集创赛

第十届全国大学生集成电路创新创业大赛

基于龙芯 SoC 的后量子密码与矩阵运算加速系统

龙芯中科杯 · 系统设计答辩

作品编号：CICC1008439· 团队：碳基生物

证据版本 d4564463 · 2026-07-15

团队介绍：围绕完整系统形成协同分工

团队名称：碳基生物

系统架构与 SoC 集成

- OpenLA500 平台集成
- AXI 、 DMA 与多时钟域
- SRAM 控制器优化

密码算法与 RTL 实现

- 全参数 ML-KEM 架构
- Keccak 、 NTT 与多项式算子
- 常量时间解封装

软件验证、测试与文档

- 板级驱动与测试程序
- 分层仿真和证据采集
- 系统报告与答辩材料

以统一接口、可重复测试和版本化证据贯通硬件、软件与文档。

目录

CONTENTS

1 **项目与系统方案**

开发过程、设计目标与系统数据流

2 **自主计算 IP**

Matmul 流水与全参数 ML-KEM

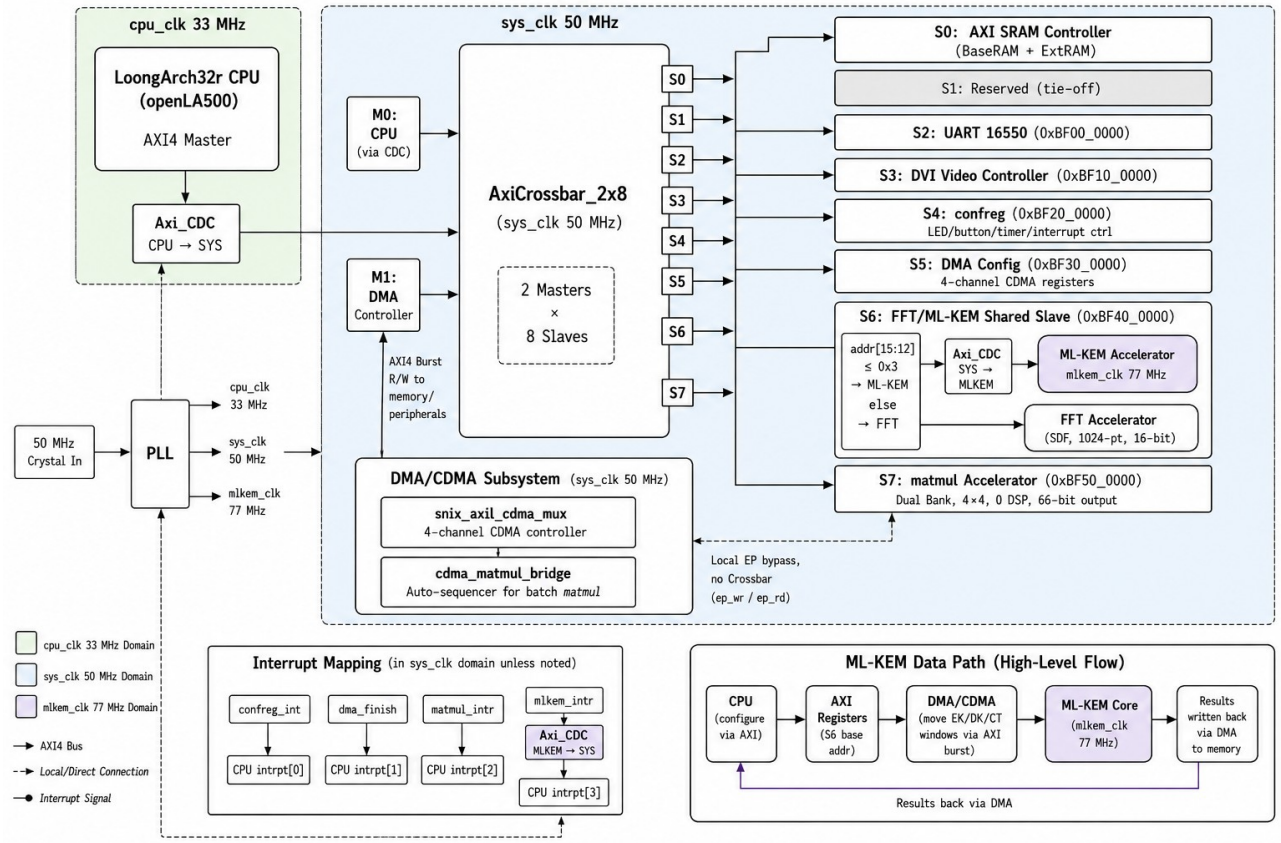
3 **验证与实现结果**

分层验证、资源时序与最终性能

4 **心得与后续工作**

工程认识、设计取舍与优化路线

作品重要亮点预览页



OpenLA500 + DMA 数据面 + 三个自主计算 IP

01 硬件自治

五千组 Matmul 任务一次启动完成

02 存储优化

SRAM 连续突发达到 1 beat/cycle

03 全参数密码

单比特流覆盖三等级、三操作

04 异步协同

三时钟域通过全五通道 AXI FIFO 连接

全系统 0 DSP · 三时钟域零违例

作品重要亮点预览页

4.911765 ms
Matmul 5000 组最终时间

827.80×
FFT DMA 相对软件加速

48.95–53.33×
ML-KEM DMA 相对软件加速

0 DSP
DSP48E1 使用量

验证对象	测试规模	结果
ML-KEM 主路径 KAT	3 等级 × 3 操作 × 1000	9000 / 9000
Decaps 隐式拒绝	3 等级 × 100	300 / 300
ML-KEM 板级诊断	3 等级 × 3 路径 × 100	900 次零失败
Matmul 最终评测	5000 组 · seed a3772ec8	4.911765 ms · 满分
FFT 板级验证	CPU / DMA 各 3 次	误差 Re=1 、 Im=2

