Chenglu Jin **Updated: January, 2026**

Contact Information

Science Park 123, 1098 XG
Amsterdam, the Netherlands

Email: chenglu.jin@cwi.nl
Website: chenglujin.github.io

Current Position

Tenured Researcher at **Centrum Wiskunde & Informatica (CWI Amsterdam)**, the national research institute for mathematics and computer science in the Netherlands

Education

University of Connecticut Storrs, CT, USA

Ph.D., Electrical Engineering, GPA: 4.08/4.0 (A+ scale) Aug'19

- Dissertation: *Cryptographic Solutions for Cyber-Physical System Security*
- Advisor: Prof. Marten van Dijk

New York University Brooklyn, NY, USA

M.S., Computer Engineering, GPA: 3.91/4.0 May'14

- Thesis: *NREPO: Normal Basis Recomputing with Permuted Operands*
- Advisor: Prof. Ramesh Karri

Xidian University Xi'an, China

B.S., Electronic Information Science and Technology, GPA: 85/100 Jun'12

Work and Research Experiences

Centrum Wiskunde & Informatica Amsterdam, the Netherlands
Tenured Researcher in the Computer Security Group Sep'24 to Present

Centrum Wiskunde & Informatica Amsterdam, the Netherlands
Tenure-track Researcher in the Computer Security Group Oct'20 to Sep'24

New York University Brooklyn, NY, USA
Research Assistant Professor at CUSP and CCS Mar'20 to Aug'20

New York University Brooklyn, NY, USA
Smart Cities Postdoctoral Associate at CUSP and CCS Sep'19 to Feb'20
Advisers: Prof. Ramesh Karri and Prof. Daniel Neill

University of Connecticut Storrs, CT, USA
Research Assistant in the ECE Department Aug'14 to Aug'19
Adviser: Prof. Marten van Dijk

Singapore University of Technology and Design Singapore
Intern at iTrust May'18 to Aug'18
Mentor: Prof. Jianying Zhou

Open Security Research Shenzhen, China
Intern Jun'16 to Aug'16
Mentor: Dr. Junfeng Fan

Open Security Research Shenzhen, China
Intern Jun'15 to Aug'15
Mentor: Dr. Junfeng Fan

New York University Brooklyn, NY, USA
Research Assistant Sep'13 to May'14
Adviser: Prof. Ramesh Karri

Publications

* denotes shared first authorship. † denotes alphabetical authorship.

Book Chapters

1. R. S. Khan, N. Noor, **C. Jin**, J. Scoggin, Z. Woods, S. Muneer, A. Ciardullo, P. H. Nguyen, A. Gokirmak, M. van Dijk, and H. Silva. (2017) "Phase Change Memory and its Application in Hardware Security." In *Security Opportunities in Nano Devices and Emerging Technologies.* CRC Press.

Journals

2. X. Cao, Z. Yang, J. Ning, **C. Jin**, Z. Liu, and J. Zhou. (2026) "Proof of Persistent Aliveness." In *IEEE Transactions on Dependable and Secure Computing (TDSC).*

3. N. Sayadi, P. H. Nguyen, M. van Dijk, and **C. Jin**. (2025) "Breaking XOR Arbiter PUFs with Chosen Challenge Attack." In *IEEE Transactions on Information Forensics and Security (TIFS).*

4. D. Gurevin, **C. Jin**, P. H. Nguyen, O. Khan, and M. van Dijk. (2025) "Secure Remote Attestation with Strong Key Insulation Guarantees." In *IEEE Transactions on Computers (TC).*

5. X. Cao*, Z. Yang*, J. Ning, **C. Jin**, R. Lu, Z. Liu, and J. Zhou. (2024) "Dynamic Group Time-based One-time Passwords." In *IEEE Transactions on Information Forensics and Security (TIFS).*

6. Z. Yang*, **C. Jin***, X. Cao, M. van Dijk, and J. Zhou. (2024) "Optimizing Proof of Aliveness in Cyber-Physical Systems." In *IEEE Transactions on Dependable and Secure Computing (TDSC).*

