How does the quantum theory change cryptography and the nature of computing? This is a central question driving my research, which I approach to with mathematically formal methods. The impact also reaches imperative real-world matters. In particular, quantum computer can break many widely deployed cryptosystems [30], and post-quantum cryptography (i.e., securing classical cryptography against quantum attacks) has been highlighted by NSA [28] and become the subject of an ongoing standardization process by NIST [27].

I have devoted to investigating whether the problems that cryptography is based on are safe against quantum computers. My main contribution here is giving efficient quantum algorithms for several long-standing problems in algebraic number theory, which have broken a few lattice-based cryptosystems that were believed quantum-secure [15, 6]. I am also keen on designing quantum algorithms for more problems from diverse fields.

Hard problems for quantum computers alone do *not* guarantee a quantum-secure cryptosystem. I have initiative work developing a formal framework and analytic tools for modeling and reasoning about security in the presence of quantum attacks [20, 21, 31]. My work has secured a variety of cryptographic constructions, from complex cryptographic protocols to basic primitives such as hash functions and block ciphers, against quantum attacks [20, 14, 23, 32, 2].

Quantum computing also offers *quantum cryptography* as a new approach to cryptography. I have designed quantum protocols that can realize what is provably impossible classically [16]. My work also spans to quantum complexity theory: we design the first zero-knowledge proof system for QMA, and construct computational quantum pseudorandom objects that have implications in quantum information theory and physics [8, 24]. All efforts, more broadly, join the fundamental pursuit of understanding and harnessing the strengths and limits of quantum computing.

PAST WORK

Quantum algorithms for problems critical to cryptography. Quantum computers have shown unprecedented power, and sometimes solve problems exponentially faster than best known classical algorithms. This can be devastating to cryptography nonetheless. Shor's quantum algorithm for factorization and discrete logarithm, for instance, will break the majority of public-key cryptography. My work has mainly been designing efficient quantum algorithms for problems critical to cryptography, especially those new candidates in post-quantum cryptography.

In joint work with Eisenträger, Hallgren and Kitaev [15], we give an efficient quantum algorithm for computing the unit group in a number field of arbitrary degree. Later we extend this work and solve the problems of computing the principle ideal, the class group and general S-unit groups in high-degree number fields [6].

These are basic problems in (algebraic) number theory, which has been a fruitful source of hard problems for cryptography (e.g., factoring can actually be viewed as a special case of the unit-group problem). Existing classical algorithms take at least super-polynomial time, and our quantum algorithms, in the same spirit to Shor's, constitute one of the few examples of quantum *exponential* speedup (not relative to an oracle) in recent years. In fact, since Hallgren's 2005 result in the constant-degree case [19], there is little progress till our work. What is more significant to cryptography, our quantum algorithms can solve a problem in lattice-based cryptography, and break some public-key encryption and multilinear mapping schemes which were deemed quantum-secure [12, 7]. Lattice-based cryptography is a promising candidate for post-quantum cryptography, and our work calls for more careful scrutiny of their hardness against quantum algorithms.

A major technical advance in our work is developing a framework of *continuous* hidden subgroup problems (HSP). HSP is an elegant framework that captures most instances of quantum exponential speedup including Shor's algorithm, which is successful mostly on finite and countable

abelian groups. Our continuous HSP framework subsumes the existing framework, and applies more generally in continuous groups as $\mathbb{R}^n$, especially in high dimensions. We also give a *conceptually* new approach to quantum Fourier sampling, the central technique for solving HSP, which admits modular analysis and is robust to disturbance to the input.

Securing cryptography against quantum attacks. To guard cryptography against quantum attacks, it is necessary to use problems that are hard for quantum computers. This is, nonetheless, *insufficient*, because breaking a cryptosystem is possible without solving the underlying hard problem. Quantum attackers make this far more challenging since they may exploit unique quantum features that have no classical counterparts. My work has been devoted to developing formal models and techniques to make classical cryptography quantum-secure.

- *Develop a quantum provably-secure framework.* Modern cryptography has revolutionized from an art to a rigorous subject built on a mathematical framework. The key component, *provable security*, encompasses defining a security model that precisely specifies the security goals and attacks under consideration, and then giving a mathematical proof of security, typically a *reduction* showing that breaking a cryptosystem is at least as hard as solving some hard problem.