实现质量

55,066
Slice LUT · 41.16%

29.5
BRAM Tile · 8.08%

88,843
时序端点

+0.070
全系统最小 WNS / ns

开发过程：以端到端证据驱动迭代

1 基础 SoC 跑通

完成处理器取指、串口及总线外设联调

2 计算 IP 接入

实现 Matmul 、 CRC32 、 FFT 与全参数 ML-KEM

3 数据通路优化

引入 DMA 端点、双 Bank 调度和 SRAM 连续突发

4 时钟与复位收敛

完成 PLL 分域、 AXI CDC 和复位顺序验证

5 分层验证闭环

建立叶模块、 IP 、 SoC 与板级四层证据

6 最终性能迭代

压缩启动与稳态空闲， Matmul 评测达到 100 分

每轮迭代同时检查功能正确性、总线可观测性、时序与板级端到端时间。

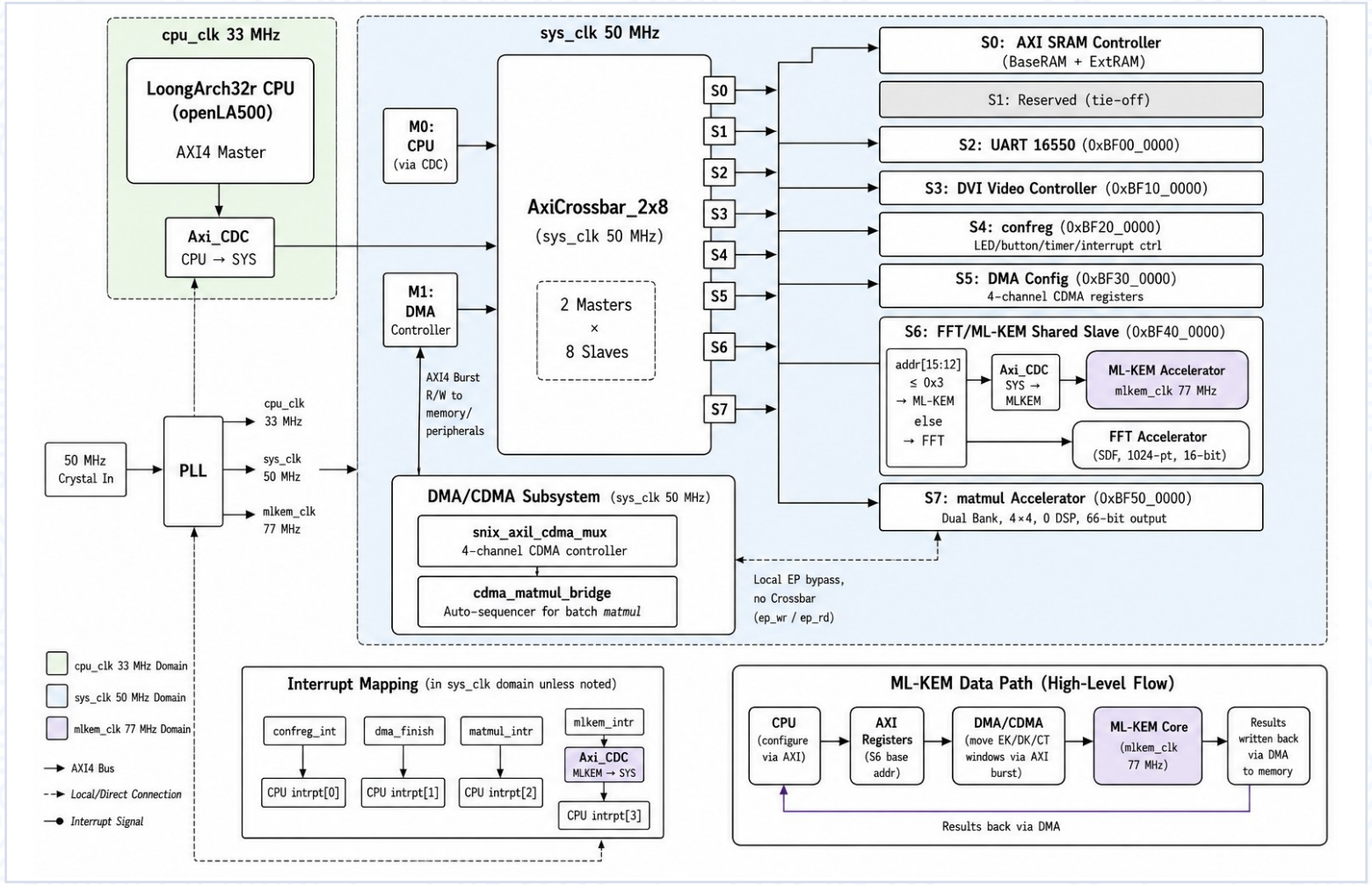
赛题要求与设计响应

赛题不是孤立 IP 设计，而是完整 SoC 中的端到端实现。

赛题要求 / 工程约束	本系统的设计响应
基于 OpenLA500 构建完整 SoC	双主八从 AXI 架构； CPU 、系统、 ML-KEM 三个异步时钟域
5000 组 4×4 矩阵乘法，禁止 DSP	全 LUT 乘加、双 Bank 序列器、在线 CRC32 与快速通道
实现 FIPS 203 ML-KEM	单比特流覆盖三等级、三操作； KAT 与隐式拒绝验证
提高端到端性能	四通道 DMA 、端点传输、 SRAM 连续突发与硬件自主调度

答辩主线：赛题约束 → 系统架构 → 数据流与自主 IP → 分层验证 → 实测结果

总体架构与自主设计边界



自主实现

- 四通道 DMA 与加速器端点
- Matmul 、批量序列器、 CRC32
- 1024 点 Radix-2^2 SDF FFT
- 全参数 ML-KEM 硬件 IP
- 两级 AXI 跨时钟域桥
- SRAM 控制器突发流水化

