Rui **WEN**

Born In Zhejiang, China, In 1997

Stuhlsatzenhaus 5, 66123 Saarbrücken, Germany

(+49) 015223666727 | s8ruwenn@stud.uni-saarland.de | wenruiustc.github.io

"Heaven is under our feet as well as over our heads."

Education

CISPA & Saarland University — *Saarbrücken, Germany*

Ph.D. Preparatory phase in Computer Science — *Oct. 2019 - PRESENT*

University of Science and Technology of China (USTC) — *Hefei, China*

B.S. in Applied Physics — *Sep. 2015 - Jun.2019*

Experience

PlatON, Intern — *Apr, 2019-May, 2019*

Supervisor: Dr. Xiang Xie — *PlatON, Shanghai, China*

- Implemented a *2-party Ed25519 Signature Scheme* using C.
- The machine learning algorithm based on privacy preserving technology is studied, and more specifically, *GBDT* algorithm is considered to be implemented using *Fully Homomorphic Encryption* and the possibility of further optimization will be considered.

Secure Search via Fully Homomorphic Encryption (Bachelor Thesis) — *Nov, 2018-Apr, 2019*

Supervisor: Prof. Yu Yu — *SJTU, Shanghai, China*

- Proposed a new *secure search* protocol based on *(Leveled) Fully Homomorphic Encryption*, advanced one major step forward in making *secure search* practical, this work has been summarized in a paper that is expected to be published soon.
- Studied *FHE* schemes based on ideal lattice, integer, RLWE and LWE, studied existing *secure search* algorithms and some relevant variants like *PSI*, *PIR*.

Security Evaluation of LWE-based Cryptosystem — *Jul, 2018-Sep, 2018*

Supervisor: Prof. Tsuyoshi Takagi — *The University of Tokyo, Tokyo, Japan*

- Studied the commonly used lattice reduction algorithms, among them, "*dimensions for free*" technique is specially studied, which plays an important role in the solution of the *uSVP* problem and the improvement of the sieving algorithm.
- Studied the difficulty of the LWE problem and attack methods such as "*Reducing BDD to uSVP*", "*Decoding Attack*" and "*BKW*" etc. Evaluated the impact of parameters selection on system security in LWE-based cryptosystems.
- The key exchange schemes based on the LWE problem were studied, such as *NewHope*, *Ding's key exchange protocol*.

Design of FPGA-based Ultrahigh Accuracy TDC — *Aug, 2017-Oct, 2017*

Supervisor: Lei Zhao — *USTC, Hefei, China*

- Utilized the internal timing structure of the FPGA (delay line) to improve the accuracy of *TDC* with rough-fine timing technology.
- The standard time pulse signal is used for calibration, and *INL* and *DNL* indexes of *TDC* are calculated, and the nonlinear degree of *TDC* is further reduced by programming.

Skills

Programming Python, C/C++, Matlab, Mathematica, LaTeX

Languages Chinese(native), English(independent user), Japanese(beginner)

Presentation

An introduction to cryptography, FHE and its applications — *Tsinghua Univ., Beijing, China*

Cooperated with professor Yu Yu and his team members — *Apr. 2019*

- Introduced FHE based privacy-preserving search

Honors & Awards

2018 **Excellent Student Scholarship,** *Hefei, China*

2017 **Endeavor Scholarship,** *Hefei, China*

2015 **Freshman Scholarship,** *Hefei, China*