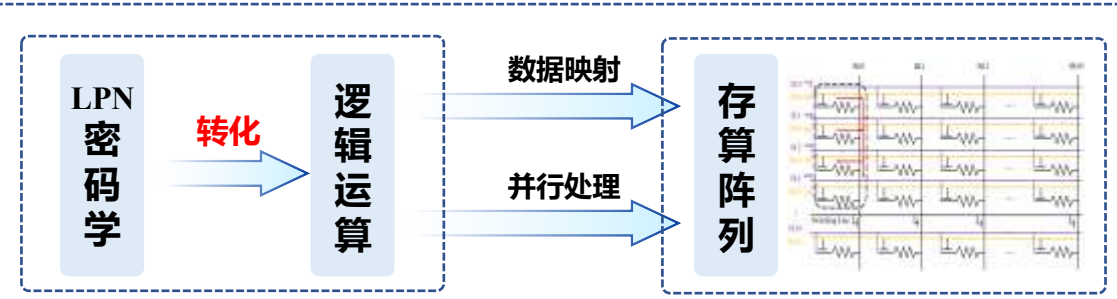
冯·诺依曼架构：存算分离



LPN大规模矩阵的传输，具有**高的传输延迟，进而导致低的整体计算效率**

基于STT-MRAM的LPN存内计算加速器





克服存储墙问题

高性能并行计算

Lin Ding, Song Bian, Jiliang Zhang, “PIMA-LPN: Processing-in-memory Acceleration for Efficient LPN-based Post-Quantum Cryptography”, In Proceedings of the 60th IEEE/ACM Design Automation Conference (DAC’23), San Francisco, CA, July 2023.

算子优化：基于MRAM的LPN密码存内计算加速器

性能对比

TABLE I
IMPROVEMENT OF PIMA-LPN$^+$ ON COMPUTATIONAL SPEED, COMPARED WITH CPU AND FPGA, RESPECTIVELY.

Hardware platform	128-bit security		256-bit security	
	Enc.	Dec.	Enc.	Dec.
Speedup over CPU	347.1 ×	223.7 ×	216.8 ×	143.4 ×
Speedup over FPGA	18.9 ×	25 ×	20.86 ×	25.5 ×

TABLE V
COMPARISON BETWEEN PIMA-LPN$^+$ AND CRYSTALS-KYEBER IN CRYPTOPIM [37] WHEN CARRYING OUT 128-BIT-SECURITY TASK.

	Latency (ms)	Energy (uJ)	# of Memory units
PIMA-LPN$^+$	0.0918	9.24	1.05×10^6
CryptoPIM	0.0759	5.02	1.62×10^7
Ratio[1]	0.83 ×	0.54 ×	15.4 ×

[1]: The ratio is calculated by dividing 2^{nd} row by the 1^{st} row.

误码率

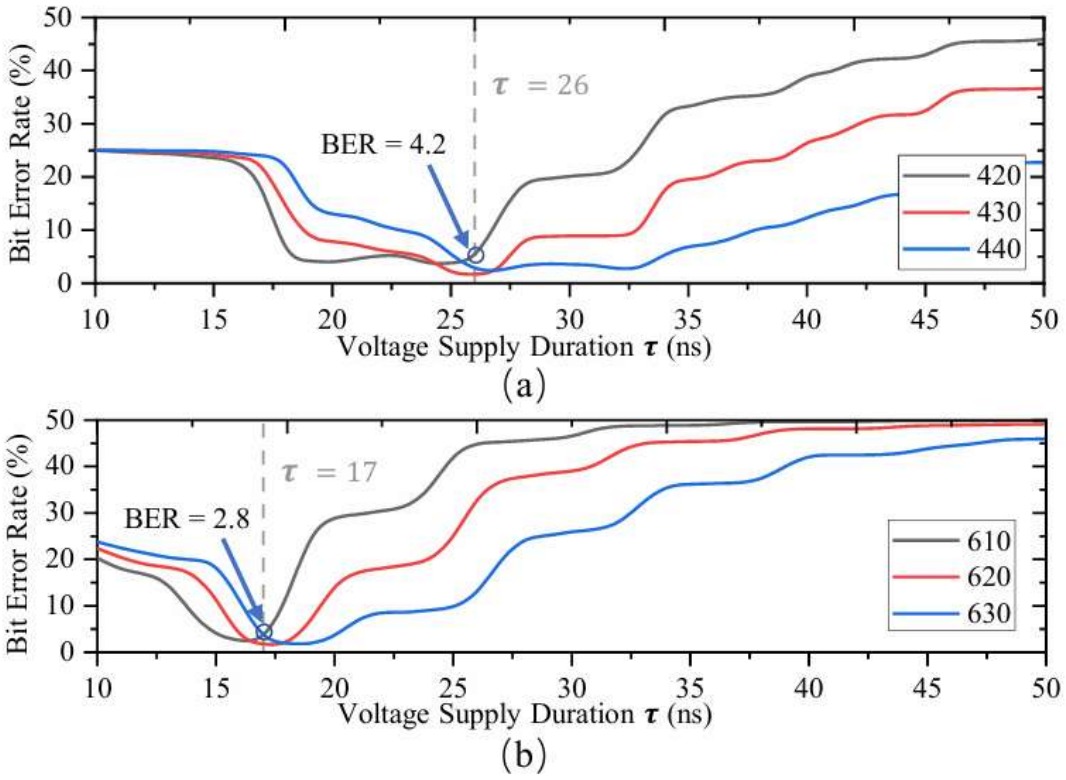


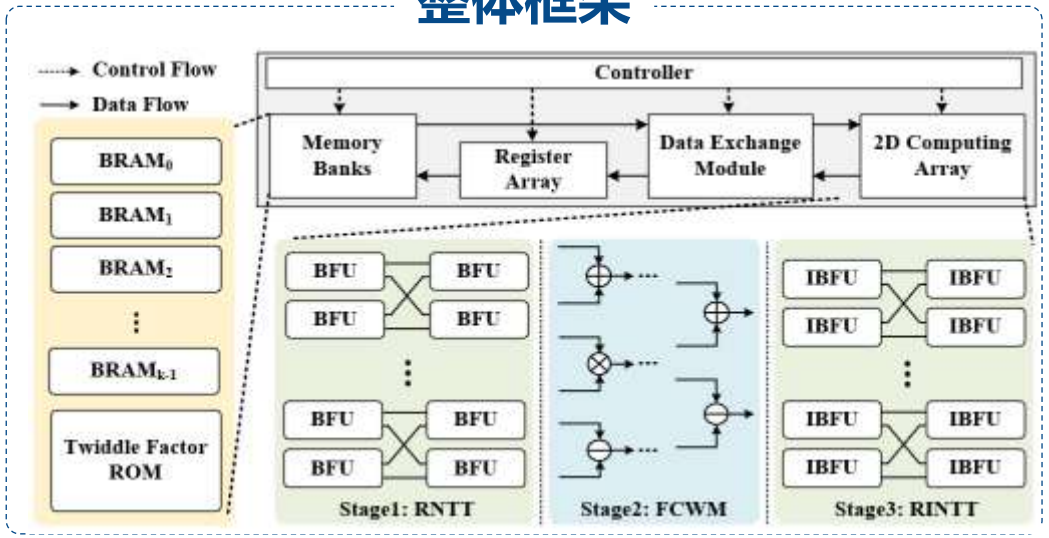
Fig. 8. The impact of working voltage $V_{0,NAND}$ and the power supply duration on BER for NAND, in which $V_{0,NAND}$ = 420/430/440 mV.

Lin Ding, Song Bian, Jiliang Zhang, “PIMA-LPN: Processing-in-memory Acceleration for Efficient LPN-based Post-Quantum Cryptography”, In Proceedings of the 60th IEEE/ACM Design Automation Conference (DAC’23), San Francisco, CA, July 2023.

