Cong Wu

Cryptography, Security, and Cloud

Love Building 365, Computer Science, Florida State University
Tallahassee, FL-32306
☎ *(850) 345-6021*
✉ *cwu4@fsu.edu*
🌐 *tsongw.github.io*

Education

2017-Present	**PhD. Candidate in Computer Science**, *Florida State University*, Tallahassee
2014-2016	**M.S. in Mathematics**, *Florida State University*, Tallahassee
2004-2008	**B.S.in in Math and Applied Math**, *Harbin Normal University*, Harbin

Experience

Aug 2018 - Present **Research Assistant**, *Florida State University*, Tallahassee

- ○ Developing efficient authenticated-encryption(AE) schemes for the TLS protocol in *https*.
- ○ Designed and implemented fast and secure logging systems for the Linux kernel.
- ○ Provided rigorous security proofs for various symmetric-key schemes.
- ○ Designed and implemented encrypted parallel and distributed communication library for High-Performance Computing (HPC) in the cloud.
- ○ Performance analysis and modeling of HPC workloads across multiple Docker containers that are deployed on multiple nodes.

Aug 2022 - Dec 2022 **Teaching Assistant**, *Florida State University*, Tallahassee

- ○ Developed and led a project on Linux kernel module programming, taught advanced topics including system calls, concurrency, and kernel-level synchronization.
- ○ Developed and led a project on file-system design and implementation, taught FAT32 concepts including cluster storage, FAT tables, and directories.

Publications

2022 Viet Tung Hoang, **Cong Wu**, and Xin Yuan (Names in Alphabetical Order), *"Faster Yet Safer: Logging System Via Fixed-Key Blockcipher"*, USENIX Security 2022, **[Best Paper Award]**

2021 Mohsen Gavahi, Abu Naser, **Cong Wu**, Mehran Sadeghi Lahijani, Zhi Wang, and Xin Yuan, *"Encrypted All-reduce on Multi-core Clusters"*, IEEE International Performance, Computing, and Communications Conference (IPCCC)

2021 Mehran Sadeghi Lahijani, Abu Naser, **Cong Wu**, Mohsen Gavahi, Viet Tung Hoang, Zhi Wang, and Xin Yuan, *"Efficient Algorithms for Encrypted All-gather Operation"*, IEEE International Parallel and Distributed Processing Symposium(IPDPS)

2020 Abu Naser, Mehran Sadeghi Lahijani, **Cong Wu**, Mohsen Gavahi, Viet Tung Hoang, Zhi Wang, and Xin Yuan, *"Performance Evaluation and Modeling of Cryptographic Libraries for MPI Communications"*, arXiv:2010.06139

2019 Abu Naser, Mohsen Gavahi, **Cong Wu**, Viet Tung Hoang, Zhi Wang, and Xin Yuan, *"An Empirical Study of Cryptographic Libraries for MPI Communications"*, IEEE International Conference on Cluster Computing (CLUSTER)

Projects

Committing Security
Developing robust and secure committing authenticated-encryption schemes that effectively counter the partition oracle attack. This attack poses a significant threat to widely adopted AEAD schemes such as AES-GCM, XSalsa20/Poly1305, and ChaCha20/Poly1305. Our goal is to set a new standard for the Transport Layer Security (TLS) protocol in *https*.

QuickLog
Developed an fast and secure logging system at the Linux kernel level, surpassing the state-of-the-art in adoptability, performance, and security. [**USENIX Badges Award**: Artifacts Available, Artifacts Functional, and Results Reproduced]

CryptMPI
Developed encrypted communication library for Cloud-based Parallel and Distributed computing architecture. Implemented C-based solution utilizing novel collective algorithms, pre-computation, multithreading, and pipelining techniques on top of MVAPICH and MPICH to accelerate encrypted communication.

EncryptedMPI
Evaluated encryption performance with MPI communication using modern cryptographic libraries such as OpenSSL, and Libsodium.

Technical Skills

Languages	C, C++, MATLAB, Python, Shell script
System	Linux Kernel
Library	OpenSSL, BoringSSL, Libsodium, CryptoPP
Parallel Programming	MPI, OpenMP