  My work [20, 21, 31] is among the early ones to establish a *quantum* provably-secure framework. In addition to formalizing general quantum security models and unfolding basic properties and relations, we also identify characteristics under which classical security proofs can carry through against quantum attacks. Proving quantum security is greatly simplified to checking classical proofs against several well-defined conditions. For instance we can establish quantum security of a class of protocols for secure two-party computation and hash-based digital signature schemes [10, 9], almost in an automated and mechanic way.

- *Securing cryptographic protocols.* In [20], we design a zero-knowledge proof of knowledge (ZKPoK) protocol, which is the first quantum-secure and composable without any trusted setup. Based on it, we construct quantum-secure protocols for computing any two-party functionality, preserving the renowned result of Goldreich, Micali and Widgerson [17] against quantum attacks.

  In designing our ZKPoK protocol, we find an alternative technique to circumvent quantum *rewinding*, a fundamental difficulty due to quantum *no-cloning* and inevitable destruction in learning a quantum state. Instead, inspired by classical techniques, we carefully embed a trapdoor to extract information from a quantum adversary without rewinding. A multitude of classical schemes that rely on rewinding arguments could benefit from our approach.

- *Analyzing (black-box) quantum security of cryptographic hash functions.* Cryptographic hash functions is ubiquitous, such as in authentication, digital signature, and crypto-currencies. In my work [23], we prove important properties, such as hardness of finding a preimage, second-preimage and collisions under *generic* quantum attacks: the hash function is modeled as a uniformly random function and is given to an adversary as a *black-box* that accepts queries in quantum superposition. We also describe quantum algorithms and prove matching complexity. Recently motivated by real-world attacks, which suggest that assuming uniform outputs may be too optimistic [33], former REU students and I consider non-uniform outputs and prove tight quantum security [2]. These results could guide the design of hash functions as well as determining the appropriate parameters for hash-based systems.

  To prove quantum security, we extend and strengthen the techniques in standard quantum query complexity, where the hardness is proven for solving a *worst-case* instance with *constant* success probability, to the cryptographic setting, where we need that solving a random instance (i.e., *average-case*) with merely *inverse polynomial* probability must be hard.

- *Developing the quantum random-oracle heuristic.* Treating a hash function as a public uniformly random oracle is in fact a common heuristic (i.e., *random-oracle* heuristic) to analyze schemes using hash functions. It often enables more efficient constructions and powerful proof techniques, which are otherwise difficult or unknown. However, if a quantum attacker can query the oracle in quantum superposition, many classical proofs no longer hold. For instance, the *lazy-sampling* trick allows answering the queries *on-the-fly* and as a result one can change the hash value at points that have not been queried (a.k.a. programming the random-oracle). However, to answer a single quantum query, apparently the entire function has to be determined.

  My work has contributed to restoring basic proof techniques for the quantum random-oracle model. In [14], we develop a technique for adaptively programming a quantum random oracle, applicable whenever predicting the points to be changed amounts to solving some hard computational problem. Before that, one often needs stronger *information-theoretical* condition on unpredictability. We later give a unified approach to programming a quantum random-oracle based on a versatile *average-case* search problem [23, 32].

- *Securing symmetric-key cryptography against quantum superposition attacks.* In contrast to public-key cryptography, symmetric-key cryptography is usually considered less susceptible to quantum attacks. Nonetheless, quantum attacks that completely break real-world symmetric-key schemes are found in recent years. In particular, several modes of operations for extending the domain of a block-cipher, including the popular CBC-MAC, are broken [25]. It is left open whether securely extending the domain of block-ciphers against quantum attacks is possible.

  In my recent work [32], we prove that HMAC, NMAC and a few other variants are quantum-secure domain-extension schemes. We obtain quantum-secure message authentication for *variable*-length messages as an immediate application. Our key technique is showing that if two distributions on *functions* are indistinguishable, then they remain indistinguishable even if exponentially many samples are given to the adversary as a quantum-accessible oracle. This generalizes Zhandry's prior result concerning distributions on *strings*, which has been extremely useful, e.g., in constructing quantum-secure pseudorandom functions [35]. We anticipate more applications of our generalized technique as well.

  We remark that this line of research concerns attackers that can issue quantum superposition queries, e.g., to a signing algorithm under a secret key. This may sound too strong to be realistic, but it ensures stringent security that could be necessary in complex environments where quantum and classical information may flow at the same time.