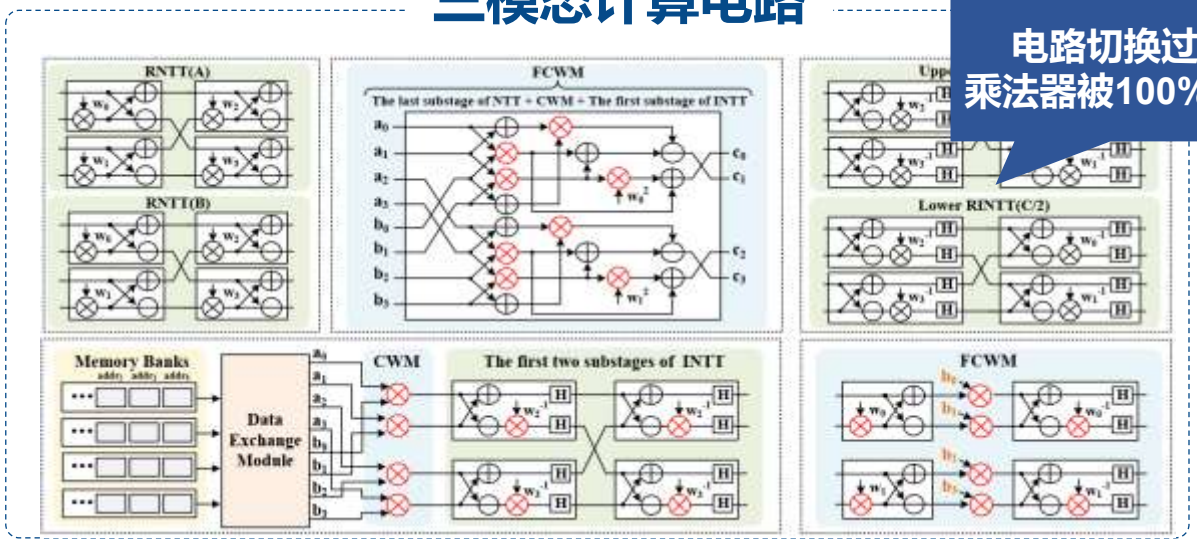
电路优化：内存高效的多项式乘法加速器设计

➢ **挑战**：现有多项式运算架构面临**硬件利用率**和**内存开销高**的问题

整体框架

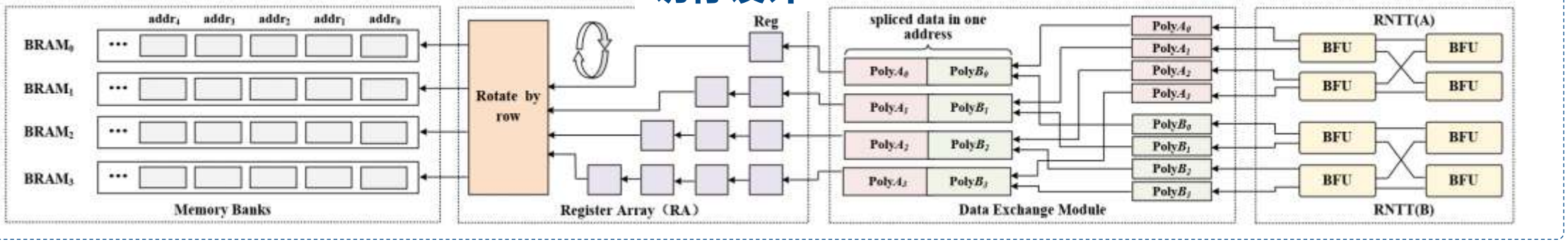


三模态计算电路



电路切换过程中乘法器被100%复用!

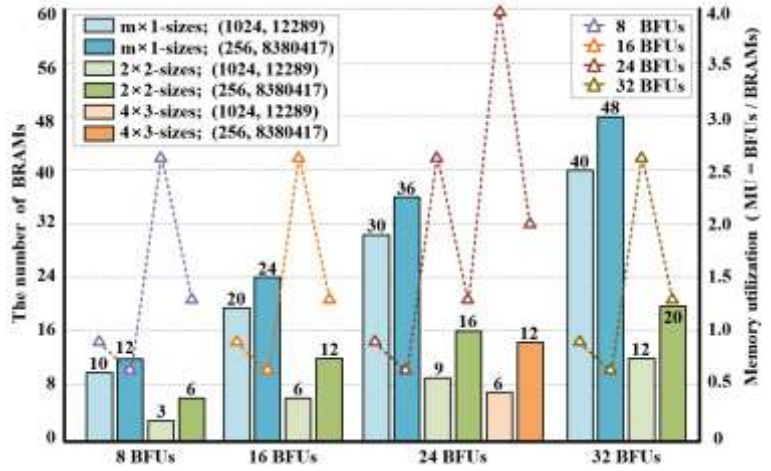
访存设计



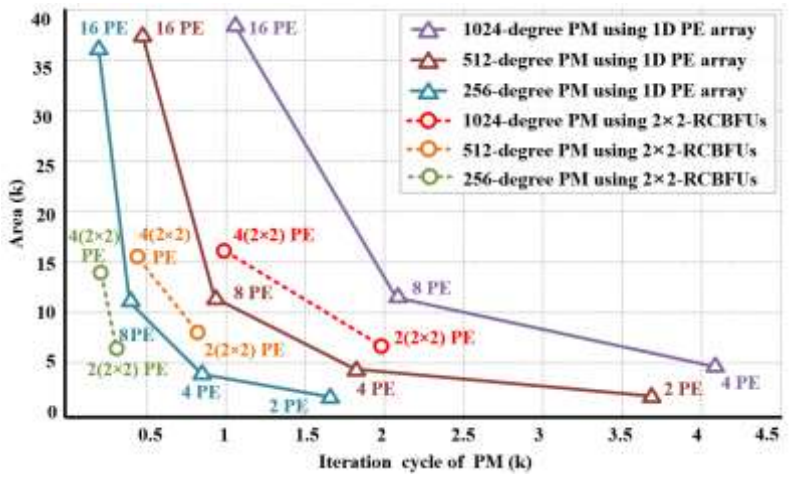
Yan Xu, Lin Ding, Penggao He, Zhaojun Lu and Jiliang Zhang, “Meta: A Memory-Efficient Tri-Stage Polynomial Multiplication Accelerator Using 2D Coupled-BFUs”, IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 72, no. 2, pp. 647-660, Feb. 2025.

电路优化：内存高效的多项式乘法加速器设计

高内存利用率



高面积效率



综合性能与内存开销的比较

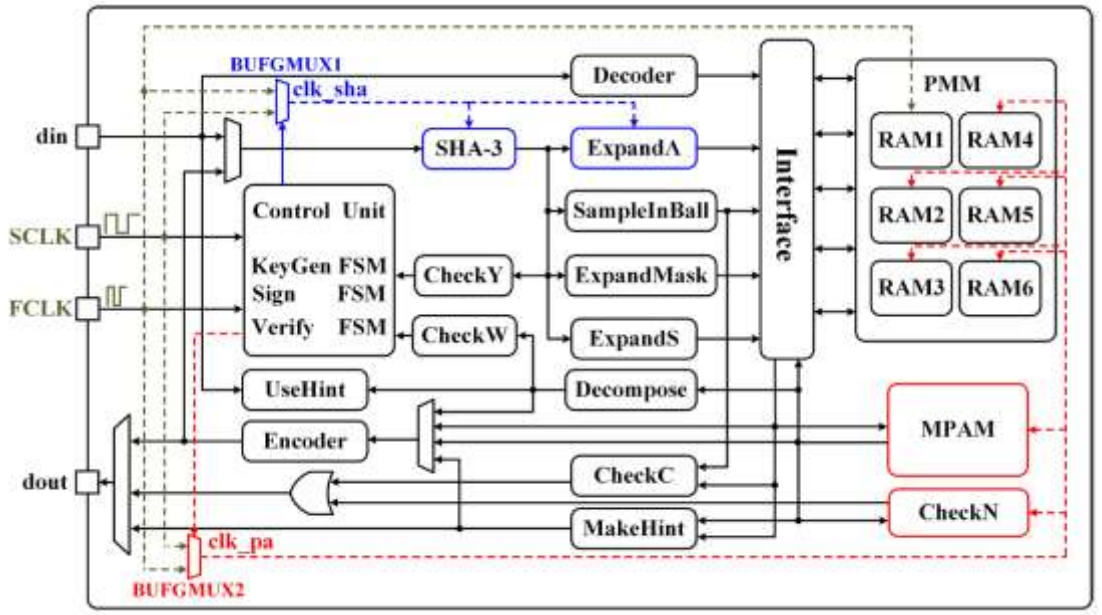
对比文献	Deg.	Mod.	Size	BFU	DSP	BRAM	Time	Area	ATP	MU
DATE’ 21	256	3329	4 × 1	4	4	9	4.7	6.4	30.1	0.4
MM’ 22	256	8380417	32 x 1	32	256	48	2.7	121.0	326.7	0.7
TVLSI’ 24	256	8380417	16 x 1	32	96	48	2.4	114.9	275.8	0.7
MM’ 22	512	12289	32 x 1	32	256	48	3.4	121.0	411.4	0.7
TCHES’ 22	1024	12289	8 x 1	8	27	10	8.9	14.1	125.5	0.8
TVLSI’ 24	1024	12289	8 x 1	8	24	20	6.6	13.9	91.7	0.4
Ours Work	256	3329	2 x 2	8	8	3	2.4	8.1	19.4	2.7
	256	8380417	2 x 2	8	16	6	2.1	11.3	23.7	1.3
	512	12289	2 x 2	8	8	3	3.9	8.3	32.4	2.7
	1024	**12289**	**4 x 3**	**24**	**24**	**6**	**3.3**	**18.6**	**61.4**	**4.0**

Yan Xu, Lin Ding, Penggao He, Zhaojun Lu and Jiliang Zhang, “Meta: A Memory-Efficient Tri-Stage Polynomial Multiplication Accelerator Using 2D Coupled-BFUs”, IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 72, no. 2, pp. 647-660, Feb. 2025.

