**郑州大学毕业设计（论文）**

题 目： 同态加密硬件加速器模拟系统设计

指导教师： 范文兵 职称： 教授

指导教师(校外)： 赵路坦 职称： 博士后

学生姓名： 蔡明 学号： 201924110803

专 业： 电子信息工程

院（系）： 电气与信息工程学院

完成时间： 2022年5月16日

2022年 5 月 16

摘要

全同态加密（Fully Homomorphic Encryption, FHE）技术保护了数据安全，但是，FHE的计算开销是明文直接计算开销的上万倍。因此，为了弥补性能上的巨大差距，最近越来越多的基于GPU、ASIC和FPGA的硬件加速器开始出现。但是在硬件加速器设计过程中，如何选择合适的加速器架构参数是很困难的，因此加速器的设计过程中往往需要软件模拟器的配合。本文通过使用python语言进行模拟加速器架构，设计了一款基于同态加密FPGA硬件加速器的软件模拟器，该模拟器可以辅助架构设计人员调整加速器架构设计中的一些参数，比如外部存储内存带宽、加速器输入缓存和输出缓存的大小以及加速器片上带宽等等。该模拟器通过模拟执行一组同态操作，来得到参数与执行这组同态操作所需总周期数的关系。最后通过分析参数与执行时间之间的关系对如何选取参数进行了介绍。

**关键词** 全同态加密，加速器，模拟器，FPGA

**Abstract**

Though Full Homomorphic Encryption (FHE) technology protects the data security, the computing cost of FHE is tens of thousands of times that of plaintext direct computing. Therefore, in order to make up for the huge gap in performance, more and more hardware accelerators based on GPU, ASIC and FPGA have emerged recently. However, it is difficult to select appropriate architecture parameters in the process of accelerator design. So, the accelerator design process often needs the cooperation of software simulator. I design a software simulator based on FPGA hardware accelerator by using python language to simulate the accelerator architecture. This simulator can help architecture designers adjust some parameters in the accelerator architecture design, such as external storage memory bandwidth, the size of accelerator input cache and output cache, on-chip bandwidth. The simulator simulates the execution of a set of homomorphic operations to obtain the relationship between parameters and the total number of cycles required to perform this set of homomorphic operations. Finally, the selection of parameters was introduced by analyzing the relationship between parameters and execution time.

**Key Words** fully homomorphic encryption, accelerator, simulator, FPGA

目 录

**摘要…………………………………………………………..……….….……..…...….I**

**Abstrct…………………………………………………………………...……..………I**

**1**绪论**………………………………………………………………….….……………1**

[1.1 研究背景和意义 1](#_Toc105099934)

[1.2 国内外研究现状 1](#_Toc105099935)

[1.3 本文主要工作 3](#_Toc105099936)

[2 同态加密介绍和理论分析**… … … …. …. … … … … … … … … … … … … … … … … … … 5**](#_Toc105099938)

[2.1 同态加密算法概述 5](#_Toc105099939)

[2.2 CKKS算法原理 6](#_Toc105099943)

[3 全同态加密加速器设计**… … … … … … … … … … … … … … … … … … … … … … … … 13**](#_Toc105099949)

[3.1 使用KCP实现UDP可靠传输 13](#_Toc105099950)

[3.2 使用io\_uring改进KCP传输 19](#_Toc105099953)

[4 模拟器设计和实现**… … … … … … … … … … … … … … … … … … … … … … … … … … 25**](#_Toc105099957)

[4.1 实验设计 25](#_Toc105099958)

[4.2 实验结果与分析 27](#_Toc105099962)

[5 模拟器的实验测试和结果分析**… … … … … … … … … … … … … … …… … … … … … 28**](#_Toc105099957)

[6 结论**… … … … … … … … … … … … … … … … … … … … … … … … ….. … … … … … … …** 34](#_Toc105099967)

[6.1 研究总结 34](#_Toc105099968)

[6.2 后续展望 34](#_Toc105099969)

**致谢 … … … … … … … … … … … … … … … … … … … … … … … … … … …. … … … … … …26**

**参考文献 … … … … … … … … … … … … … … … … … … … … … … … … … … … … … … … 26**

**附录1 外文资料翻译… … … … … … … … … … … … … … … … … … … … … … … … … … 27**

A1.1 译文：×××……×××…………………….……..…………………..………….…......….27

A1.2 原文：×××……×××…………………….……..………………………………….…….…31

1. 绪论

1.1研究背景和意义

同态加密可以在保持数据的加密的同时进行计算，这颠覆了传统加密方式无法加密计算的局面。同态加密可以广泛应用于云计算、金融科技、多方安全计算和健康医疗等领域，为保护数据安全提供了安全和高效的解决方案。在云计算领域，同态加密可以解决在云平台上进行计算时数据隐私泄露的问题。同时，同态加密可以减少多方参与计算时数据交换的问题，大大提高计算速度。在金融科技领域，同态加密可以实现保证隐私的交易处理，可以有效防止黑客入侵和数据窃取。在健康医疗领域，同态加密可以保护个人隐私，同时允许研究人员访问高度敏感的健康数据，以促进医学研究的进步。

但是同态加密，尤其是全同态加密的运算会导致计算成本、时间开销达到明文直接计算的上万倍。因此，为了提高FHE的效率，加速器的设计是一个不可避免的方向，近年来也出现了越来越多的基于FPGA、GPU和ASIC的硬件加速器。但是，为了设计出合理高效的硬件架构，在设计过程中往往需要进行繁琐的实验进行架构参数调整，而通过模拟器进行硬件加速器的设计调参可以大大降低研究时间和成本。因此，一种能够辅助研究者进行加速器设计调参的模拟器是非常必要的。

1.2国内外研究现状

1.2.1 同态加密加速器设计的研究现状

目前同态加密的硬件加速器设计已经有很多加速方案，主要是基于数字理论变换（Number Theoretic Transform,NTT）和其它多级并行设计进行加速。比如Nikola Samardzic等人提出的CraterLake加速器和Riazi等人提出的基于FPGA的CKKS FHE加速器。在针对模拟器设计方面目前还缺乏针对同态加密硬件加速器的模拟器设计，但是已经有Ananda Samajdar等人针对CNN卷积神经网络脉动阵列加速器设计的周期精准的SCALE-SIM模拟器以及其他相关模拟器比如DRAM模拟器DRAM-SIM2等。

1.2.2 硬件加速器模拟器设计的研究现状