Wen Wang

wen.wang.ww349@yale.edu • caslab.csl.yale.edu/~wen

Research Interest

My research goal is to provide agile and cost-effective cryptographic solutions to keep hardware devices secure against existing attacks as well as potential threats from the future. Recently I have worked on building efficient hardware architectures for post-quantum cryptography, that is, cryptosystems deployed in classical computers conjectured to be secure against attacks utilizing large-scale quantum computers.

Education

Yale University, New Haven, CT, USA **Aug. 2015 – May. 2021 (expected)**
Ph.D. Candidate
M.S., Electrical Engineering *and* M.Phil., Electrical Engineering
Advisor: *Prof.* Jakub Szefer
Thesis: Building Hardware Architectures for Post-Quantum Cryptography (in progress)

University of Science and Technology of China, Hefei, Anhui, China **Sep. 2011 – Jun. 2015**
B.S., Applied Physics
Thesis: FPGA-Based Massive Data Sorting in Multi-Channel Transient Electromagnetic Method (MTEM) Systems

Professional Experience

Microsoft Research, Redmond, WA, USA Research Intern **Jun. 2020 – Aug. 2020**
Advisor: Patrick Longa, Security and Cryptography Group
Project: Construction and destruction of SIKE on hardware.

Continental AG, Frankfurt, Hessen, Germany Security Research Intern **Jun. 2019 – Aug. 2019**
Advisor: Marc Stöettinger, Security and Privacy Competence Center
Project: Post-quantum secure automotive hardware security modules.

TU Darmstadt, Darmstadt, Hessen, Germany Graduate Researcher **Jun. 2018 – Sep. 2018**
Advisor: Johannes Buchmann, Cryptography and Computer Algebra Group
Project: Software-hardware co-design for qTESLA on RISC-V.

TU Darmstadt, Darmstadt, Hessen, Germany Graduate Researcher **Oct. 2017 – Dec. 2017**
Advisor: Johannes Buchmann, Cryptography and Computer Algebra Group
Project: Software-hardware co-design for XMSS on RISC-V.

Selected Honors and Awards

- Selected to Participate in the Rising Stars in EECS Workshop 2020
- Selected as Barlow Fellow with Fellowship by Yale Graduate School 2016
- Yale Sheffield Fellowship 2015
- Outstanding Graduates of University of Science and Technology of China 2014
- National Scholarship of China 2014
- Scholarship of Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences 2014
- Grand Prize in the Competition of Physical Research Experiments of University 2013
- Outstanding Student Scholarship in University of Science and Technology of China 2011 – 2013

Teaching Experience

Teaching Assistant for Introduction to Computer Engineering (EENG 201) Yale University Spring 2017 & 2018
Topics include Boolean algebra, finite state machines, and basic computer architecture principles.
Assisted Prof. Szefer in preparing lab materials, leading lab sessions, holding office hours and grading.

Cryptography Standardization Efforts

Classic McEliece. ***Finalist*** in the **NIST's Post-Quantum Cryptography Standardization Project**
Submission by Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, **Wen Wang**, Martin Albrecht, Carlos Cid, Kenneth G. Paterson, Cen Jung Tjhai, and Martin Tomlinson.

Research Projects

Construction and Destruction of SIKE on Hardware [ePrint 2020/1457, in submission]
Advisor: Prof. Jakub Szefer, Dr. Patrick Longa (Microsoft Research, Redmond, US)
- Proposed algorithm-level optimizations for the extension field arithmetic.
- Designed and implemented parameterized hardware accelerators for elliptic curve point and isogeny operations.
- Prototyped a real-world hardware-software co-design for the isogeny-based key encapsulation mechanism SIKE based on a RISC-V platform, achieved a 200-450× speedup for the encapsulation operation.
- Assisted in developing a hardware-focused, budget-based cost model for SIKE cryptanalysis by using the ASIC synthesis results of the same set of hardware accelerators developed for constructing the SIKE hardware design.
- Demonstrated that current SIKE parameters offer a wide security margin and we can use significantly smaller primes for SIKE which would enable more efficient and compact implementations with reduced bandwidth.