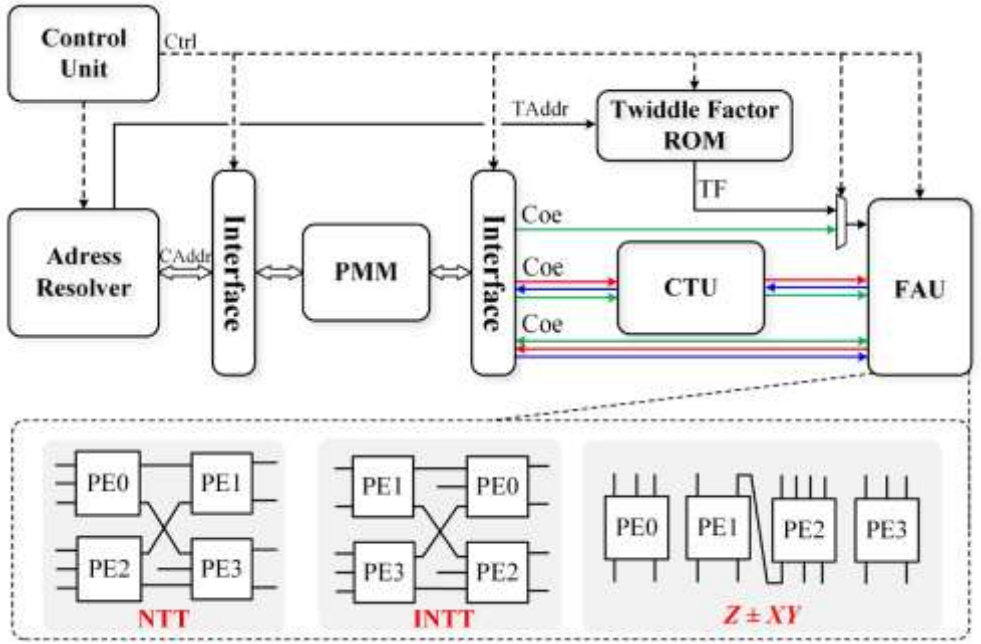
电路优化：ML-DSA硬件加速器设计

- **背景**：Dilithium（已标准化为ML-DSA）是一种后量子密码签名算法
- **挑战**：现有硬件架构面临**硬件资源利用率低**与**性能不足**的瓶颈。

整体架构设计



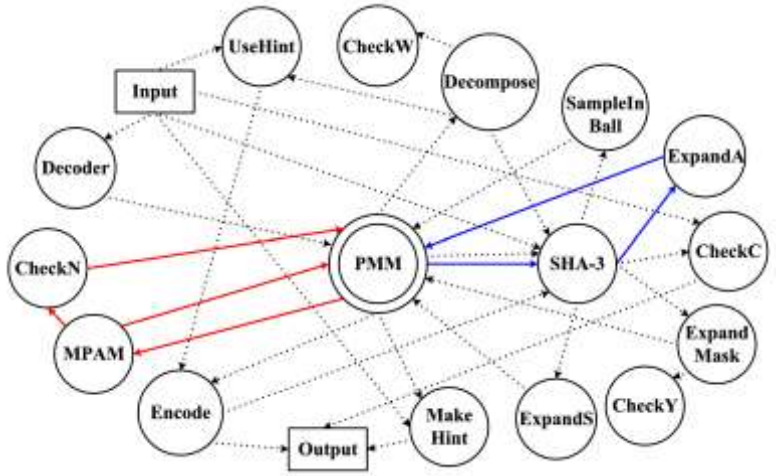
多模态乘法算术电路



Jinwei Pu, Yan Xu, Yuan Zhang, Jiliang Zhang*, “An Area-Efficient ML-DSA Accelerator With Interleaved and Dynamic Execution”, IEEE Transactions on Circuits and Systems I: Regular Papers, 2025.

电路优化：ML-DSA硬件加速器设计

数据执行路径

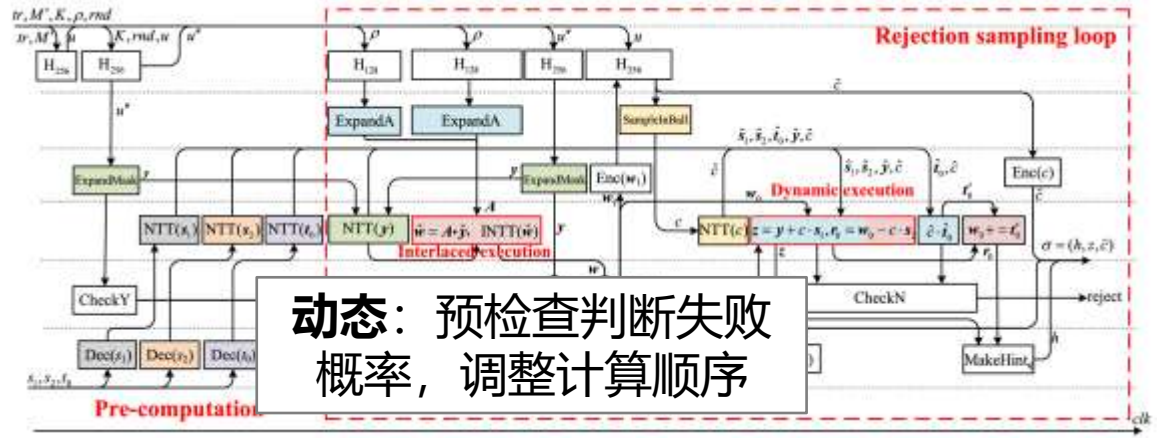


时钟域划分

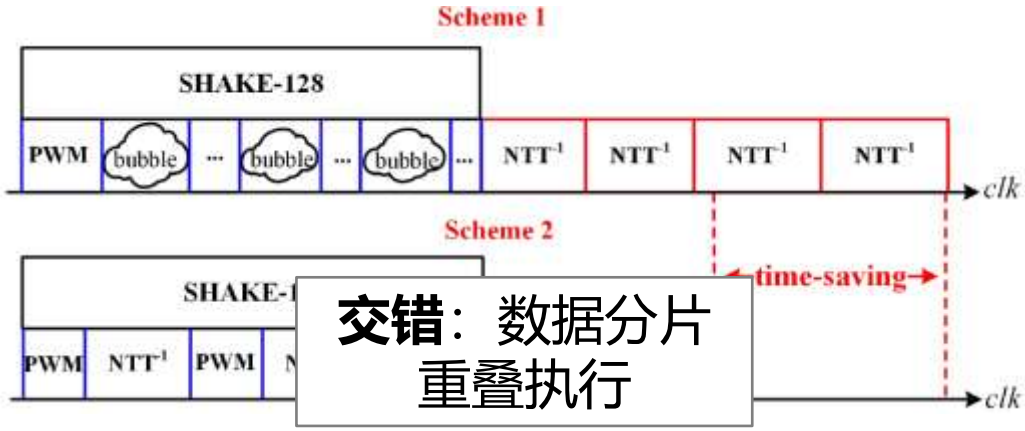
将整个流程划分为多个数据路径，将每条数据路径分配到不同的时钟域中，有效解决了频率不匹配问题

Data path	Domain
PMM → MPAM → PMM	FCLK
PMM → SHA-3 → ExpandA → PMM	FCLK
PMM → MPAM → CheckN → PMM	FCLK
PMM → SHA-3 → ExpandS → PMM	SCLK
PMM → SHA-3 → ExpandMask → PMM	SCLK
PMM → SHA-3 → Decompose$_q$ → SampleInBall → PMM	SCLK
Others	SCLK

动态&交错执行数据流



动态：预检查判断失败概率，调整计算顺序



交错：数据分片重叠执行

Jinwei Pu, Yan Xu, Yuan Zhang, Jiliang Zhang*, “An Area-Efficient ML-DSA Accelerator With Interleaved and Dynamic Execution”, IEEE Transactions on Circuits and Systems I: Regular Papers, 2025.

