Research Statement

Haiyang Xue
School of Computing and Information Systems, Singapore Management University
Tel: (65) 6828-1367; Email: haiyangxue@smu.edu.sg
19/Dec/2024

Background

My research interests lie in the field of cryptography, with a particular focus on addressing real-world security and privacy issues using cryptographic tools.

Throughout my research in this domain, I have become increasingly aware of a significant gap that exists between the theoretical aspects of cryptography and the practical challenges faced in the broader realm of cybersecurity. This gap often comes from the complex nature of cryptographic algorithms and the difficulty in using them in a way that is both secure and user-friendly for real-world applications. Cryptography is rich with elegant solutions and proofs of security that are based on mathematical hardness assumptions. These solutions, however, are often abstract and not directly applicable to the practical scenarios. For example, while a cryptographic protocol might be provably secure in a theoretical model, its implementation with tiny modification by non-expert may be vulnerable, or it might not be compatible with existing systems due to bad performance.

My research goal is to bridge this gap by developing innovative cryptographic solutions. In pursuit of this goal, I aim to establish an active research team consisting of graduate students and research fellows, dedicated to conducting impactful research in the field of cryptography and cybersecurity.

Research Areas

The following is an overview of my research on (1) post-quantum cryptography; (2) threshold cryptography (a.k.a. distributed cryptographic schemes); and (3) authenticated key exchange.

A. Post-quantum Cryptography

In recent years, the implementation of quantum computers has made significant progress. However, this has been bad news for cryptographers as these machines have the potential to efficiently break deployed public key cryptosystems in real-world systems, such as RSA and elliptic curve cryptography used in the TLS protocol suite. To address this threat, governments and cryptographers have made great efforts to design post-quantum cryptographic schemes that remain secure even of quantum computers are available. The post-quantum cryptography standardization[1] process held by the National Institute of Standards and Technology (NIST) has had the greatest impact in this regard.

I have made some contributions to the field of post-quantum cryptography for long-term cyber security. We designed a lattice-based cryptosystem [LAC'18], called LAC, which was a second-round candidate in NIST's standardization process and was awarded 1st prize in the Chinese post-quantum cryptography competition [LAC.PK'20]. It is worth highlighting that Kyber, the algorithm selected by NIST for standardization, adopted the modulus choice presented in our paper [Ins'18, AC'18].

B. Threshold Cryptography

Threshold cryptography is concerned with the ability to distribute cryptographic operations across multiple servers to address the problem of a single-point-of-failure. For instance, the

[1] https://csrc.nist.gov/projects/post-quantum-cryptography

loss of a secret key in blockchain-based cryptocurrencies can result in financial loss, and threshold ECDSA can enhance wallet security by distributing the secret key. The significance of threshold cryptography is evidenced by the upcoming call for multi-party threshold cryptography[2] by NIST.

However, designing secure threshold cryptography, such as threshold ECDSA, is not an easy task and often involves complicated tools. To address this problem, in [CCS'21], we conducted research to propose an online-friendly two-party ECDSA signature with the best offline performance. In addition, we [CCS'23] identified the multiplicative to additive functionality (MtA) as the most complex aspect and gave a better MtA from Joye-Libert cryptosystem. Recently, we also optimize the zero-knowledge proof for Paillier cryptosystem which is useful for threshold ECDSA. Our work was published in ACM CCS 2021, 2023, and 2024, top security conferences, respectively, and has real-world impact.

C. Authenticated Key Exchange

Authenticated key exchange (AKE) provides security guarantees for a wide variety of Internet protocols, including TLS, SSH, and others. However, prior to our work, constructing a secure AKE was considered to be complicated and error-prone, often resulting in vulnerabilities. To address this issue, we proposed a framework for designing AKE that not only encompasses celebrated works but also offers new constructions with the best performance based on new assumptions. Our research [AC'18, AC'19] was published in ASIACRYPT 2018 and ASIACRYPT 2019, two of the top three cryptographic conferences.

Future Directions

A. Post-quantum cryptography

I am eager to continue my research in the field of post-quantum cryptography (PQC). While the quantum-resistant encryption primitive is gaining significant attention and moving towards standardization, the digital signature primitive still lags behind. There is a noticeable gap between the state-of-the-art signature schemes and the standardization efforts. Furthermore, PQC migration should be put on the table since several governments have announced their plan to replace cryptographic algorithms with PQC algorithms.

My ultimate goal is to bridge these gaps and promote the adoption of quantum-resistant cryptography in practical applications. Specifically, I plan to focus on designing post-quantum digital signature schemes and updating existing authenticated key exchange protocols to be quantum resistant. By addressing these challenges, I hope to contribute to the development of a more secure and robust cryptographic infrastructure that can withstand the emerging threat of quantum computing. My research will help ensure that sensitive information remains secure and protected in the face of quantum computers.

B. Threshold Cryptography

Threshold cryptography and its standardization have garnered significant attention from academia, industry (including blockchain companies), and government. The upcoming call for multi-party threshold cryptography standardization by NIST highlights its importance. Based on our experience in post-quantum standardization, we anticipate that the standardization process will take around 4-5 years.