Parameterized Lattice-based Signature Scheme qTESLA on RISC-V Based SoC [CHES '20]
Advisor: Prof. Jakub Szefer
- Proposed novel algorithms for binary-search CDT sampler and NTT-based polynomial multiplier.
- Designed and implemented the following open-sourced hardware accelerators applicable to different lattice-based schemes:
  – a unified and scalable core for SHAKE-128/256 and cSHAKE-128/256,
  – a novel, parameterized, and lightweight CDT-based Gaussian sampler,
  – a novel, parameterized, and fully pipelined NTT-based polynomial multiplier, and
  – a parameterized sparse polynomial multiplier.
- Prototyped a real-world hardware-software co-design based on a RISC-V platform for the lattice-based digital signature scheme qTESLA, achieved a 40-100× speedup for key generation, a 10× speedup for signing, and a 16× speedup for verification.
- Demonstrated the practicability and efficiency of running provably-secure lattice-based signature schemes on resource-constraint embedded systems.

Efficient Hash-based XMSS Signature Scheme on Embedded Systems [SAC '19]
Advisor: Prof. Jakub Szefer, Dr. Ruben Niederhagen (Fraunhofer SIT, Darmstadt, Germany)
- Proposed two algorithm-level software optimizations targeting the hash functions used in the stateful hash-based signature scheme XMSS, these optimizations brought a 1.5× speedup in software.
- Designed and implemented the following hierarchical and open-sourced hardware accelerators for XMSS:
  – a general-purpose SHA-256 accelerator,
  – an XMSS-specific SHA-256 accelerator, integrating the algorithmic optimizations we proposed,
  – a hash-chain accelerator, and
  – a Winternitz one-time signature accelerator.
- Prototyped a real-world hardware-software co-design based on a RISC-V platform for XMSS, achieved an over 50× speedup for XMSS key generation, signing, and verification.
- Demonstrated the practicability and efficiency of running compute-intensive hash-based signature schemes on resource-constraint embedded systems.

ASIC Chip Design of Post-Quantum Cryptographic Schemes [ICCD '20]
Advisor: Prof. Jakub Szefer, Prof. Ken Mai (Carnegie Mellon University, Pittsburgh, US)
- Designed and implemented a set of pipelined accelerators for the hash-based signature scheme XMSS.
- Implemented and evaluated both the non-pipelined and piplined XMSS accelerators on 28nm Artix-7 FPGAs.
- Developed protocols and interfaces for the ASIC chip and the testing platform.
- Assisted in the implementation and evaluation of the XMSS accelerators in a 28nm CMOS process.
- Presented practical post-quantum secure ASIC chips that have small area, low power, and high performance.

Practical Code-Based Niederreiter Cryptosystem on Hardware [CHES '17, PQCrypto '18, ReConfig '16]
Advisor: Prof. Jakub Szefer, Dr. Ruben Niederhagen (Fraunhofer SIT, Darmstadt, Germany)
- Designed and implemented the following hardware accelerators for the code-based Niederreiter cryptosystem:
  – Gaussian systemizer: matrix systemization for any large-sized matrix with elements from any binary field,
  – additive FFT based polynomial evaluator: the Gao-Mateer additive FFT algorithm was first-time applied for polynomial evaluation in hardware, achieved a 7× better time×area compared to schoolbook algorithm,
  – error-decoding unit: applied constant-time Berlekamp-Massey algorithm, and
  – constant-time permutation/sorting: applied constant-time merge-sort algorithm.
- Presented the first, fastest-to-date, constant-time, fully parameterized, and open-sourced hardware design for the full Niederreiter cryptosystem, demonstrated the practicability of this complex scheme on hardware.

