Cathie Yun

Security Engineer, Cryptographer

cathieyun@gmail.com
cathieyun.github.io
cathieyun.medium.com

Interested in bridging the gap between research and applied cryptography.

Apple - SEAR Cryptography Engineering / Cryptography Engineer
2023 - present

Working on cryptography libraries: corecrypto, CryptoKit, CommonCrypto
Bringing cryptographic expertise to Apple features and products

Google - FHE / Cryptography Engineer
2022 - 2023

Implemented the TFHE scheme in JAX, targeting TPU and GPUs: Jaxite
Optimizations and integrations for the general purpose transpiler for FHE

Google - ISE Crypto / Cryptography and Security Engineer
2019 - 2022

Reviewed security: Trust Tokens, VPN (RSA Blind Sigs), Exposure Notifications
Penetration tested Ads infrastructure with the OffSec team
Implemented input validation for Secure Aggregation with ZKPs: ACORN

Interstellar / Applied Cryptographer, Software Engineer
2018-2019

Designed and implemented a zero-knowledge smart contract language: ZkVM

Chain / Applied Cryptographer, Software Engineer
2017-2018 (acquired by Interstellar)

Implemented the Bulletproofs zero-knowledge proof protocol - range proofs, circuit proofs, and a programmable constraint system: Bulletproofs, Notes

MIT CSAIL PDOS Group / Graduate Researcher, Teaching Assistant
2015-2017

Designed and implemented a multi-party computation system for a user to query a public database while keeping their query private: Splinter

Teaching Assistant for Computer Systems Engineering (6.033)

Publications

F. Wang, **C. Yun**, M. Zaharia, V. Vaikuntanathan, and S. Goldwasser. Splinter: Practical Private Queries on Public Data. (NSDI '17).

J. Bell, A. Gascón, T. Lepoint, B. Li, S. Meiklejohn, M. Raykova, **C. Yun**. ACORN: Input Validation for Secure Aggregation. (USENIX '23).

Talks

"AMA: Cryptographers Panel" at Real World Crypto 2022 - video
"Trust Tokens: How Much Do We Trust Them?" at DEFCON's 0x0G - video
"Explaining Zero Knowledge Proofs" at DEFCON's Crypto Village - video
"Smart Contracts with Bulletproofs" at the ZKProof Workshop - video

Education

MIT
2012-2017

M.S. in Computer Science, with a concentration in Systems Engineering
CSAIL Parallel and Distributed Operating Systems, supervised by Vinod Vaikuntanathan
B.S. in Computer Science, Minor in Music