

## Research Interests

cryptography (in particular quantum-safe cryptography), quantum algorithm design, computational complexity, formal verification of cryptography, theoretical computer science

## Employment

- Sept. 2016 - present: **Assistant Professor**  
Computer Science Department  
Portland State University, Portland, OR, USA
- Sept. 2013 - Aug. 2016 **Postdoctoral Fellow**  
Institute for Quantum Computing, and  
Department of Combinatorics & Optimization  
University of Waterloo, Waterloo, ON, Canada  
Supervisors: Andrew Childs, Debbie Leung, Michele Mosca

## Education

- Aug. 2008 - Aug. 2013 PhD, Computer Science and Engineering  
Pennsylvania State University, University Park, PA, USA  
Thesis: Quantum Computing: A Cryptographic Perspective  
Advisor: Dr. [Sean Hallgren](#)
- Sept. 2004 - Jun. 2008 Bachelor of Science, Department of Information Security  
University of Sci. and Tech. of China (USTC), Hefei, Anhui, China  
Thesis: Primitives on Quantum Anonymous Communications  
Advisor: Dr. Liusheng Huang & Dr. Baosen Shi

## Honors & Awards

- Jan. 2015 **Plenary** talk at *QIP'15*, Sydney, Australia.  
(Prestigious honor in quantum community)
- Sept. 2013 - Aug. 2016 Support from Cryptoworks21, Ontario Research Fund (ORF),  
Natural Sciences and Engineering Research Council of Canada (NSERC)
- May 2012 **Outstanding Teaching Assistant Award**, Pennsylvania State University
- August 2008 College of Engineering Fellowship, Pennsylvania State University
- July 2008 Outstanding Undergraduate Thesis Award, USTC

## ◇ External Funding

- (Pending) NSF CCF CRII, AF:Medium:Collaborative Research, AF:Small under review
- (Pending) NSF CISE Research Infrastructure (CRI)

## Publications

(Note: authors are listed in **alphabetical** order by default, as is convention in theoretical computer science.)

### ◇ Publications in Refereed Conferences

1. Quantum Security of NMAC and Related Constructions  
Authors: Fang Song and Aaram Yun  
In *37th International Cryptology Conference (CRYPTO)*, August 2017.
2. Zero-knowledge proof systems for QMA  
Authors: Anne Broadbent, Zhengfeng Ji, Fang Song and John Watrous  
In *57th Annual Symposium on Foundations of Computer Science (FOCS)*, October 2016.  
Contributed talk at the *20th Annual Conference on Quantum Information Processing (QIP)*, January 2017.
3. Mitigating multi-target attacks in hash-based signatures  
Authors: Andreas Hülsing, Joost Rijneveld and Fang Song  
In *19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC)*, March 2016.  
This work has been adopted as a guideline in an [Internet Research Task Force draft](#) v10, July 2017.
4. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields.  
Authors: Jean-François Biasse and Fang Song.  
In *27th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, January 2016.  
Contributed talk at the *20th Annual Conference on Quantum Information Processing (QIP)*, January 2017.
5. Making existentially unforgeable signatures strongly unforgeable in the quantum-random oracle model  
Authors: Edward Eaton and Fang Song  
In *10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)*, May 2015.
6. A note on quantum security for post-quantum cryptography  
Authors: Fang Song  
In *6th International Conference on Post-Quantum Cryptography (PQCrypto)*, October 2014.
7. A quantum algorithm for computing the unit group of an arbitrary degree number field  
Authors: Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev and Fang Song  
In *46th Annual ACM Symposium on Theory of Computing (STOC)*, June 2014.  
**Plenary** talk at *18th Conference on Quantum Information Processing (QIP)*, January 2015.
8. Feasibility and completeness of cryptographic tasks in the quantum world  
Authors: Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou and Vassilis Zikas  
In *10th Theory of Cryptography Conference (TCC)*, March 2013.  
Also presented in *6th International Conference on Information Theoretic Security (ICITS)*, workshop track, August 2012.
9. Classical cryptographic protocols in a quantum world  
Authors: Sean Hallgren, Adam Smith and Fang Song

In *Advances in Cryptology, 31st Annual Cryptology Conference (CRYPTO)*, August 2011.  
Feature talk at *14th Workshop on Quantum Information Processing (QIP)*, January 2011.

#### ◇ **Publications in Refereed Journals**

10. Classical cryptographic protocols in a quantum world  
Authors: Sean Hallgren, Adam Smith, Fang Song  
*International Journal of Quantum Information*, Volume 13, Issue 04, 2015. (by invitation)

#### ◇ **Manuscripts and Preprints**

11. Pseudorandom states and unitaries, and applications to quantum money  
Authors: Zhengfeng Ji, Yi-Kai Liu, Fang Song  
*Under submission*. Available at [arXiv:1711.00385](https://arxiv.org/abs/1711.00385), November 2017
12. Basing cryptography on NP-hardness using quantum reductions  
Authors: Nai-Hui Chia, Sean Hallgren, Fang Song  
*Under submission*. October 2017
13. Quantum Collision-Finding in Non-Uniform Random Functions  
Authors: Marko Balogh and Edward Eaton and Fang Song  
*Under submission*. Available at *Cryptology ePrint Archive: Report 2017/688*, July 2017
14. On quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in  $\mathbb{Q}(\zeta_p^n)$   
Authors: Jean-François Biasse and Fang Song  
*CACR Tech Report CACR2015-12*, September 2015.  
Poster at *19th Conference on Quantum Information Processing (QIP)*, January, 2016.  
Mentioned in “A Tricky Path to Quantum-Safe Encryption”, *Quanta Magazine*, September 9, 2015.

