Chenglu Jin **Updated: Friday 15th December, 2017**

CONTACT INFORMATION
ITE Building 423, 371 Fairfield Way,
Storrs, CT 06269
Email: chenglu.jin@uconn.edu
LinkedIn: www.linkedin.com/in/chenglujin

EDUCATION

University of Connecticut, Storrs, CT

Ph.D., Computer Engineering, GPA: 4.08/4.0 *Expected:* May 2018

- Advisor: Marten van Dijk, Ph.D

New York University, New York, NY

M.S., Computer Engineering, GPA: 3.91/4.0 May 2014

- Thesis Topic: *NREPO: Normal Basis Recomputing with Permuted Operands*
- Advisor: Ramesh Karri, Ph.D

Xidian University, Xi'an, China

B.S., Electronic Information Science and Technology, GPA: 85/100 Jun 2012

RESEARCH INTERESTS

Hardware Security and Embedded System Security

- Physical Unclonable Function (Interface) Design, Attack and Application
- Supply Chain Security
- Hardware Trojan Design and Detection
- Fault Attack and Concurrent Error Detection
- Side Channel Analysis and Countermeasures

WORK EXPERIENCE

University of Connecticut, Storrs, CT Jul 2014 to present
Research Assistant at Secure Computation Lab

- **Physical Unclonable Functions:**
  - Implemented a logically erasable PUF interface and proposed backward secure key management scheme.
  - Developed and Implemented an adaptively chosen challenge attack on XOR Arbiter PUFs.
  - Implemented an LPN-based PUF on ZedBoard by a software hardware codesign approach. (Open Source: github.com/scluconn/LPN-based_PUF)
  - Proposed a silicon time lock puzzle scheme by binding the puzzle solving time to the delay of PUF evaluation.
  - Collaborated with device group in the design of reliable and secure PUFs/POKs.
- **Supply Chain Security:**
  - Broke DARPA's SHIELD protocol and proposed secure and efficient initialization and authentication protocols to track and authenticate ICs in an untrusted supply chain.
  - Implemented a NVM-based supply chain management protocol controller.
- **Hardware Trojans:**
  - Presented a rigorous framework for Hardware Trojan design and detection.
  - Investigated the feasibility of hardware Trojan attacks in smart grids.
- **Course Developments:**
  - Codeveloped two graduate level courses at UCONN: *Advanced Microprocessor Application Lab* and *Introduction to Hardware Security*

Open Security Research, Shenzhen, China Jun 2016 to Aug 2016
Summer Intern under the supervision of Dr. Junfeng Fan

- **Threshold Implementation:**
  - Developed threshold implementation of AES.

University of Connecticut, Storrs, CT Spring 2016, Fall 2016
Teaching Assistant for ECE3411 Microprocessor Applications Laboratory

- Developed and graded seven quizzes and programming lab tests, which cover UART, LCD, interrupts, Timers, PWM, ADC and Real-Time Operating System.
- Conducted the AVR microcontroller programming labs sessions.

Open Security Research, Shenzhen, China Jun 2015 to Aug 2015
Summer Intern under the supervision of Dr. Junfeng Fan

- **Fault Injection Simulator:**
  - Developed a ModelSim-based fault injection simulation platform that can inject transient/permanent, stuck-at/bit-flipping faults into a netlist during simulation.
  - Implemented an 8051-based SoC with a hardware AES circuitry, and analyzed the behavior after fault injection using this fault injection simulator platform.
- **Side Channel Analysis:**
  - Evaluated one DES implementation on chip by differential power analysis with Riscure Inspector, and recovered the secret key from power traces successfully.
- **True Random Number Generation:**
  - Evaluated two true random number generators under AIS20/AIS31 framework.

