**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 全同态加密硬件加速器**… … … … … … … … … … … … … … … … … … … … … … … … 13**](#_Toc105099949)

[3.1 现有加速器架构分析 13](#_Toc105099950)

[3.2 本文所模拟的加速器架构介绍 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

对于同态加密技术的应用场景，如云计算和物联网中，计算速度和保护隐私往往是一对矛盾。在这种情况下，研究人员已经开始探讨使用硬件加速器来提高同态加密算法的计算性能。目前主要的研究成果如下：

2018年，Axel Feldmann等人提出了一种名为F1的计算加速器[1]，用于支持全同态加密（FHE）技术下的安全高效计算。该加速器是使用Verilog HDL描述并实现，在Xilinx Virtex-7 FPGA平台上进行了测试。

2020年，Nikola Samardzic等人基于Axel Feldmann等人提出的F1加速器，结合FHE的密文大小通常非常大这一背景对加速器进行了改进，提出了CraterLake加速器[2]。

此外还有Yinghao Yang等人提出的Poseidon加速器[3]、Rashmi Agrawal[4]等人提出的FAB加速器以及Soran Ahmed[5]等人提出的一种针对RSU资源受限网络中全同态加密应用和安全性需求特点的加速器设计，实现了FHE算法的低功耗和高效计算。

1.2.2 硬件加速器模拟器设计的研究现状

硬件加速器模拟器是一个用于模拟硬件加速器的软件工具，它可以在不需要专用硬件平台的情况下，评估加速器的性能、功耗等指标。模拟器又分为系统级模拟器、功能级模拟器和行为级模拟器，本文主要考虑功能级模拟器。在针对功能级模拟器设计方面目前有:

Ananda Samajdar等人针对DNN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[6]。SCALE-Sim是一个专为深度学习应用设计的模拟器，可以支持各种常见的DNN架构（如CNN、RNN、LSTM等）及其优化技术。

Daniel J.Sorin等人开发用于内存模拟的DRAM-Sim2[7]，它主要关注模拟DRAM中存储单元和数组的操作，以及内存控制器的操作。通过模拟内存的具体操作行为，DRAM-Sim2可以帮助开发者进行内存系统的性能分析和优化。相比于功能级模拟器，行为级模拟器更加逼真，能够更好地反映实际系统的行为。

Binkert M.I等人出的用于通用处理器的GEM5模拟器[8] 。通常被用于CPU架构相关的模拟器和仿真领域。它支持多种ISA（Instruction Set Architecture）CPU体系结构（如ARM、x86、MIPS等），可以用于研究微处理器和计算机系统的各种性能指标、缓存一致性、功耗以及体系结构调优等方面的研究。

目前还没有用于同态加密加速器设计的专用模拟器。

1.3本文主要工作

本文主要是基于现有的全同态加密加速器架构设计一种用于辅助调整同态加密加速器架构设计参数的行为级周期精准模拟器。

基于同态加密算法本身影响加速器架构，加速器架构影响模拟器设计的这样一个思路将本文主要工作分为以下内容：

（1）对同态加密算法的基本概念、应用场景以及各种同态算法进行了基本介绍，然后针对本文采用的CKKS（Cheon-Kim-Kim-Song）全同态算法进行了算法原理的分析以便后文的加速器设计和模拟器设计的阐述更加清晰。

（2）对现有的基于ASCI和FPGA的同态加密硬件加速器的架构进行了分析，根据其架构特点指出一种用于架构设计的模拟器的必要性和实用性，并详细介绍了本文所模拟的加速器架构。

（3）对基于python设计的模拟器的软件系统框图、各模块子框图以及所采用的的数据结构、数据流图等进行了介绍。

（4）介绍如何通过设计好的模拟器进行分析加速器架构参数和加速器性能关系，并对所使用的程序进行了阐述和分析。

1. 同态加密介绍和理论分析

2.1 同态加密算法概述

2.1.1 同态加密算法的介绍

在密码学领域中，使用同态作为一种加密类型。同态加密（HE）是一种加密方案，它允许云服务商这样的第三方对加密的数据执行某些可计算的功能，同时保留加密数据的功能和格式的特征。第三方在得到同态加密的数据之后，对密文进行特定的计算，得到的计算结果再进行同态解密就可以得到和使用明文直接进行计算相同的结果。

