魏凌霄

lxwei@outlook.com · (+852) 5647-6448 · lingxiao-wei · ultracold273

教育背景

香港中文大学，香港 2013 -- 2017

在读博士研究生 计算机科学与工程

南京大学，江苏南京 2008 -- 2012

学士 电子科学与工程

实习经历

国民技术股份有限公司 深圳 2013 年 7 月 -- 2013 年 9 月

实习 TPM2.0 芯片测试与验证

- TPM2.0 芯片是可信计算平台的基础，提供可靠的密钥存储和多种可靠密码算法
- TPM 芯片现已被广泛的运用于个人电脑和平板电脑中
- 主要工作职责为 TPM2.0 芯片编写测试程序，确保其满足设计的安全需求
- 协助公司将该芯片通过国家密码安全局的测试，获取认证上市证书

上海盐巴科技有限公司 上海 2016 年 2 月 -- 2016 年 4 月

实习 智能体感手套硬件设计和驱动编写

- 智能体感手套可实时捕捉手部的姿态，可用于手势识别和体感游戏等
- 工作内容为设计体感手套硬件电路，包括芯片选型，PCB 设计等
- 为硬件编写驱动程序，实现 USB 通讯和蓝牙通讯等功能

研究项目与论文

研究方向主要与硬件安全有关，包括密码设备的安全性分析，硬件木马的设计和防护，硬件安全原型和安全系统的构建等。

密码设备针对探针攻击的脆弱性研究 [1] 2013 年 -- 2014 年

- 探针台可用于获取芯片运行过程中其内部数据的值，而密码芯片的安全性依赖于其中间数据，因而密码芯片会受到探针攻击的威胁
- 本研究为芯片中信号提出了其受威胁性的量化模型，可用于指导设计者更好的防范探针攻击

基于印刷电路板的物理不可克隆函数的研究 [2] 2014 年 -- 2015 年

- 物理不可克隆函数利用不可复制的工艺偏差为设备提供唯一的认证编码
- 本研究在印刷电路板上设计了一种电容结构，可用于印刷电路板的防伪需求

高精度高性能注错仿真平台研究 [8] 2015 年 -- 2016 年

- 传统芯片设计行业为提高芯片的可靠性需要对其功能进行注错验证
- 本研究设计了一种基于 FPGA 的注错平台，包括硬件平台和软件工具
- 芯片设计者可以很方便的利用该平台实现注错仿真

基于深度学习系统的功耗侧信道攻击 [7] 2016 年 -- 2017 年

- 随着深度学习系统的的广泛应用，其隐私和安全也成为越来越重要的课题
- 本研究展示了一种针对 FPGA 实现的卷积神经网络攻击，攻击者可通过对 FPGA 功耗的测量恢复其输入的图片

技能

- 编程语言: C/Python/C++/Verilog
- 专业软件: Synopsys DC/SPICE/Altium Designer
- 语言能力: 熟练使用普通话、英语

活动和演讲

ASPDAC'2015 演讲者，日本东京 2015 年 1 月
ICCAD'2015 演讲者，美国奥斯汀 2015 年 11 月
CTC'2016 演讲者，南通 2016 年 7 月

助教经历

数字系统和微处理器导论 2013 年秋季
计算机组成与设计 2014 年春季
计算导论 2014 年，2015 年秋季
数字逻辑设计实验 2015 年春季

获奖情况

研究生奖学金，香港中文大学 2013 年 8 月 -- 2017 年 7 月
国家奖学金，南京大学 2011 年 12 月
TI 杯全国大学生电子设计大赛一等奖 2010 年 9 月

发表论文列表

[1] **L. Wei**, J. Zhang, F. Yuan, Y. Liu, J. Fan, and Q. Xu, "Vulnerability Analysis for Crypto Devices against Probing Attack," in *Proceedings of IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC), Chiba, Japan, January 19-22, 2015*, pp. 827--832.

[2] **L. Wei**, C. Song, Y. Liu, J. Zhang, F. Yuan, and Q. Xu, "BoardPUF: Physical unclonable functions for printed circuit board authentication," in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, TX, USA, November 2-6, 2015*, pp. 152--158.

[3] J. Zhang, F. Yuan, **L. Wei**, Z. Sun, and Q. Xu, "VeriTrust: Verification for Hardware Trust," in *Proceedings of IEEE/ACM Design Automation Conference (DAC), Austin, TX, USA, May 29 - June 07, 2013*, pp. 61:1--61:8.

[4] J. Zhang, G. Su, Y. Liu, **L. Wei**, F. Yuan, G. Bai, and Q. Xu, "On Trojan Side Channel Design and Identification," in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, November 3-6, 2014*, pp. 278--285.

[5] Y. Liu, J. Zhang, **L. Wei**, F. Yuan, and Q. Xu, "DERA: Yet another Differential Fault Attack on Cryptographic Devices based on Error Rate Analysis," in *Proceedings of IEEE/ACM Design Automation Conference (DAC), San Francisco, CA, USA, June 7-11, 2015*, pp. 31:1--31:6.

[6] Y. Liu, **L. Wei**, Z. Zhou, K. Zhang, W. Xu, and Q. Xu, "On Code Execution Tracking via Power Side-Channel," in *Proceedings of ACM SIGSAC Conference on Computer and Communication Security (CCS), Vienna, Austria, October 24-28, 2016*, pp. 1019--1031.

[7] **L. Wei**, Y. Liu, B. Luo, Y. Li, and Q. Xu, "On Power Side-Channel Attack of Convolution Neural Networks," submitted to *Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 16-18, 2018*.

[8] **L. Wei**, Y. Liu, and Q. Xu "FISim: a High-Fidelity and High-Performance Full-system Fault Emulation Framework, " submitted to *IEEE/ACM Design Automation, Test in Europe (DATE), Dresden, Germany, March 19-23, 2018*.