Quantum cryptography, complexity and more. Quantum computing also allow honest users to use quantum technology to protect classical data. In addition to offering alternative solutions to classical cryptography, one can sometimes bypass what is impossible otherwise. When quantum communication becomes popular (cf. the quantum Internet project in Europe [29]), we will need cryptographic tools to protect sensitive *quantum* information. I have worked on quantum cryptography targeting both ends. My work goes more broadly to quantum complexity theory and other areas that emerge from the influence of the quantum paradigm.

- *Quantum cryptography for classical tasks that are impossible classically.* A notable example demonstrating the power of quantum cryptography is quantum key distribution. It allows negotiating a secret key between two parties in the presence of any computationally unbounded eavesdropper [4], which is proven *impossible* using only classical protocols.

  In [16], we design a quantum protocol for securely computing a two-party functionality called oblivious transfer assuming a trusted implementation of another functionality called 2-bit cut-

and-choose, whereas no classical protocols can achieve this. The only example of this flavor before our work is between oblivious transfer and bit commitment [5]. We develop a "quantum inference" technique for proving security, which allows estimating the state of a quantum population by a random sampling procedure that is partially controlled by an adversary. This has found useful in other work [13].

- *Quantum zero-knowledge proof systems for QMA.* Zero-knowledge proof systems are interactive protocols that allow a prover to convince a verifier about the validity of an assertion without revealing nothing more to the verifier. The seminal work [18] that constructs zero-knowledge proof systems for all NP languages has nurtured a myriad of novel directions in cryptography.

  In [8], we construct the first zero-knowledge proof systems for all problems in QMA, the quantum analogue of NP. Our work identifies a new QMA-complete problem that admits simple verification. The new insights to QMA may shed light on quantum Hamiltonian complexity and a quantum PCP theorem. The main technical tool we design is a quantum authentication code that admits transversal evaluation of Clifford operations on encoded states. This nice property enables reducing verifying a quantum witness of our QMA-complete problem to verifying an NP-relation, which can be done by known quantum-secure zero-knowledge proofs for NP [34].

- *Quantum pseudorandom states, unitary operators and applications.* Pseudorandomness, as efficient approximations to perfectly random distributions, is a central object in cryptography, algorithm design, complexity and coding theory. Haar-random distributions are considered perfect randomness in the quantum setting and are a powerful analytical tool.

  In a recent work [24], we propose pseduroandom quantum states as *computational* approximations to Haar randomness. We consider efficient observers that have arbitrarily many copies of the given state. In contrast, extensive previous work focuses on approximations up to a bound t, called t-designs, although the observers may be computationally unbounded (analogous to t-wise independence). We are able to construct a collection of pseudorandom states efficiently based on a pseudorandom function.

  One striking property we show is that a pseudorandom state cannot be cloned efficiently even if many copies are given. This immediately gives a simple construction of (private-key) quantum money schemes. Interestingly, pseudorandom states also provide a toy example that demonstrates *thermalization*. Thanks to our generic construction based on pseudorandom functions, our toy example can be made much more efficient than existing ones (e.g., when instantiated with the low-depth pseudorandom function in [3]).

Future work

Securing cryptography against quantum attacks, which is critical to a trustworthy communication and computation infrastructure, remains a long-term endeavor. I will also further explore the capacity of quantum algorithms and quantum cryptography, and how the quantum paradigm reshapes the foundations of complexity theory and information theory. Moreover, I will seek for broad collaboration to develop programming language tools for quantum computing, address emerging security and privacy issues, and attack problems beyond computer science, by quantum-inspired approaches. I elaborate on some directions below.

- *Fine-grained quantum security of hash functions and block ciphers.* Most quantum cryptanalysis on hash functions so far falls in the black-box model without considering their internal design. I will take a modular approach to open up the black-box by first analyzing two dominating iterated

designs: the Merkle-Damgård family behind SHA-2, and the Sponge construction behind SHA-3. Then I will look into the basic unit in the iteration, typically block ciphers.

