Sihang Pu

Curriculum Vitae

Interests

I am interested in applied cryptography and system security where I can address realistic privacy problems via practical methods.

Research experience

Oct. 2017 – Dec. 2017

Lab of Crypto and Computer Security, SJTU

Extract ECDSA Keys from Mobile Devices

Trying to extract ECDSA keys from mobile phones (iOS & Android) via electromagnetic channels divulged from CPU. We aimed to improve attack performance and correctness during key extraction by exploiting some new analysis methods.

Jun. 2016 – Mar. 2017

Lab of Crypto and Computer Security, SJTU

Achieving Robustness in Side-channel Attacks

Designed and implemented a pre-processing method to generate robust model during side-channel attacks. The idea was derived from data augmentation to expand and distort the original dataset to improve generality of it. Such method could be combined with any existing technique (including PCA, LDA, SVM, etc.) to effectively obtain results. These works has been published on CARDIS'2017.

Oct. 2015 – Apr. 2016

Lab of Crypto and Computer Security, SJTU

Countermeasure Scheme against Side-channel Attacks

Implemented a countermeasure scheme (using 'masking' technique) to defend mainstream block cipher algorithms (AES for instance) from side-channel attacks. This scheme was designed by one of co-authors of our published paper. I discussed with him to optimize the matrix multiplication operation and improved its performance dramatically on AVR and x86 platforms. These works has been published on CARDIS'2016.

Jul. 2015 – Nov. 2015

Lab of Crypto and Computer Security, SJTU

Attacking 3G USIM Card

Analyzed the communication protocol of 3G USIM card and recover the secrets via side-channel attacks (using power channels). We were able to recover AES keys used in 3G authentication process within 300 power traces which can be collected from a sim-card-reader in several minutes.

✍ Pudong New Area District,
Shanghai, China

☎ +86 16602150943 (primary)
+86 13122213103

✉ push.beni@gmail.com

➚ Google Scholar Page

Education

2015 – 2018 **Shanghai Jiao Tong University, China**
Master of Engineering
Computer Technology
GPA: 3.39

2011 – 2015 **Northwestern Polytechnical University, China**
Bachelor of Engineering
Underwater Acoustic Engineering
GPA: 3.26 (8/58)

Knowledge

Encryption Algo	AES, DES, RSA, ECDSA, SHA-2
Privacy	Oblivious Transfer, Garbled Curcuit, Cut'n'Choose Game
Compression Algo	gzip, DEFLATE, LZ77/78
Others	Blockchain, Machine Learning

Software projects

2016 **Music Genre Classifiers**
Implemented several classifiers to predict the genre of a song given a .wav file as input.

2016 **A Protection Scheme for AES Encryption**
Implemented a provable protection scheme for AES and other block ciphers, written in C and targeted on AVR.

2016 **FPGA Implementation of Block Ciphers**
Implemented AES and DES algorithms on FPGA using Verilog.

2015 **A FAT32 File Interface**
Implemented a FAT32 file interface for MCU, written in C.

Other experience

Jul 2017 – Sep 2017	**University of California, Los Angeles** *Summer Session*
Mar 2018 – Mar 2019	**Autodesk Inc.** *Software Engineer*

Software skills

Good level	C, C++, Java, CPU Architecture, Operating System
Intermediate	Python, Objective-C, Verilog, LaTeX, MATLAB
Basic level	R, Swift, Javascript, HTML

Communication skills

English	Oral: fair – Written: good
Chinese	Native

Publications

2017 **Trace Augmentation: What Can Be Done Even Before Preprocessing in a Profiled SCA?**
CARDIS'2017, Lugano, Switzerland
***Sihang Pu**, Yu Yu, Weijia Wang, Zheng Guo, Junrong Liu, Dawu Gu*
[acceptance rate 29%)

2017 **Boolean Matrix Masking for SM4 Block Cipher Algorithm**
CIS'2017, Hong Kong, China
***Sihang Pu**, Zheng Guo, Junrong Liu and Dawu Gu*

2016 **Inner Product Masking for Bitslice Ciphers and Security Order Amplification for Linear Leakages**
CARDIS'2016, Cannes, France
*Weijia Wang, François-Xavier Standaert, Yu Yu, **Sihang Pu**, Junrong Liu, Zheng Guo and, Dawu Gu*