New York University, New York, NY Sep 2013 to May 2014
Research Assistant at Information System and Internet Security Lab

- **Fault Attack and Countermeasures:**
  - Proposed, implemented and evaluated a bit-level error detection mechanism (NREPO) for AES with low area overhead.
  - Proposed two metrics: fault entropy and fault differential entropy, to evaluate different concurrent error detection schemes (CEDs) of AES.
  - Designed a generic CED for stream ciphers (Grain, Achterbahn and Trivium) based on algorithm diversity.
- **Power Side Channel Analysis:**
  - Implemented Correlation Power Analysis and Template Attack on hardware implementation of AES with its side channel protected versions: Masking and MDPL.
  - Investigated the circuit aging effect on the side channel resistance of countermeasures.

Skills

Programming Languages
- Verilog, VHDL
- Python, C/C++, MATLAB, tcl, FORTRAN

Digital Design
- Mentor Graphics ModelSim
- Cadence RTL Compiler, Cadence SoC Encounter, Cadence Virtuoso
- Synopsys Design Compiler, Synopsys NanoSim, Synopsys TetraMax
- Xilinx ISE, Vivado, Xilinx SDK, Xilinx ChipScope Pro

Side Channel Analysis Tools
- Riscure Inspector, Riscure Power Tracer

Embedded System Design
- Atmel Studio, Arduino, Keil, Raspberry Pi

Publications

1. van Dijk, M., **Jin, C.**, Maleki, H., Nguyen, P. H., and Rahaeimehr, R. (2018, February), "Weak-Unforgeable Tags for Secure Supply Chain Management." In *2018 International Conference on Financial Cryptography and Data Security (FC).*

2. **Jin, C.**, Herder, C., Ren, L., Nguyen, P. H., Fuller, B., Devadas, S., and van Dijk, M. (2017). "FPGA Implementation of a Cryptographically-Secure PUF based on Learning Parity with Noise." In *Cryptography.*

3. Yan, W., **Jin, C.**, Tehranipoor, F., and Chandy, J. (2017, September), "Phase calibrated ring oscillator PUF design and implementation on FPGAs". In *2017 International Conference on Field-Programmable Logic and Applications (FPL).*

4. Haider, S. K., **Jin, C.**, and van Dijk, M. (2017, August). "Advancing the State-of-the-Art in Hardware Trojans Design" (Invited). In *2017 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS).*

5. Maleki, H., Rahaeimehr, R., **Jin, C.**, and van Dijk, M. (2017, May). "New Clone-Detection Approach for RFID-Based Supply Chains". In *2017 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST).*

6. **Jin, C.**, Ren, L., Liu, X., Zhang, P., and van Dijk, M. (2017, April). "Mitigating Synchronized Hardware Trojan Attacks in Smart Grids". In *2017 Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG).*

7. **Jin, C.**, and van Dijk, M. (2017). "Secure and Efficient Initialization and Authentication Protocols for SHIELD". In *IEEE Transactions on Dependable and Secure Computing (TDSC).*

8. Haider, S. K., **Jin, C.**, Ahmad, M., Shila, D. M., Khan, O., and van Dijk, M (2017). "Advancing the State-of-the-Art in Hardware Trojans Detection". In *IEEE Transactions on Dependable and Secure Computing (TDSC).*

9. Guo, X., **Jin, C.**, Zhang, C., Papadimitriou, A., Hély, D., and Karri, R. (2016). "Can Algorithm Diversity in Stream Cipher Implementation Thwart (Natural and) Malicious Faults?". In *IEEE Transactions on Emerging Topics in Computing (TETC).*

10. Guo, X., Karimi, N., Regazzoni, F., **Jin, C.**, and Karri, R. (2015, May). "Simulation and Analysis of Negative-Bias Temperature Instability Aging on Power Analysis Attacks". In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST).*

11. Guo, X., Mukhopadhyay, D., **Jin, C.**, and Karri, R. (2015). "Security Analysis of Concurrent Error Detection against Differential Fault Analysis". In *Journal of Cryptographic Engineering (JCEN).*