As part of this process, I plan to submit several proposals for the coming multi-party threshold cryptography standardization. More cryptographic tools are needed to push it towards standardization, mainly due to the lack of efficient cryptographic techniques. I intend to address this issue by advancing new cryptographic tools and investigating their potential

[2] https://csrc.nist.gov/Projects/threshold-cryptography

applications in threshold cryptography. Furthermore, I plan to explore the joint area of post-quantum threshold cryptography in the coming years. I am committed to contributing to this field and look forward to collaborating with students/colleagues to advance the state of the art in threshold cryptography.

C. Privacy Enhancing Technologies

The recent advances in technology have resulted in an explosive growth of data, which has motivated the development of several applications based on the sharing of data/algorithm and the outsourcing of computation power. However, there is a significant gap between the usability of these sharing technologies and their security and privacy requirements. A significant example is the privacy-preserving problem when applying machine learning. Cryptographic tools provide solutions to this gap, such as secure *multi-party computation* and *zero-knowledge proof*. The significant of privacy enhancing technology can also be evidenced by a project by NIST on privacy enhancing cryptography[3].

As a researcher, I am interested in applying my knowledge of theoretical cryptography to privacy-enhancing technology in real-world systems. Examples include our work in zero knowledge proof for Paillier cryptosystem [S&P'24, CCS24] and applying of zero knowledge proof on fair exchange over internet [TIFS'24]. In this direction, my goal is to develop new techniques of zero-knowledge proofs, multi-party computation, and fully homomorphic encryption to bridge this gap between the usability of sharing technologies and their security and privacy.

Selected Publications and Outputs

[CCS'24] Zhikang Xie, Mengling Liu, Haiyang Xue, Man Ho Au, Robert H. Deng, Siu-Ming Yiu: Direct Range Proofs for Paillier Cryptosystem and Their Applications. CCS 2024: 899-913

[S&P'24] Borui Gong, Wang Fat Lau, Man Ho Au, Rupeng Yang, Haiyang Xue, Lichun Li: Efficient Zero-Knowledge Arguments For Paillier Cryptosystem. IEEE, S&P 2024. pp. 1813-1831

[TIFS'24] Xiao Yang, Chengru Zhang, Haiyang Xue, Man Ho Au: Efficient Verifiably Encrypted ECDSA Schemes from Castagnos-Laguillaumie and Joye-Libert Encryptions. IEEE Trans. Inf. Forensics Secur. (2024). pp. 4161-4173

[CCS'23] Haiyang Xue, Man Ho Au, Mengling Liu, Kwan Yin Chan, Handong Cui, Xiang Xie, Tsz Hon Yuen, Chengru Zhang: Efficient Multiplicative-to-Additive Function from Joye-Libert Cryptosystem and Its Application to Threshold ECDSA. ACM CCS 2023. pp. 2974-2988

[CCS'21] Haiyang Xue, Man Ho Au, Xiang Xie, Tsz Hon Yuen, Handong Cui: Efficient Online-friendly Two-Party ECDSA Signature. ACM CCS 2021. pp. 558-573.

[LAC.PK'20] Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, Zhenfei Zhang, Zhe Liu, Hao Yang, Bao Li, Kunpeng Wang: LAC.PKE, first prize in the Chinese post-quantum cryptography competition.

[LAC.KE'20] Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, Zhenfei Zhang, Zhe Liu, Hao Yang, Bao Li, Kunpeng Wang: LAC.KEX, second prize in the Chinese post-quantum cryptography competition.

[3] https://csrc.nist.gov/projects/pec

[AC’19] Xiu Xu, Haiyang Xue, Kunpeng Wang, Man Ho Au, Song Tian: Strongly Secure Authenticated Key Exchange from Supersingular Isogenies. ASIACRYPT (1) 2019. pp. 278-308.

[AC’18] Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang, Jingnan He: Understanding and Constructing AKE via Double-Key Key Encapsulation Mechanism. ASIACRYPT (2) 2018. pp. 158-189.

[LAC’18] Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, Zhenfei Zhang, Zhe Liu, Hao Yang, Bao Li, Kunpeng Wang: LAC: Lattice-based Cryptosystem, NIST post-quantum standardization process.

[Ins’18] Shuai Zhou, Haiyang Xue, Daode Zhang, Kunpeng Wang, Xianhui Lu, Bao Li, Jingnan He: Preprocess-then-NTT Technique and Its Applications to Kyber and NewHope. Inscrypt 2018. pp. 117-137.

[RSA’18] Yu Chen, Baodong Qin, Haiyang Xue: Regularly Lossy Functions and Applications. CT-RSA 2018. pp. 491-511.

Why I am interest in cryptography?

Cryptography provides a good balance between maintaining security and enabling functionality. Sometimes, cryptography is kind of magic. To see this, consider two amusing scenarios.

1) Imagine you possess a “secret knowledge” such as the solution to a complex mathematical problem and wish to demonstrate the fact you have such knowledge to others without revealing the knowledge itself. Cryptography (to be specific, zero knowledge proof) can help.

2) Additionally, suppose Bob and Alice are interested in dating but Alice is hesitant to risk rejection. They seek a protocol that ensures if one of them says no, the outcome will always be no, regardless of the other’s response. Cryptography (to be specific, multi-party computation) can help.