



JUNG-WOO CHANG

Fourth-year Ph.D. Candidate, Department of Electrical and Computer Engineering, UC San Diego, CA, 92093
✉ juc023@ucsd.edu  [linkedin.com/in/jung-woo-chang](https://www.linkedin.com/in/jung-woo-chang)  github.com/juc023  sites.google.com/ethanjungwoochang

RESEARCH INTEREST

- (i) **Wireless and Network Security**
- (ii) **ML and Computer Security**
- (iii) **Mobile Privacy and Side-Channel Attacks**
- (iv) **Cyber-Physical System Security**
- (v) **Privacy-Preserving Computation**
- (vi) **Multimedia System Design**

EDUCATION

UC San Diego **Sep. 2021 – Summer 2025**
Ph.D. Candidate in Computer Engineering *La Jolla, CA*

Advisor: Prof. Farinaz Koushanfar

Sogang University **Feb. 2019**
M.S. in Electronic Engineering *Seoul, South Korea*

Advisor: Prof. Suk-Ju Kang

Sogang University **Feb. 2016**
B.S. in Electronic Engineering *Seoul, South Korea*

INDUSTRIAL PROFESSIONAL EXPERIENCE

NXP Semiconductors **June 2024 – Sep. 2024**
Wireless Research Intern *San Jose, CA*

Chainlink Labs **June 2022 – Sep. 2022**
Cryptography Research Intern *Remote*

LG Uplus **Jan. 2019 – July. 2022**
AI Research Engineer *Seoul, South Korea*

PUBLICATION

- [P12] **Nocturne: Disrupting Neural Codec-Based Video Streaming and Analytics with Hardware Fault Injection**
Jung-Woo Chang, Ke Sun, Xinyu Zhang, Farinaz Koushanfar
Under Review from top-tier security conference
- [P11] **EveGuard: Defeating Vibration-based Side-Channel Eavesdropping with Audio Adversarial Perturbations**
Jung-Woo Chang, Ke Sun, David Xia, Xinyu Zhang, Farinaz Koushanfar
arXiv preprint arXiv:2411.10034 (Under Review from top-tier security conference)
- [P10] **Magmaw: Modality-Agnostic Adversarial Attacks on Machine Learning-Based Wireless Communication Systems**
Jung-Woo Chang, Ke Sun, Nasimeh Heydaribeni, Seira Hidano, Xinyu Zhang, Farinaz Koushanfar
Network and Distributed System Security (NDSS) Symposium, 2025
- [P9] **RoVISQ: Reduction of Video Service Quality via Adversarial Attacks on Deep Learning-based Video Compression**
Jung-Woo Chang, Mojan Javaheripi, Seira Hidano, Farinaz Koushanfar
Network and Distributed System Security (NDSS) Symposium, 2023
- [P8] **VideoFlip: Adversarial Bit-Flips for Reducing Video Service Quality**
Jung-Woo Chang, Mojan Javaheripi, Farinaz Koushanfar
ACM/IEEE Design Automation Conference (DAC), 2023
- [P7] **NetFlick: Adversarial Flickering Attacks on Deep Learning Based Video Compression**
Jung-Woo Chang, Nojan Sheybani, Shehzeen Hussain, Mojan Javaheripi, Seira Hidano, Farinaz Koushanfar
ICLR 2023 Workshop on Machine Learning for Internet of Things(IoT): Datasets, Perception, and Understanding, 2023

