Zhenfei Zhang

Cryptography Engineer	zhenfei.zhang@hotmail.com
Algorand	https://zhenfeizhang.github.io/
Boston, MA	https://www.linkedin.com/in/zhenfeizhang/

Experience

Cryptography Engineer, *Algorand*, 2018-now

Identify, develop and standardize cryptographic tools to be used by Algorand blockchain protocol.

- Design: Identify suitable cryptography for Algorand blockchain;
- Coding: Product level **Rust** code for
  - **Pixel aggregatable signature**;
  - **BLS signature**;
  - **Pointproofs**: Aggregating Proofs for Multiple Vector Commitments;
- Standardization: **Internet draft** for BLS signature scheme, IETF/CFRG working group.

Director of Cryptography Research, *Security Innovation* -> *OnBoard Security*, 2014-2018

- Homomorphic encryptions (IARPA project);
- Post-quantum cryptography;
- blockchain cryptography.

Highlights

Standards

Contribute to **2** out of 7 finalists of NIST's **post-quantum standardization process**: **Falcon** and **NTRU**.

LAC won the first prize of **Chinese post-quantum cryptography competition**.

Internet draft: **BLS-signature**, Quantum safe hybrid for **TLS 1.2** and **TLS 1.3**.

Former member of ETSI **Quantum-safe Cryptography (QSC)** working group.

Former member of **ISO/SC27** working group.

Publication and patents

3 U.S. patents; **25+** peer reviewed paper at ACM CCS 2020, PKC 2020, Asiacrypt 2019, Crypto 2019, Asiacrypt 2018, PKC 2018, IEEE Transaction on Computers, etc.;

See next pages for full list.

Programming Languages

Rust: Cryptographic library at product level.

C: Cryptographic library, nearly product level code.

Python/Sage: Proof of concept codes.

Software

Pixel A pairing based, forward-secure and aggregatable signature, written in python (PoC) and rust (product level). Improves existing (non-aggregatable) solution by 100x, open sourced and external audited. **Source code**.

Pointproofs: A pairing based, aggregatable prove system over multiple vector commitments, written in rust (product level). **Source code**.

Raptor A lattice based (linkable) ring signature, written in C as a PoC, aiming to protect user's anonymity against quantum adversaries. **Source code**.

NTRUEncrypt A C implementation of NTRUEncrypt, submitted to NIST PQC standardization process. **Source code**.

Ring multiplication A C library for fast ring multiplication using AVX-2; improving prior codes by a factor of 2.23. **Source code**

libgcrypt-ntru Enabling NTRUEncrypt for libgcrypt. **Source code**.

Education

2010-2014 **PhD, Computer Science**, *University of Wollongong, Australia*;

Thesis title: Revisiting Fully Homomorphic Encryption Schemes and Their Cryptographic Primitives

2008-2009 **Master of Engineering - Research**, *University of Wollongong, Australia*;

2007 **Master of Internet Technology**, *University of Wollongong, Australia*;

2001-2005 **Bachelor of Computer Science**, *BeiHang University, China*.

Research Interest

- Practical aspects of lattice based cryptography;
- Cryptographic primitives for blockchains privacy, such as ring signatures, zero knowledge proofs;

`See next pages for the full list of patents, standards and publications.`

Patents

- **Chameleon Hash technique and linkable ring signature technique**
  - *Zhenfei Zhang*
  - Provisional patent, 2018.
- **Digital signature technique**
  - *Jeffrey Hoffstein, Jill Pipher, William J Whyte, Zhenfei Zhang*
  - United States Patent Application, 2018.
- **Digital signature method and apparatus**
  - *Jeffrey Hoffstein, Jill Pipher, Joseph H Silverman, William J Whyte, Zhenfei Zhang*
  - United States Patent 15530762, 2017.

