

QIAN WANG

OFFICE: Intel Jones Farm Campus, 2111 NE 25th AVE, Hillsboro, OR

EMAIL: wangqian2010bupt@gmail.com

EDUCATION

University of Maryland, College Park

Ph.D. in Electrical Engineering

Dissertation: "Hardware Assisted Solutions for Automobile Security"

August 2014 - August 2019

Advisor: Prof. Gang Qu

Tsinghua University

M.S. in Electrical Engineering

Thesis: "Fault Sensitivity Analysis and Countermeasures against Fault Attacks of Block Cipher"

September 2011 - July 2014

Advisor: Prof. Liji Wu

Beijing University of Post and Telecommunications

B.S. in Electrical Engineering

September 2007 - July 2011

INDUSTRIAL EXPERIENCES

Intel Corp

2019-present

Research Scientist at Intel Security & Privacy Lab

- Conduct research projects on Post quantum crypto (PQC). Analysis of performance or resource requirements for PQC candidates; Investigate the PQC impacts on existing applications and protocols (e.g., changes needed to accommodate for specific network applications); Study Substantial improvements for the implementation of algorithms and conduct a security analysis of properties of finalists.
- Lead project on security analysis of automotive Radar for autonomous driving applications; Conduct threat analysis on automotive Radars by identifying attacks and vulnerabilities; Conduct research on machine learning/deep learning-based mitigation targeted for automotive Radar.
- Develop machine/deep learning operations on vehicular data for detecting/preventing/recovering from intrusions in in-vehicle and vehicular networks.
- Contribute to platform integration of sensing and actuation function for autonomous driving tests. Work on prototyping test-beds, such as FPGAs, ECUs, Raspberry Pi, etc.

Robert Bosch LLC

2016.5-2016.8

Security Research Intern

- Develop & implement key exchange protocol on Controller Area Network (CAN) bus system for in-vehicle communications. of vehicle.

HONORS AND AWARDS

Best Paper Award of AsianHOST

2018

Summer Research Fellowship of University of Maryland, College Park

2015

Chenming (Calvin) Hu Scholarship of Tsinghua University

2014

Excellent Undergraduate Thesis Award of Beijing University of Posts and Telecommunications

2011

Outstanding Student Scholarship (Silver) of Beijing University of Posts and Telecommunications

2009,2010

ACADEMIC ACTIVITIES AND SERVICES

- **Technical Program Committee Member:** RSDA'20, SOCC'20, SOCC'21, ITC-Asia'21
- **Reviewer for the following journals:** Computers and Electrical Engineering, IEEE Wireless Communications Magazine-WCM, IEEE Transactions on Emerging Topics in Computing (TETC), Information Sciences, ACM Transactions on Embedded Computing Systems (TECS), IEEE Transactions on Circuits and Systems II (TCAS-II), IEEE Transactions on Vehicular Technology (TVT), IEEE Access, Vehicular Communications, Journal of Information Security and Applications (JISA), Integration, the VLSI Journal.

- **Reviewer for conferences:** ISCAS'20, ISTC'18, RSDA '20, SOCC'20, SWPC'20, DTTC'21, SOCC'21, DTTC'22.
- **Funding reviewer:** Resilient & Intelligent NextG Systems (RINGS) (NSF21-581).
- **Academic Projects mentor:**
 1. Mentoring two Full Stack Security projects in Resilient & Intelligent NextG Systems (RINGS) [program link](#) (collaborates with PIs from MIT, Brown University and Florida Atlantic university)
 2. Mentoring Intel funded Post-Quantum Cryptography projects in the Intel Crypto Frontiers Research Center [program link](#) (collaborates with faculties and researchers from KU Leuven, University of Maryland, University of Michigan, etc)