赛事基础平台

OpenLA500 、板级 SRAM 器件、 UART 及基础外设

数据搬运、 SRAM 与三时钟域协同

CPU 域 · 33.333 MHz
OpenLA500 / Cache / AXI 主端

→ AXI 双时钟 FIFO →

系统域 · 50 MHz
Crossbar / DMA / SRAM / Matmul / FFT

→ AXI 双时钟 FIFO →

ML-KEM 域 · 76.923 MHz
AXI 前端 / Keccak / NTT / FSM

硬件数据通路

CPU 配置 → DMA → ExtRAM → 加速器

CPU 只配置任务， DMA 、 SRAM 与加速器完成批量搬运和计算。

复位顺序： sys → mlkem → cpu ； 释放前 AXI valid 保持为 0 。

SRAM 连续突发优化

200 MB/s
理论单向带宽

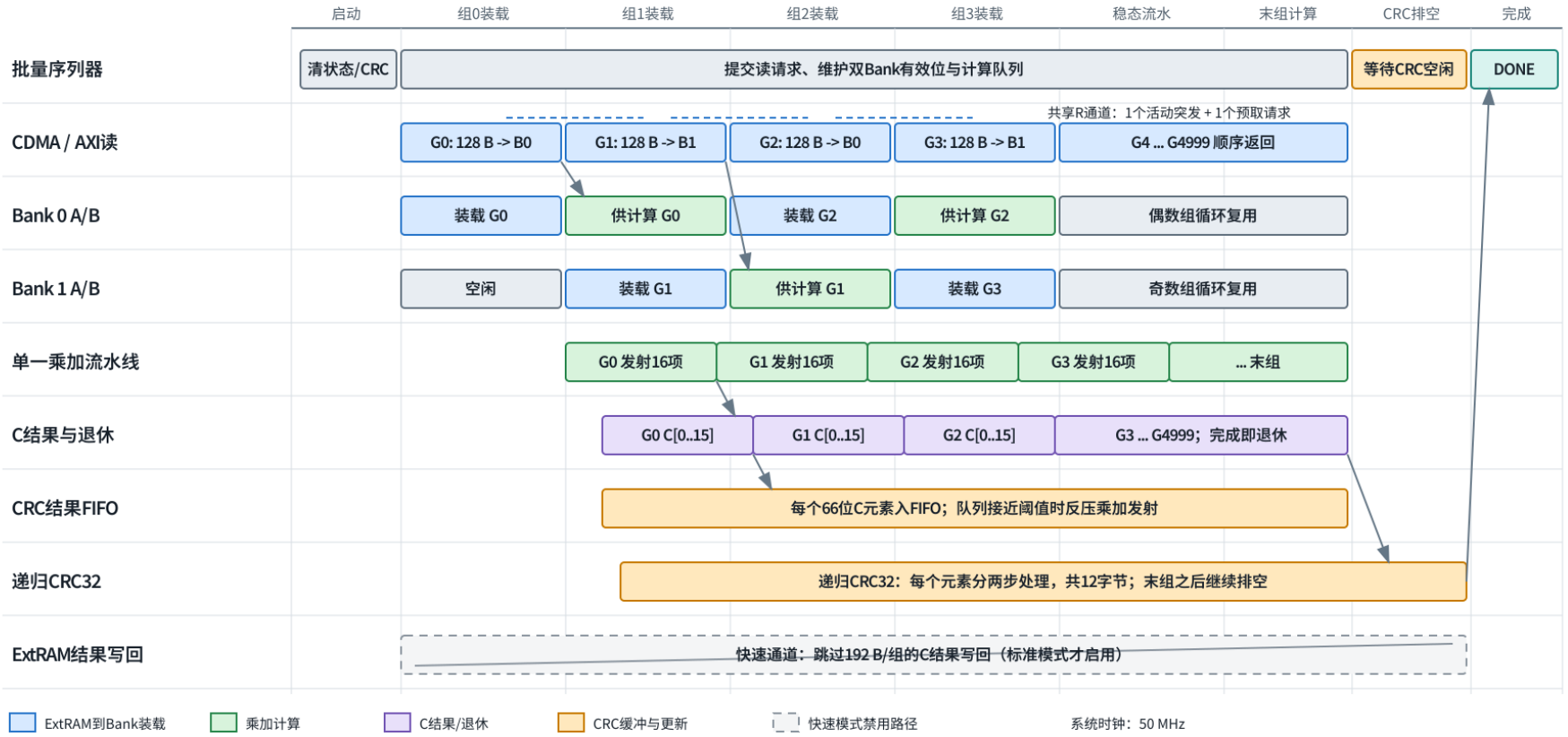
1 beat/cycle
