SHIH-CHUN YOU

+44-7494-047267 ⋄ Cambridge, UK
andersen12282015@gmail.com ⋄ https://www.cl.cam.ac.uk/∼scy27⋄ https://github.com/SCYou27

EDUCATION

Ph.D. in Computer Science, University of Cambridge, UK 2018 – 2023

- Security analysis on cryptographic algorithm implementations, with **3 relevant peer-reviewed papers**.

M.Sc. in Electrical Engineering, National Taiwan University, Taiwan 2015 – 2017

- Relevant Courses: Cryptography, Cryptanalysis, Information theory, Digital signal processing, Machine learning.

B.Sc. in Electrical Engineering (Minor in Economics), National Taiwan University, Taiwan 2011 – 2015

- Relevant Courses: Computer programming (C++), Electronics, Electromagnetics, Switching circuit and logic design, Time-frequency analysis and wavelet transform, Numerical method, Algorithms, Game theory and information.

TEACHING, TUTORING, AND SUPERVISIONS

MPhil. Co-supervisor in Department of Computer Science and Technology (Dept. CST), Cambridge 2023 – 2024

- Co-supervised an MPhil. student project **Side-channel analysis on ChaCha implementations**.

Undergraduate Supervisor of two courses in Dept. CST, Cambridge 2019 – 2024

- **Digital Signal Processing:** teaching basic concepts including Fourier transform, window functions, etc.
- **Cryptography:** teaching concepts including chosen-plaintext and chosen-ciphertext attacks, block ciphers, hash functions, MAC, asymmetric cryptography, key-exchange protocols, digital signature, etc.
- Supervised or tutored **over 50 students** in small groups.

Affiliated Lecturer of Hardware Security Practicals in Dept. CST, Cambridge 2020 – 2021

PROJECTS AND RESEARCH EXPERIENCES

Security analysis of permutation-based cryptography implemented on 32-bit device 2020 – 2023

- Focused on **Template Attack** to extract **information more than Hamming weights** of intermediate values (in 32-bit registers), and then reconstructed the secrets with my **Python** implementation.
- The target implementations mainly ran on STM32F303RCT7, with one **ARM Cortex-M4** core.
- Used a National Instruments (NI) platform, including an **oscilloscope**, a wave generator, a power supply, to record power traces.
- Read the **C source code and assembly** to help locate the clock cycles where secret information leaks.
- Analyzed the effects on my attrack with different compiler optimization options (`-Os` and `-O3`).
- Applied **belief propagation** and **key enumeration** to higher the success rate of secret reconstruction.
- Achieved success rate over 95% to recover the key in **ASCON AEAD** and the inputs of **SHA-3**, which are both NIST's standardized algorithms.

Security analysis of permutation-based cryptography implemented on 8-bit device 2018 – 2020

- The target **C implementation** mainly ran on ATxmega256A3U.
- Achieved success rate over 99% to recover the secret inputs of SHA3-512

Reverse engineering project of Elliptic Curve Cryptography (ECC) 2018 – 2020

- Used **Ghidra** decompiler and read the decompiled C code to understand the protocol between a secure device (Infineon Optiga Trust B) and a host device with no knowledge of critical parameters.
- built the **Python** equivalent implementation, including the **ECDSA** to verify the signature of the public key and ID in the secure device, and the **key exchange protocol** between the two devices.
- Verified the secret key in the secure device reconstructed from side-channel information by my colleague.

Archery learning system 2014 – 2015

- Helped beginners learn archery by monitoring their electromyographic (EMG) signals.
- Used **C++** on **Arduino** platform for sensor control and **MATLAB** for digital signal processing.

SKILLS

Python, Julia, and MATLAB

- Performed side-channel attacks and implemented related algorithms including template attack (TA), correlation power analysis (CPA), mutual information analysis (MIA), linear discriminant analysis (LDA), belief propagation, efficient key enumeration, and key rank estimation.
- Experiences in implementations of cryptographic algorithms such as AES, SHA-3, ASCON, ECC and ECDSA (on both prime-number field and Galois field).
- Scripts to control power trace recording platforms and target boards such as ChipWhisperer.

C and C++

- Modified official or third-party implementations of cryptographic algorithms on side-channel attack platforms.
- Experiences on microcontrollers and embedded systems such as Arduino and Infneon XMC4500 Relax Lite Kit (ARM Cortex-M4 based).

Others

- Verilog: experiences in undergraduate course "Switching circuit and logic design".
- Circuit design related skills: circuit simulation (Qucs), PCB design (EAGLE), soldering on PCB.
- Mandarin native speaker and proficient in English.
- Familiar with LaTeX paper writing.

PUBLICATIONS

- **Single-trace template attacks on permutation-based cryptography**, PhD thesis, 2022, Apollo - University of Cambridge Repository
- **Low trace-count template attack on 32-bit implementations of Ascon AEAD**, CHES 2023, Co-authors: Markus G. Kuhn, Sumanta Sarker, and Feng Hao.
- **Single-trace fragment template attack on a 32-bit implementation of Keccak**, CARDIS 2021, Co-author: Markus G. Kuhn.
- **A template attack to reconstruct the input of SHA-3 on an 8-bit device**, COSADE 2020, Co-author: Markus G. Kuhn.

LEADERSHIP

Treasurer of Cambridge Taiwanese Society (over 30 members) 2019 – 2020

Treasurer of Chien Kuo Senior High School Alumni Wind Ensemble (over 30 members) 2012 – 2015

President, Activity Officer of National Taiwan University Wind Band (over 70 members) 2012 – 2013

SERVICE

Substitute Military Service in New Taipei City Veteran Service Center 2017 – 2018

- Made short videos about the stories of Taiwanese veterans.