7. Q. Liu, Y. Huang, **C. Jin**, X. Zhou, Y. Mao, C. Catal, and L. Cheng. (2024) "Privacy and Integrity Protection for IoT Multimodal Data using Machine Learning and Blockchain." In *ACM Transactions on Multimedia Computing Communications and Applications (TOMM).*

8. M. van Dijk and **C. Jin**. (2023) "A Theoretical Framework for the Analysis of Physical Unclonable Function Interfaces and its Relation to the Random Oracle Model." In *Journal of Cryptology (JoC).*

9. **C. Jin***, Z. Yang*, T. Xiang, S. Adepu, and J. Zhou. (2023) "HMACCE: Establishing Authenticated and Confidential Channel from Historical Data for Industrial Internet of Things." In *IEEE Transactions on Information Forensics and Security (TIFS).*

10. **C. Jin**, W. Burleson, M. van Dijk, and U. Rührmair. (2022) "Programmable Access-Controlled and Generic Erasable PUF Design and Its Applications." In *Journal of Cryptographic Engineering (JCEN).*

11. Z. Yang, Z. Bao, **C. Jin**, Z. Liu, and J. Zhou. (2021) "PLCrypto: A Symmetric Cryptographic Library for Programmable Logic Controllers." *In IACR Transactions on Symmetric Cryptology (ToSC, formerly known as Fast Software Encryption conference (FSE)).* (Acceptance rate of Issue 3: **7/44 = 15.9%**. Acceptance rate of FSE 2022: **57/242 = 23.6%**.)

12. M. Linares*, N. Aswani*, G. Mac, **C. Jin**, F. Chen, N. Gupta, and R. Karri. (2021) "HACK3D: Crowdsourcing the Assessment of Cybersecurity in Digital Manufacturing." *In IEEE Computer.*

13. P. Mahesh, A. Tiwari, **C. Jin**, P. R. Kumar, A. L. N. Reddy, S. T. S. Bukkapatanam, N. Gupta, and R. Karri. (2021) "A Survey of Cybersecurity of Digital Manufacturing." In *Proceedings of the IEEE (PIEEE).*

14. P. H. Nguyen, D. P. Sahoo, **C. Jin**, K. Mahmood, U. Rührmair, and M. van Dijk. (2019) "The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks." In *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*. (Acceptance rate of Issue 4: **9/66 = 13.6%**. Overall acceptance rate of CHES 2019: **42/214 = 19.7%**)
    - **Shortlisted for Top Picks in Hardware and Embedded Security 2025**

15. **C. Jin** and M. van Dijk. (2019) "Secure and Efficient Initialization and Authentication Protocols for SHIELD." In *IEEE Transactions on Dependable and Secure Computing (TDSC)*.

16. S. K. Haider, **C. Jin**, M. Ahmad, D. M. Shila, O. Khan, and M. van Dijk. (2019) "Advancing the State-of-the-Art in Hardware Trojans Detection." In *IEEE Transactions on Dependable and Secure Computing (TDSC)*.
    - **Featured in the Jan/Feb 2019 Issue of IEEE TDSC**
    - **Featured in "Spotlight on Transactions" in IEEE Computer, June 2019**

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

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

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

Conferences

20. Z. Zhou, Q. Zhu, H. Lan, H. Zhu, W. Yan, **C. Jin**, X. An, and X. Ye. (2025, Oct) "CacheGuardian: A Timing Side-Channel Resilient LLC Design." In *2025 International Conference on Computer-Aided Design (ICCAD)*. (Acceptance rate: **266/1078 = 24.7%**)

21. H. Zhang, S. Shen, X. Hu, and **C. Jin**. (2025, Oct) "Ransomware Negotiation: Dynamics and Privacy-Preserving Mechanism Design." In *2025 Conference on Game Theory and AI for Security (GameSec)*.