无反压连续读写

读数据寄存保持 R 通道稳定； Bank 选择随事务锁存。

Matmul：一次启动完成 5000 组流水任务

Matmul 快速通道数据流甘特图

展示前四组进入稳态及最后收尾过程；阶段宽度用于表达依赖和重叠关系，不按周期严格缩放



关键节拍

128 B
每组 A/B 读取

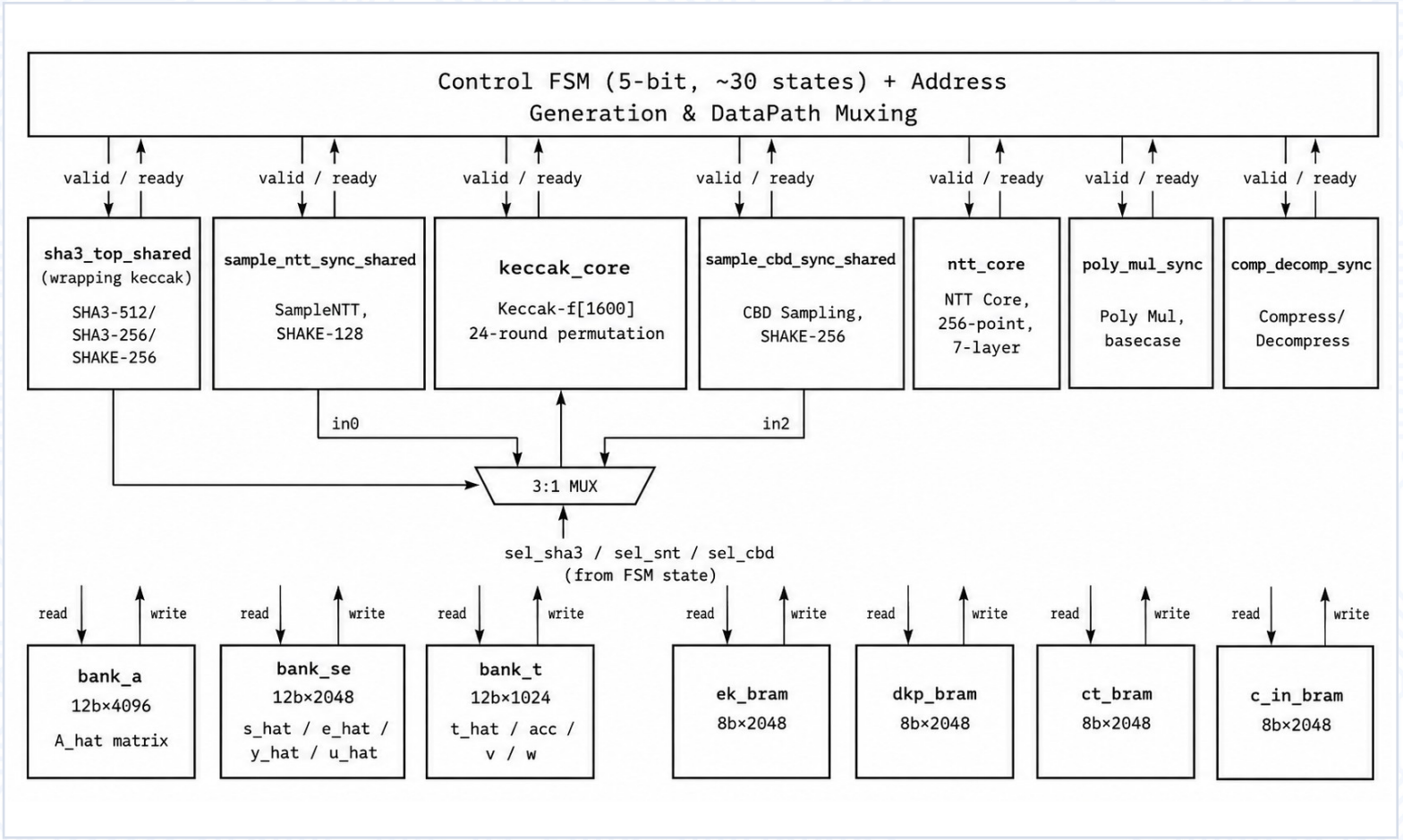
≈22 cyc
单 Bank 乘加延迟

2×6 B
每元素 CRC 更新

0 B
快速模式结果写回

最后一组退休后仍等待 CRC FIFO 排空，再产生 DONE 。

ML-KEM： 单比特流覆盖三等级与三操作



运行时配置

3

512 / 768 / 1024

3

KeyGen / Encaps / Decaps

- 参数在 start 时锁存
- 存储按 KMAX=4 静态分配
- 控制、算子、 BRAM 三级组织
- 公钥 / 私钥 / 密文支持 AXI 突发窗口
- 无需按安全等级重新综合