PUBLICATIONS

PATENTS

22. "Occupancy grid map computation, v2x complementary sensing, and coordination of cooperative perception data transmission in wireless networks", US Patent App. 17/483,528, 2022
21. "Leader Bootstrapping and Recovery of Time in Time Sensitive Networks", US Patent App. 17/706,939, 2022
20. "Inference models for intrusion detection systems in time sensitive networks", US Patent App. 17/706,955, 2022
19. "Re-Training Intrusion Detection Fingerprints in the Presence of an Attacker", US Patent App. 17/484,689, 2022
18. "Glitch Attack Mitigation for In-Vehicle Networks", US Patent App. 17/484,627, 2022
17. "Attacker localization based on tracking anomaly propagation in time-sensitive networking", US Patent App. 17/484,197, 2022
16. "Signal-to-Noise Ratio Range Consistency Check for Radar Ghost Target Detection", , US Patent App. 17/357,892 2021
15. "Context-based response to attacks against autonomous systems", US Patent App. 17/357,885, 2021
14. "Post-gateway bus-off attack mitigation", US Patent App. 17/356,033, 2021
13. "Range Doppler Consistency Check for Radar Ghost Target Detection", US Patent App. 17/357,291, 2021
12. "Controlled Message Error for Message and Electronic Control Unit Mapping", US Patent App. 17/214,444, 2021
11. "Malicious request detection in automated resource dispatch", US Patent App. 17/133,076, 2021
10. "Agile Reconfigurable Approach for Real-Time Replacement of On-Chip Safety-Critical Modules", US Patent App. 17/031,140, 2021
9. "Speculative and Accelerated Classification based on Incomplete Feature Sets", US Patent App. 17/025,797, 2021
8. "Machine learning voltage fingerprinting for ground truth and controlled message error for message and ecu mapping", US Patent App. 17/024,232, 2021
7. "One-Point Relative Voltage Fingerprinting", US Patent App. 16/994,147, 2020
6. "Continuous Integrity Monitoring for Autonomous Transportation Services", US Patent App. 16/994,089, 2020
5. "Lightweight electronic control unit fingerprinting", US Patent App. 16/994,219, 2020
4. "Method to mitigate timing based attacks on key agreement schemes over controller area network", US Patent 10,805,339, 2020
3. "Methods and arrangements for multi-layer in-vehicle network intrusion detection and characterization", US Patent App. 16/727,565, 2020
2. "Method to mitigate transients based attacks on key agreement schemes over controller area network", US Patent 10,554,241, 2020
1. "Method to Mitigate Voltage Based Attacks on Key Agreement over Controller Area Network (CAN)", US Patent App. 15/915,933, 2018

JOURNAL

25. [TVLSI'19] Zhaojun Lu, Qian Wang, Gang Qu, Haichun Zhang, Zhenlin Liu. "A Blockchain-based Privacy-preserving Authentication Scheme for VANETs." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(12), 2792-2801, 2019.
24. [TDSC'18] Qian Wang, Gang Qu. "A Silicon PUF Based Entropy Pump." *IEEE Transactions on Dependable and Secure Computing*, 16(3), 402-414, 2018.
23. [IEEE Access'18] Zhaojun Lu, Wenchao Liu, Qian Wang, Gang Qu, Zhenlin Liu. "A Privacy-Preserving Trust Model Based on Blockchain for VANETs." *IEEE Access* 6, 45655-45664, 2018.
22. [SCI'18] An Wang, Yu Zhang, Weina Tian, Qian Wang, Guoshuang Zhang, Liehuang Zhu . "Right or Wrong Collision Rate Analysis without Profiling: Full-Automatic Collision Fault Attack." *Science China Information Sciences* 61 (3), 032101, 2018.
21. [Computer'17] Mingze Gao, Qian Wang, Md Tanvir Arafin, Yongqiang Lyu, Gang Qu . "Approximate Computing for Low Power and Security in the Internet of Things." *Computer*, 27-34, 2017.
20. [TMCS'17] Qian Wang, An Wang, Gang Qu, Guoshuang Zhang. "New Methods of Template Attack based on Fault Sensitivity Analysis." *IEEE transactions on multi-scale computing systems*, 3 (2), 113-123, 2017.
19. [Science Advances'17] Qian Wang, An Wang, Gang Qu, Jiliang Zhang. "A New Zero Value Attack Combined Fault Sensitivity Analysis on Masked AES." *Science Advances*, 3(7), e1700518(2017), 2017.