电路优化：ML-DSA硬件加速器设计

硬件资源与性能对比

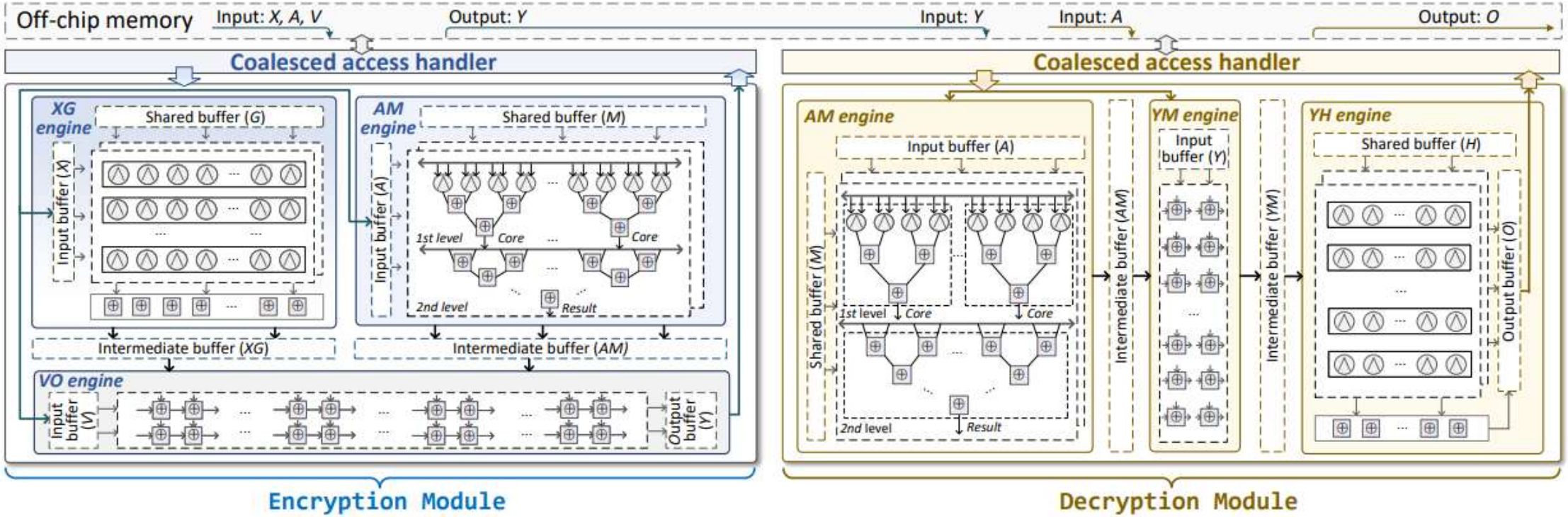
Work	Platform	Utilization LUT/FF/DSP/BRAM	Freq. (MHz)	EqS‡ (Slices)	Latency-KeyGen° (cycles/μs)	Latency-Sign° (cycles/μs)	Latency-Verify° (cycles/μs)	ATP (time×EqS)
Security strength 2 / ML-DSA-44								
CARDIS′21 [8]	Artix-7	27433 / 10681 / 45 / 15	163	14979	18761 / 115	76613 / 470	19687 / 121	10.57(4.62×)
ICFPT′21 [10]	Artix-7	53187 / 28318 / 16 / 29	116	21726	4875 / 42	29876 / 258	6582 / 57	7.76(3.39×)
TCHES′22 [11]	Artix-7	29998 / 10366 / 10 / 11	96.6	11099	4172 / 43	31600 / 326.1	4422 / 45.6	4.60(2.00×)
TCASII′23 [16]	Artix-7	32320 / 9734 / 14 / 24	130	13791	4400 / 33.8	30100 / 231.5	5000 / 38.5	4.19(1.83×)
ACISP′24 [26]	Artix-7	26521 / 8144 / 8 / 16	114.6	11100	5200 / 45.8	33000 / 292.5	4900 / 43	4.23(1.87×)
TVLSI′22 [17]	Zynq-7000	18558 / 7342 / 10 / 17	159	9614	7757 / 49	52038 / 327	7675 / 48	4.08(1.78×)
TC′25 [18]	Artix-7	52888 / 31213 / 38 / 11	191	19670	4800 / 25.1	28800 / 150.1	5200 / 27.2	3.98(1.74×)
HOST′24 [25]	Artix-7	30304 / 13585 / 16 / 28	119	15722	3900 / 33	12800 / 108	4200 / 36	2.78(1.21×)
This work	Artix-7	24833 / 15653 / 8 / 10.5	121 / 194	**9468**	3276 / 27.1	21840 / 180.5	4202 / 34.7	**2.29(1.0)**
Security strength 3 / ML-DSA-65								
CARDIS′21 [8]	Artix-7	27433/10681/45/15	145	14979	33102/228.2	123218/850.0	32050/221.0	19.46 (5.31×)
ICFPT′21 [10]	Artix-7	53187 / 28318 / 16 / 29	116	21726	8291 / 71	49437 / 426	9724 / 84	12.62(3.45×)
TCHES′22 [11]	Artix-7	29998 / 10366 / 10 / 11	96.6	11099	5851 / 60.4	49496 / 510.8	6181 / 63.8	7.05(1.93×)
TCASII′23 [16]	Artix-7	32320 / 9734 / 14 / 24	130	13791	7300 / 56.1	49500 / 381	8000 / 61.6	6.88(1.88×)
ACISP′24 [26]	Artix-7	23378 / 9079 / 8 / 20	109	11311	7800 / 72.2	54000 / 490.6	7600 / 69.7	7.15(1.95×)
TVLSI′22 [17]	Zynq-7000	19614 / 8466 / 10 / 21	159	10807	12982 / 82	89213 / 561	11232 / 71	7.72(2.11×)
TC′25 [18]	Artix-7	52888 / 31213 / 38 / 11	191	19670	7900 / 41.4	48600 / 254.5	8500 / 44.5	6.69(1.83×)
HOST′24 [25]	Artix-7	30304 / 13585 / 16 / 28	119	15722	6500 / 54	21400 / 180	6900 / 58	4.59(1.25×)
This work	Artix-7	24833 / 15653 / 8 / 10.5	121 / 194	**9468**	5076 / 42.0	35467 / 293.1	6165 / 51.0	**3.66(1.0)**

Jinwei Pu, Yan Xu, Yuan Zhang, Jiliang Zhang*, “An Area-Efficient ML-DSA Accelerator With Interleaved and Dynamic Execution”, IEEE Transactions on Circuits and Systems I: Regular Papers, 2025.

架构优化：AI架构启发的后量子密码LPN硬件设计

➢ **挑战**：现有架构专注独立操作，忽略**整体执行流程**交互，面临**数据传输瓶颈**

整体架构设计



□ 异构多核硬件架构

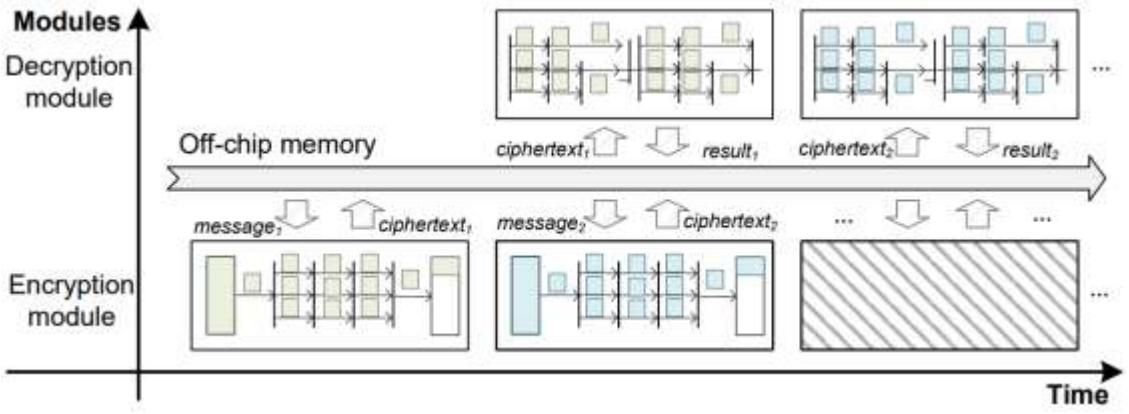
□ 批处理 -> 流式执行

Yingxue Gao, Jiliang Zhang, “Leveraging AI-Inspired Hardware Architecture to Enhance LPN Acceleration in Post-Quantum Cryptography”, In Proceedings of the 63th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, 2026.

