Research Plan

August 2024 – July 2026:

2 years to complete basic coursework as per school guidance.

Research activities:

- Redacting the first article (pending to define the specific subject with the doctoral advisor). My suggestion for this paper will be regarding the state-of-the-art survey on quantum-based technologies for privacy protection and their potential vulnerabilities.

August 2026 – July 2027:

Research activities:

- Redaction the second article to submit to a congress or journal. It is still pending to coordinate the specific topic with the doctoral advisor. My suggestion for this paper will be to propose an efficient solution based on quantum technologies and share them with the academic community. Because basic privacy protection schemes (such as secure multi-party computing, zero knowledge proof, dynamic encryption, etc.) face significant efficiency bottlenecks, I would like to try to solve this problem through quantum methods.

August 2027 – July 2028:

- Completing the doctoral dissertation.

For details about PhD thesis, I would like to consider quantum-based homomorphic cryptographic methods(Since homomorphic encryption can be a way to achieve privacy protection mechanism such as secure multi-party computing). Here are the relevant candidate papers published in the last three years.

[1]. Zeuner, Jonas, et al. "Experimental quantum homomorphic encryption." npj Quantum Information 7.1 (2021): 25.
[2]. Zhang, Jing-Wen, et al. "Improved multiparty quantum private comparison based on quantum homomorphic encryption." Physica A: Statistical Mechanics and its Applications 610 (2023): 128397.
[3]. Wang, Cheng, and Ri-Gui Zhou. "Secure multi-party convex hull protocol based on quantum homomorphic encryption." Quantum Information Processing 22.1 (2022): 24.
[4]. Yuanjing, Zhang, Shang Tao, and Liu Jianwei. "A multi-valued quantum fully homomorphic encryption scheme [J]." Quantum Information Processing 20.3 (2021).
[5]. Liu, Wen, et al. "A New Quantum Private Protocol for Set Intersection Cardinality Based on a Quantum Homomorphic Encryption Scheme for Toffoli Gate." Entropy 25.3 (2023): 516.
[6]. Yu, Wenbin, et al. "A phase estimation algorithm for quantum speed-up multi-party computing." Cmc-Comput. Mater. Contin 67 (2021): 241-252.
[7]. Cheng, Zhen-Wen, et al. "A secure crossing two qubits protocol based on quantum homomorphic encryption." Quantum Science and Technology 7.2 (2022): 025027.
[8]. Zhang, Jing-Wen, et al. "A Secure Multiparty Quantum Homomorphic Encryption Scheme." Computers, Materials & Continua 73.2 (2022).
[9]. Liu, Jiang, et al. "Efficient quantum homomorphic encryption scheme with flexible evaluators and its simulation." Designs, Codes and Cryptography 90.3 (2022): 577-591.
[10]. Tham, Weng Kit, et al. "Experimental demonstration of quantum fully homomorphic encryption with application in a two-party secure protocol." Physical Review X 10.1 (2020): 011038.
[11]. Gong, Changqing, et al. "Grover algorithm-based quantum homomorphic encryption ciphertext retrieval scheme in quantum cloud computing." Quantum Information Processing 19 (2020): 1-17.
[12]. Zhu, Hongfeng, Liwei Wang, and Chaonan Wang. "Privacy-enhanced multi-user quantum private data query using partial quantum homomorphic encryption." International Journal of Theoretical Physics 60.6 (2021): 2090-2101.
[13]. Zhang, Kejia, et al. "Privacy-Preserving Decision Protocols Based on Quantum

Oblivious Key Distribution." Computers, Materials & Continua 64.3 (2020).
[14]. Deng, Zhiliang, et al. "Privacy-preserving quantum multi-party computation based on circular structure." Journal of Information Security and Applications 47 (2019): 120-124.
[15]. Gong, Changqing, et al. "Quantum Ciphertext Dimension Reduction Scheme for Homomorphic Encrypted Data." 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2021.
[16]. Ma, Guangsheng, and Hongbo Li. "Quantum Fully Homomorphic Encryption by Integrating Pauli One-time Pad with Quaternions." Quantum 6 (2022): 866.
[17]. Zhu, Hongfeng, Chaonan Wang, and Xueying Wang. "Quantum fully homomorphic encryption scheme for cloud privacy data based on quantum circuit." International Journal of Theoretical Physics 60 (2021): 2961-2975.
[18]. Chen, Xiu-Bo, et al. "Quantum homomorphic encryption scheme with flexible number of evaluator based on (k, n)-threshold quantum state sharing." Information Sciences 501 (2019): 172-181.
[19]. Xu, Xin, and Aihan Yin. "Quantum Homomorphic Broadcast Multi-Signature Based on Homomorphic Aggregation." Chinese Physics B (2022).
[20]. Chen, Geng, et al. "Quantum identity authentication protocol based on flexible quantum homomorphic encryption with qubit rotation." Journal of Applied Physics 133.6 (2023).
[21]. Lu, Changbin, et al. "Quantum multiparty cryptosystems based on a homomorphic random basis encryption." Quantum Information Processing 19 (2020): 1-14.
[22]. Ji, ZhaoXu, et al. "Quantum protocols for secure multi-party summation." Quantum Information Processing 18 (2019): 1-19.
[23]. Zhou, Qing, et al. "Quantum search on encrypted data based on quantum homomorphic encryption." Scientific reports 10.1 (2020): 5135.
[24]. Chardouvelis, Orestis, Nico Döttling, and Giulio Malavolta. "Rate-1 quantum fully homomorphic encryption." Theory of Cryptography Conference. Cham: Springer International Publishing, 2021.
[25]. Xu, Gang, et al. "Secure multi-party quantum summation based on quantum homomorphic encryption." Intell. Autom. Soft Comput. 34.1 (2022): 531-541.
[26]. Li, Zhen-zhen, et al. "Secure quantum network coding based on quantum homomorphic message authentication." Quantum Information Processing 18.1 (2019): 14.
[27]. Liang, Min. "Teleportation-based quantum homomorphic encryption scheme with quasi-compactness and perfect security." Quantum Information Processing 19.1 (2020): 28.
[28]. Zhang, Jing-Wen, et al. "Universal quantum circuit evaluation on encrypted data using probabilistic quantum homomorphic encryption scheme." Chinese Physics B 30.7 (2021): 070309.