## **Teaching & Advising**

#### ◇ **Advising**

- Ph.D. Sept. 2017 - Asher Toback  
Portland State University
- Undergraduate Sept. 2016 - Jun. 2017 Marko Balogh, *Honors Baccalaureate Thesis*  
Portland State University  
A research paper under submission
- May 2014 - Aug. 2014 Edward Eaton, *Undergraduate Research Opportunities*  
(and continuing) Institute for Quantum Computing, University of Waterloo  
A research paper accepted in *TQC 2015*  
Awarded *Outstanding Achievement in Graduate Studies*  
as a M.Sc student at University of Waterloo

## ◇ Courses

- Spring 2017 [CS 410/510 Introduction to Quantum Computing](#), Portland State University
- Winter 2017 [CS 485/585 Introduction to Cryptography](#), Portland State University
- Spring 2016 [QIC 891 Topics in Quantum Safe Cryptography](#), Module 1: [Post-Quantum Cryptography](#), University of Waterloo
- Spring 2015 [QIC 890/891 Selected Advanced Topics in Quantum Information](#), Module 1: Quantum Algorithms for Number Theory Problems, University of Waterloo

## ◇ Teaching Assistant

- Fall 2011, Spring 2011 [CMPSC464 Introduction to Theory of Computation](#), Department of CSE, Pennsylvania State University  
Received Outstanding Teaching Assistant Award
- Fall 2008 [CMPSC311 Introduction to Systems Programming](#)  
Department of CSE, Pennsylvania State University

## Professional Activities

### ◇ Conference Program Committee member

- Post-quantum Cryptography (PQC) Fort Lauderdale, Florida, April, 2018
- IACR Asiacrypt (ASIACRYPT) Hong Kong, China, December 2017
- Post-quantum Cryptography (PQC) Utrecht, the Netherlands, June, 2017
- Public Key Cryptography (PKC) Amsterdam, The Netherlands, March 2017
- Quantum Information Processing (QIP) Seattle, WA, January 2017

### ◇ (Organizing)

- Jan. 2017 [Quantum day symposium at PDX](#), Portland State University
- Apr. 2015 - Aug. 2016 [Post-quantum crypto seminar](#) at University of Waterloo  
founder and organizer
- Jun. 2012 [Graduate summer school on cryptography and principles of computer security](#), Pennsylvania State University  
helper and poster session coordinator

### ◇ Referee

- JOURNAL REVIEWER [Algorithmica](#), [IEEE Transaction on Information Theory](#), [International Journal of Quantum Information](#), [Theoretical Computer Science](#)
- CONFERENCE REVIEWER [PKC 2018](#), [QIP 2018](#), [Eurocrypt 2018](#), [QCrypt 2017](#), [Eurocrypt 2017](#), [Crypto 2017](#), [PQCrypto 2016](#), [ISAAC 2015](#), [QIP 2015](#), [Asiacrypt 2014](#), [QCrypt 2014](#), [TQC 2014](#), [TCC 2014](#), [Crypto 2013](#), [PQCrypto 2013](#), [FOCS 2012](#), [Crypto 2011](#)

## ◇ Misc

- CONFERENCES ATTENDED Crypto 2017, Asia PQC Forum 2017, QIP17, FOCS16, Dagstuhl Workshop on Quantum Cryptanalysis, September 2015, Simon's Institute Crypto Workshop, June 2015, QIP, January 15, PQCrypto, October 2014; STOC, June 2014, NIST-UMD Workshop on Quantum Information and Computer Science, April 2014; Dagstuhl Workshop on Quantum Cryptanalysis, September 2013; QIP, January 2013; STOC June 2012, QIP'12, December 2011; Crypto, August 2011; STOC, June 2011; QIP, January 2011; STOC, June 2010; SODA, January 2009.

## Selected Talks & Presentations

### ◇ Conference Presentations

- Zero-knowledge proof systems for QMA
  - *QIP 2017*, Seattle, WA, January 2017
  - *FOCS 2016*, New Brunswick, NJ. October 2016
- A quantum algorithm for computing the unit group in a number field of arbitrary degree *QIP 2015*, **plenary** talk , Sydney, Australia. January 2015.
- Quantum security for post-quantum cryptography: quantum-friendly reductions *PQCrypto 2014*, Waterloo, Canada. October 2014.
- Feasibility and completeness of cryptographic tasks in the quantum world Poster at *STOC 2012*, New York, NY. June 2012.
- Classical cryptographic protocols in a quantum world
  - *CRYPTO 2011*, Santa Barbara, CA. August 2012.
  - *QIP 2011*, **featured** talk, Singapore. January 2011.

### ◇ Invited Talks

- Quantum computing and post-quantum computation 2nd PQC Asia Forum, Seoul, Korea. November 2016.
- Zero-knowledge proof systems for QMA QUICS, University of Maryland, College Park, MD. October 2016.
- A quantum algorithm for computing the unit group in a number field of arbitrary degree
  - Academia Sinica, Taiwan. December 2014.
  - Department of Pure Mathematics, University of Waterloo. October 2014.
  - IQC, Quantum complexity seminar. December 2013.
- Cryptography in a quantum world
  - Institute for Quantum Computing. February 2013.
  - Cryptography group, Aarhus University. January 2013.

## Contact

- Email: fang.song@pdx.edu
- Phone: +1 (503) 725-4060
- Homepage: <http://www.fangsong.info/>
- Address: FAB 120-07, 1900 SW 4th Avenue Suite 120 Portland, OR 97201

☞ **References available upon request**