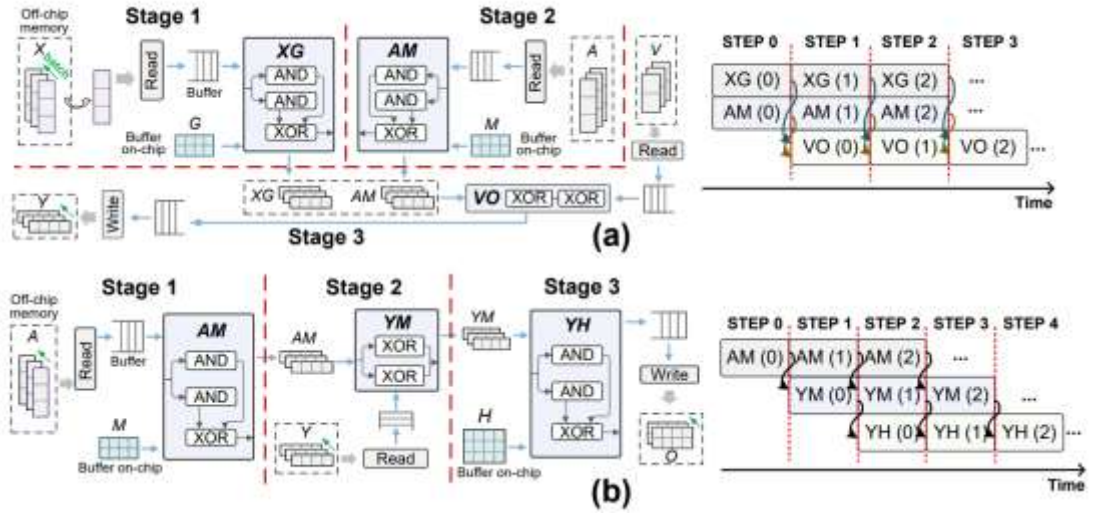
架构优化：AI架构启发的后量子密码LPN硬件设计

➢ **挑战**：现有架构专注独立操作，忽略**整体执行流程**交互，面临**数据传输瓶颈**

模块级调度策略



操作级调度策略



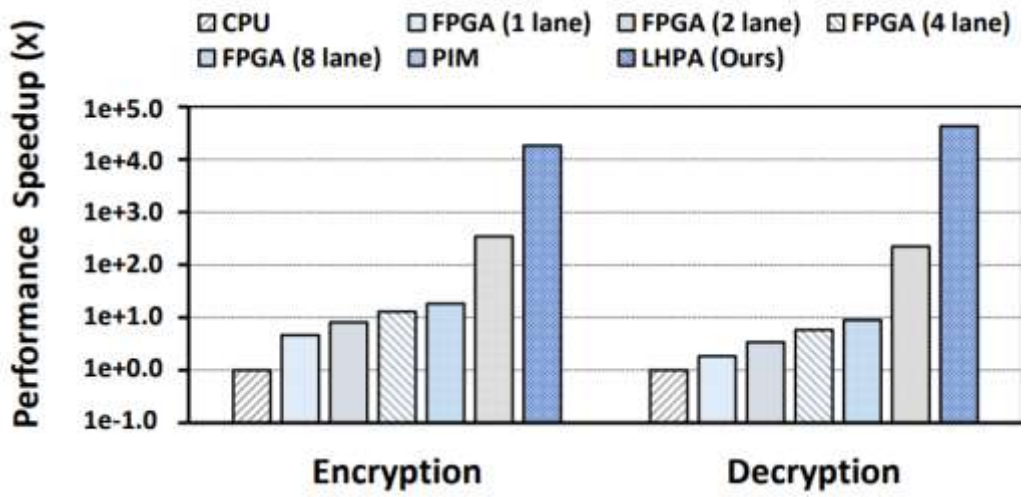
□ 多核并行 & 任务级流水并行 -> 提高架构吞吐率

Yingxue Gao, Jiliang Zhang, “Leveraging AI-Inspired Hardware Architecture to Enhance LPN Acceleration in Post-Quantum Cryptography”, In Proceedings of the 63th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, 2026.

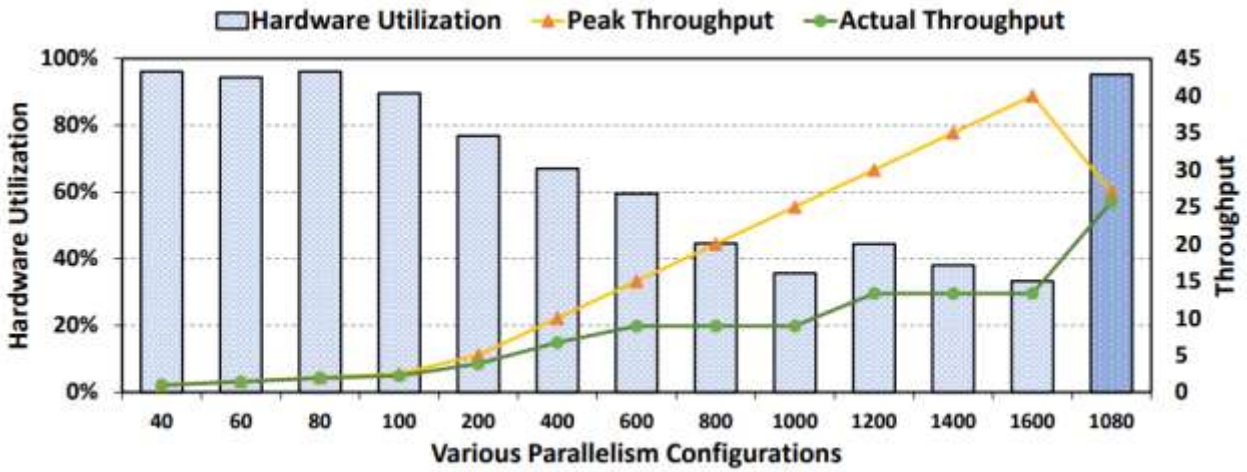
架构优化：AI架构启发的后量子密码LPN硬件设计

- **实验结果**：LHPA相较于最先进的LPN架构，加解密性能分别提升了**53倍**（加密）和**192倍**（解密），同时硬件利用率高达**95.24%**。

实验对比



架构高效性分析



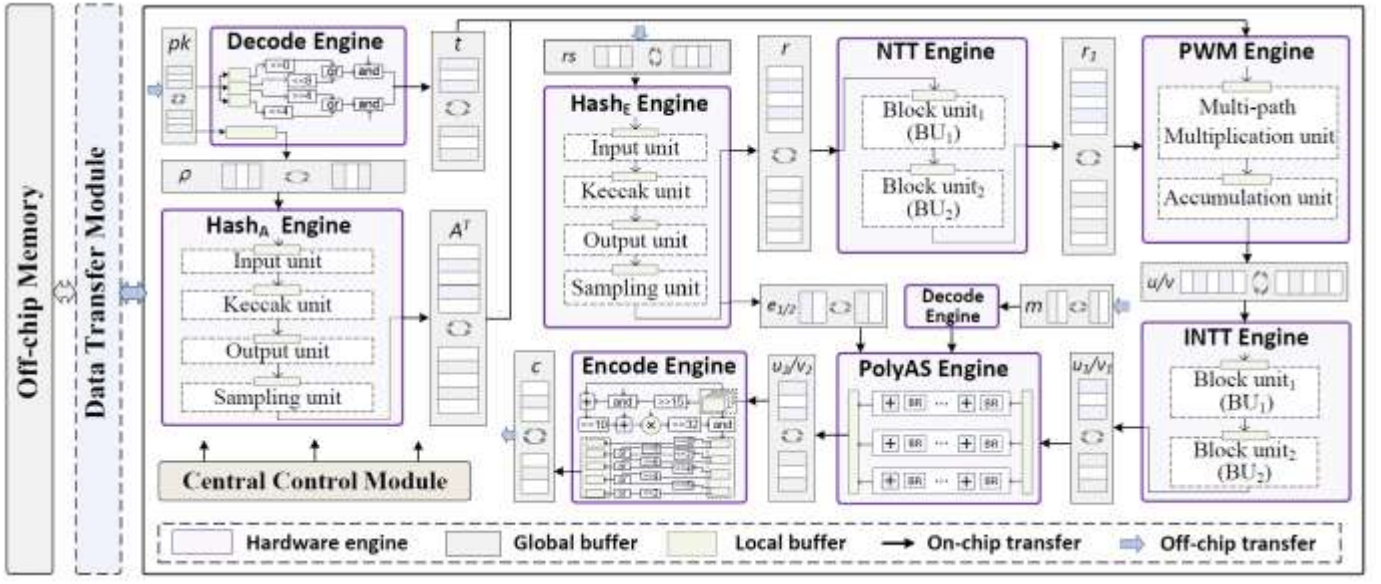
Yingxue Gao, Jiliang Zhang, “Leveraging AI-Inspired Hardware Architecture to Enhance LPN Acceleration in Post-Quantum Cryptography”, In Proceedings of the 63th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, 2026.

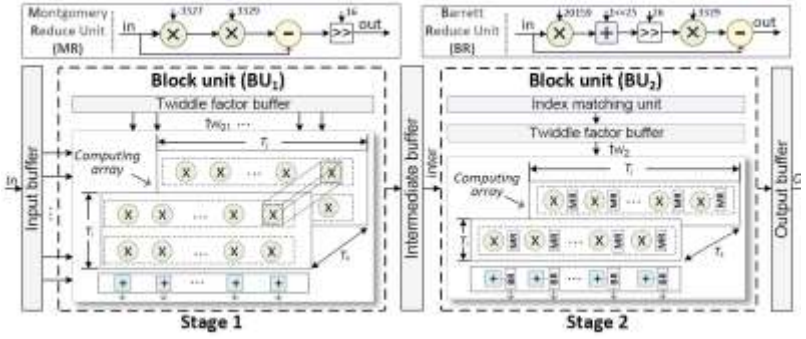
架构优化：ML-KEM硬件加速器设计

背景 & 挑战

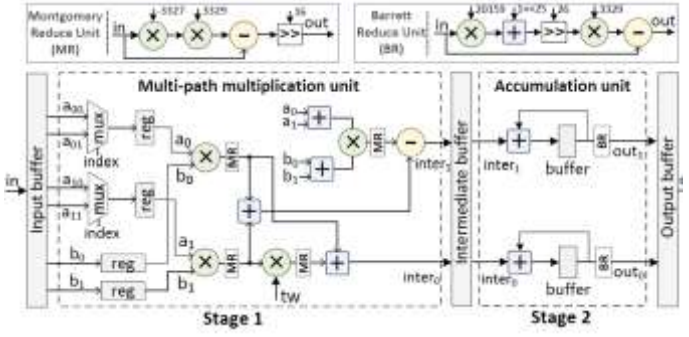
- Kyber（已标准化为ML-KEM）是一种**密钥封装算法**
- 算子**计算模式和访存行为**差异较大
- 算子间的**复杂数据依赖**交互
- 架构的**低效数据流**执行
- —> 阻碍高性能硬件架构部署

