

SHIYU LI

tkp2ra@virginia.edu

+1 (434) 3658517

<https://shiyuuli.github.io>

RESEARCH SUMMARY

My research spans both theoretical and applied cryptography. On the theoretical side, I am particularly interested in impossibility results that can identify the limits of cryptographic techniques and guide the design of constructions. On the applied side, I have experience on privacy-preserving protocols for distributed systems.

EDUCATION

University of Virginia

Ph.D. student in Computer Science

Advisor: Prof. Wei-Kai Lin

Sept. 2024 - present

University of Electronic Science and Technology of China

M.Eng. in Cyber Security

Advisor: Prof. Yuan Zhang

Thesis: Secure and Portable Data Sharing in Untrusted Environment

Sept. 2021 - Jun. 2024

GPA: 3.75/4.00

University of Electronic Science and Technology of China

B.Eng. in Information Security

Sept. 2017 - Jun. 2021

GPA: 3.87/4.00

PUBLICATIONS & MANUSCRIPTS

Publications marked with * use contribution-based author ordering. For unmarked publications, authors are listed alphabetically.

- [1] Public-Key PIR à la Merkle (Manuscript)
Shiyu Li, Wei-Kai Lin, and Ethan Mook.
- [2] On the Limitations of Relativized Succinct Arguments in Many Oracle Worlds (Manuscript)
Shiyu Li and Wei-Kai Lin.
- [3] Lower Bounds on Inner-Product Functional Encryption from All-or-Nothing Encryption Primitives
Jinye He, **Shiyu Li**, and Wei-Kai Lin.
In Theory of Cryptography (TCC), 2025.
https://link.springer.com/chapter/10.1007/978-3-032-12293-3_5
- [4] EpiOracle: Privacy-Preserving Cross-Facility Early Warning for Unknown Epidemics*
Shiyu Li, Yuan Zhang, Yaqing Song, Kan Yang, Fan Wu, Feng Lyu, and Qiang Tang.
In Proceedings on Privacy Enhancing Technologies (PETS), 2025.
<https://petsymposium.org/popets/2025/popets-2025-0020.pdf>, [Prototype] in Java
- [5] Beyond Security: Achieving Fairness in Mailmen-Assisted Timed Data Delivery*
Shiyu Li, Yuan Zhang, Yaqing Song, Hongbo Liu, Nan Cheng, Hongwei Li, and Kan Yang.
IEEE Transactions on Information Forensics and Security (TIFS), 2024.
<https://doi.org/10.1109/TIFS.2024.3416049>, [Prototype] in Python

RESEARCH EXPERIENCE

Public-Key PIR from Symmetric-Key Cryptography [1]

Mentor: Wei-Kai Lin

Private information retrieval (PIR) allows a client to efficiently retrieve a database entry from a server without revealing which entry it wants. Existing PIR schemes rely on computationally expensive public-key primitives like fully homomorphic encryption (FHE). Can we construct PIR using only lightweight symmetric-key primitives?

We construct a variant of PIR called public-key PIR (pk-PIR) using only symmetric-key primitives. Our construction achieves fine-grained security: an adversary must expend substantially more computational effort to compromise security than the honest parties.

Separating IPFE and All-or-Nothing Encryptions [3]

Mentor: Wei-Kai Lin

A functional encryption (FE) is a versatile encryption, where a ciphertext generated by FE can be decrypted using different functional keys to reveal specific functions of the underlying plaintext. Which cryptographic primitives are sufficient to construct an FE?

This work proves negative results: FEs cannot be implied by many encryption primitives that are “all-or-nothing”, such as fully homomorphic encryption (FHE), identity-based encryption (IBE), attribute-based encryption (ABE), and predicate encryption (PE).

Our results rule out a broad class of constructions based solely on all-or-nothing encryption primitives like FHE, demonstrating the necessity of different techniques for functional encryption constructions.

Privacy-Preserving Early Epidemic Warning [4]

Mentor: Yuan Zhang, Kan Yang

Early warning systems for unknown epidemics monitor the frequencies of similar symptom lists across healthcare facilities to detect potential outbreaks. However, existing cloud-assisted systems expose sensitive symptom data and frequency statistics to the cloud. Can we enable cross-facility epidemic detection without compromising privacy?

Proposed EpiOracle, a privacy-preserving protocol supporting similarity detection over encrypted symptom lists and confidential frequency aggregation. It uses only lightweight symmetric-key primitives.

Independently implemented a [\[Java Prototype\]](#) and received the [PETS Reproduced artifact badge](#). Evaluated on 200 real-world and 2,000 synthetic COVID-19 symptom lists, grouping ~70% and ~68% of the lists as similar under the tested configurations, respectively.

Impossibilities of Relativized SNARG [2]

Mentor: Wei-Kai Lin

A relativized SNARG is a SNARG in an oracle world: the language, prover, and verifier may all query the oracle. Compared with plain non-relativized SNARGs, relativized ones work better with recursive composition. It is known that relativized SNARGs do not exist in the random oracle model. But can they exist in stronger oracle models like Shoup’s generic-group model and black-box obfuscation?

We prove that relativized SNARGs do not exist in many natural and well-studied oracle worlds, including Shoup’s generic-group model and black-box obfuscation.

Our results show the limitations of generic relativized SNARG constructions, which provide motivation for designing SNARG-friendly cryptographic algorithms, such as FHE bootstrapping tailored for efficient SNARG proving.