典型的同态操作有加法同态和乘法同态，如图2.1所示，假设有两条明文消息m1和m2，则有：

对于同态加法，可以满足等式（2.1）和（2.2），其中Dec是同态解密函数、Enc是同态加密函数。

(2.1)

Enc(m1) + Enc(m2) = Enc(m1 + m2) (2.2)

对于同态乘法，可以满足等式（2.3）和（2.4），其中Dec是同态解密函数、Enc是同态加密函数。 对于HE（Homomorphic Encryption）中的表示法，它只允许加法和乘法运算。对于任何布尔电路，只能通过XOR门执行加法和和And门执行乘法[9]。

(2.3)

Enc(m1) \* Enc(m2) = Enc(m1 \* m2) (2.4)

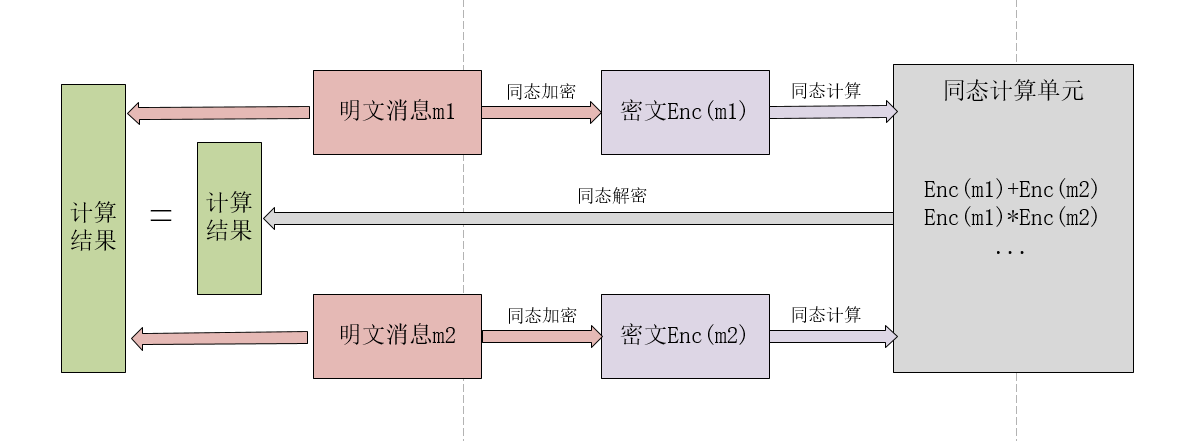


图2.1 同态加密计算示意图

2.1.1 同态加密算法的分类

在同态加密技术中，为了能够实现在加密状态下进行计算，需要将明文经过加密算法转换成密文，同时添加一个随机噪声。当使用同态加法或者同态乘法对密文进行运算时，这个随机噪声会随着运算而不断累加，导致密文中的噪声变得越来越大。

当密文中的噪声超过一定的阈值后，就会影响计算结果的准确性，从而导致解密结果的错误。一般情况下，同态加密算法会规定一个最大的可以容忍的噪声上限，如果噪声超过这个上限，则需要重新生成密文或者采用其他技术处理。因此，同态加密算法并不是都可以进行无数次的同态加法或者同态乘法的，同态加密算法可以根据对允许操作的数量的加密数据整齐地归类为三种类型的方案：

PHE（Partially Homomorphic Encryption）部分同态加密，如Paillier加密算法EIGamal加密算法和RSA（Rivest–Shamir–Adleman）加密算法[9]，由于其设计的简单性，可以运行在资源有限的设备上，并且不需要过多的密文噪声控制。因此，PHE通常拥有很快的运行速度和较低的计算成本，但其功能受到了一定程度的限制。下面对典型PHE算法进行简单的介绍：