整体硬件架构实现

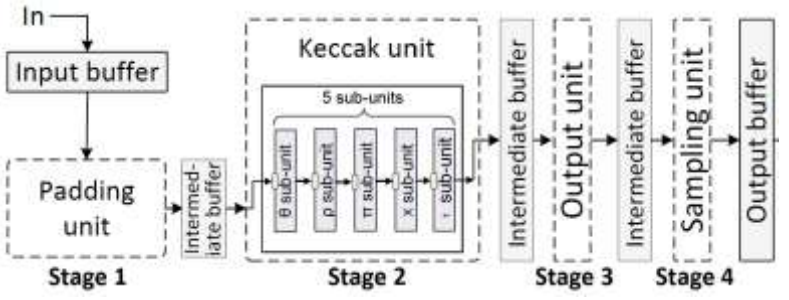




基于迭代的NTT单元设计



PWM单元设计

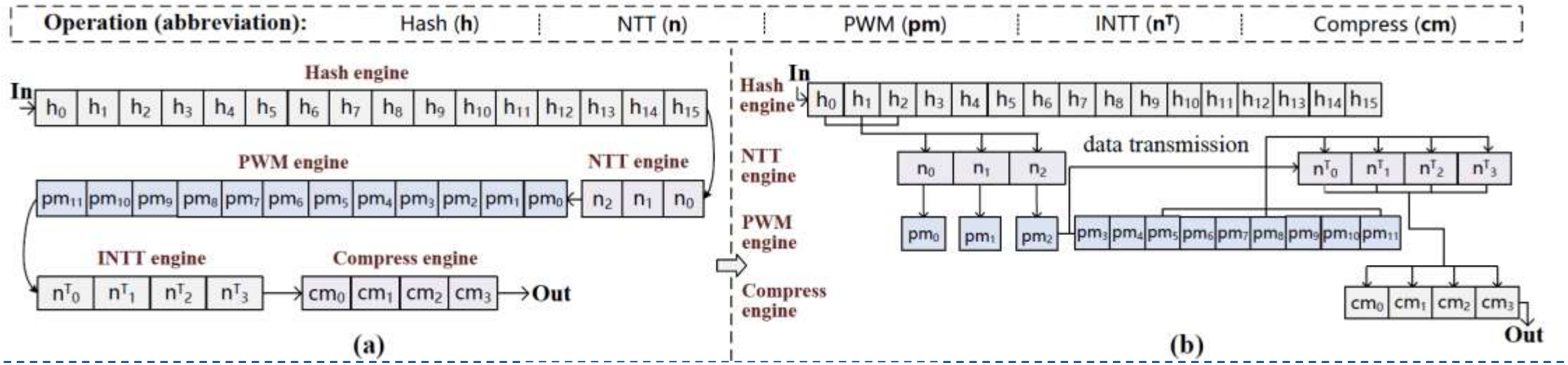


Hash单元设计

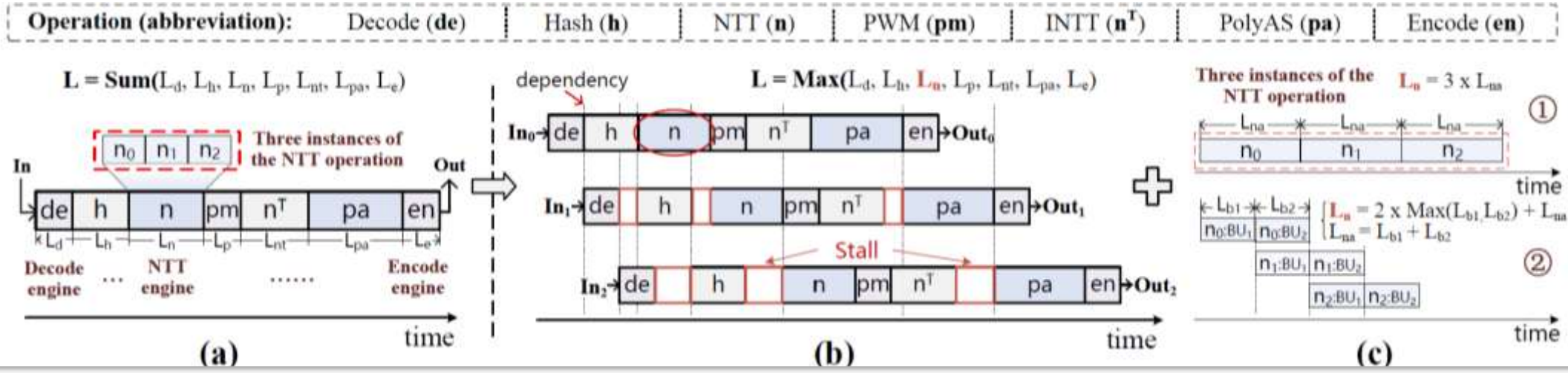
Yingxue Gao, Jiliang Zhang, “Enhancing Kyber Acceleration in Post-Quantum Cryptography through Configurable Hardware Architecture and Efficient Dataflow Mapping”, submitted.

架构优化：ML-KEM硬件加速器设计

先前数据流



多层级数据流



Yingxue Gao, Jiliang Zhang, “Enhancing Kyber Acceleration in Post-Quantum Cryptography through Configurable Hardware Architecture and Efficient Dataflow Mapping”, submitted.

架构优化：ML-KEM硬件加速器设计

实验对比结果

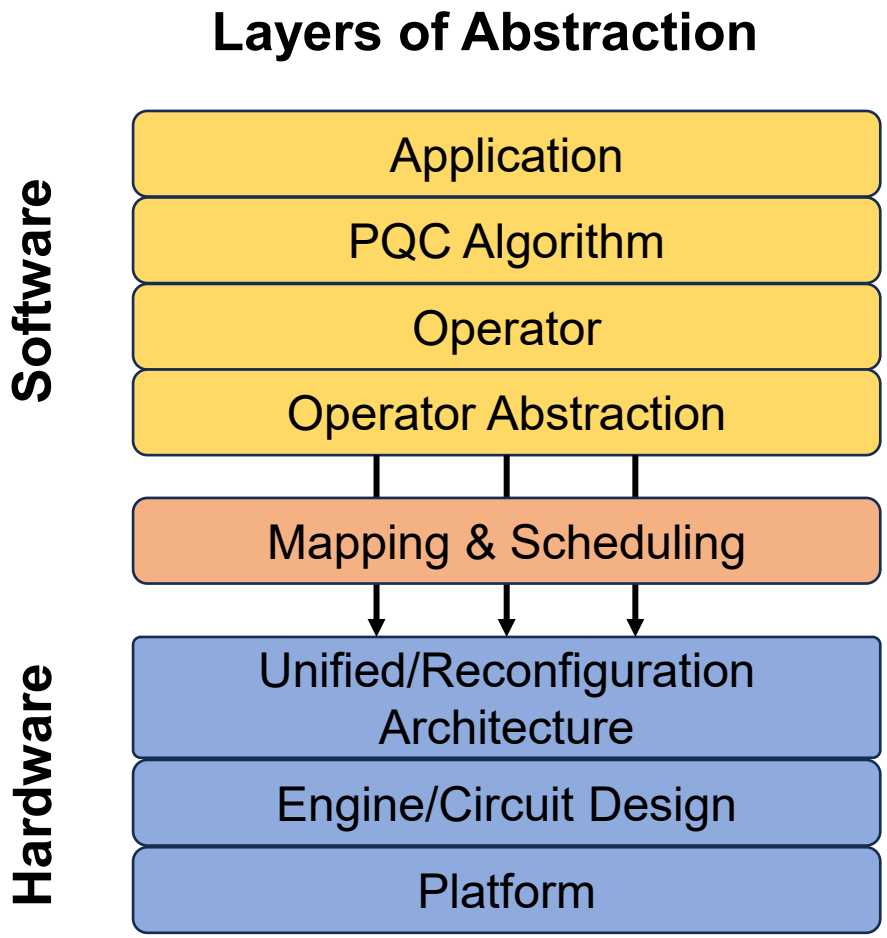
Related Work	Config-urable	Freq. (MHz)	LUT	DSP	BRAM	Key/Enc/Dec (cycle k)	Key/Enc/Dec/Total (latency μs)	Platform
NIST PQC Security Level 1 (Kyber512)								
Sapphire (CHES'19) [30]	Y	25	14,975	11	14	NA/31.7/43.0	NA/1,266.8/1,720.7/NA	Artix-7
ISKyber (TCASI'21) [16]	N	115	18,000	6	15	4.0/7.0/10.0	34.8/60.9/86.9/182.6	Artix-7
HSKyber (TC'23) [31]	N	450	9,435	4	6	2.1/3.3/4.5	4.8/7.2/9.9/21.9	Zynq
HPKA (TC'23) [18]	N	435	13,300/16,004	2	0	1.1/1.5/2.1	2.5/3.4/4.8/10.7	Zynq
CKyber (TCASII'24) [17]	Y	210	25,757	21	14	1.8/1.9/3.2	8.57/9.05/15.24/32.86	Artix-7
LKyber (TCASI'25) [32]	Y	185	5,500	2	3.5	3.3/4.5/6.1	17.84/24.32/32.97/75.13	Artix-7
KyberHP [Ours]	**Y**	450	30,517/31,511	10/25	35.5/33	**0.7/0.8/1.3**	**1.55/1.76/2.95/6.27**	Zynq
NIST PQC Security Level 3 (Kyber768)								
Sapphire (CHES'19) [30]	Y	25	14,975	11	14	111.5/177.5/190.6	4,461.0/7,101.6/7,623.2/19,185.8	Artix-7
ISKyber (TCASI'21) [16]	N	115	16,000	9	16	7.0/10.0/14.0	60.9/86.9/121.7/269.5	Artix-7
HSKyber (TC'23) [31]	N	450	10,512	6	8.5	2.7/3.9/5.0	6.0/8.6/11.2/25.8	Zynq
HPKA (TC'23) [18]	N	435	15,196/16,797	2	0	1.7/2.4/3.0	3.9/5.5/6.9/16.3	Zynq
CKyber (TCASII'24) [17]	Y	210	25,757	21	14	2.6/2.7/4.1	12.38/12.86/20.95/46.19	Artix-7
LKyber (TCASI'25) [32]	Y	185	5,500	2	3.5	5.6/7.1/9.2	30.27/38.38/49.73/118.38	Artix-7
KyberHP [Ours]	**Y**	450	23,642/23,825	8/15	38/36.5	**1.7/2.1/2.9**	**3.80/4.63/6.40/14.83**	Zynq
NIST PQC Security Level 5 (Kyber1024)								
Sapphire (CHES'19) [30]	Y	25	14,975	11	14	148.6/223.5/241.0	5,941.9/8,938.8/9,639.1/24,519.7	Artix-7
ISKyber (TCASI'21) [16]	N	112	16,000	12	17	10.0/14.0/18.0	86.9/121.7/156.5/365.1	Artix-7
HSKyber (TC'23) [31]	N	450	11,598	8	10.5	3.6/4.8/6.0	8.0/10.6/13.2/31.8	Zynq
HPKA (TC'23) [18]	N	435	15,544/17,812	2	0	2.7/3.4/4.1	6.2/7.8/9.4/23.4	Zynq
CKyber (TCASII'24) [17]	Y	210	25,757	21	14	3.4/3.5/5.8	16.19/16.67/27.62/60.48	Artix-7
LKyber (TCASI'25) [32]	Y	185	5,500	2	3.5	8.5/10.1/12.9	45.95/54.59/69.73/170.27	Artix-7
KyberHP [Ours]	**Y**	450	22,199/23,513	12/30	40/38	**2.9/2.9/4.0**	**6.52/6.52/8.89/21.94**	Zynq