KeyGen 生成 ek/dk → Encaps 生成 c/ss → Decaps 恢复或拒绝 ss

ML-KEM 关键设计：复用、并行与常量时间

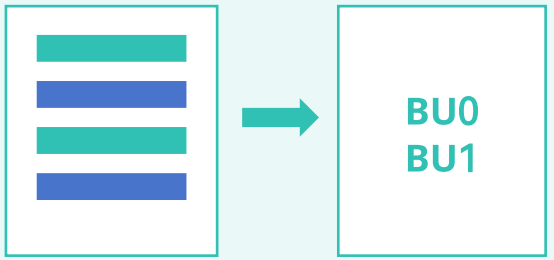
共享 Keccak

G/H/J 哈希
SampleNTT
CBD 采样

→ 单一 Keccak-f[1600]

避免两份额外实例
约节省 10.6k LUT

双蝶形 NTT



4 路 BRAM 无冲突供数
读 - 算 - 写三级调度

4 coeff/cycle · 0 DSP

Decaps 复用

D1–D5 解密恢复
↓
D6 复用 Encaps
↓
D7 常量时间比较

Accept 与 Reject 路径
总周期数完全相等

设计取舍：以资源共享和运行时可配置性换取更低的面积与部署复杂度。

四层验证：从算子正确到板级闭环

板级系统 真实 FPGA 、 CPU 软件、 DMA 与串口日志

SOC 集成 AXI 解码、 CDC 、复位释放、 SRAM 取指

IP 集成 Matmul / FFT / DMA / ML-KEM 端到端

叶模块 Keccak 、 NTT 、蝶形、 FIFO 、 CRC32

算法逐字节比对；板级以零失败、 CRC 匹配和误差阈值为判据。

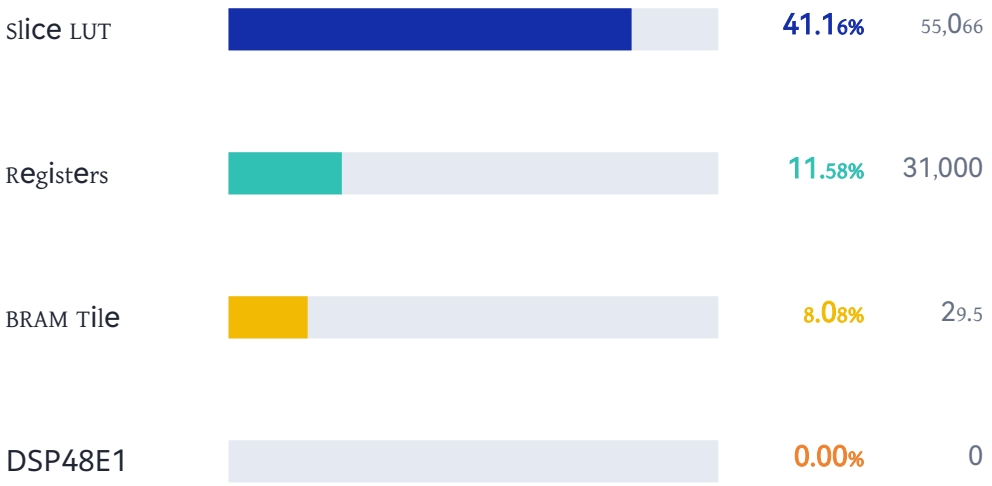
验证结果

9000	主路径 KAT
300	隐式拒绝向量
900	ML-KEM 板级运行
100%	Matmul 最终得分
6	FFT 板级测试

全部通过

实现结果：资源可控，三个时钟域全部收敛

FPGA 资源利用



xc7a200tfbg676-1 · 布局布线 100% 完成

布局布线后时序

时钟域	频率	Setup WNS	端点
cpu_clk	33.333 MHz	+0.737 ns	17,197
sys_clk	50.000 MHz	+0.125 ns	22,307
mlkem_clk	76.923 MHz	+0.070 ns	31,646

