FANG SONG

RESEARCH STATEMENT

fang.song@uwaterloo.ca

My research centers around the exciting subjects of cryptography and quantum computing. I have been driven by a basic question in particular: *how does quantum computing change the landscape of cryptography*? Trained as a theoretical computer scientist, I approach this question guided by formal and mathematically rigorous methods. The consequences, nonetheless, go beyond purely theoretical interests, and they bring about new threats and opportunities in modern cybersecurity as quantum technology advances. More and more entities (e.g., standardization organizations NIST and ETSI) are getting concerned, and NSA recently announced preliminary plans for transitioning to quantum resistant ciphersuites [1].

Specifically, my previous work can be categorized by three broad questions. The first two are concerned with the security of *classical* cryptosystems in the presence of quantum adversaries, and the third explores constructing *quantum* schemes to protect classical as well as quantum information.

1. Are the computational problems that cryptography is based on safe against quantum algorithms? The majority of public-key cryptography deployed on the Internet today, such as those used in HTTPS and TLS, will be broken by quantum computers. This is because the computational problems underlying these cryptosystems, which are believed hard to solve for classical computers, can be solved efficiently by quantum algorithms. Due to promising progress on the physical implementation of quantum computers in recent years [18], the threats are becoming more and more worrisome. To address this, people started seeking alternative computational problems in order to build cryptography that is safe against quantum adversaries. One of the most promising directions employs an algebraic object called *lattices*, and many cryptosystems are proposed which are believed to be quantum-safe [19].

Surprisingly, my work [11, 4, 5] showed that some lattice-based schemes are broken by quantum computers. This includes a fully homomorphic encryption scheme by Smart and Vercauteren, a multilinear mapping scheme due to Garg, Gentry and Halevi, and the Soliloquy encryption scheme designed by GCHQ as a quantum-safe candidate [7, 8]. This attack has started active discussion within the research community and general public [2, 3], forcing more careful evaluation of lattice problems as well as other candidates for building quantum-safe cryptography.

The key to the attack above is efficient quantum algorithms for computational problems in a special number field that these lattices reside in. These algorithms represent part of my results on designing quantum algorithms for basic computational problems in number fields. Specifically, we gave quantum algorithms for computing the unit-group and the principal ideal problem, which induce the aforementioned attack, as well as computing the class group and the S-units for any collection of prime ideals S. All of them are efficient in any number fields of arbitrary degree. The best algorithms before ours, quantum or classical, needed at least exponential time in the degree of the number fields, and there had been little progress for almost a decade. One of our technical contributions strengthens *quantum Fourier sampling* substantially, which is the core of most quantum exponential speedups and is one of the most successful quantum algorithmic tools.

2. Are cryptosystems secure against quantum attacks, even if they are built on problems that are computationally hard for quantum computers? It is clear that cryptosystems are broken if one solves their underlying computational problems. However, even assuming these problems are hard to solve by quantum algorithms, a quantum adversary may still be able to break the cryptosystems. In fact, there is a scheme proven *information-theoretically* secure classically, but it is broken by a quantum attack feasible by present-day technology already [9]. This is a general problem coming from unique quantum features of quantum adversaries not considered by classical security analyses, which as a result may completely break down. For instance, the quantum *no-cloning* theorem, stating that copying an unknown quantum state is impossible, makes numerous classical security proofs no longer apply in the presence of quantum adversaries. Another unique quantum feature challenges hash functions, a ubiquitous building block in cryptography. Classical security analyses often treat hash functions as an ideal random black-box (a.k.a. *random-oracle* model). However, a quantum adversary naturally can access the black-box in quantum *superposition*, in contrast to classical adversaries who can only query the black-box one entry each time. All of this makes it extremely tricky and difficult to argue security in the presence of quantum attacks. Previously proposals for quantum-safe schemes rarely analyze quantum adversaries.

I have devoted much effort to developing formal models and techniques for reasoning about quantum adversaries [14, 15, 12, 20, 10, 17]. They are often among the first to carefully analyze and construct classical systems to withstand quantum attacks for a multitude of important applications, which span from basic primitives such as digital signatures and hash functions, to more complex cryptographic protocols.