Yingxue Gao, Jiliang Zhang, "Enhancing Kyber Acceleration in Post-Quantum Cryptography through Configurable Hardware Architecture and Efficient Dataflow Mapping", submitted.

目录

未来研究展望：软硬件协同实现PQC硬件加速

- 旨在提供一套垂直整合的方法，通过一个full-stack integration，提供一个软硬件框架，让程序员不必要了解底层硬件（由多个异构处理器单元组成），但仍然可以充分的利用硬件的效率。

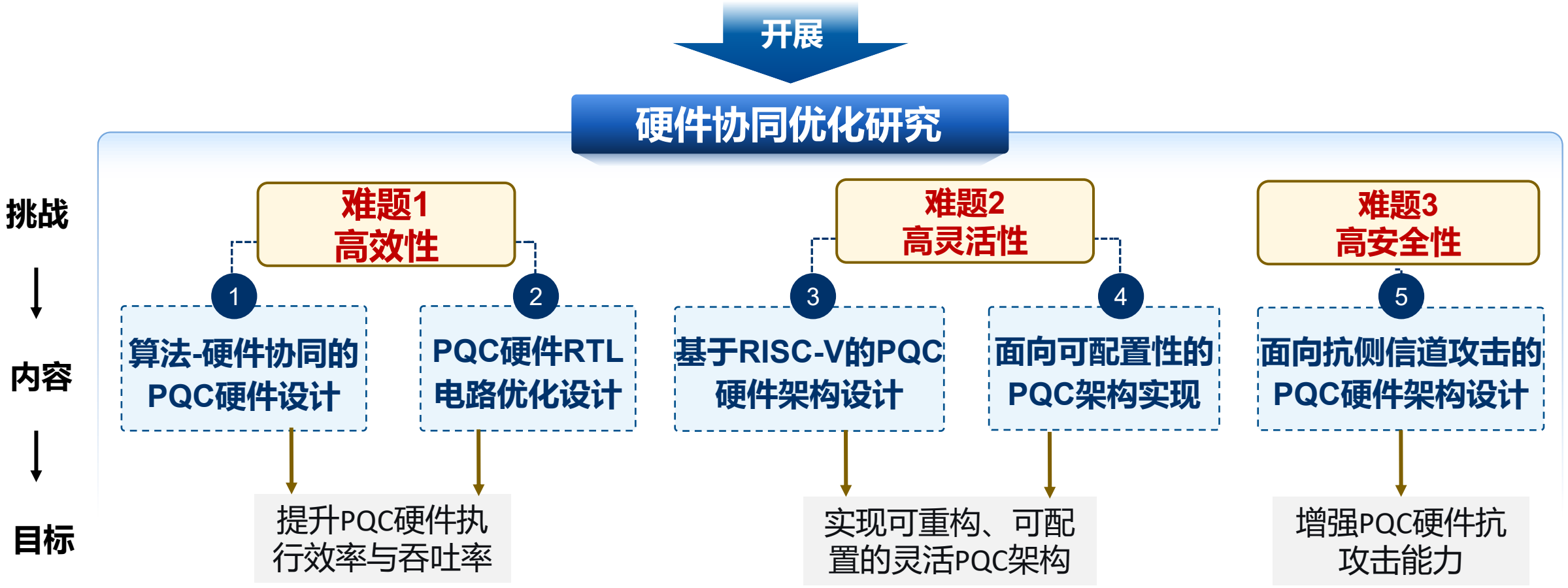


Domain-Specific System on Chip (DSSoC) is developing a system-on-chip (SoC) to improve software performance within an operational domain. Applications within a domain have similar functional and system requirements.

- **算子抽象**：算子如何进行抽象为统一形式
- **映射调度**：抽象后的算子如何映射到硬件架构上
- **整体架构模式**：是统一架构，多核架构，还是混合架构
- **高效 & 可重配置电路设计**：高效灵活的电路设计
- **自动参数空间探索**：架构中放置多少计算单元，能够支持多少种算法，计算单元参数配置如何?