- *Quantum algorithms for cryptographic and optimization problems.* Many new candidate problems in post-quantum cryptography are lacking careful examination of the hardness against quantum algorithms. The *unique* shortest vector problem in lattice-based cryptography is particularly interesting to me. I will revisit its connection to the hidden shift problem to design an efficient quantum algorithm; or as a win-win strategy, develop a new cryptographic primitive from the (generalized) hidden shift problem as initiated in [1]. Beyond cryptography, I will also design quantum algorithms for optimization problems (e.g., improving the quantum linear system algorithm [22] by our new quantum Fourier sampling technique [15]), which is beneficial in machine learning and simulating quantum systems in physics, chemistry and biology.
- *Revisiting complexity theory with quantum reductions.* In complexity theory, we relate the hardness of various problems typically by *classical polynomial-time* reduction algorithms. What happens if we allow reductions to be efficient *quantum* algorithms? One direction concerns worst-case to average-case reductions, e.g., *can we based one-way functions on NP-hardness or QMA-hardness*, a top wish of cryptographers? We have some preliminary work indicating both negative and positive evidence [11]. Another direction I will pursue concerns relating cryptogrpahic primitive using quantum reductions. There exist hard-core predicates that can be proven secure using quantum reductions whereas classical proofs are unknown [26].
- *Strong quantum security models and new primitives in quantum cryptography.* Quantum security models still demand extensive developing and refining. For instance, I am working on a new security definition for authenticating and signing classical messages, where existing definitions may fall apart on a special quantum attack. This could also resolve the difficulty of a suitable security notion for multiple-time authentication of *quantum* states. My recent work on quantum cryptography inspires envisioning novel primitives such as proofs of quantum knowledge, and tokenized cryptography where we can produce unclonable quantum tokens to delegate cryptographic errands with fine-grained control.
- *Emerging security issues in IoT and machine learning.* One pressing security challenge arising with Internet of things is the vast imbalance of computational resources available to different entities (e.g., a sensor vs. a cloud). This inevitably opens weak links to attacks. I intend to investigate light-weight cryptography and especially guard them against quantum attacks. At a comprehensive level, I want to refine existing security models for multi-party computation, which typically coarsely treat everyone as a poly-time machine, to suit the heterogeneous reality of IoT. I am also keen on to collaborate with machine learning and big data experts to address the security issues when handling huge amount of sensitive data of individuals.
- *Formal proof checker for post-quantum cryptography.* Since my appointment at Portland State University, I have the opportunity to interact with the programming language group and set foot out of my expertise on formal verification. With a graduate student, we have started developing a proof checking system based on Coq to verify security proofs for some post-quantum cryptographic proposals. This may be useful in the NIST standardization process of post-quantum cryptography [27]. In the long-term, I look forward to collaboration on further incorporating quantum computing and the logic of programming.

Bibliography

[1] Gorjan Alagic and Alexander Russell. "Quantum-secure symmetric-key cryptography based on hidden shifts." In: *Advances in Cryptology – Eurocrypt 2017*. Springer. 2017, pp. 65–93.

[2] Marko Balogh, Edward Eaton, and Fang Song. "Quantum Collision-Finding in Non-Uniform Random Functions." In: *IACR Cryptology ePrint Archive* 2017 (2017). ia.cr/2017/688, p. 688.

[3] Abhishek Banerjee, Chris Peikert, and Alon Rosen. "Pseudorandom functions and lattices." In: *Advances in Cryptology–EUROCRYPT 2012* (2012), pp. 719–737.

[4] Charles H. Bennett and Gilles Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing." In: *Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India*. December 1984, pp. 175–179.

[5] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. "Practical Quantum Oblivious Transfer." In: *CRYPTO*. 1991, pp. 351–366.

[6] Jean-François Biasse and Fang Song. "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields." In: *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016*. SIAM, 2016, pp. 893–902. DOI: 10.1137/1.9781611974331.ch64.

[7] Jean-François Biasse and Fang Song. *On the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in* $\mathbb{Q}(\zeta_{p^n})$. Tech Report CACR 2015-12. Sept. 2015.

[8] Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous. "Zero-Knowledge Proof Systems for QMA." In: *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016*. IEEE Computer Society, 2016, pp. 31–40. DOI: 10.1109/FOCS.2016.13.

[9] Johannes Buchmann, Erik Dahmen, and Andreas Hülsing. "XMSS-a practical forward secure signature scheme based on minimal security assumptions." In: *Post-Quantum Cryptography* (2011), pp. 117–129.

[10] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. "Universally composable two-party and multi-party secure computation." In: *STOC*. 2002, pp. 494–503.

[11] Nai-Hui Chia, Sean Hallgren, and Fang Song. *Basing cryptography on NP-hardness using quantum reductions*. Manuscript. 2017.

[12] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. "Recovering short generators of principal ideals in cyclotomic rings." In: *Advances in Cryptology – Eurocrypt 2016*. Springer. 2016, pp. 559–585.

