Jinming (Jamie) Cui

jamie.cui@outlook.com

(+86) 13261602458

Github: Jamie-Cui

Linkedin: Jamie Cui

Education

- **University of Edinburgh** — Edinburgh, UK
  MSc. Computer Science — *2017 - 2018*
    - Thesis: A Bitcoin Wallet Implementation using Trusted Execution Environment
      Supervisor: Dr. Myrto Arapinis
    - Realated Courses: Introduction to Modern Cryptography, Blockchains and Distributed
      Ledgers, Computer Security, Secure Programming

- **Queen Mary University of London** — London, UK
  BSc.(Engineering) Telecommunications Engineering with Management — *2013 - 2017*
    - Thesis: Measurement Study of live video streaming infrastructure in China
      Supervisor: Dr. Felix Cuadrado

Experience and Projects

- **BGI Research** — Shenzhen, China
  Mid-level Software Engineer (Full-time) — *Jan 2019 - Present*
    - Researched privacy and security issues in genetic data lifecycle.
    - Designed and developed cryptographic part of biostatistics analysis software using start-of-art
      Multiparty Computation Frameworks (C++). The software is currently used by Chinese
      National Gene Bank.
    - Designed and developed a practical random forest training protocol based on MPC and a
      practical hybrid privacy-preserving system.
    - Participated in IEEE "Federated Machine Learning" Standard drafting.

- **Privacy-Preserving Computation over Genetic data** — IJCAI 19' workshop
  Research project, BGI Research — *August 2019*
    - This work uses MPC to address the privacy issues in conventional genetic computation. It
      provides a privacy-preserving solution for Human Leukocyte Antigen (HLA) matching and two
      popular biostatistics tests: χ^2 test and odds-ratio test.
    - This work produces a user-friendly software.

- **Boosting Paillier Encryption to Support Degree-2 Evaluation**
  Self project — *Sep 2018 - Oct 2018*
    - This project implements paper: "Boosting Paillier Encryption Function to Support Degree-2
      Homomorphic Encryption"
    - Project URL: https://github.com/Jamie-Cui/Degree-2-Homomorphic-Paillier

- **Bitcoin Wallet Implementation based on TEE**
  Master's thesis, University of Edinburgh — *June 2018 - Aug 2018*
    - This project aims to develop a bitcoin wallet android application which uses Trusted
      Execution Environment(TEE) to secure the application. The implementation takes advantages
      of GlobalPlatfrom APIs including secure storage, secure operation etc. and further uses Java
      Native Interface to establish a communication between C-side implementation(CA and TA)
      and Java-side implementation(Android app).

- This project is the first attempt to build a high-level android bitcoin wallet app compliant with BIP39 and BIP32 standards (enables HD wallet). And also it gives an analysis of using Trusted User Interface to secure user interactions to provide more security.
    - Project URL: https://github.com/Jamie-Cui/bitcoin-wallet-using-TEE
- **Measurement Study of live video streaming infrastructure in China**
  Bachelor's thesis, Queen Mary University of London
    - The project aims to perform a measurement study to foot print the infrastructure from the most popular Chinese platform (Douyu.com). This study involves estimating the size of the infrastructures, as well as its geographical location and server selection strategies. In order to successfully locate the infrastructure, this project uses a combination of active measurement and networking techniques including ip-to-location, DNS-based name resolution and address space exploration.

Awards and Certificates

- Aug 2014, **Third Class National Scholarship (National Level)**.

- Nov 2014, **Outstanding Volunteer of International School (University Level)**.

- Nov 2015, **Second Prize for China College Students' "Internet+" Innovation Competition (National Level)**.
  — Project name: An Intelligent Web Robot Application based on Unity 3D

- Oct 2019, **NIGMS and PlatON Award for 2019 IDASH Genome Privacy & Security Competition**.

Knowledges and Skills

- **Knowledges in following areas:** Secure Multiparty Computation, Oblivious Transfer, Homomorphic Encryption, Blockchains, Anonymous System, General Computer Security, Computer Networking.

- **Programming Languages and Tools:** C/C++ (3-year experience), Linux (2-year experience), Java (2-year experience), Python (1-year experience), Bash (1-year experience), Latex.

References

- Dr. Myrto Arapinis (Tutor and Supervisor)
  Lecturer in Computer Security School of Informatics
  University of Edinburgh
  Tel: +44 (0) 131 650 9981
  Email: marapini@inf.ed.ac.uk