22. S. Shen and **C. Jin**. (2024, Dec) "Reading It Like an Open Book: Single-trace Blind Side-channel Attacks on Garbled Circuit Frameworks." In *2024 Annual Computer Security Applications Conference (ACSAC)*. (Acceptance rate: **83/381 = 21.8%**)
    - **Runner-up for the Dutch Cyber Security Best Research Paper (DCSRP) Award, Technical Track 2025**
    - **Artifacts Reviewed**

23. **C. Jin***, C. Yin*, M. van Dijk, S. Duan, F. Massacci, M. K. Reiter, and H. Zhang (2024, Oct) "PG: Byzantine Fault-Tolerant and Privacy-Preserving Sensor Fusion with Guaranteed Output Delivery." In *2024 ACM Conference on Computer and Communications Security (CCS)*. (Acceptance rate: **328/1964 = 16.7%**)
    - **Artifacts Evaluated Functional**

24. Z. DiMeglio, J. Bustami, D. Gurevin, **C. Jin**, M. van Dijk, and O. Khan. (2024, May) "Masked Memory Primitive for Key Insulated Schemes." In *2024 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. (Acceptance rate: **32/139 = 23.0%**)

25. Z. Yang, **C. Jin**, J. Ning, Z. Li, T. T. A. Dihn, and J. Zhou. (2021, Dec) "Group Time-based One-time Passwords and its Application to Efficient Privacy-Preserving Proof of Location." In *2021 Annual Computer Security Applications Conference (ACSAC)*. (Acceptance rate: **80/326 = 24.5%**)

26. Z. Yang, **C. Jin**, Y. Tian, J. Lai, and J. Zhou. (2020, Oct) "LiS: Lightweight Signature Schemes for Continuous Message Authentication in Cyber-Physical Systems." In *2020 ACM Asia Conference on Computer and Communications Security (AsiaCCS)*. (Acceptance rate: **67/308 = 21.8%**)

27. **C. Jin***, Z. Yang*, M. van Dijk, and J. Zhou. (2019, Dec) "Proof of Aliveness." In *2019 Annual Computer Security Applications Conference (ACSAC)*. (Acceptance rate: **60/266 = 22.6%**)
    - **Artifacts Evaluated Functional**

28. R. S. Khan, N. Noor, **C. Jin**, S. Muneer, F. Dirisaglik, A. Cywar, P. H. Nguyen, M. van Dijk, A. Gokirmak, and H. Silva. (2019, Jul) "Exploiting Lithography Limits for Hardware Security Applications." In *2019 IEEE Conference on Nanotechnology (IEEE-NANO)*.
    - **Best Paper Award Candidate**

29. **C. Jin**, S. Valizadeh, and M. van Dijk. (2018, May) "Snapshotter: Lightweight Intrusion Detection and Prevention System for Industrial Control Systems." In *2018 IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*.

30. M. van Dijk†, **C. Jin**†, H. Maleki†, P. H. Nguyen†, and R. Rahaeimehr†. (2018, Feb) "Weak-Unforgeable Tags for Secure Supply Chain Management." In *2018 International Conference on Financial Cryptography and Data Security (FC)*. (Acceptance rate for full papers: **27/110 = 24.5%**)

31. W. Yan, **C. Jin**, F. Tehranipoor, and J. Chandy. (2017, Sep) "Phase Calibrated Ring Oscillator PUF Design and Implementation on FPGAs." In *2017 International Conference on Field-Programmable Logic and Applications (FPL)*. (Acceptance rate for full papers: **49/208 = 23.6%**)

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

33. H. Maleki, R. Rahaeimehr, **C. Jin**, and M. van Dijk. (2017, May) "New Clone-Detection Approach for RFID-Based Supply Chains." In *2017 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. (Acceptance rate for full papers: **18/106 = 17.0%**)

34. X. Guo, N. Karimi, F. Regazzoni, **C. Jin**, and R. Karri. (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)*. (Acceptance rate for full papers: **17/71 = 23.9%**)

35. X. Guo, D. Mukhopadhyay, **C. Jin**, and R. Karri. (2014, May) "NREPO: Normal Basis Recomputing with Permuted Operands." In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. (Acceptance rate for full papers: **18/65 = 27.7%**)