In [20], I gave a list of clean characterizations for classical security proofs that still hold against quantum adversaries. This provides a convenient tool that complements classical proofs under quantum attacks, especially in the realm of basic primitives such as encryption and signature.

Several results of mine dealt with hash functions in the presence of quantum superposition attacks. In [20], I gave abstract conditions under which security proofs in the classical random-oracle model still go through against quantum adversaries. In joint work with Eaton [10], we showed, how to use a random hash function to amplify the security of signature schemes (from existentially to strongly unforgeable). We developed a quantum analogue of an essential classical technique on programming a random function adaptively, which had been proven difficult to establish. A recent work of mine [17] gave exact bounds for optimal quantum attacks on random hash functions, which established that various desired properties such as second-preimage resistance (with multiple targets) remain valid against quantum attacks.

In joint work with Hallgren and Smith [14], we showed that the celebrated result that two-party Secure Function Evaluation (SFE) is feasible [13] continues to hold against quantum adversaries. Namely we showed that there are classical protocols secure against quantum adversaries that allow two players to jointly evaluate an arbitrary function without compromising their respective private inputs. We also constructed for the first time a quantum-safe zero-knowledge proof of knowledge (ZKPoK) protocol which is fully simulatable. Simulatable ZKPoK is an essential building block in classical cryptography, and our protocol could be a crucial ingredient to establish quantum security of more classical schemes.

3. How do honest users use quantum technology for both classical and quantum cryptographic tasks? The power of quantum information processing is available to honest users too. We can construct quantum schemes to defeat quantum attacks. More excitingly, quantum schemes can realize some classical tasks where no classical schemes can, such as distributing a secret key against any unbounded eavesdropper using quantum key distribution (QKD) schemes. Meanwhile, *quantum* tasks such as keeping sensitive quantum data confidential require designing new quantum cryptographic tools.

In [12], we constructed several quantum protocols for securely evaluating some classical circuit, which is provably impossible by classical protocols alone. They are among the few examples of this kind beyond QKD. We also developed new techniques for dealing with unbounded quantum adversaries, adding to the limited toolkit of quantum cryptography.

In a recent work [6], we constructed a zero-knowledge proof system for problems that can be verified given a succinct quantum witness (termed QMA as quantum analogue of NP). This quantum cryptographic tool parallels the renowned classical zero-knowledge proof systems for NP. In this work, we designed an authentication scheme that protects the integrity of quantum data. It admits many additional features beyond existing schemes. We also identified an extremely simple variant of the local Hamiltonian problem and proved that this variant remains QMA-complete. This characterization may give insights to a primary area in theoretical computer science and physics called quantum Hamiltonian complexity .

Future directions

Research is always unpredictable but rewarding. The interplay between cryptography and quantum computing, which will remain a central theme of my research, will certainly bring about more surprises. In addition to addressing pressing issues of cybersecurity in a quantum world, I am passionate to pursue new concepts which expand the spectrum of traditional cryptography and computer science in general. The non-conventional lens to studying strengths and weakness of quantum computation that my research features may shed light on a long quest regarding what kinds of computation the physical world offers. Meanwhile, I am eager to extending my primary zone and reaching out for exciting collaboration from other fields. Below I give a few concrete proposals for the near and intermediate future.

Determining the quantum hardness of candidate problems, which helps establish a solid foundation for quantum-safe cryptography, will remain a major direction of mine. A natural question concerns generalizing the quantum attack induced by our quantum algorithms on lattice-based schemes. A particularly interesting scheme with similar structure to those broken is the NTRU encryption system [16], which has survived almost two decades of cryptanalysis.

More generally, I want to investigate the possibility of attacking more lattice problems by quantum algorithms directly. One problem that interests me the most is the *unique* shortest vector problem (uSVP), which is as hard as several standard lattice problems and there are cryptosystems based on it. There was indication of a possible route for solving it by quantum algorithms. I believe that any meaningful quantum speedup will be a considerable progress.