CONFERENCES

18. [NIST PQC'22] Qian Wang, Thomas Hanson, Santosh Ghosh, Fernando Virdia, Anne Reinders, Manoj R. Sastry. "Optimization for SPHINCS+ using Intel® Secure Hash Algorithm Extensions." *2022 4th Fourth PQC Standardization Conference*, 2022.
17. [ESCAR'21] Vuk Lesi, Marcio Juliato, Shabbir Ahmed, Christopher Gutierrez, Qian Wang, Manoj Sastry. "Intrusion Detection and Localization for Networked Embedded Control Systems." *2021 9th Embedded Security in Cars(escar) USA*, 2021.
16. [ASP-DAC'20] Qian Wang*, Pengfei Qiu*, Dongxing Wang, Yongqiang Lyu, Zhaojun Lu, Gang Qu . "Mitigating Adversarial Attacks for Deep Neural Networks by Input Deformation and Augmentation." *2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC)*, 157-162., 2020. *These authors contributed equally.
15. [ISQED'20] Qian Wang, Omid Aramoon, Pengfei Qiu, Gang Qu . "Efficient Transfer Learning on Modeling Physical Unclonable Functions." *2020 21st International Symposium on Quality Electronic Design (ISQED)*, 2020.
14. [ITSC'19] Zhaojun Lu, Qian Wang, Xi Chen, Gang Qu, Zhenlin Liu. "Leap: A Lightweight Encryption and Authentication Protocol for In-Vehicle Communications." *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*, 1158-1164, 2019.
13. [ISVLSI'19] Mingze Gao, Qian Wang, Gang Qu . "Energy and Error Reduction using Variable Bit-width Optimization on Dynamic Fixed Point Format." *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 152-157, 2019.
12. [ISQED'19] Qian Wang, Mingze Gao, Gang Qu . "PUF-PassSE: A PUF based Password Strength Enhancer for IoT Applications." *20th International Symposium on Quality Electronic Design (ISQED)*, 198-203, 2019.
11. [AsianHOST'18] Qian Wang, Yiming Qian, Zhaojun Lu, Yasser Shoukry, Gang Qu . "A Delay based Plug-in-Monitor for Intrusion Detection in Controller Area Network." *2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 86-91, 2018.
10. [AsianHOST'18] Shalabh Jain, Qian Wang, Md Tanvir Arafin, Jorge Guajardo . "Probing Attacks on Physical Layer Key Agreement for Automotive Controller Area Networks." *2018 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 86-91, 2018.
9. [DSP'18] Qian Wang, Zhaojun Lu, Mingze Gao, Gang Qu . "Edge Computing based GPS Spoofing Detection Methods." *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*, 1-5 , 2018.
8. [SOCC'18] Qian Wang, Zhaojun Lu, Gang Qu . "An Entropy Analysis based Intrusion Detection System for Controller Area Network in Vehicles." *2018 31st IEEE International System-on-Chip Conference (SOCC)*, 90-95,

2 , 2018.

