Xianrui **Qin**

(+852) 67694764 | xrqin@cs.hku.hk | xrqin.github.io | @Qinxrr

Research Interest

Cryptography

- Zero knowledge proof, Multiparty computation, Privacy-preserving primitives and protocols

Blockchain

- ZKRollup, Payment Channel, Confidential Transactions

Educational Background

Shandong University

Sep. 2015 - Jun. 2019

- Major: Mathematics (Bachelor Degree)

The University of Hong Kong

Sep. 2019 - Aug. 2023

- Computer Science (PhD)
- supervisor:Tsz Hon Yuen (Primary), Siu Ming Yiu

Research Experience

Nanyang Technological University

Research Assistant *Sep. 2018 - Dec. 2018*

- Learned boomerang connectivity table (a new cryptanalysis tool) under the guidance of Professor GUO JIAN.
- Output:
  Song Ling, Qin Xianrui, Lei Hu. Boomerang Connectivity Table Revisited and Application to SKINNY and AES

Monash University

Visiting Student *Feb. 2023 - May. 2023*

- Investigate more efficient blockchcain layer-2 protocol under the guidance of Professor Joseph K. Liu.

Skills & Language

Computer	Proficient in C language, C++, Python, Rust
English	Fluent
Cantonese	Native
Mandarin	Native

Publication

Robust Publicly Verifiable Covert Security: Limited Information Leakage and Guaranteed Correctness with Low Overhead

Yi Liu, Junzuo Lai, Qi Wang, **Xianrui Qin**, Anjia Yang, Jian Weng

- *Asiacrypt 2023*
- Key Point: We propose a multiparty computation solution where even if the misbehavior remains undetected, the malicious party can only gain an additional 1-bit of information about the honest party's input while maintaining the correctness of the output.

BlindHub: Bitcoin-Compatible Privacy-Preserving Payment Channel Hubs Supporting Variable Amounts

Xianrui Qin, Shimin Pan, Arash Mirzaei, Zhimei Sui, Oguzhan Ersoy, Amin Sakzad, Muhammed Esgin, Jiangshan Yu, Joseph K. Liu, Tsz Hon Yuen

- *IEEE S&P 2023*
- Key Point: payment channel hubs (PCH) constitute a promising solution to the inherent scalability problem of blockchain technologies, but all the current bitcoin-compatible PCH protocols require the amount to be fixed. In this paper, we give the first solution to overcome this limitation.

Monet: A Fast Payment Channel Network for Scriptless Cryptocurrency Monero

Zhimei Sui, Jiangshan Yu, Joseph K. Liu, **Xianrui Qin**

- *ICDCS 2022*
- Key Point: we propose the first bi-directional payment channel network with unlimited lifetime for Monero, which is the most capitalized privacy-preserving cryptocurrency.

Tight Leakage-Resilient Identity-based Encryption under Multi-challenge Setting

Cailing Cai, **Xianrui Qin**, Tsz Hon Yuen

- *ASIACCS 2022*

One-more Unforgeability of Blind ECDSA

Xianrui Qin, Cailing Cai, Tsz Hon Yuen

- *ESORICS 2021*
- Key Point: we propose the first formal security proof for Blind ECDSA, which can be used to build blind coinswaps or trustless tumbler services for cryptocurrencies like Bitcoin or Ethereum.

Security on SM2 and GOST Signatures against Related Key Attacks

Handong Cui,**Xianrui Qin**, Cailing Cai, Lei Hu

- *TrustCom 2021*
- Key Point: We analysis the security on SM2 and GOST Signatures against Related Key Attacks.

Boomerang Connectivity Table Revisited

Ling Song,**Xianrui Qin**,Lei Hu

- *FSE 2019*
- Key Point: we propose a generalized framework of boomerang connectivity table, which can better evaluate the probability of boomerang attack.