

# 黎广言

(+86) 137-0849-3221 · guangyali5-c@my.cityu.edu.hk · GitHub@GavinLlgy

## 个人总结

本人在校成绩优秀、乐观向上，工作负责、自我驱动力强、热爱尝试新事物，认同以数据为中心、尊重市场规律、开放易用的技术工具在未来的不可替代性。数理基础扎实，在校期间长期从事 FPGA 高速设计、并行计算相关研究。

## 教育背景

香港城市大学, 电机工程学系, 博士 2020.08 - 2025.02

研究生免学费奖学金 (2 次), 国家级竞赛一等奖, 广东省竞赛三等奖

香港城市大学, 电机工程学系, 工学学士 (甲等荣誉) 2016.08 - 2020.07

院长嘉许名单 (6 次), 暑期交换项目-法国蒙彼利埃

## 技术能力

- 软件编程语言: Python(Numpy, Pandas, TensorFlow), C++, CUDA, Bash, Matlab;
- 操作系统与工程构建: Linux/MySQL/Git/CMake/CICD pipeline;
- 硬件描述语言: Verilog HDL, VHDL, Scala(SpinalHDL);
- 硬件设计工具: Xilinx Vivado, Xilinx Vivado HLS, Verilator, VCS;

## 实习经历

香港华为研究所 | 理论部, 研究实习生 2023.12 - 2024.06

- 团队参与开发大规模**集群优化求解器**, 并部署于分布式 Intel x86 HPC 集群上。
- 独立负责 **稀疏矩阵**底层算子库的高性能调优。通过优化内存排布、线程绑定等, 在 **4 机 288 线程**下, 实现算子端到端提速 20%, 并完成**代码合入**全流程。
- 利用团队自研图切分/超图切分工具, 尝试实现低延迟**数值计算**自适应匹配硬件环境工具套件。

杭州之江实验室, 研究实习生 2023.07 - 2023.10

- 团队参与基于 **NVIDIA A100 GPU**, 并用于密态计算的 CUDA 算子库。
- 独立负责**离散向量卷积核**的性能调优。通过 kernel fusion、优化流水线等, 端到端性能超越同期 SOTA。
- 后期独立负责 CUDA 算子库向**华为昇腾 NPU(ASCEND 910B)**的迁移工作, 包括前期调研、底层算子重构、测试框架搭建等。

## 研究项目

FPGA 上的多项式乘法算子的设计空间探索 2022.07 - 2023.10

- 提出了针对多项式乘法 (类似离散卷积算子) 的算法 Radix-4 DGT, 增加了并行性。
- 设计了一种高度可扩展的硬件加速器生成器, 采用了所提出的 Radix-4 DGT 算法。在 Xilinx Artix-7、Virtex-7 和 Alveo U250 FPGA 上的性能超越了同时期 SOTA 工作。
- 产出试验报告, 技术分享, 以及研究论文。

FPGA 上的后量子密码硬件高速设计 2020.07 - 2022.7

- 提出了针对多项式乘法 (类似离散卷积算子) 的算法 Split-radix DGT, 降低了计算复杂度。
- 设计了一个高效的后量子密码硬件系统, 采用了所提出的 Split-radix DGT 算法。在 Xilinx Artix-7 FPGA 上的性能超越了同时期 SOTA 工作。
- 产出试验报告, 技术分享, 专利以及研究论文。

## 学术论文 (3 OUT OF 7)

- (SCI Q1 期刊) Li, G., Chen, D., Mao, G., Dai, W., Sanka, A. I., and Cheung, R. C. (2023). Algorithm-Hardware Co-Design of Split-Radix Discrete Galois Transformation for KyberKEM. *IEEE Trans. Emerg. Top. Comput.*
- (SCI Q2 期刊) Li, G., Ye, Z., Chen, D., Dai, W., Mao, G., Huang, K., and Cheung, R. C. (2024). Program-Galois: A Programmable Generator of Radix-4 Discrete Galois Transformation Architecture for Lattice-based Cryptography. *ACM T. Reconfigurable Technol. Syst.*

- (SCI Q1 期刊) Mao, G., Liu, Y., Dai, W., **Li, G.**, Zhang, Z., Lam, A. H. F., and Cheung, R. C. (2024). REALISE-IoT: RISC-V-Based Efficient and Lightweight Public-Key System for IoT Applications. *IEEE Internet Things J.*
- Jin, S., Gu, Z., **Li, G.**, Chen, D., Koç, C. K., Cheung, R. C., and Dai, W. (2024). Efficient Key-Switching for Word-Type FHE and GPU Acceleration. *Under Review*
- Mao, G., Chen, D., **Li, G.**, Dai, W., Sanka, A. I., Koç, Ç. K., and Cheung, R. C. (2022). High-Performance and Configurable SW/HW Co-design of Post-Quantum Signature CRYSTALS-Dilithium. *ACM T. Reconfigurable Technol. Syst.*

## 专利发表

---

- Cryptosystem With Utilizing Split-Radix Discrete Galois Transformation 已授权,US 2024/0430075 A1, 一种用于高性能密钥封装处理器的方法和系统
- A Processor For A Cryptosystem 已授权,US 12,093,198 B2, 一种支持数字签名服务的方法及系统

## 竞赛获奖

---

- 2023 年海峡两岸暨港澳大学生集成电路与电子设计邀请赛**全国一等奖**,2023 年 9 月
- 2023 年广东省计算机学会优秀论文奖三等奖,2023 年 12 月
- 香港城市大学研究生免学费奖学金**学费全免奖**,2023 学年, 2024 学年
- 香港城市大学电机工程学系研究生论坛**一等奖**, 2023 年 6 月