7. [TrustCom'18] Zhaojun Lu, Qian Wang, Gang Qu, Zhenlin Liu . “Bars: A Blockchain-based Anonymous Reputation System for Trust Management in VANETs.” *2018 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*,98-103, 2018.
6. [GLSVLSI'18] Qian Wang, Mingze Gao, Gang Qu, Gang Qu . “A Machine Learning Attack Resistant Dual-mode PUF.” *Proceedings of the 2018 on Great Lakes Symposium on VLSI*, 177-182, 2018.
5. [WOCC'17] Qian Wang, Timothy Dunlap, Youngho Cho, Gang Qu . “DoS Attacks and Countermeasures on Network Devices.” *Nanoscale 2017 26th Wireless and Optical Communication Conference (WOCC)*, 1-6, 9, 12288-12294(2017), 2017.
4. [ASP-DAC'17] Mingze Gao, Qian Wang, Akshaya S Kankanhalli Nagendra, Gang Qu. “Template attack on masking AES based on fault sensitivity analysis.” *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, 390-395, 2017.
3. [HOST'15] Qian Wang, An Wang, Liji Wu, Gang Qu, Guoshuang Zhang. “Template attack on masking AES based on fault sensitivity analysis.” *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 96-99, 2015.
2. [CIS'13] Qian Wang, Liji Wu, Xiangmin Zhang, Xiangyu Li, Jun Guo. “Efficient Countermeasures against Fault Attacks for 3DES Crypto Engine in Bank IC Card.” *2013 Ninth International Conference on Computational Intelligence and Security*, 729-733, 2013.

BOOK CHAPTER

1. Zhaojun Lu, Qian Wang, Gang Qu, Zhenlin Liu. “Security of in-vehicle controller area network: a review and future directions.” *Frontiers in Hardware Security and Trust: Theory, design and practice*, Institution of Engineering and Technology. 2020

PRESENTATIONS

1. Oral presentation: “Efficient Transfer Learning on Modeling Physical Unclonable Functions.”, *ISQED*, Santa Clara, California, USA, March 2020.
2. Oral presentation: “Energy and Error Reduction using Variable Bit-width Optimization on Dynamic Fixed Point Format.”, *ISVLSI*, Miami, Florida, USA, July 2019 .
3. Poster presentation: “Intellectual Property Protection for Generative Neural Network.”, *3st WISE Workshop [Co-located with HOST 2019]*, Arlington, Virginia, USA, May 2019.
4. Oral presentation: “PUF-PassSE: A PUF based Password Strength Enhancer for IoT Applications.”, *ISQED*, Santa Clara, California, USA, March 2019.
5. Oral presentation: “Edge Computing based GPS Spoofing Detection Methods.”, *DSP 2018*, Shanghai, China, November 2018.
6. Oral presentation: “An Entropy Analysis Based Intrusion Detection System for Controller Area Network in Vehicles.”, *SOCC 2018*, Arlington, Virginia, USA, September 2018.
7. Poster presentation: “An Entropy Analysis based Intrusion Detection System for Controller Area Network in Vehicles.”, *DAC 2018*, San Francisco, California, USA, June 2018.
8. Poster presentation: “An Entropy Analysis based Intrusion Detection System for Controller Area Network in Vehicles.”, *2nd WISE Workshop [Co-located with HOST 2018]*, Washington DC, USA, May 2018.
9. Hardware Demo: “Configurable Ring Oscillator PUF as an Entropy Pump.”, *HOST 2016*, McLean, Virginia, USA, May 2016.
10. Poster presentation: “Template attack on masking AES based on fault sensitivity analysis.”, *HOST 2015*], McLean, Virginia, USA, May 2015.

TEACHING EXPERIENCE

- **Teaching Assistant at UMD:** ENEE 222 (Elements of Discrete Signal Analysis), ENEE 245 (Digital Circuits & Systems Lab) , ENEE 459E/CMSC 498R (Introduction to Cryptography), ENEE 446 (Digital Computer Design)

- Held office hours, designed homework and exam questions, graded homework, exam questions and computer assignments
- Held lab sessions, design routines for digital circuit lab and mentor students to conduct lab procedure.
- **Guest lecturer at UMD:** for ENEE140 Introduction to Programming Concepts for Engineers
 - Gave lectures for two sections (50+ students), held office hours.