Standards

- **BLS Signature Scheme**
  - *D. Boneh, S.Gorbunov, R. Wahby, H.Wee, Z.Zhang*
  - Internet-Draft.
- **Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.2**
  - *J. M. Schanck, W. Whyte and Z. Zhang*
  - Internet-Draft.
- **Criteria for selection of public-key cryptographic algorithms for quantum-safe hybrid cryptography**
  - *J. M. Schanck, W. Whyte and Z. Zhang*
  - Internet-Draft.
- **Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.3**
  - *W. Whyte, Z. Zhang, S. Fluhrer and O. Garcia-Morchon*
  - Internet-Draft.
- **Efficient Embedded Security Standards (EESS) #1: Implementation Aspects of NTRUEncrypt**
  - *W. Whyte and Z. Zhang*
  - Consortium for Efficient Embedded Security
- **Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges**
  - One of 22 contributors
  - European Telecommunications Standards Institute(ETSI) white paper

Publications

2020

- **Practical Post-Quantum Few-Time Verifiable Random Function with Applications to Algorand**
  - *Muhammed F. Esgin and Veronika Kuchta and Amin Sakzad and Ron Steinfeld and Zhenfei Zhang and Shifeng Sun and Shumo Chu*
  - Pre-print. **IACR eprint**. **Source code**.
- **Pointproofs: Aggregating Proofs for Multiple Vector Commitments**
  - *Sergey Gorbunov, Leonid Reyzin, Hoeteck Wee, Zhenfei Zhang*
  - ACM CCS 2020. **IACR eprint**. **Source code**.
- **MPSign: A Signature from Small-Secret Middle-Product Learning with Errors**
  - *Shi Bai, Dipayan Das, Ryo Hiromasa, Miruna Rosca, Amin Sakzad, Damien Stehle, Ron Steinfeld, Zhenfei Zhang*
  - PKC 2020. **IACR eprint**. **Source code**
- **Modular Lattice Signatures, revisited**
  - *Dipayan Das, Jeffrey Hoffstein, Jill Pipher, William Whyte, Zhenfei Zhang*
  - Design, Codes and Cryptography. **IACR eprint**. **Source code**.
  - **1st round**, NIST post-quantum cryptography standardization process.

2019

- **Middle-Product Learning with Rounding Problem and its Applications**
  - *Shi Bai, Katharina Boudgoust, Dipayan Das, Adeline Roux-Langlois, Weiqiang Wen, Zhenfei Zhang*
  - Asiacrypt 2019. **IACR eprint**.
- **Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications**
  - *Rupeng Yang, Man Ho Au, Zhenfei Zhang, Qiuliang Xu, Zuoxia Yu, William Whyte*
  - Crypto 2019. **IACR eprint**.
- **(Linkable) Ring Signature from Hash-Then-One-Way Signature**
  - *Xingye Lu, Man Ho Au, Zhenfei Zhang*
  - TrustCom 2019. **IACR eprint**.
- **Ring Signatures based on Middle-Product Learning with Errors Problems**
  - *Dipayan Das, Man Ho Au, Zhenfei Zhang*
  - Africacrypt 2019.
- **Raptor: A Practical Lattice-Based (Linkable) Ring Signature**
  - *Xingye Lu, Man Ho Au, Zhenfei Zhang*
  - ACNS 2019. **IACR eprint**. **Source code**.
- **Round5: Compact and Fast Post-Quantum Public-Key Encryption**
  - *Hayo Baan, Sauvik Bhattacharya, Scott Fluhrer, Oscar Garcia-Morchon, Thijs Laarhoven, Ronald Rietman, Markku-Juhani O. Saarinen, Ludo Tolhuizen, Zhenfei Zhang*
  - PQCrypto 2019. **IACR eprint**. **Website**.
  - **2nd round**, NIST post-quantum cryptography standardization process.
- **Cryptanalysis of an NTRU-based Proxy Encryption Scheme from ASIACCS'15**

— *Zhen Liu, Yanbin Pan, Zhenfei Zhang*
— PQCrypto 2019. **IACR eprint**.