88,843
时序端点

0
建立 / 保持违例

+0.070
全系统最小 WNS / ns

ML-KEM 独立高速时钟域隔离了系统总线布线压力。

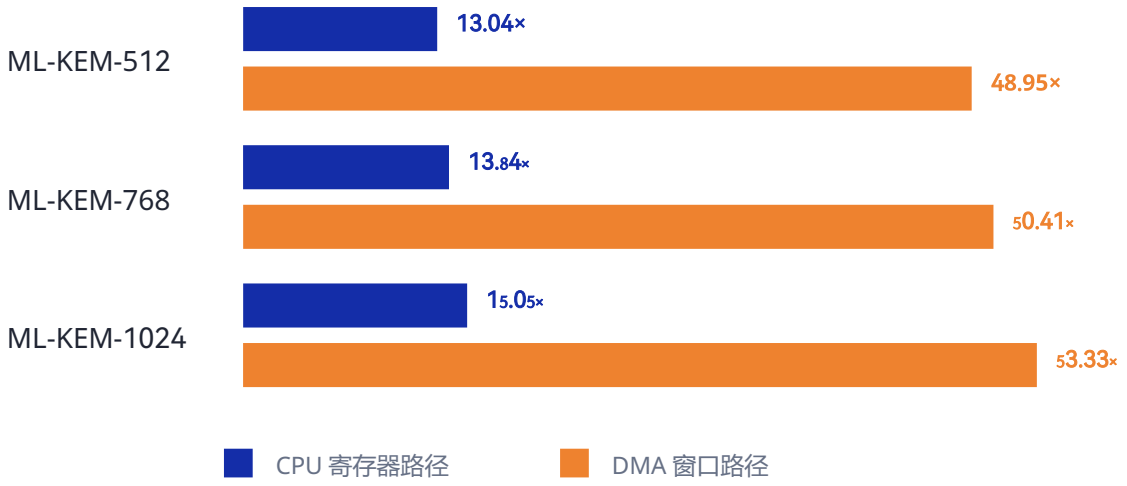
最终性能： Matmul 满分与端到端加速

4.911765 ms
Matmul 5000 组最终时间

827.80×
FFT DMA 相对软件加速

48.95–53.33×
ML-KEM DMA 相对软件加速

ML-KEM 三路径完整往返加速比



结果解释

- Matmul CRC32 0x0417d761 匹配
- FFT DMA 延迟 296.73 μs， 误差 Re=1 、 Im=2
- ML-KEM-512 DMA 往返约 1.605 ms
- SRAM 连续突发理论带宽 200 MB/s

随机种子 0xa3772ec8 · 最终得分 100.00%

项目心得：从单点优化走向系统工程

01 端到端优先

计算核延迟不是唯一指标；启动、搬运、调度和校验共同决定评测时间。

02 先正确再加速

先建立 CRC 、状态寄存器和分层测试等可观测手段，再压缩流水空闲。

03 取舍必须显式

Keccak 复用、双蝶形 NTT 和零 DSP 策略是在面积、吞吐与部署复杂度间的选择。

04 证据需要版本化

报告、软件、 RTL 和实测日志必须共享同一数据基线，才能保证结论可复现。

最终满分来自软硬件协同，而不是单一模块参数的堆叠。

后续工作：沿性能、验证与工程化继续演进

01	ML-KEM 并行度	增加 Keccak 并行路径，扩展 NTT 蝶形单元并评估面积收益比。
02	存储专项验证	补充 SRAM 随机反压、跨 Bank 边界与持续带宽微基准。
03	实现与功耗证据	完善 I/O 约束，使用 SAIF/VCD 活动率回标提高功耗估计可信度。
04	版本与回归体系	统一 RTL 、软件、测试向量和报告指标，形成自动化回归基线。

目标：在不牺牲标准完整性和可验证性的前提下继续提高系统吞吐。

总结：完成从算法 IP 到板级系统的闭环

01	系统	构建 CPU 、 DMA 、存储与三个计算加速器协同的异构 SoC
02	数据流	以 SRAM 连续突发、 DMA 端点和双 Bank 调度降低搬运开销
03	密码 IP	单比特流覆盖 ML-KEM 三等级、三操作和常量时间拒绝
04	工程验证	零 DSP 、三个时钟域收敛，并通过仿真与板级分层验证

最终结果： 5000 组 Matmul 用时 4.911765 ms · CRC32 匹配 · 得分 100.00%

感谢聆听

Q&A

中国集成电路未来之星从这里起步！

备用：地址空间与软件控制流程

AXI 从端	基地址	功能
S0	0x1c00_0000	BaseRAM / ExtRAM ， 共 8 MB
S5	0x1f30_0000	DMA 与矩阵批量序列器
S6	0x1f40_0000	FFT / ML-KEM 共享窗口
S7	0x1f50_0000	Matmul 控制与数据 Bank

