WEI, LINGXIAO

lxwei@cse.cuhk.edu.hk · (omitted for privacy) · lingxiao-wei

Education

The Chinese University of Hong Kong (CUHK), Hong Kong, China 2013 -- exp. 2017

Ph.D candidate in Computer Science and Engineering (CSE)

Nanjing University, Nanjing, China 2008 -- 2012

B.S. in Electronics Engineering (EE)

Working Experience

Nationz Inc. Shenzhen, China July 2013 -- Sept. 2013

Intern Test and Verification of TPM2.0 Product

- TPM2.0 chip is the core part of trusted computing and it is widely deployed on PCs and tablets.
- Responsible for writing testing programs of TPM chips to verify its functionality
- Help to pass test and get certificate from State Cryptographic Administration.

Shanghai Inbestech Co. Shanghai, China Feb. 2016 -- Apr. 2016

Intern Design of a smart motion sensing glove

- Smart glove captures hand motion in real-time
- Potential application includes gesture recognition and motion sensing games
- Responsible for hardware and firmware design/implementation

Research Projects

Vulnerability Analysis on Cryptographic Devices against Probing Attacks[1] 2013 -- 2014

- Probing station can acquire intermediate values during normal operation of a chip
- Security of cryptographic devices can be broken by exploitation of intermediate signals
- Proposed a method to quantitize vulnerability of each intermediate signal, providing guidance for protection

Printed Circuit Board Based Physical Unclonable Function[2] 2014 -- 2015

- Physical Unclonable Function (PUFs) utilizing unduplicated process variations for device authentication
- Designed a PUF with capacitor-like structures on PCB to prevent PCB from counterfeiting

High-Performance and High-Fidelity Fault Emulation Framework 2015 -- 2016

- IC designers usually adopt FPGA to verify IC's reliability by analyzing fault behaviors
- Design a set of hardware modules and software tools facilitating system level fault emulation

Power Side-Channel Analysis on Deep Learning Platforms 2016 -- 2017

- Dedicated hardware for deep learning lacks protection and leaks information about data it processed
- Demonstrate an attack on a hardware CNN on FPGA to recovered the input image

Skills

- Programming Languages: C/Python/C++/Verilog
- Professional Software: Synopsys DC/SPICE/Altium designer/
- Languages: English -- Fluent, Mandarin Chinese -- Native Speaker

Talks and Activities

Presentor at ASPDAC'2015, Tokyo, Japan Jan. 2015
Presentor at ICCAD'2015, Austin, TX, USA Nov. 2015
Presentor at CTC'2016, Nantong, China July 2016

Teaching Assistant

ENGG2120, Introduction to Digital and Microprocessor Systems	Fall, 2013
CENG3420, Computer Organization and Design	Spring, 2014
ENGG1100, Problem Solving by Programming (C)	Fall, 2014, 2015
CENG2010, Digital Logic Design Laboratory	Spring, 2015

Honors and Awards

Postgraduate Scholarship, The Chinese University of Hong Kong	2013 -- 3017
National Scholarship, Nanjing University	2011
TI Cup National Electronics Design Contest First Prize	2010

Publication List

[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.