Paillier加密算法，该算法的分析主要包括密钥生成、加密、解密和同态操作实现。

。

(2.5)

。其中lcm（a,b）是指获得a和b的最小公倍数。

(2.6)

(2.7)

步骤3：随机选择一个满足等式（2.8）的g，等式（2.8）中的函数T如公式（2.9）所示。

(2.8)

(2.9)

步骤4：通过公式（2.10）和（2.11）生成公钥pubk和私钥seck。

(2.10)

(2.11)

。

步骤2：通过公式（2.12）对一个明文pla进行加密得到密文cic。

(2.12)

* 通过公式（2.13）可以将密文cic转成明文pla。

(2.13)

* 公式（2.14）表示了Paillier加密算法是如何实现对密文和密文同态乘法的。

(2.14)

SWHE（Somewhat Homomorphic Encryption）有限同态加密，如Gentry-Halevi-Smart(TFHE)算法、Brakerski-Gentry-Vaikuntanathan(BGV)算法和Van Dijk-Landais Encrypt Scheme(VLLE)算法。其通常支持多个同态运算类型，如同态加法和少量同态乘法。相比于PHE，SWHE提供的更大的功能集，可以执行更复杂、更实用的计算任务。由于SWHE使用了更复杂的算法并且需要对噪声进行更精细的控制，在效率方面会稍逊于PHE。

FHE（Fully Homomorphic Encryption）完全同态加密，如Gentry-Full Homomorphic EncryptionAlgorithm、Brakerski-Gentry-Vaikuntanathan-Smart(FV)算法和Cheon-Kim-Kim-Song(CKKS)算法，其是同态加密中最强的形式。FHE支持任何同态运算类型，包括任意多次的同态加法和同态乘法，即便密文也能直接执行相应操作。FHE相比于前两者具有更高的安全级别和更高的功能性，但由于其使用了更加复杂的算法和更精细的噪声控制，因此在效率方面通常比SWHE和PHE更慢。

2.2 CKKS算法的原理

由于FHE算法可以进行任意多次的同态加法和同态乘法，所以FHE的实用性更高，并且FHE的功能性和安全性也更高。此外，FHE算法中CKKS算法由于其采用近似计算，所以它的细节得到了很大的简化，并且计算效率也有很大的提升，所以现在的加速器主要针对的便是CKKS算法。本小节将分析本文模拟的加速器所采用的CKKS算法的原理。

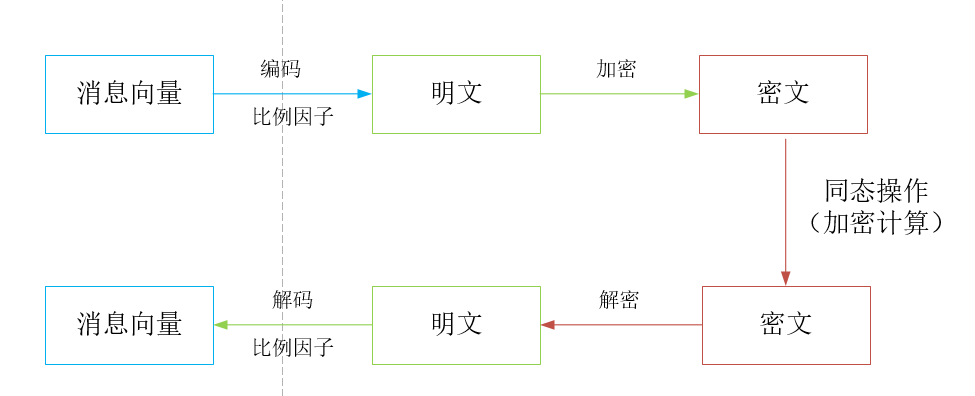


图2.2 同态加密计算示意图

如图2.2所示，

参考文献：

[5]An Energy-Efficient Implementation of Fully Homomorphic Encryption for Resource-Constrained Networks

[7] 《DRAMSim2: A Cycle Accurate Memory System Simulator》

[8] 《The gem5 Simulator》

[9] Survey on Homomorphic Encryption and Address of New Trend