Publications

Invited Articles

1. **[GLSVLSI '18]** **Wen Wang**, Jakub Szefer, and Ruben Niederhagen, "Post-Quantum Cryptography on FPGAs: the Niederreiter Cryptosystem: Extended Abstract", in Proceedings of the Great Lakes Symposium on VLSI, 2018.
   [PDF]

Refereed Conference Publications

1. **[ICCD '20]** Prashanth Mohan†, **Wen Wang**†, Bernhard Jungk, Ruben Niederhagen, Jakub Szefer, and Ken Mai, "ASIC Accelerator in 28 nm for the Post-Quantum Digital Signature Scheme XMSS", in Proceedings of the IEEE International Conference on Computer Design, 2020. † The authors contributed equally.
   [PDF]
2. **[CHES '20]** **Wen Wang**, Shanquan Tian, Bernhard Jungk, Nina Bindel, Patrick Longa, and Jakub Szefer, "Parameterized Hardware Accelerators for Lattice-Based Cryptography and Their Application to the HW/SW Co-Design of qTESLA", in IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020.
   [PDF]
3. **[FPT '19]** Shanquan Tian, **Wen Wang**, and Jakub Szefer, "Merge-Exchange Sort Based Discrete Gaussian Sampler with Fixed Memory Access Pattern", in Proceedings of the International Conference on Field-Programmable Technology, 2019.
   [PDF]
4. **[FPT '19]** Jingwei Hu, **Wen Wang**, Ray Cheung and Huaxiong Wang, "Optimized Polynomial Multiplier over Commutative Rings on FPGAs. A Case Study on BIKE", in Proceedings of the International Conference on Field-Programmable Technology, 2019.
   [PDF]
5. **[SAC '19]** **Wen Wang**, Bernhard Jungk, Julian Wälde, Shuwen Deng, Naina Gupta, Jakub Szefer, and Ruben Niederhagen, "XMSS and Embedded Systems – XMSS Accelerators for RISC-V", in Proceedings of the Selected Areas in Cryptography Conference, 2019.
   [PDF]
6. **[PQCrypto '18]** **Wen Wang**, Jakub Szefer, and Ruben Niederhagen, "FPGA-based Niederreiter Cryptosystem using Binary Goppa Codes", in Proceedings of International Conference on Post-Quantum Cryptography, 2018.
   [PDF]
7. **[CHES '17]** **Wen Wang**, Jakub Szefer, and Ruben Niederhagen, "FPGA-based Key Generator for the Niederreiter Cryptosystem using Binary Goppa Codes", in Proceedings of the Conference on Cryptographic Hardware and Embedded Systems, 2017.
   [PDF]
8. **[ReConFig '16]** **Wen Wang**, Jakub Szefer, and Ruben Niederhagen, "Solving Large Systems of Linear Equations over GF(2) on FPGAs", in Proceedings of the International Conference on Reconfigurable Computing and FPGAs, 2016.
   [PDF]
9. **[FPT '16]** Sumedh Guha, **Wen Wang**, Shafeeq Ibraheem, Mahesh Balakrishnan, and Jakub Szefer, "Design and Implementation of Open-Source SATA III Core for Stratix V FPGAs", in Proceedings of the International Conference on Field-Programmable Technology, 2016.
   [PDF]

In Submission

1. **[USENIX Security '21]** Patrick Longa, **Wen Wang**, and Jakub Szefer, "The Cost to Break SIKE: A Comparative Hardware-Based Analysis with AES and SHA-3". [ePrint PDF]
2. **[CHES '21]** Jingwei Hu, **Wen Wang**, San Ling, and Huaxiong Wang, "Engineering Practical Rank-code-based Cryptographic Schemes on Embedded Hardware. A Case Study on ROLLO".
3. **[DAC '21]** Changsu Kim, Yongwoo Lee, Shinnung Jeong, **Wen Wang**, Jakub Szefer, and Hanjun Kim, "Area-Efficient Task-Level Pipelining in High-Level Synthesis for Post-Quantum Cryptography".