[13] Frédéric Dupuis, Serge Fehr, Philippe Lamontagne, and Louis Salvail. "Adaptive Versus Non-Adaptive Strategies in the Quantum Setting with Applications." In: *Advances in Cryptology – Crypto 2016*. Springer. 2016, pp. 33–59.

[14] Edward Eaton and Fang Song. "Making Existential-unforgeable Signatures Strongly Unforgeable in the Quantum Random-oracle Model." In: *10th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2015*. Schloss Dagstuhl, 2015, pp. 147–162. DOI: 10.4230/LIPIcs.TQC.2015.147.

[15] Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song. "A quantum algorithm for computing the unit group of an arbitrary degree number field." In: *Proceedings of the 46th STOC*. ACM, 2014, pp. 293–302. DOI: 10.1145/2591796.2591860.

[16] Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas. "Feasibility and completeness of cryptographic tasks in the quantum world." In: *Theory of Cryptography*. Springer, 2013, pp. 281–296. DOI: 10.1007/978-3-642-36594-2_16.

[17] Oded Goldreich, Silvio Micali, and Avi Wigderson. "How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority." In: *STOC*. 1987, pp. 218–229.

[18] Oded Goldreich, Silvio Micali, and Avi Wigderson. "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems." In: *Journal of the ACM (JACM)* 38.3 (1991), pp. 690–728.

[19] Sean Hallgren. "Fast quantum algorithms for computing the unit group and class group of a number field." In: *STOC*. 2005, pp. 468–474.

[20] Sean Hallgren, Adam D. Smith, and Fang Song. "Classical Cryptographic Protocols in a Quantum World." In: *Advances in Cryptology – CRYPTO 2011*. Springer, 2011, pp. 411–428. DOI: 10.1007/978-3-642-22792-9_23.

[21] Sean Hallgren, Adam Smith, and Fang Song. "Classical cryptographic protocols in a quantum world." In: *International Journal of Quantum Information* 13.04 (2015), p. 1550028. DOI: 10.1142/S0219749915500288.

[22] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. "Quantum algorithm for linear systems of equations." In: *Physical review letters* 103.15 (2009), p. 150502.

[23] Andreas Hülsing, Joost Rijneveld, and Fang Song. "Mitigating Multi-target Attacks in Hash-Based Signatures." In: *PKC 2016*. Springer, 2016, pp. 387–416. DOI: 10.1007/978-3-662-49384-7_15.

[24] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. *Pseudorandom States, Non-Cloning Theorems and Quantum Money*. arXiv:1711.00385. https://arxiv.org/abs/1711.00385. 2017.

[25] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and Mara Naya-Plasencia. "Breaking symmetric cryptosystems using quantum period finding." In: *Advances in Cryptology – Crypto 2016*. Springer. 2016, pp. 207–237.

[26] Akinori Kawachi and Tomoyuki Yamakami. "Quantum hardcore functions by complexity-theoretical quantum list decoding." In: *SIAM Journal on Computing* 39.7 (2010), pp. 2941–2969.

[27] *NIST Post-Quantum Cryptography Standardization*. https://goo.gl/w6FVpN. 2017.

[28] *NSA Information Assurance web page*. https://goo.gl/iD3gei. Aug. 2015.

[29] *Quantum Internet Alliance*. http://quantum-internet.team/. 2017.

[30] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." In: *SIAM J. Comput.* 26.5 (1997), pp. 1484–1509.

[31] Fang Song. "A Note on Quantum Security for Post-Quantum Cryptography." In: *Post-Quantum Cryptography*. Springer, 2014, pp. 246–265. DOI: 10.1007/978-3-319-11659-4_15.

[32] Fang Song and Aaram Yun. "Quantum Security of NMAC and Related Constructions - PRF Domain Extension Against Quantum attacks." In: *Advances in Cryptology - CRYPTO 2017*. Springer, 2017, pp. 283–309. DOI: 10.1007/978-3-319-63715-0_10.

[33] Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov. *The first collision for full SHA-1*. Cryptology ePrint Archive, Report 2017/190. https://shattered.io/. 2017.

[34] John Watrous. "Zero-Knowledge against Quantum Attacks." In: *SIAM J. Comput.* 39.1 (2009). Preliminary version in STOC 2006, pp. 25–58.

[35] Mark Zhandry. "How to Construct Quantum Random Functions." In: *FOCS'12*. IEEE Computer Society, 2012, pp. 679–687.