分类号 TP309 密 级

U D C 编 号 10486

武漢大學

博 士 学 位 论 文

XXX 关键技术研究

研 究 生 姓 名：X X X

指 导 教 师 姓 名：X X 教 授

学 科、专 业 名 称：网 络 空 间 安 全

研 究 方 向：X X X X

二〇二四年一月

Research on Key Techniques for XXXX

Candidate：XXX

Supervisor：Prof. XX

Major：Cyberspace Security

Speciality：XXXX

School of Cyber Science and Engineering

WUHAN UNIVERSITY

Jan 2024

论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的研究成果。除文中已经标明引用的内容外，本论文不包含任何其他个人或集体已发表或撰写的研究成果。对本文的研究做出贡献的个人和集体，均已在文中以明确方式标明。本声明的法律结果由本人承担。

学位论文作者（签名）：

年　　月　　日

武汉大学学位论文使用授权协议书

本学位论文作者愿意遵守武汉大学关于保存、使用学位论文的管理办法及规定，即：学校有权保存学位论文的印刷本和电子版，并提供文献检索与阅览服务；学校可以采用影印、缩印、数字化或其它复制手段保存论文；在以教学与科研服务为目的前提下，学校可以在校园网内公布部分或全部内容。

一、在本论文提交当年，同意在校园网内以及中国高等教育文献保障系统（CALIS）、高校学位论文系统提供查询及前十六页浏览服务。

二、在本论文提交 □ 当年/ □ 一年/ □ 两年/ □ 三年以后，同意在校园网内允许读者在线浏览并下载全文，学校可以为存在馆际合作关系的兄弟高校用户提供文献传递服务和交换服务。（保密论文解密后遵守此规定）

论文作者（签名）：_____

学　　号：_____

学　　院：_____

日期：　　年　　月　　日

论文创新点

目　录

插图索引

表格索引

中英文缩略语对照表

AES	Advanced Encryption Standard	高级加密标准
API	Application Programming Interface	应用程序编程接口
ARM	Advanced RISC Machine	高级精简指令集机器
ASLR	Address Space Layout Randomization	地址空间布局随机化
BHB	Branch History Buffer	分支历史缓冲区
BHI	Branch History Injection	分支历史注入
BPU	Branch Prediction Unit	分支预测单元
BRB	Branch Retention Buffer	分支保留缓冲区
BTB	Branch Target Buffer	分支目标缓冲区
CNN	Convolutional Neural Network	卷积神经网络
CPU	Central Processing Unit	中央处理器
CVE	Common Vulnerabilities and Exposures	通用漏洞披露

摘　要

摘要。

关键词: 侧信道攻击

ABSTRACT

Abstract.

Key words: Side-Channel Attack

1 绪论

1.1 研究背景与意义

随着 XXXX[1]发展，

XXXX

进一步 XXXXXX。

1.2 国内外研究现状

XXXX

1.2.1 XXXX 技术研究现状

XXXX

1.2.2 XXXX 技术研究现状

XXXX

1.2.3 XXXX 技术研究现状

2 相关工作综述

3 面向 XXXXX 的 XXXXX

4　针对 XXXXX 的 XXXXX

5 基于 XXXXX 的 XXXXX

6　针对 XXXXX 的 XXXXX

7 总结与展望

7.1 本文总结

7.2 未来工作展望

参考文献

[1] Acıiçmez O, Brumley B B, Grabher P. New results on instruction cache attacks[C]//Cryptographic Hardware and Embedded Systems, CHES 2010. Springer, 2010: 110-124.

作者简历及攻博期间发表的科研成果目录

作者简历

XXX（19XX—），男，湖北武汉人，武汉大学 XXX 学院博士研究生

研究方向：XXXX

2021 年 9 月——至今，武汉大学，XXXX

学术论文

[1] **XXX**, XXX*. Title. *Jounral/Conference*

（CCF-A 类会议，对应论文第 3 章）

发明专利

[1] 一种 XXXX 方法及系统，发明人：XXX、**XXX**，申请中，申请号：XXXXX，申请日：XXXX 年 XX 月 XX 日

获奖情况

[1] 武汉大学 XXXX 奖学金，一等奖，2021

[2] 武汉大学 XXXX 奖学金，一等奖，2022

致　谢