On the flip side, I keen to explore the limits of quantum algorithms. There are computational problems known to resist a special form of quantum attacks. I want to extend the study to other quantum-safe candidates and to larger classes of quantum attacks. Basing lattice-based cryptography on weaker assumptions is another important goal of mine, which would give more confidence of lattice-based schemes. My tentative approach is to improve the existing worst-case to average-case reductions that establish the security of lattice-based schemes, possibly via extending techniques in my previous work [11].

Analyzing and designing cryptographic schemes against quantum attacks need to be carried out soon, ahead of quantum threats becoming practical. One critical primitive that remain unclear against quantum attacks is the Luby-Rackoff construction of a pseudorandom permutation from pseudorandom functions. I have made preliminary progress and completing a quantum-safe construction is on my agenda. I also intent to look into the internal design of hash functions when analyzing security against quantum adversaries. There is little work along this line but it is of high stakes.

Dramatic efficiency improvement on secure computation protocols has occurred in recent years, and some protocols have been deployed in practical applications. However, they are not known to be quantum-safe. A natural step is to improve my previous feasibility result [14]. For instance, can we reduce polynomial-round to *constant-round*? Can we weaken the computational assumptions? How about multi-party setting against quantum attacks? These could be possible projects for my potential graduate students.

Formal modeling of security in presence of quantum adversaries is an important point in my previous work which I did not elaborate on. Such experience also inspires me to reflect what security should capture in other emerging adversarial settings. For instance, the drastic asymmetry in the computational power between clouds and users challenges the usual notion of polynomial-time for potentially malicious clouds. More and more security and privacy issues arise, inevitably, from rapidly advancing areas such as big data and Internet of Things. I am enthusiastic to keep close interaction with scholars in these areas and jointly strive for a safer digital world.

References

[1] NSA information assurance web page, August 2015. `https://goo.gl/iD3gei`.

[2] Soliloquy. Google groups on Cryptanalytic algorithms, 2015. `https://goo.gl/Kss6Y1`.

[3] A tricky path to quantum-safe encryption. Quanta Magazine, September 2015. `https://goo.gl/8UJ64F`.

[4] 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, September 2015.

[5] Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. To appear in 27th ACM-SIAM Symposium on Discrete Algorithms (SODA'16), January 2016.

[6] Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous. Zero-knowledge proof systems for QMA. Under Submission, November 2015.

[7] Peter Campbell, Michael Groves, and Dan Shepherd. Soliloquy: A cautionary tale. ETSI/IQC 2nd Quantum-Safe Crypto Workshop, 2014.

[8] Ronald Cramer, Lo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. Cryptology ePrint Archive, Report 2015/313, October 2015.

[9] Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two provers in isolation. In *ASIACRYPT*, pages 407–430, 2011.

[10] 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)*, pages 147–162, 2015.

[11] 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*, pages 293–302. ACM, 2014.

[12] 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*, pages 281–296. Springer, 2013.

[13] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *STOC*, pages 218–229, 1987.

[14] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. In *Advances in Cryptology–Crypto 2011*, pages 411–428, 2011.

[15] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. *International Journal of Quantum Information*, 13(04):1550028, 2015. Preliminary version appeared in Crypto'11.

[16] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. NTRU: A ring-based public key cryptosystem. In *Algorithmic number theory*, pages 267–288. Springer, 1998.

[17] Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. To appear in 19th Public Key Cryptography–PKC 2016, October 2016.

[18] J Kelly, R Barends, AG Fowler, A Megrant, E Jeffrey, TC White, D Sank, JY Mutus, et al. State preservation by repetitive error detection in a superconducting quantum circuit. *Nature*, 519(7541):66–69, 2015.

[19] Chris Peikert. A decade of lattice cryptography. Cryptology ePrint Archive, Report 2015/939, 2015.

[20] Fang Song. A note on quantum security for post-quantum cryptography. In *Post-quantum cryptography*, pages 246–265. Springer, 2014.