Jingwei Hu – Curriculum Vitae

Address SPMS-MAS 04-21,
School of Physical and Mathematical Sciences,
Nanyang Technological University,
Singapore

Telephone +(65) 8730 3610

Email davidhu@ntu.edu.sg

Research Interests

Embedded Cryptographic Hardware, Side Channel Security, Post-quantum Cryptography, Fully Homomorphic Encryption

Education

2014-2018 Ph.D., Electronic Engineering - City University of Hong Kong, Hong Kong

2011-2014 M.Eng., Computer Engineering - Tianjin University, Tianjin, China

2007-2011 B.Sc., Electronic Engineering - Dalian Maritime University, Dalian, China

Employment History

May 2018 - Now Division of Mathematical Sciences, Nanyang Technological University, Singapore
Postdoctoral Research Fellow
Participated in system design and security for post-quantum cryptography and fully homomorphic encryption.

Sep 2017 - Apr 2018 Department of Electronic Engineering, City University of Hong Kong, Hong Kong
Research Assistant
Participated in the algorithm and hardware design for code-based cryptography.

Apr 2014 - Aug 2014 Department of Electronic Engineering, City University of Hong Kong, Hong Kong
Research Assistant
Participated in the ASIC/FPGA design of finite field arithmetic for public-key cryptography.

Research Activity

Jul 2016 - Nov 2016 Mathematics/Computer Science Section, Universität Bremen, Bremen, Germany
Visiting Student
Performed research work on exploring efficient hardware and algorithm design for code-based cryptography.

Research Projects

Accelerating Homomorphic Encryption, *Agency for Science, Technology, and Research, Singapore.*

New Post-Quantum Cryptographic Constructions, Singapore Ministry of Education under Research Grant, *No.MOE2016-T2-2-014(S)*

Side-Channel Resistance of Secure Processor Architecture, *Germany/HK Joint Research Scheme, No.9053016*

Novel security Architectures and Methods for Internet of Things, *Early Career Scheme, No.9041799*

Efficient Public-key Cryptography using Spectral Arithmetic and Residue Number Systems, *CityU Strategic Research Grant, No.7008185*

Teaching Experience

2019-2020, Fall Bachelor Degree Program, Division of Mathematical Sciences, Nanyang Technological University
Teaching Assistant (with Prof. Huaxiong Wang and Prof. Jian Guo)
MH1812: Discrete Mathematics

2016, Fall Bachelor Degree Program, Department of Electronic Engineering, City University of Hong Kong
Teaching Assistant (with Mr. Van Ting)
EE4216: Internet Client-server Computing

2015, Fall Bachelor Degree Program, Department of Electronic Engineering, City University of Hong Kong
Teaching Assistant (with Prof. Ray Cheung)
EE2311: Object-Oriented Programming and Design

Academic Award

2020 the 9th Global Young Scientists Summit Nomination, Prime Minister Office, Singapore

2019 3rd Place Winner, CRCR Cryptologic Algorithm Design Competition, China

2017 Outstanding Academic Performance Award, City University of Hong Kong, Hong Kong

2009 National Scholarship Award, Ministry of Education, China

Publications

Journal Papers:
Jingwei Hu, Yao Liu, Ray C.C. Cheung, Bhasin Shivam, Ling San, and Huaxiong Wang. "Compact Code-based Signature for Reconfigurable Devices with Side Channel Resilience."[J] *IEEE Transactions on Circuits and System I,* 2020. LINK

Jingwei Hu, Marco Baldi, Paolo Santini, Neng Zeng, Ling San, and Huaxiong Wang. "Lightweight Key Encapsulation Using LDPC Codes on FPGAs."[J] *IEEE Transactions on Computers,* 2019. LINK

Jingwei Hu, and Ray C.C. Cheung. "Towards Practical Code Based Signature: Implementing Fast and Compact QC-LDGM Signature Scheme on Embedded Hardware."[J] *IEEE Transactions on Circuits and System I,* 2017. LINK

Jingwei Hu, and Ray C.C. Cheung. "Area-Time Efficient Computation of Niederreiter Encryption on QC-MDPC Codes for Embedded Hardware."[J] *IEEE Transactions on Computers,* 2017. LINK

Jingwei Hu, Ray C.C. Cheung, and Tim Güneysu. "Compact Constant Weight Coding Engines for the Code Based Cryptography."[J] *IEEE Transactions on Circuits and System II,* 2017. LINK

Jingwei Hu, Wei Guo, Jizeng Wei, and Ray C.C. Cheung. "Fast and Generic Inversion Architectures Over $GF(2^m)$ Using Modified Itoh-Tsujii Algorithms."[J] *IEEE Transactions on Circuits and System II,* 2015. LINK

Jingwei Hu, Wei Guo, Jizeng Wei, and Ray C.C Cheung. "A scalable RNS Montgomery multiplier over F2m."[J] *IEICE Electronics Express,* 2013. LINK

Wei Guo, **Jingwei Hu**, Weiji Zeng. "A TTA-like Processor for Fast RSA Key Generation Using RNS."[J] *Journal of Computers,* 2013, 8(1): 33-40.LINK

Conference Papers:

Jingwei Hu, Wen Wang, Ray C.C. Cheung, and Huaxiong Wang, "Optimized Polynomial Multiplier over Commutative Rings on FPGAs. A Case Study on BIKE"[C] *International Conference on Field-Programmable Technology (FPT'19)* 2019.LINK

Liping Wang and **Jingwei Hu**, "Two new module-code-based KEMs with rank metric"[C] *The 24th Australasian Conference on Information Security and Privacy (ACISP'19),* 2019. LINK

Jingwei Hu, Wangchen Dai, Yao Liu, and Ray C.C. Cheung. "An Application Specific Instruction Set Processor (ASIP) for the Niederreiter Cryptosystem"[C] *International Symposium on Digital Forensic and Security,* 2018. LINK

Jingwei Hu, Wei Guo, et al. "A novel architecture for fast RSA key generation based on RNS."[C] *Fourth International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), IEEE,* 2011.LINK

Book Chapters:

Jingwei Hu, and Ray C.C. Cheung. "A new approximation method for constant weight coding and its hardware implementation"[B] *Recent Advances in Cryptography and Network Security, InTechOpen,* 2018.