WENHAO WANG

(+86)15210983075 ⋄ wangwenhao@iie.ac.cn

EDUCATION

University of Chinese Academy of Sciences *Sept. 2009 - Jan. 2015*
Ph.D. in Information Security

Ocean University of China *Sept. 2005 - July 2009*
B.E. in Computer Science and Technology

WORK EXPERIENCE

Institute of Information Engineering, CAS *Since Dec. 2018*
Research Associate Professor

Indiana University Bloomington *Apr. 2016 - Aug. 2018*
Visiting Researcher

Institute of Information Engineering, CAS *Feb. 2015 - Dec. 2018*
Research Assistant Professor

SELECTED PUBLICATIONS IN 5 YEARS

- (Manuscript) *Toward Scalable Fully Homomorphic Encryption Through Light Trusted Computing Assistance.* ***Wenhao Wang***, Yichen Jiang, Qintao Shen, Weihao Huang, Hao Chen, Shuang Wang, XiaoFeng Wang, Haixu Tang, Kai Chen, Kristin Lauter, Dongdai Lin
- *Enabling Rack-scale Confidential Computing using Heterogeneous Trusted Execution Environment.* Jianping Zhu, Rui Hou, XiaoFeng Wang, ***Wenhao Wang***, Jiangfeng Cao, Boyan Zhao, Zhongpu Wang, Yuhui Zhang, Jiameng Ying, Lixin Zhang, Dan Meng. 2020 IEEE Symposium on Security and Privacy (***S&P***) (to appear, CCF-A).
- *Bluethunder: A 2-level Directional Predictor Based Side-Channel Attack against SGX.* Tianlin Huo, Xiaoni Meng, ***Wenhao Wang***, Chunliang Hao, Pei Zhao, Jian Zhai, Mingshu Li. IACR Transactions on Cryptographic Hardware and Embedded Systems (***CHES'2020***) (CCF-B, *Corresponding Author*)
- *Beware of Your Screen: Anonymous Fingerprinting of Device Screens for Off-line Payment Protection.* Zhe Zhou, Di Tang, ***Wenhao Wang***, XiaoFeng Wang, Zhou Li, Kehuan Zhang. Annual Computer Security Applications Conference (***ACSAC'2018***) (CCF-B)
- *Symbolic-Like Computation and Conditional Differential Cryptanalysis of QUARK.* Jingchun Yang, Meicheng Liu, Dongdai Lin, ***Wenhao Wang***. 13th International Workshop on Security (***IWSEC'2018***) (CCF-C)
- *Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery.* Meicheng Liu, Jingchun Yang, ***Wenhao Wang***, Dongdai Lin. 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (***Eurocrypt'2018***) (CCF-A)
- *Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races.* [Guoxing Chen, ***Wenhao Wang***], Tianyu Chen, Sanchuan Chen, Yinqian Zhang, XiaoFeng Wang, Ten-Hwang Lai, Dongdai Lin. 2018 IEEE Symposium on Security and Privacy (***S&P***) (CCF-A, Co-first Author & Corresponding Author)
- *iDASH secure genome analysis competition 2017.* XiaoFeng Wang, Haixu Tang, Shuang Wang, Xiaoqian Jiang, ***Wenhao Wang***, Diyue Bu, Lei Wang, Yicheng Jiang, Chenghong Wang. ***BMC Medical Genomics 2018***

- *Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX.* ***Wenhao Wang***, Guoxing Chen, Xiaorui Pan, Yinqian Zhang, XiaoFeng Wang, Vincent Bindschaedler, Haixu Tang, Carl A. Gunter. ***ACM CCS 2017*** (CCF-A, First Author)
- *Binary Code Retrofitting and Hardening Using SGX.* Shuai Wang, ***Wenhao Wang***, Qinkun Bao, Pei Wang, XiaoFeng Wang, Dinghao Wu. 2nd Workshop on Forming an Ecosystem Around Software Transformation, 2017, co-located with CCS 2017.
- *Searching Cubes for Testing Boolean Functions and Its Application to Trivium.* Meicheng Liu, Dongdai Lin, ***Wenhao Wang***. 2015 IEEE International Symposium on Information Theory. (IIE-B)

PROFESSIONAL SERVICES

- Reviewer for journals *CyberSecurity*, *SCN*, *JNCA*.
- Sub-reviewer for *CCS* (2018), *NDSS* (2017, 2018), *S&P* (2017), *Usenix Security* (2017, 2018), *HPCA* (2019), *ESORICS* (2018), *AsiaCCS* (2017, 2018, 2019) and *RECOMB* (2019) etc.
- TPC member for *ACM CCS 2019*.

AWARDS

- 2018 ACM SIGSAC China Rising Star Award, and ACM China Rising Star Nomination Award
- 2017 Young Star Award of Institute of Information Engineering, CAS

TALKS

- *Confidential Computing, in Chinese.* China Conference on Data Security and Privacy (ChinaPrivacy2019), Oct. 2019, Guilin
- *Confidential Computing, in Chinese.* Nankai University, July 2019, Tianjin
- Institute of Software, July 2019, Beijing
- *Side Channel Risks in Hardware Trusted Execution Environments (TEEs).* ACM TURC 2019 (SIGSAC), May 2019, Chengdu
- *Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX.* ACM CCS 2017, Nov. 2017, Dallas