Workshops

36. H. Zhang, X. Hu, and **C. Jin**. (2025, Mar) "Making Deals with the Devils: The Art of Negotiation after Ransomware Attacks." In *2025 International Workshop on Security Protocols (SPW).*

37. Z. Yang, C. Yin, **C. Jin**, J. Ning, and J. Zhou. (2021, Jun) "Lightweight Delegated Authentication with Identity Fraud Detection for Cyber-Physical Systems." In *2021 ACM Cyber-Physical System Security Workshop (CPSS@AsiaCCS).*

38. **C. Jin**, W. Burleson, M. van Dijk, and U. Rührmair. (2020, Nov) "Erasable PUFs: Formal Treatment and Generic Design." In *2020 Workshop on Attacks and Solutions in Hardware Security (ASHES@CCS).*

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

Pre-prints

40. C. Yin, Z. Huang, **C. Jin**, M. van Dijk, and F. Massacci. (2026) "Function Recovery Attacks in Gate-Hiding Garbled Circuits using SAT Solving." *arXiv.*

41. S. Shen, Z. Huang and **C. Jin**. (2026) "Proving Circuit Functional Equivalence in Zero Knowledge." *arXiv.*

42. Z. Huang and **C. Jin**. (2025) "Approximate Optimal Active Learning of Decision Trees." *arXiv.*

43. M. van Dijk†, D. Gurevin†, **C. Jin**†, O. Khan†, and P. H. Nguyen†. (2021) "Autonomous Secure Remote Attestation even when all Used and to be Used Digital Keys Leak." *Cryptography ePrint Archive.*

44. **C. Jin**, V. Gohil, R. Karri, and J. Rajendran. (2020) "Security of Cloud FPGAs: A Survey." *arXiv.*

Awards

• Runner-up	Dutch Cyber Security Best Research Paper Award Technical Track, 2025
• Shortlisted	Top Picks in Hardware and Embedded Security, 2025
• Best Paper Award Candidate	IEEE-NANO, 2019
• First Place Overall	MITRE eCTF, 2017
• Iron Flag Award	MITRE eCTF, 2017
• Doctoral Dissertation Fellowship	UConn Graduate School, 2019
• Predoctoral Summer Research Fellowship	UConn ECE Department, 2017
• Student Travel Award	CHES, 2019
• Student Scholarship	BlackHat USA, 2017
• Student Travel Award	HOST, 2017
• Student Travel Award	Real World Crypto, 2016

Teaching Experiences

Advanced School for Computing and Imaging (ASCI) Utrecht, the Netherlands
Guest Lecturer (on Physical Unclonable Functions):

- *Hardware and System Security* May 2025

University of Amsterdam Amsterdam, the Netherlands
Mentor:

- *Research Project in Security and Network Engineering* Spring 2024

Guest Lecturer (on Physical Unclonable Functions):

- *Cryptographic Engineering* Mar 2023, Mar 2024, Mar 2025

Guest Lecturer (on Garbled Circuits):

- *Data Protection Technologies* Mar 2025

Guest Lecturer (on Anonymity & Privacy):

- *Introduction to Security* Sep 2024

King Abdullah University of Science and Technology Thuwal, Saudi Arabia
Guest Lecturer (on Hardware Security):

- *Computer Systems Security* Apr 2022, Nov 2022, Nov 2023, Nov 2024

New York University Brooklyn, NY, USA
Course Co-developer:

- *Cybersecurity in Additive Manufacturing* Fall 2020

Master Capstone Project Mentor:

- *Urban Science Intensive* Spring 2020, Summer 2020

Teaching Assistant:

- *Introduction to Hardware Security and Trust* Spring 2020
- *Advanced Computer Hardware Design* Fall 2019

University of Connecticut Storrs, CT, USA
Instructor and Course Developer:

- *Seminar on Cyber-Physical System Security* Spring 2019

Course Co-developer:

- *Advanced Microprocessor Application Lab* Spring 2017
- *Introduction to Hardware Security and Trust* Spring 2017

Teaching Assistant:

- *Microprocessor Applications Laboratory* Spring 2016, Fall 2016

Students

Centrum Wiskunde & Informatica Amsterdam, the Netherlands
Ph.D. Students:

