

'JARRON' JIE-REN SHIH

JARRONSHIH@GMAIL.COM
(+886) 953-959-662

3F., No. 7, Aly. 4, Ln. 345,
Sec. 4, Ren-ai Rd., Da-an Dist.,
Taipei City 106, Taiwan

Education

National Taiwan University

Master of Science, Electrical Engineering

Taipei, Taiwan, Sep. 2010 - Jun. 2012

- G.P.A.: **4.00/4.00**.
- Join Fast Crypto Lab hosted by Prof. Chen-Mou Cheng.
- Thesis: An efficient ASIC implementation of Lattice-based and Multivariate Post-Quantum Cryptography

National Taiwan University

Bachelor of Science, Electrical Engineering

Taipei, Taiwan, Sep. 2006 - Jun. 2010

- Major G.P.A.: **3.86/4.00**, Cumulative G.P.A.: 3.73/4.00.
- Earn **First Prize** in 2010 NTUEE Undergraduate Outstanding Project, "Practical Attack on MIFARE Classic".

Experience

Trend Micro

Senior Software Engineer

Taipei, Taiwan, Jan. 2015 - Present

In **Cloud and Data Center Security** Product team (Deep Security), responsible for SAP virus scan on Windows platform, including Anti-Malware, Javascript active script scan and Mail scan.

- Integrate Anti-Malware solution and active script scan solution to prevent Cross Site Scripting Attack (XSS).
- Develop virus scan interface for SAP on Windows platform to meet the market demand.

Software Engineer

Taipei, Taiwan, Sep. 2012 - Dec. 2014

In **Cloud Storage Encryption** Product Team (SecureCloud), responsible for development boot device encryption feature and Linux software agents on cloud service platform.

- Implement boot disk encryption feature to prevent boot data leakage on Windows and variant Linux distributions, including Ubuntu, CentOS, RHEL, AmazonLinux and SUSE.
- Implement software agent on major cloud service providers including Amazon EC2, Microsoft Azure and HP-Cloud
- 2013 Q2 Trend Engineer of Quarter

Intel

Research Assistant, part time

Taipei, Taiwan, Jan. 2011 - Jun. 2012

Intel-NTU Connected Context Computing Center, M2M crypto processor Project

An energy-efficient programmable cryptographic coprocessor based on elliptic-curve and post-quantum cryptography.

As chief designer of hybrid model, build up high level hardware simulation and scalable ASIC analysis.

- Implement scalable ASIC with NTRU and TTS cryptography with 25% area reduction.
- Determine the optimal degree of parallelism from software simulation

Certifications

Certified ScrumMaster

Scrum Alliance, 000425860

Jun. 2015 - Jun. 2017

Patents

Root Volume Encryption in Para-virtualized Virtual Machine

patent pending, United States, 14/325221

Author: Po-Hsun Yen, Chuan-Hung Lin, **Jie-Ren Shih**.

Publications

Securing M2M with Post-quantum Public-key Cryptography

Emerging and Selected Topics in Circuits and Systems, IEEE Journal

Mar. 7, 2013

Author: **Jie-Ren Shih**, Yongbo Hu, etc.

MIFARE Classic: Practical Attacks and Defenses

Chinese Cryptology and Information Security Association

May 27, 2010

Author: Ming-Yang Chih, **Jie-Ren Shih**, etc.

Skills

Programming: Python (mostly used), C, C++, JavaScript, HTML, CSS, shell script.

Linux System: Software Development, Boot Process Programming, Encryption Driver.

Cloud Platform: AWS (Xen), Microsoft Azure (HyperV), HP-Cloud (KVM).

Language: Chinese (native), English (fluent).