XIN WANG

+1 (540) 514-0557 ⋄ xinw@vt.edu ⋄ *https : //people.cs.vt.edu/xinw/*

RESEARCH INTERESTS

My research interests generally lie on computer architecture and security. The goal of my current research is designing high-performance computing systems (e.g., servers in Cloud) which are secure against attacks such as physical attacks. My works are published in top-tier architecture venues, e.g., ISCA and MICRO.

EDUCATION

Ph.D. in Computer Science. August 2018 - *present*
Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, VA.
Research Area: Computer Architecture and Hardware Security.

M.S. with thesis in Computer Science. July 2017
Beihang University, Beijing, China.
Research Area: Cryptography in Multi-core Systems.

B.S. in IoT Engineering. June 2014
Soochow University, Suzhou, China.

TECHNICAL SKILLS AND TOOLS

C, C++, Python, Java, Gem5 Simulator, OpenMP, MPI, Shell scripting

RESEARCH EXPERIENCE

Graduate Research Assistant at HEAP Lab (Virginia Tech) Fall 2018 - *present*
Supervisor: Dr. Xun (Steve) Jian

- Addressing the metadata access latency overheads for memory encryption via hardware optimization. Explicitly, this research explores caching and using write counters directly in L2 to parallelize the access and use of counters with data access while caching counters in LLC.
- Addressing the cipher calculation latency overheads faced by counter mode memory encryption. Explicitly, this research explores memoizing cryptography calculations for frequently-used counter values. When a counter arrives from memory, MC can use the counter value to look up a memoization table to quickly obtain the counter's memoized results instead of slowly recalculating them.
- Addressing the performance overhead of counterless memory encryption. Explicitly, this research explores how to combine both counterlss and counter mode encryption to achieve the best of both worlds. For irregular workloads, this proposed memory encryption achieves 98% the average performance of no memory encryption.

SoC Architect at Samsung Semiconductor Inc. Spring 2024
Supervisor: Dr. Li Zhao and Dr. Miseon Han

- Performance modeling and feature exploration of LPDDR for Samsung's flagship mobile SoC.

Graduate Research Assistant at Sino-German Joint Software Institute (BUAA) Fall 2014 - Spring 2017
Supervisor: Dr. Yunchun Li

- Optimizing the implementation of a block cipher (i.e., SM4) on Tilera multiprocessor. Explicitly, this research improves the nonlinear transformation of the block cipher by extending the sbox of it and improves the linear transformation of the cipher (in ECB mode) with the help of SIMD instructions that Tilera processor provides.
- Designing a hybrid encryption method for VPN server which uses both general-purpose CPU and multi-core network processor. Explicitly, the server adaptively offloads encryption tasks to network processor according to the encryption loads of the server. The effectiveness of the proposed design is verified by implementation based on open-source software.

PUBLICATIONS

"Counter-light Memory Encryption", **Xin Wang**, Jagadish Kotra, Alex Jones, Wenjie Xiong, Xun Jian. *51st IEEE/ACM International Symposium on Computer Architecture (ISCA 2024)*

"Self-Reinforcing Memoization for Cryptography Calculations in Secure Memory Systems", **Xin Wang**, Daulet Talapkaliyev, Matthew Hicks, Xun Jian. *55th IEEE/ACM International Symposium on Microarchitecture (MICRO 2022)*

"Eager Memory Cryptography in Caches", **Xin Wang**, Jagadish Kotra, Xun Jian. *55th IEEE/ACM International Symposium on Microarchitecture (MICRO 2022)*

"Flow-Based SM4 Encryption via Tilera Multiprocessor", **Xin Wang**, Yunchun Li, Xiaoxiang Zou. *IEEE 18th International Conference on High Performance Computing and Communications (HPCC 2016)*

SELECTED TALKS

Counter-light Memory Encryption, at the 51st ISCA, Virtual

Self-Reinforcing Memoization for Cryptography Calculations in Secure Memory Systems, at the 55th MICRO, Chicago

Eager Memory Cryptography in Caches, at the 55th MICRO, Chicago

Flow-Based SM4 Encryption via Tilera Multiprocessor, at the 18th HPCC, Sydney

HONORS

Second Scholarship, 2015, Beihang University, China

Renmin Zonghe Scholarship, 2013, Soochow University, China

Second Prize of Lanqiao Cup, 2012, Jiangsu Province, China

Huazang Scholarship, 2011, Soochow University, China

TEACHING EXPERIENCES

- **Graduate Teaching Assistant at Virginia Tech** for *CS2506:* Computer Organization II (Spring 2022, Fall 2022, Spring 2023, and Fall 2023)
- **Graduate Teaching Assistant at Virginia Tech** for *CS4504/CS5504/ECE5504:* Computer Architecture (Spring 2023)