- Niloufar Sayadi, 2023 - present (Co-advised with Prof. Marten van Dijk)
- Sirui Shen, 2023 - present (Co-advised with Prof. Marten van Dijk)

Ph.D. Interns:

- Mingfei Yu, 2025 (3-month visit from EPFL, Switzerland)

University of Amsterdam Amsterdam, the Netherlands
Master Students:

- Isaac Santhagens, 2024
- James Karsten, 2024
- Roberto Volpe Garcia, 2024
- Jan Laan and Wendy Roks, 2024

Wageningen University & Research Wageningen, the Netherlands
Master Students:

- Yuchen Huang, 2022 (Co-advised with Dr. Qingzhi Liu)

New York University Brooklyn, NY, USA
Master Students:

- Shreeraman Arunachalam Karikalan, Aparna Bhutani, Siqi Huang, and Vivek Patel, 2020
- Guilherme Louzada, Chenjie Su, Akash Yadav, and Eric Zhuang, 2020

Competition Experiences

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

- 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 whole competition.

PROFESSIONAL SERVICES

Co-Leader
- Hardware and Cyber-Physical System Security Working Group in ACademic Cyber Security Society in the Netherlands (ACCSS)

Guest Editor
- Wireless Communications and Mobile Computing (WCMC), Special Issue on "Intelligent and Flexible Security of Next-Generation Wireless Networks "

Funding Proposal Reviewer
- Luxembourg National Research Fund (FNR)

Program Committee Co-Chair & Co-Founder
- International Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS'21, 22)

Program Committee Member for Major Security Conferences
- ACM Conference on Computer and Communications Security (CCS'25, 26)
- ACM Asia Conference on Computer and Communications Security (AsiaCCS'25, 26)
- IACR Conference on Cryptographic Hardware and Embedded Systems (CHES'25, 26)
- International Conference on Financial Cryptography and Data Security (FC'25, 26)
- Information Security Conference (ISC'25)
- IEEE Conference on Communications and Network Security (CNS'22 - 24)
- International Conference on Information and Communications Security (ICICS'19 - 22)

Program Committee Member for Other Conferences and Workshops
- ACM Cloud Computing Security Workshop (CCSW'21 - 25)
- ACM Workshop on Privacy in the Electronic Society (WPES'25)
- IEEE International Conference on Omni-Layer Intelligent Systems (COINS'23 - 25)
- ACM Cyber-Physical System Security Workshop (CPSS'24, 25)
- International Symposium on Quality Electronic Design (ISQED'20 - 25)
- Workshop on Attacks and Solutions in Hardware Security (ASHES'20 - 24)
- International Workshop on Security and Trust Management (STM'21 - 24)
- Malicious Software and Hardware in Internet of Things (MaL-IoT'23, 24)
- IEEE International Conference on Cyber, Physical and Social Computing (CPSCom'24)
- Applied Research Competition in North American Region (CSAW'20, 23)
- IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom'23)
- IFIP International Internet of Things Conference (IFIP IoT'21, 22)
- Euromicro Conference on Digital Systems Design (DSD'21)
- International Conference on Science of Cyber Security (SciSec'19)

Student Program Committee Member
- IEEE Symposium on Security and Privacy (S&P'16)

Reviewer

Journals
- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Power Systems (TPWRS)

- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)
- IEEE/ACM Transactions on Networking (TON)
- IEEE Transactions on Very Large Scale Integration Systems (TVLSI)
- IEEE Transactions on Circuits and Systems I (TCAS-I)
- IEEE Transactions on Industrial Informatics (TII)
- IEEE Transactions on Reliability (TR)
- IEEE Transactions on Consumer Electronics (TCE)
- IEEE Security & Privacy (SP)
- IEEE Computer Architecture Letters (CAL)
- IEEE Internet of Things Journal (IOT-J)
- IEEE Consumer Electronics Magazine (CEM)
- IEEE Access
- ACM Computing Surveys (CSUR)
- ACM Transactions on Privacy and Security (TOPS)
- ACM Transactions on Reconfigurable Technology and Systems (TRETS)
- ACM Transactions on Design Automation of Electronic Systems (TODAES)
- ACM Transactions on Embedded Computing Systems (TECS)
- ACM Journal on Emerging Technologies in Computing Systems (JETC)
- IOS Journal of Computer Security (JCS)
- Springer Journal of Cryptographic Engineering (JCEN)
- Springer Journal of Electronic Testing (JETTA)
- Springer Journal of Hardware and Systems Security (HASS)
- Springer International Journal of Information Security (IJIS)
- Springer Cybersecurity
- Springer Discover Internet of Things
- IET Circuits, Devices & Systems
- MDPI Cryptography
- MDPI Electronics
- MDPI Sensors
- MDPI Applied Sciences
- Journal of Internet Technology (JIT)

Conferences

- ACM/EDAC/IEEE Design Automation Conference (DAC'18 - 20)
- IEEE International Midwest Symposium on Circuits and Systems (MWSCAS'18)
- Cryptographers' Track at the RSA Conference (CT-RSA'17)

Sub-Reviewer

Journals

- IEEE Transaction on Computers (TC)
- Nature Communications
- Journal of Manufacturing Systems (JMS)
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)

Conferences

- Design, Automation and Test in Europe Conference (DATE'22)
- International Test Conference (ITC'20)
- ACM/EDAC/IEEE Design Automation Conference (DAC'15 - 17, 20)
- ACM conference on Computer and Communications Security (CCS'17, 19)
- IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'15 - 18)
- IEEE International Conference on Computer Design (ICCD'16, 17)
- IEEE Symposium on Security and Privacy (S&P'17)
- ACM Great Lakes Symposium on VLSI (GLSVLSI'17)

- Theory of Implementation Security Workshop (TIs'16)

Publicity Chair

- International Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS'23)
- EAI International Conference on Applied Cryptography in Computer and Communications (EAI AC3'22)

TALKS

1. Efficient Remotely Verifiable RAM-based Computation without Digital Secrets. *CWI Lectures*. Amsterdam, the Netherlands, 2025/11.
2. The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks. *Top Picks in Hardware and Embedded Security Workshop*. Munich, Germany, 2025/10.
3. PG: Byzantine Fault-Tolerant and Privacy-Preserving Sensor Fusion with Guaranteed Output Delivery. *CompSys*, Utrecht, the Netherlands, 2025/5.
4. PG: Byzantine Fault-Tolerant and Privacy-Preserving Sensor Fusion with Guaranteed Output Delivery. *Computer Science Seminar at King Abdullah University of Science and Technology*, Thuwal, Saudi Arabia, 2024/11.
5. PG: Byzantine Fault-Tolerant and Privacy-Preserving Sensor Fusion with Guaranteed Output Delivery. *ACM Conference on Computer and Communications Security (CCS)*, Salt Lake City, UT, USA, 2024/10.
6. Optimizing Proof of Aliveness in Cyber-Physical Systems. *International Workshop on Re-design Industrial Control Systems with Security (RICSS)*, Salt Lake City, UT, USA, 2024/10.
7. PG: Byzantine Fault-Tolerant and Privacy-Preserving Sensor Fusion with Guaranteed Output Delivery. *Seminar at Radboud University*, Nijmegen, the Netherlands, 2024/6.
8. Recent Advances in the Attacks and Applications of Silicon PUFs. *Seminar at University of Twente*, Enschede, the Netherlands, 2024/6.
9. Towards Remote Verifiable Computation without Digital Secrets. *Seminar at Shandong University*, Virtual, 2023/11.
10. Towards Remote Verifiable Computation without Digital Secrets. *Crypto Working Group Meetup*, Utrecht, the Netherlands, 2023/9.
11. HMACCE: Establishing Authenticated and Confidential Channel from Historical Data for IIoT. *ICT.OPEN*, Utrecht, the Netherlands, 2023/4.
12. HMACCE: Establishing Authenticated and Confidential Channel from Historical Data for Industrial Internet of Things. *Invited Talk at University of Strathclyde*, Virtual, 2023/2.
13. Attacking Physical Unclonable Functions Using Machine Learning. *Amsterdam Data Science Meetup*, Amsterdam, the Netherlands, 2022/12.
14. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. *CWI Scientific Meeting*, Amsterdam, the Netherlands, 2022/5.
15. Group Time-based One-time Passwords and its Application to Efficient Privacy-Preserving Proof of Location. *2021 Annual Computer Security Applications Conference (ACSAC)*, Virtual, 2021/12.

