Sihang Pu

Curriculum Vitae

✍ Pudong New Area District,
Shanghai, China

☎ +86 16602150943 (primary)
+86 13122213103

✉ push.beni@gmail.com

➚ Google Scholar Page

Research experience

Jun. 2017 – Dec. 2017

Lab of Crypto and Computer Security, SJTU

Analyze ECDSA Running on Mobile Phone

Aiming for recovering the ECDSA secret key of some app running on a mobile phone (iOS & Android) via analyzing electronic magnetic signals divulged from the system.

Jun. 2016 – Mar. 2017

Lab of Crypto and Computer Security, SJTU

Achieving Robustness in Side-channel Attacks

Design and implement a pre-processing method to generate robust model during side-channel attacks. The idea is derived from data augmentation to expand and distort the original dataset to improve generality of it. Such method can be combined with any existing techniques (including PCA, LDA, SVM, etc) to effectively employ attacks.

Oct. 2015 – Apr. 2016

Lab of Crypto and Computer Security, SJTU

Countermeasure Scheme against Side-channel Attacks

Implement a countermeasure scheme ('masking' technique) to defend mainstream block cipher algorithms (i.e., AES) from side-channel attacks. This scheme is designed by a co-author of our published paper. I discussed with him to optimize the matrix multiplication operation and improve the performance on AVR.

Jul. 2015 – Nov. 2015

Lab of Crypto and Computer Security, SJTU

Attacking 3G USIM Card

Analyze the communication protocol of 3G USIM card and recover the secrets by exploiting side-channel attacks. After collecting power assumptions traces of a SIM card, we are able to recover the secret key of AES algorithm used in authentication process.

Interests

System security and applied cryptography to address realistic privacy problems.

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 Eng* *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

2017	**A Simple Raytracing Renderer** *A basic raytracing renderer written in C++.*
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.*
2015	**A LaTeX Template** *Implemented a LaTeX template for NWPU Bachelor thesis.*
2015	**A FAT32 File Interface** *Implemented a FAT32 file interface for MCU, written in C.*

Software skills

Good level	C, C++, Java, CPU Architecture, Linux kernel
Intermediate	Python, Objective-C, 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*