未来研究展望

围绕PQC硬件架构的高效性（协同设计+电路优化）、灵活性（RISC-V+可配置抽象）与安全性（抗侧信道攻击），开展系统性的系列研究。



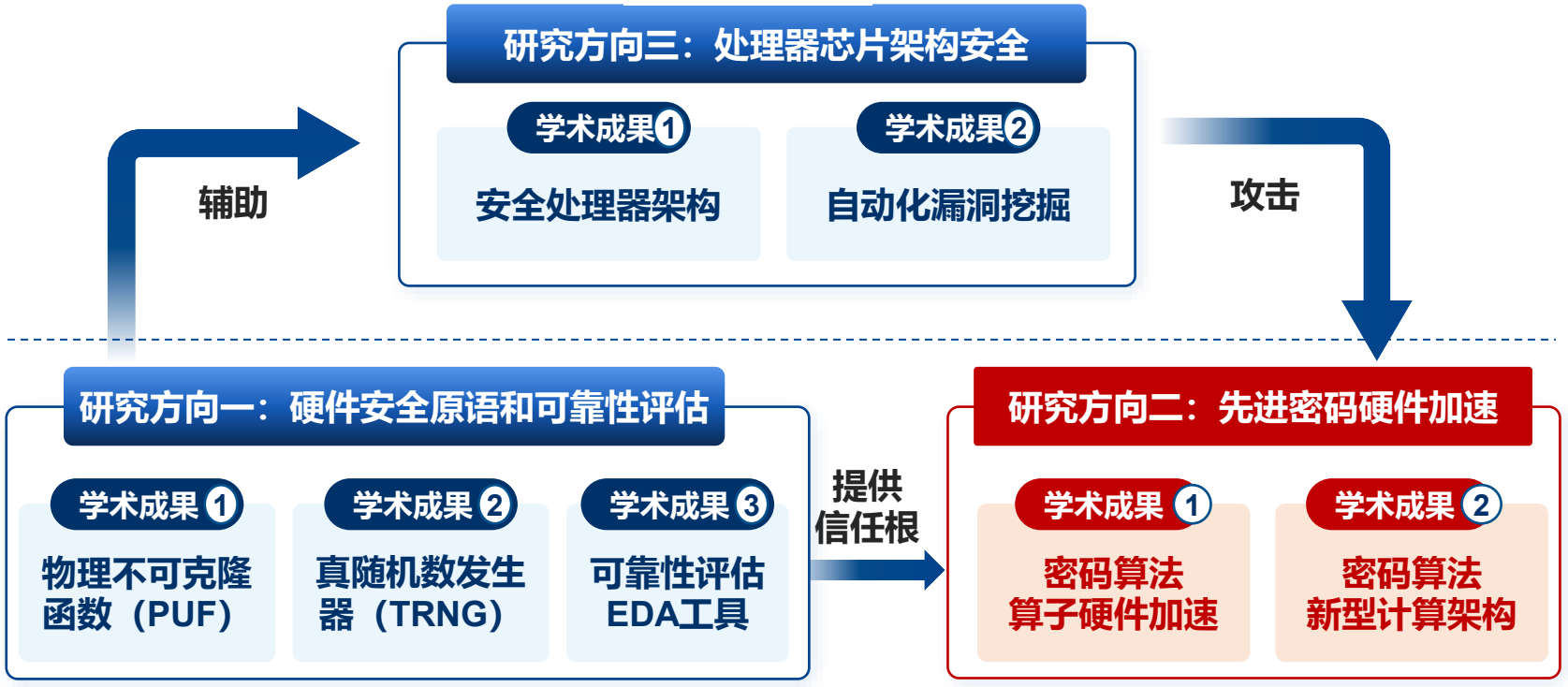
目录

团队简介：集成电路设计与硬件安全团队

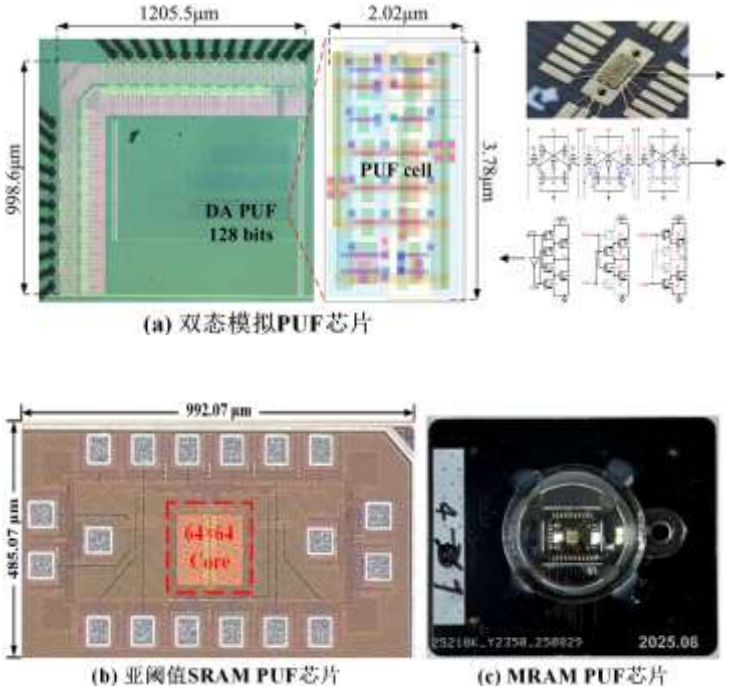
团队简介

集成电路设计与硬件安全团队聚焦于安全芯片面临的安全性、可靠性和性能瓶颈的研究，现有教师9名（含教授1名、副教授3名、讲师7名）。**张吉良教授为团队负责人，南京邮电大学集成电路学院院长**、CCF容错计算专业委员会主任，CCF理事。承担了**NSFC重点项目（2项）、NSFC优青、JKW 173基金重点等20余项**。在**ISCA、DAC、IEEE TC、TCAD、TCASI**等领域顶会、顶刊发表论文**百余篇**，部分研究成果应用于**陆军和空军某系列装备及空间站北斗项目等国家重大工程。**

研究概述



研究成果



(a) 双态模拟PUF芯片

(b) 亚阈值SRAM PUF芯片

(c) MRAM PUF芯片

团队简介：近年来代表项目及相关论文

近年来代表项目

- RISC-V处理器IP安全验证与漏洞挖掘关键技术研究，**国家自然科学基金联合基金重点项目（主持）**
- 物理不可克隆安全芯片设计方法及应用研究，**国家自然科学基金联合基金重点项目（主持）**
- ****安全芯片设计，**国防173基金重点项目（主持）**
- 具备弹性扩展能力的PNT传感器存算一体硬件研制，**国家重点研发计划课题任务（主持）**
- 高效可重构抗量子密码芯片技术研发，**省重点研发计划（主持）**

相关论文列表

- Yingxue Gao, Jiliang Zhang*, "*Leveraging AI-Inspired Hardware Architecture to Enhance LPN Acceleration in Post-Quantum Cryptography*", In Proceedings of the 63th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, 2026.
- Lin Ding, Penggao He, Jiliang Zhang*, "*PIMA-SecDB: Processing-in-memory Acceleration for Fully Homomorphic Encryption Databases*", In Proceedings of the 63th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, 2026.
- Lin Ding, Song Bian, Penggao He, Jiliang Zhang*, "*APACHE: A Processing-Near-Memory Architecture for Multi-Scheme Fully Homomorphic Encryption*", IEEE Transactions on Computers, 2026.
- Jinwei Pu, Yan Xu, Yuan Zhang, Jiliang Zhang*, "*An Area-Efficient ML-DSA Accelerator With Interleaved and Dynamic Execution*", IEEE Transactions on Circuits and Systems I: Regular Papers, 2025.
- Yan Xu, Lin Ding, Penggao He, Zhaojun Lu and Jiliang Zhang*, "*Meta: A Memory-Efficient Tri-Stage Polynomial Multiplication Accelerator Using 2D Coupled-BFUs*", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 72, no. 2, pp. 647-660, Feb. 2025.
- Zhaojun Lu, Weizong Yu, Peng Xu, Wei Wang, Jiliang Zhang*, Dengguo Feng, "*An NTT/INTT Accelerator with Ultra-High Throughput and Area Efficiency for FHE*", in Proceedings of the 61st ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 2024, pp. 1-6.
- Lin Ding, Song Bian and Jiliang Zhang*, "*PIMA-LPN: Processing-in-memory Acceleration for Efficient LPN-based Post-Quantum Cryptography*", in Proceedings of the 60th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 2023.

团队简介：近年来代表项目及相关论文

近年来代表项目

- RISC-V处理器IP安全验证与漏洞挖掘关键技术研究，**国家自然科学基金联合基金重点项目（主持）**
- 物理不可克隆安全芯片设计方法及应用研究，**国家自然科学基金联合基金重点项目（主持）**
- ****安全芯片设计，**国防173基金重点项目（主持）**
- 具备弹性扩展能力的PNT传感器存算一体硬件研制，**国家重点研发计划课题任务（主持）**
- 高效可重构抗量子密码芯片技术研发，**省重点研发计划（主持）**

招聘教授/副教授/讲师（事业编制），面向海内外优秀青年学者长期开放，提供具有竞争力薪酬和事业编制，诚邀有志青年加入团队。

相关论文列表

- Yingxue Gao, Jiliang Zhang*, "*Leveraging AI-Inspired Hardware Architecture to Enhance LPN Acceleration in Post-Quantum Cryptography*", In Proceedings of the 63th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, 2026.
- Lin Ding, Penggao He, Jiliang Zhang*, "*PIMA-SecDB: Processing-in-memory Acceleration for Fully Homomorphic Encryption Databases*", In Proceedings of the 63th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, 2026.
- Lin Ding, Song Bian, Penggao He, Jiliang Zhang*, "*APACHE: A Processing-Near-Memory Architecture for Multi-Scheme Fully Homomorphic Encryption*", IEEE Transactions on Computers, 2026.
- Jinwei Pu, Yan Xu, Yuan Zhang, Jiliang Zhang*, "*An Area-Efficient ML-DSA Accelerator With Interleaved and Dynamic Execution*", IEEE Transactions on Circuits and Systems I: Regular Papers, 2025.
- Yan Xu, Lin Ding, Penggao He, Zhaojun Lu and Jiliang Zhang*, "*Meta: A Memory-Efficient Tri-Stage Polynomial Multiplication Accelerator Using 2D Coupled-BFUs*", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 72, no. 2, pp. 647-660, Feb. 2025.
- Zhaojun Lu, Weizong Yu, Peng Xu, Wei Wang, Jiliang Zhang*, Dengguo Feng, "*An NTT/INTT Accelerator with Ultra-High Throughput and Area Efficiency for FHE*", in Proceedings of the 61st ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 2024, pp. 1-6.
- Lin Ding, Song Bian and Jiliang Zhang*, "*PIMA-LPN: Processing-in-memory Acceleration for Efficient LPN-based Post-Quantum Cryptography*", in Proceedings of the 60th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 2023.

Thanks