16. Securing Critical Infrastructures in Smart Cities. *Cryptographic Engineering Research Forum at Nanjing University of Aeronautics and Astronautics*, Virtual, 2021/8.

17. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. *The Amsterdam Coordination Group (ACG) Meeting at CWI Amsterdam*, Virtual, 2021/3.

18. Securing Critical Infrastructures in Smart Cities. *ENS Seminar at Delft University of Technology*, Virtual, 2021/3.

19. Lightweight Signature Schemes for Cyber-Physical Systems. *ICT.OPEN*, Virtual, 2021/2.

20. Erasable PUFs: Formal Treatment and Generic Design. *The Amsterdam Coordination Group (ACG) Meeting at CWI Amsterdam*, Virtual, 2020/12.

21. Erasable PUFs: Formal Treatment and Generic Design. *Workshop on Attacks and Solutions in Hardware Security (ASHES)*, Virtual, 2020/11.

22. Enhancing Cyber-Physical Systems Security with Cryptography and Hardware Security Primitives. *ECE Department Seminar at Iowa State University*, Ames, IA, USA, 2020/2.

23. Securing the Infrastructures in Smart Cities with Cryptography and Hardware Primitives. *Seminar at Virginia Commonwealth University*, Richmond, VA, USA, 2020/2.

24. Securing the Infrastructures in Smart Cities using Cryptography and Hardware Primitives. *Research Seminar at Villanova University*, Villanova, PA, USA, 2020/2.

25. Securing the Infrastructures in Smart Cities. *Center for Urban Science and Progress (CUSP) Research Seminar at New York University*, Brooklyn, NY, USA, 2019/9.

26. The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks. *Conference on Cryptographic Hardware and Embedded Systems (CHES)*. Atlanta, GA, USA, 2019/8.

27. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Seminar at Tennessee State University*, Nashville, TN, USA, 2019/3.

28. Efficient Erasable PUFs from Programmable Logic and Memristors. *Connecticut Microelectronics and Optoelectronics Consortium Symposium at University of New Haven*, Orange, CT, USA, 2019/3.

29. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Seminar at California State University*, Long Beach, CA, USA, 2019/3.

30. Enhancing Cyber-Physical System Security with Cryptographic Primitives. *Seminar at DePaul University*, Chicago, IL, USA, 2019/2.

31. Enhancing Cyber-Physical System Security with Cryptography and Hardware Security Primitives. *Graduate Seminar at University of Utah*, Salt Lake City, UT, USA, 2019/2.

32. Cryptographic Solutions for Cyber-Physical System Security. *Seminar at United Technologies Research Center*, East Hartford, CT, USA, 2018/9.

33. PwoP: Intrusion-Tolerant and Privacy-Preserving Sensor Fusion. *Security Seminar at University of Connecticut*, Storrs, CT, USA, 2018/9.

34. Secure Sensor Fusion. *Modular Approach to Cloud Security (MACS) Project Meeting at Boston University*, Boston, MA, USA, 2018/1.

35. Advancing the State-of-the-Art in Hardware Trojans Design. *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, Medford, MA, USA, 2017/8.

36. Mitigating Synchronized Hardware Trojan Attacks in Smart Grids. *Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, Pittsburgh, PA, USA, 2017/4.

37. Secure and Efficient Initialization and Authentication Protocols for SHIELD. *Security Seminar at University of Connecticut*, Storrs, CT, USA, 2016/9.

38. NREPO: Normal Basis Recomputing with Permuted Operands. *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Washington, DC, USA, 2014/5.