2018

- **LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus**
  — *Xianhui Lu, Yamin Liu, Zhenfei Zhang, Dingding Jia, Haiyang Xue, Jingnan He, Bao Li*
  — Pre-print. **IACR eprint**. **Source code**. **talk**
  — **First prize** of **Chinese post-quantum cryptography competition**.
  — **2nd round**, NIST post-quantum cryptography standardization process.
- **Shorter Messages and Faster Post-Quantum Encryption with Round5 on Cortex M**
  — *Markku-Juhani O. Saarinen, Sauvik Bhattacharya, Oscar Garcia-Morchon, Ronald Rietman, Ludo Tolhuizen, Zhenfei Zhang*
  — Cardis 2018. **IACR eprint**.
- **On the Hardness of the Computational Ring-LWR Problem and its Applications**
  — *Long Chen, Zhenfeng Zhang, Zhenfei Zhang*
  — Asiacrypt 2018. **IACR eprint**.
- **A signature scheme from the finite field isomorphism problem.**
  — *Jeffrey Hoffstein, Joseph H. Silverman, William Whyte, Zhenfei Zhang*
  — MathCrypt 2018. **IACR eprint**, **Slides**.
  — Journal of Mathematical Cryptology. **Journal version**
- **Practical Signatures from the Partial Fourier Recovery Problem Revisited: A Provably-Secure and Gaussian-Distributed Construction.**
  — *Xingye Lu, Zhenfei Zhang, Man Ho Au*
  — ACISP 2018.
- **Optimizing polynomial convolution for NTRUEncrypt.**
  — *Wei Dai, William Whyte, Zhenfei Zhang*
  — IEEE Transaction on Computers. **IACR eprint**, **Source code**.
- **Fully Homomorphic Encryption from the Finite Field Isomorphism Problem.**
  — *Yarkin Doröz, Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, Berk Sunar, William Whyte, Zhenfei Zhang:*
  — PKC 2018. **IACR eprint**.

2017

- **Choosing parameters for NTRUEncrypt**
  — *Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, William Whyte, Zhenfei Zhang*
  — CT-RSA 2017. **IACR eprint**.
- **Round2: KEM and PKE based on GLWR.**
  — *Hayo Baan, Sauvik Bhattacharya, Óscar García-Morchón, Ronald Rietman, Ludo Tolhuizen, Jose Luis Torre-Arce, Zhenfei Zhang*
  — NIST PQC submission. **IACR eprint**.
- **A signature scheme from Learning with Truncation.**
  — *Jeffrey Hoffstein, Jill Pipher, William Whyte, Zhenfei Zhang*
  — Pre-print. **IACR eprint**.
- **Anonymous Announcement System (AAS) for Electric Vehicle in VANETs.**

— *Man Ho Au, Joseph K. Liu, Zhenfei Zhang, Willy Susilo, Jin Li*
— The Computer Journal.

2016

- **Circuit-extension handshakes for Tor achieving forward secrecy in a quantum world.**
  — *John M. Schanck, William Whyte, Zhenfei Zhang*
  — PoPETs 2016. **IACR eprint**, **Tor feature request**, **Source code**.
- **NTRU modular lattice signature scheme on CUDA GPUs.**
  — *Wei Dai, Berk Sunar, John M. Schanck, William Whyte, Zhenfei Zhang*
  — HPCS 2016. **IACR eprint**.

2015 and earlier

- **LLL for ideal lattices: re-evaluation of the security of Gentry-Halevi's FHE scheme.**
  — *Thomas Plantard, Willy Susilo, Zhenfei Zhang*
  — Design, Codes and Cryptography.
- **DA-Encrypt: Homomorphic Encryption via Non-Archimedean Diophantine Approximation.**
  — *Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, William Whyte, Zhenfei Zhang*
  — Pre-print. **IACR eprint**.
- **Fully Homomorphic Encryption Using Hidden Ideal Lattice.**
  — *Thomas Plantard, Willy Susilo, Zhenfei Zhang*
  — IEEE Transation on Information Forensics and Security.
- **Adaptive Precision Floating Point LLL.**
  — *Thomas Plantard, Willy Susilo, Zhenfei Zhang*
  — ACISP 2013.
- **On the CCA-1 Security of Somewhat Homomorphic Encryption over the Integers.**
  — *Zhenfei Zhang, Thomas Plantard, Willy Susilo*
  — ISPEC 2012.
- **Lattice Reduction for Modular Knapsack.**
  — *Thomas Plantard, Willy Susilo, Zhenfei Zhang*
  — SAC 2012.
- **Reaction Attack on Outsourced Computing with Fully Homomorphic Encryption Schemes.**
  — *Zhenfei Zhang, Thomas Plantard, Willy Susilo*
  — ICISC 2011.