- [P6] **AccHASHTAG: Accelerated Hashing for Detecting Fault-Injection Attacks on Embedded Neural Networks**
Mojan Javaheripi, **Jung-Woo Chang**, Farinaz Koushanfar
ACM Journal on Emerging Technologies in Computing Systems (JETC), 2022
- [P5] **TouchNAS: Efficient Touch Detection Model Design Methodology for Resource-Constrained Devices**
Saehyun Ahn*, **Jung-Woo Chang***, Hyeon-Seok Yoon, Suk-Ju Kang
IEEE Sensors Journal, 2022
- [P4] **An Energy-Efficient FPGA-based Deconvolutional Neural Networks Architecture for Single Image Super-Resolution**
Jung-Woo Chang, Keon-Woo Kang, Suk-Ju Kang
IEEE Transactions on Circuits and Systems for Video Technology (TCSVT), 2020
- [P3] **Towards Design Methodology of Efficient Fast Algorithms for Accelerating Generative Adversarial Networks on FPGAs**
Jung-Woo Chang, Saehyun Ahn, Keon-Woo Kang, Suk-Ju Kang
IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC), 2020
- [P2] **SDCNN: An efficient sparse deconvolutional neural network accelerator on FPGA**
Jung-Woo Chang, Keon-Woo Kang, Suk-Ju Kang
IEEE/ACM Design Automation and Test in Europe Conference (DATE), 2019
- [P1] **Optimizing FPGA-based convolutional neural networks accelerator for image super-resolution**
Jung-Woo Chang, Suk-Ju Kang
IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC), 2018

POSTERS, DEMO, WORKSHOP PAPERS AND TECHNICAL REPORTS

- [D1] **AccHASHTAG: Accelerated Hashing for Detecting Fault-Injection Attacks on Embedded Neural Networks**
Nojan Sheybani, Mojan Javaheripi, **Jung-Woo Chang** and Farinaz Koushanfar
IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2022
- [W2] **On-chip CNN Accelerator for Image Super-Resolution**
Jung-Woo Chang, Suk-Ju Kang
ACM/IEEE Design Automation Conference (DAC), 2018
- [W1] **Real-time temporal quality compensation technique for head mounted displays**
Jung-Woo Chang, Suk-Ju Kang, Min-Woo Seo, Song-Woo Choi, Sang-Lyn Lee, Ho-Chul Lee, Eui-Yeol Oh, Jong-Sang Baek
SIGGRAPH Asia, 2017

SELECTED HONORS AND AWARDS

- 2025 **NDSS Symposium Fellowship @ NDSS**
- 2025 **Travel Grant @ NSF NeTS Early Career Investigator Workshop**
- 2022 **Richard Newton Young Student Fellowship @ IEEE/ACM DAC**
- 2021 **ECE Department Fellowship @ UCSD**
- 2021 **Industry-Academic Cooperation Paper Award @ Samsung Electronics Semiconductor**
- 2018 **Industry-Academia Scholarship Recipient @ LG**
- 2016 **Design Project Paper Award @ Qualcomm Korea**

TEACHING EXPERIENCE

- 2023 **UCSD ECE 226 Optimization and Acceleration of DL on Various Hardware Platforms**
- 2017 **SGU EE Automatic Control Systems**
- 2017 **SGU EE Microprocessor-Based System Design**

TECHNICAL SKILLS

Languages: Python, Matlab, Verilog, VHDL, C

Developer Tools: Pytorch, Tensorflow, Xilinx Vivado HDL, GNURadio, mmWave Studio, Android Studio

PROFESSIONAL SERVICES

Program Committee

2025 **USENIX Security, Artifact Evaluation Committee**

Reviewer

2025 **Proceedings of the IEEE**

2024 **ACM Mobicom, ACM WiSec, IEEE MILCOM, ACM TOMM**

2022 **IEEE TCAS-I**

2021 **IEEE TCAS-I, IEEE TCSVT**

2020 **IEEE TCAS-I, IEEE TCSVT**

2019 **IEEE/ACM DAC**

OTHERS

2014 **Aircraft Weapon Maintenance Mechanic @ Republic of Korea Air Force**

REFERENCE

- **Dr. Farinaz Koushanfar (Doctoral advisor)**
Siavouche Nemat-Nasser Endowed Chair Professor and Henry Booker Faculty Scholar
Department of Electrical and Computer Engineering
University of California, San Diego
✉ farinaz@ucsd.edu
- **Dr. Xinyu Zhang**
Professor
Department of Electrical and Computer Engineering
University of California, San Diego
✉ xyzhang@ucsd.edu
- **Dr. Tara Javidi**
Jerzy (George) Lewak Chair and Professor
Department of Electrical and Computer Engineering
University of California, San Diego
✉ tjavidi@ucsd.edu
- **Dr. Ke Sun**
Assistant Professor
Department of Computer Science and Engineering
University of Michigan, Ann Arbor
✉ kesuniot@umich.edu