Technical Reports

1. **[ePrint 2020/026]** **Wen Wang**, and Marc Stöettinger, "Post-Quantum Secure Architectures for Automotive Hardware Secure Modules". [ePrint PDF]

Presentations

Invited Talks

1. October 2019 – (One of 8 Invited Speakers) Invited Talk on **"Post-Quantum Secure Digital Signatures on Embedded Systems"** at IBM Research Workshop on the Future of Computing Architectures (FOCA), New York, United States.
2. May 2018 – Invited talk on **"Post-Quantum Cryptography on FPGAs: the Niederreiter Cryptosystem"** at ACM Great Lakes Symposium on VLSI (GLSVLSI), Chicago, United States.

Conference and Workshop Talks

1. October 2020 – Contributed talk (virtual) on **"Post-Quantum Secure Digital Signatures on Embedded Systems"** at Post-Quantum Cryptography for Embedded Systems Workshop, 2020.
2. September 2020 – Conference talk (virtual) on **"Parameterized Hardware Accelerators for Lattice-Based Cryptography and Their Application to the HW/SW Co-Design of qTESLA"** at International Conference on Cryptographic Hardware and Embedded Systems (CHES), 2020.
3. August 2020 – Talk (virtual) on **"Construction and Destruction of SIKE on Hardware"** at Microsoft Research.
4. November 2019 – Talk on **"Post-Quantum Secure Digital Signatures on Embedded Systems"** at YINQE/CRISP Seminar, Yale University, United States.
5. September 2019 – Talk on **"Post-Quantum Secure Architectures for Automotive Hardware Secure Modules"** at Continental AG, Frankfurt, Germany.
6. May 2019 – Talk on **"XMSS and Embedded Systems: XMSS Hardware Accelerators for RISC-V"** at CASLAB Day, Yale University, United States.
7. July 2018 – Invited talk on **"Hardware Architectures for Post-Quantum Cryptography"** at the Oberseminar, TU Darmstadt, Germany.
8. April 2018 – Conference talk on **"FPGA-based Niederreiter Cryptosystem using Binary Goppa Codes"** at International Conference on Post-Quantum Cryptography (PQCrypto), Fort Lauderdale, United States.
9. October 2017 – Invited talk on **"Hardware Architectures for Post-Quantum Cryptography – Key Generator for the Niederreiter Cryptosystem"** at the CROSSING seminar, TU Darmstadt, Germany.
10. September 2017 – Conference talk on **"FPGA-based Key Generator for the Niederreiter Cryptosystem using Binary Goppa Codes"** at International Conference on Cryptographic Hardware and Embedded Systems (CHES), Taipei, Taiwan.
11. November 2016 – Conference talk on **"Solving Large Systems of Linear Equations over GF(2) on FPGAs"** at International Conference on Recongigurable Computing and FPGAs (ReConFig), Cancun, Mexico, .

Posters

- May 2018 – **"Post-Quantum Cryptography on FPGAs: the Niederreiter Cryptosystem"** at CASLAB Day, Yale University, United States.

Hardware Demo

- May 2018 – **"FPGA-based Post-Quantum Secure Niederreiter Cryptosystem Demonstration"**, Live Demo at IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington DC, USA.

Service

PC of 12th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2021),
reviewer for Transactions on Computers (2020),
shadow PC of 41st IEEE Symposium on Security and Privacy: reviewed 4 papers and 2 posters (S&P 2020),
reviewer for Transactions on Computer-Aided Design of Integrated Circuits and Systems (2019),
and reviewer for Journal Microprocessors and Microsystems (2017 & 2018).

Skills

- Programming Language: C/C++, Python, Sage, Verilog, SystemVerilog, VHDL, Matlab, Bash.
- Tools: Quartus, Vivado, ISE, iVerilog, Verilator, NCverilog.