软件控制流程

写配置寄存器

配置 DMA 窗口

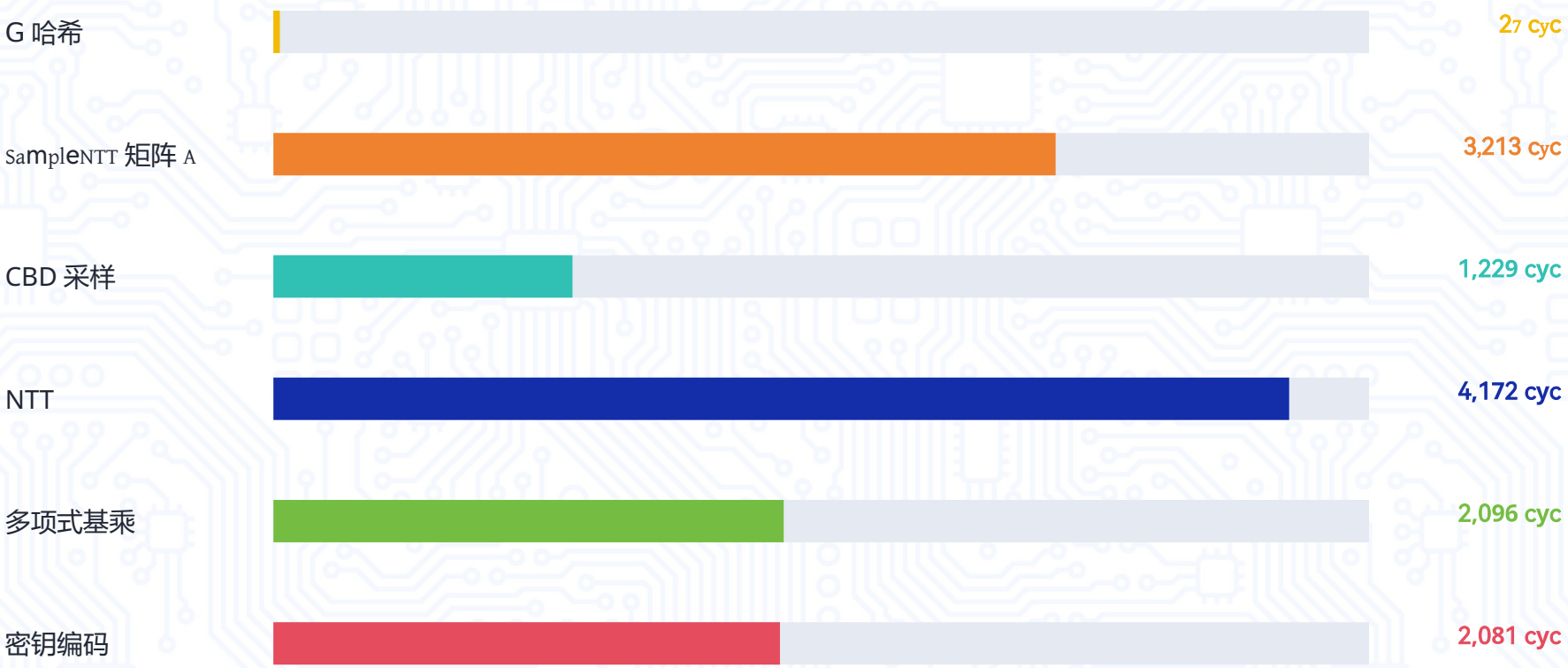
启动硬件

轮询 done

读取结果 / CRC

快速路径中 CPU 不参与逐组 Matmul 调度； ML-KEM DMA 路径只进行少量批量窗口配置。

备用： ML-KEM-512 KeyGen 逐状态周期分解



主要瓶颈

NTT
30.2%

SampleNTT
23.3%

两者合计
53.5%

优化优先级：增加采样路径 Keccak 并行度，其次扩展 NTT 蝶形单元数量。

备用：设计取舍与优化路线

维度	当前选择	优势	代价
安全等级	运行时 k=2/3/4	单比特流部署	地址与控制逻辑增加
Keccak	单核时分复用	节省约 10.6k LUT	状态间无法重叠
NTT	双蝶形、 4 coeff/cycle	BRAM 无冲突、 0 DSP	吞吐低于多 BU 实现
控制	30 状态硬连线 FSM	行为清晰、易验证	串行调度限制性能

优化路线

1 **双 Keccak 或专用采样核**

预计 KeyGen 下降 15%–20%

2 **扩展多 BU NTT**

提高至 8 coeff/cycle

3 **完善约束与活动率回标**

提高时序与功耗结论置信度