Wenhao Wang

No. 89A Minzhuang Road
Haidian District, Beijing 100093
Mobile: (+86) 15210983075
wangwenhao@iie.ac.cn
Homepage: **https://heartever.github.io/**

I am a research assistant professor at Institute of Information Engineering (IIE). I have been visiting Prof. XiaoFeng Wang's group in Indiana University Bloomington since April 2016. My research interests now focus on protecting user privacy data with the help of hardware features, such as Intel SGX. I also work closely with Prof. Wang and Prof. Haixu Tang in organizing the Genomic data privacy and security protection competition (http://www.humangenomeprivacy.org/2017).

EDUCATIONAL BACKGROUND

- Ph.D. in Information Security, University of Chinese Academy of Sciences *Jan 2015*
  Dissertation Title: Optimization of time memory tradeoff algorithms
  Abstract: Time memory tradeoff, a generic method to invert one-way functions, is widely used in password cracking applications. The dissertation shows how to obtain optimized parameters based on theoretical analysis of tradeoff coefficient with different parameter sets. A prototype system to verify the theoretical results is also built.
- B.E. in Computer Science and Technology, Ocean University of China *July 2009*
  Rank: 1st of 33. *Thesis*: A design of travelling path recommendation system in railway networks
  Abstract: Design and implementation of a user-friendly path recommendation system. It integrated a weighted Dijkstra algorithm with a database based representation of railway timetables from all over the country. It is the primary part of the work under the National Undergraduates Innovative Experimentation Project.

SELECTED PUBLICATIONS

- (EuroCrypt 2018) Meicheng Liu, Jingchun Yang, **Wenhao Wang**, Dongdai Lin. Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery. Proceeding of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques. (acceptance rate: 23%, CCF-A)
- (S&P 2018) Guoxing Chen, **Wenhao Wang (co-first author, corresponding author)**, Tianyu Chen, Sanchuan Chen, Yinqian Zhang, XiaoFeng Wang, Ten-Hwang Lai, Dongdai Lin. Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races. 2018 IEEE Symposium on Security and Privacy. (acceptance rate: ~10%, CCF-A)
- (CCS 2017) **Wenhao Wang**, Guoxing Chen, Xiaorui Pan, Yinqian Zhang, XiaoFeng Wang, Vincent Bindschaedler, Haixu Tang, Carl A. Gunter. Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX. ACM Conference on Computer and Communications Security (acceptance rate: 18%, CCF-A).

- (FEAST 2017) Shuai Wang, **Wenhao Wang**, Qinkun Bao, Pei Wang, XiaoFeng Wang, and Dinghao Wu. Binary Code Retrofitting and Hardening Using SGX. In the 2nd Workshop on Forming an Ecosystem Around Software Transformation, 2017, co-located with CCS 2017.
- (ISIT 2015) Meicheng Liu, Dongdai Lin, **Wenhao Wang**. Searching Cubes for Testing Boolean Functions and Its Application to Trivium. In Proc. of 2015 IEEE International Symposium on Information Theory.
- **Wenhao Wang**, Meicheng Liu, Yin Zhang. Comments on "A design of Boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation". Cryptography and Communications.
- (ICICS 2013) **Wenhao Wang**, Dongdai Lin. Analysis of Multiple Checkpoints in Non-perfect and Perfect Rainbow Tradeoff Revisited. In Proc. of the 15th International Conference on Information and Communications Security. (acceptance rate: 20%)
- (ICICS 2011) **Wenhao Wang**, Dongdai Lin, Zhenqi Li, Tianze Wang. Improvement and Analysis of VDP Method in Time/Memory Tradeoff Applications. In Proc. of the 13th International Conference on Information and Communications Security. (acceptance rate: 23%)

Work Experience

APR 2016 – PRESENT

Visiting Researcher / Indiana University, Bloomington

FEB 2015 – PRESENT

Research Assistant Professor / Institute of Information Engineering, Chinese Academy of Sciences

MAY 2012 – JAN 2015

Research Assistant / Institute of Information Engineering, Chinese Academy of Sciences

SEPT 2009 – APR 2012

Research Assistant / Institute of Software, Chinese Academy of Sciences

SELECTED ENGINEERING PROJECTS

JAN 2014 ~ JAN 2015

GPU-based Distributed Computing Platform (*primary developer*)

Responsibility: Build the communication framework for a server *scheduler* process and a client *computer* process.

AUG 2013 ~ OCT 2013

Supportive platform for GPU-based password cracking (*sole developer*)

Responsibility: Investigate and implement in c# various password-based authentication algorithms.

SEP 2009 ~ MAY 2010

GnoMoN: a cryptographic computer algebra system (*primary developer*)

Responsibility: Build the user command parsing module using lex/yacc and c++.

TECHNICAL SKILLS

- *Programming languages*: C/C++, C#, SQL, Linux Shell, GPU kernel
- *Professional knowledge:* Applied cryptography, Stream cipher, Cryptanalysis, Boolean function, Password cracking method

MISCELLANY

- *Honors*: National Scholarship (< 3%, 3 times), Outstanding Graduates (3%), Merit Student (5%), etc.
- *Academic activities*: External reviewer of conferences, including Asiacrypt, ESORICS, AsiaCCS, etc.
- *Personal hobbies:* Climbing, Basketball, Badminton, etc.
- *Self-evaluation:* High sense of responsibility, Self-motivation, Willing to learn and progress