Sihang Pu

<蒲思行>
mail: <push.beni@gmail.com> • tel: <+86 131 2221 3103> • home page: <http://push-beni.github.io>

EDUCATION

Shanghai Jiao Tong University (SJTU), Minhang, Shanghai, China
Department of Computer Science and Engineering

- Master in Computer Technology — Sep 2015 – Present
  - Adviser: Prof. Dawu Gu
  - Focus: big data, side-channel analysis
  - Cumulative GPA: B+ (3.45/4.0)

Northwestern Polytechnical University (NWPU), Xi’an, Shaanxi, China
School of Marine Science and Technology, Department of Electronic and Information

- Bachelor in Underwater Acoustic Engineering — Sep 2011 – Jun 2015
  - Cumulative GPA: B+ (80.1/100)
  - Ranked top 30% in my major

RESEARCH EXPERIENCE

Laboratory of Cryptology and Computer Security (LoCCS), Shanghai Jiao Tong University

- Postgraduate Research Student — Aug 2015 – Present
  - Supervisors: Prof. Dawu Gu and Prof. Yu Yu
  - Focus: side-channel analysis, cryptography.

PUBLICATIONS

CONFERENCES

[1] **Sihang Pu**, Yu Yu, Weijia Wang, Zheng Guo, Junrong Liu, Dawu Gu, “Trace Augmentation: What Can Be Done Even Before Preprocessing in a Profiled SCA?,” in *Proceedings of Smart Card Research and Advanced Applications (CARDIS) 2017*, Lugano, Switzerland;
(acceptance rate is 29% this year); final version->

[2] **Sihang Pu**, Zheng Guo, Junrong Liu, Dawu Gu, “Boolean Matrix Masking for SM4 Block Cipher Algorithm,” in *Proceedings of International Conference on Computational Intelligence and Security (CIS) 2017*, Hong Kong, China; final version->

[3] Weijia Wang, François-Xavier Standaert, Yu Yu, **Sihang Pu**, Junrong Liu, Zheng Guo and, Dawu Gu, “Inner Product Masking for Bitslice Ciphers and Security Order Amplification for Linear Leakages,” in *Proceedings of Smart Card Research and Advanced Applications (CARDIS) 2016*, Cannes, France; final version->.

AWARDS

- Undergraduate Second-class Scholarship of Institute — Nov 2012
  For high grades and ranking in the first year’s study

PROJECTS

A simple ray-tracer, written in C++,

- Using a novel method instead of classical approaches to handle intersection with cubes.

A protection scheme of AES encryption algorithm, written in C

- Design and implement fast calculations for byte-matrices.

OTHER EXPERIENCE

Shanghai Viewsource Information Science and Technology Company,
Shanghai, China

- Software Engineer (part-time intern) — Jul 2016 – Jul 2017

University of California—Los Angeles,
California, USA

- Enrolled in a Summer Session — Aug 2017 – Sep 2017

LANGUAGES TOEFL: 100 GRE: 323

SKILLS C, C++, Java; Python, R, MATLAB, $\LaTeX$; WebGL, OpenGL, JavaScript

INTERESTS Ray racing and shading, FEM simulation of 3D solids, machine learning, cryptography;