Zhenfei Zhang
Ph.D. of Computer Science

Director of Cryptographic Research
OnBoard Security Inc.
zhenfei.zhang@hotmail.com

Biography

2018–present : Director of Cryptographic Research, *OnBoard Security Inc., U.S.*

2017 : Senior Research Scientist, *OnBoard Security Inc., U.S.*

2014–2017 : Research Scientist, *Security Innovation Inc., U.S.*

2010–2014 : Ph.D. Student on Computer Science, *University of Wollongong, Australia*

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

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

2005–2006 : System Engineer, *Tsinghua Tongfang Computer Corporation, China*

2001–2005 : Bachelor Degrees in Computer Science, *BeiHang University, China*

Achievement highlights

- **Standardization**
  - NIST: Lead contributor of **2** candidates to NIST PQC competition
    - NTRUEncrypt public key encryption algorithm;
    - pqNTRUSign digital signature scheme;
  - NIST: Co-contributor of **3** candidates to NIST PQC competition
    - Round2: in collaboration with Phillips;
    - Falcon: in collaboration with IBM, Thales UK, Brown University;
    - LAC: in collaboration with Chinese Academy of science;
  - ETSI: Member of Quantum-safe Cryptography (QSC) working group;
  - ISO: expert member of SC27 working group, U.S. delegate;
  - IETF: Author of **4** Internet Drafts.
- **Selected publications** (full list: see my DBLP page)
  - Journals: IEEE transaction on computers, IEEE Transactions on Information Forensics and Security, ...
  - Conferences: PKC 2018, CT-RSA 2017, PETs 2016, ...
  - Invited talks: Hong Kong Polytech University, Chinese Academic of Science, ...
- **Selected POC software**
  - Importing NTRU to libgcrypt; link.
  - NTRU NIST PQC submission package; link.
  - Fast ring multiplication using AVX-2; improving a factor of 2.23; link
  - Raptor: a lattice based one time linkable ring signature as fast as ECDSA; TBD.

Current Research Interest

- Post Quantum Cryptography
  - Design and improve the state of the art cryptographic algorithms that resist quantum attackers;
  - Use case: TPM - lattice based Direct Anonymous Attestation schemes;
  - Use case: Blockchain - lattice based linkable ring signature schemes.
- Fully Homomorphic Encryption
  - Improve the performance of existing FHE schemes for practical use;
  - Use case: AI - private preserving machine learning algorithms;
  - Use case: Health data - private preserving genome matching and recognition.

Standards

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

Ph.D.

Subject : *Fully Homomorphic Encryption schemes.*

Supervisors: Prof. Willy Susilo - University of Wollongong
: Dr. Thomas Plantard - University of Wollongong.

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

Examiners : Prof. Josef Pieprzyk - Macquarie University, Australia
: Prof. Damien Stehlé - École Normale Supèrieure de Lyon, France

Awards : UPA - University Postgraduate Award, University of Wollongong.

Keywords : Fully Homomorphic Encryption, Cryptography, Lattice theory.

Publications

Practical Signatures from the Partial Fourier Recovery Problem Revisited: A Provably-Secure and Gaussian-Distributed Construction.
Xingye Lu, Zhenfei Zhang and Man Ho Au
Australasian Conference on Information Security and Privacy, 2018

Optimizing polynomial convolution for NTRUEncrypt.
Wei Dai, William Whyte, Zhenfei Zhang
IEEE Transaction on Computers, 2018

Fully Homomorphic Encryption from the Finite Field Isomorphism Problem.
Y. Doroz, J. Hoffstein, J. Pipher, J.M. Schanck, J.H. Silverman, B. Sunar, W. Whyte and Z. Zhang
Public Key Cryptography, 2018

Choosing parameters for NTRUEncrypt
J. Hoffstein, J. Pipher, J.M. Schanck, J.H. Silverman, W. Whyte and Z. Zhang
Cryptographers' Track at the RSA Conference (CT-RSA), 2017

Anonymous Announcement System (AAS) for Electric Vehicle in VANETs
M.H. Au, J.K. Liu, Z. Zhang, W. Susilo, J. Li and J. Zhou
The Computer Journal 2016

Circuit-extension handshakes for Tor achieving forward secrecy in a quantum world
J.M. Schanck, W. Whyte, Z. Zhang
Proceedings on Privacy Enhancing Technologies (PETs), 2016

NTRU modular lattice signature scheme on CUDA GPUs
W. Dai, B. Sunar, J.M. Schanck, W. Whyte, Z. Zhang
High Performance Computing & Simulation (HPCS), 2016

LLL for Ideal Lattice: Re-evaluation of the Security of Gentry-Halevi's FHE Scheme.
T. Plantard, W. Susilo and Z. Zhang
Designs, Codes and Cryptography (DCC).

Fully Homomorphic Encryption Scheme using Hidden Ideal Lattice.
T. Plantard, W. Susilo and Z. Zhang
IEEE Transactions on Information Forensics and Security (TIFS), Nov. 2013.

Adaptive Precision Floating Point LLL
T. Plantard, W. Susilo and Z. Zhang
18th Australasian Conference Information Security and Privacy (ACISP 2013), Lecture Notes in Computer Science, Springer-Verlag, 2013.

Lattice Reduction for Modular Knapsack
T. Plantard, W. Susilo and Z. Zhang
The Conference on Selected Areas in Cryptography (SAC 2012), Lecture Notes in Computer Science, Springer-Verlag, 2012.

On the CCA-1 Security of Somewhat Homomorphic Encryption over the Integers
Z. Zhang, T. Plantard and W. Susilo
The 8th International Conference on Information Security Practice and Experience (ISPEC 2012), Lecture Notes in Computer Science 7232, Springer-Verlag, pp. 353 - 368, 2012.

Reaction Attack on Outsourced Computing with Fully Homomorphic Encryption Schemes
Z. Zhang, T. Plantard and W. Susilo
The 14th International Conference on Information Security and Cryptology (ICISC 2011), Lecture Notes in Computer Science, Springer-Verlag, 2011.

Pre-prints

Raptor: a lattice based one-time linkable ring signature
To appear

On the Hardness of the Computational Ring-LWR Problem and its Applications
Long Chen, Zhenfeng Zhang, Zhenfei Zhang
IACR Cryptology ePrint Archive 2018, 536

Round2: KEM and PKE based on GLWR.
H. Baan, S. Bhattacharya, Ó. García-Morchón, R. Rietman, L. Tolhuizen, J. L. Torre-Arce, Z. Zhang
IACR Cryptology ePrint Archive 2017, 1183

A signature scheme from Learning with Truncation.
J. Hoffstein, Jill Pipher, W. Whyte and Z. Zhang
IACR Cryptology ePrint Archive 2017, 995

A quantum-safe circuit-extension handshake for Tor.
J.M. Schanck, W. Whyte, Z. Zhang
IACR Cryptology ePrint Archive 2015, 287

DA-Encrypt: Homomorphic Encryption via Non-Archimedean Diophantine Approximation-Preliminary Report.
J. Hoffstein, J. Pipher, J.M. Schanck, J.H. Silverman, W. Whyte, Z. Zhang
IACR Cryptology ePrint Archive 2015, 844