12. Guo, X., Mukhopadhyay, D., **Jin, C.**, and Karri, R. (2014, May). "NREPO: Normal Basis Recomputing with Permuted Operands". In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST).*

Informal Publications

13. Nguyen, P. H., Sahoo, D. P., **Jin, C.**, Mahmood, K., and van Dijk, M. (2017). "MXPUF: Secure PUF Design against State-of-the-art Modeling Attacks". *Cryptography ePrint Archive.*

14. Khan, R. S., Kanan, N., **Jin, C.**, Scoggin, J., Noor, N., Muneer, S., Dirisaglik, F., Nguyen, P. H., Silva, H., van Dijk, M., and Gokirmak, A. (2017). Intrinsically Reliable and Lightweight Physical Obfuscated Keys, *arXiv.*

15. **Jin, C.**, Xu, X., Burleson, W., Rührmair, U., and van Dijk, M. (2015). "PLayPUF: Programmable Logically Erasable PUFs for Forward and Backward Secure Key Management". *Cryptography ePrint Archive*.

Competition Experiences

MITRE Embedded System CTF 2017 (**First Place Overall**, **Iron Flag Award**)
The goal of this competition is to build a secure bootloader for a microcontroller. Each team requires to design their own secure bootloader and attack the bootloaders designed by the other teams. Competitors are CMU, NEU, RPI, WPI, UMass, etc.

- Designed encryption and integrity checking scheme of our own secure bootloader with side channel resistance.
- Found flaws in the encryption and integrity checking scheme of other teams' bootloaders.
- Won **First Place Overall** counting all the points gained by attacks and defenses.
- Won **Iron Flag Award** for successfully designing a secure system that defended every flag from its attackers in the competition.

CSAW Embedded Security Challenge 2017 (**Finalist**)
The theme of this competition is cyberattack detection, isolation, and mitigation for Programmable Logic Controllers (PLCs). PLCs are embedded systems deployed in cyber-physical environments, controlling critical infrastructure.

- Implemented a lightweight intrusion detection system called *Snatshotter* on OpenPLC framework.
- *Snapshotter* can report all the events on the PLCs to the server in a secure and stealthy way, such that even if the adversaries have compromised the encryption key for encrypting the logs, they are still not able to infer whether this intrusion gets caught or not.

Professional Service

Student Program Committee

- IEEE Symposium on Security and Privacy (SP'16)

Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC)
- ACM/EDAC/IEEE Design Automation Conference (DAC'18)
- Cryptographers Track at the RSA Conference (CT-RSA'17)
- Journal of Hardware and Systems Security (HASS)
- Journal of Internet Technology (JIT)

Sub-reviewer

- IEEE Int. Symp. on Hardware-Oriented Security and Trust (HOST'15, 16, 17, 18)
- Journal of Manufacturing Systems (JMS)
- IEEE International Conference on Computer Design (ICCD'16, 17)
- ACM conference on Computer and communications security (CCS'17)
- ACM/EDAC/IEEE Design Automation Conference (DAC'15, 16, 17)
- IEEE Symposium on Security and Privacy (SP'17)
- ACM Great Lakes Symposium on VLSI (GLSVLSI'17)
- Theory of Implementation Security Workshop (TIs'16)
- IEEE Transactions on Computer-Aided Design of Integrated Systems (TCAD)

Coursework

University of Connecticut

- Modern Cryptography (A+)
- Secure Computation and Storage (A+)
- Advanced Computer Architecture (A+)
- Multicore Computing (A)
- Operating Systems (A)
- Natural Computation (A)

- Advanced Storage System (A-)
- Introduction to Martial Arts: Aikido (A)

New York University
- Hardware Security (A)
- Computer Architecture I (A)
- Computer Architecture II (A)
- Introduction to VLSI System Design (A)
- Digital VLSI System Testing (A)
- Modern Microprocessor (A-)
- Advanced Hardware Design (A-)
- Real Time Embedded System Design (A-)