FANG SONG 宋方
www.fangsong.info CURRICULUM VITAE fang.song@pdx.edu

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

Publications

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

◇ Publications in Refereed Conferences

1. Fang Song and Aaram Yun (2017). "Quantum Security of NMAC and Related Constructions - PRF Domain Extension Against Quantum attacks". In: *Advances in Cryptology - CRYPTO 2017*. Vol. 10402. Lecture Notes in Computer Science. Springer, pp. 283–309. URL: https://doi.org/10.1007/978-3-319-63715-0_10
2. Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous (2016). "Zero-Knowledge Proof Systems for QMA". in: *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016*. IEEE Computer Society, pp. 31–40. URL: https://doi.org/10.1109/FOCS.2016.13
3. Andreas Hülsing, Joost Rijneveld, and Fang Song (2016). "Mitigating Multi-target Attacks in Hash-Based Signatures". In: *19th IACR International Conference on Practice and Theory in Public-Key Cryptography – PKC 2016*. Vol. 9614. Lecture Notes in Computer Science. Springer, pp. 387–416. URL: https://doi.org/10.1007/978-3-662-49384-7_15
4. Jean-François Biasse and Fang Song (2016). "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, pp. 893–902. URL: https://doi.org/10.1137/1.9781611974331.ch64
5. Edward Eaton and Fang Song (2015). "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*. Vol. 44. LIPIcs. Schloss Dagstuhl, pp. 147–162. URL: https://doi.org/10.4230/LIPIcs.TQC.2015.147
6. Fang Song (2014). "A Note on Quantum Security for Post-Quantum Cryptography". In: *Post-Quantum Cryptography – 6th International Workshop, PQCrypto 2014*. Vol. 8772. Lecture Notes in Computer Science. Springer, pp. 246–265. URL: https://doi.org/10.1007/978-3-319-11659-4_15
7. Kirsten Eisenträger, Sean Hallgren, Alexei Y. Kitaev, and Fang Song (2014). "A quantum algorithm for computing the unit group of an arbitrary degree number field". In: *Proceedings of the forty-sixth annual ACM Symposium on Theory of Computing, STOC 2014*. ACM, pp. 293–302. URL: http://doi.acm.org/10.1145/2591796.2591860
8. Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas (2013). "Feasibility and Completeness of Cryptographic Tasks in the Quantum World". In: *Theory of Cryptography - 10th Theory of Cryptography Conference, TCC 2013*. Vol. 7785. Lecture Notes in Computer Science. Springer, pp. 281–296. URL: https://doi.org/10.1007/978-3-642-36594-2_16
9. Sean Hallgren, Adam D. Smith, and Fang Song (2011). "Classical Cryptographic Protocols in a Quantum World". In: *Advances in Cryptology – CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*. Ed. by Phillip Rogaway. Vol. 6841. Lecture Notes in Computer Science. Springer, pp. 411–428. DOI: 10.1007/978-3-642-22792-9_23. URL: https://doi.org/10.1007/978-3-642-22792-9_23

◇ Publications in Refereed Journals

10. Sean Hallgren, Adam Smith, and Fang Song (2015). "Classical cryptographic protocols in a quantum world". In: *International Journal of Quantum Information* 13.04, p. 1550028. URL: https://doi.org/

10.1142/S0219749915500288

◇ Manuscripts and Preprints

11. Zhengfeng Ji, Yi-Kai Liu, and Fang Song (October 2017). *Pseudorandom states and unitaries, and applications to quantum money*. Under submission
12. Nai-Hui Chia, Sean Hallgren, and Fang Song (October 2017). *Basing cryptography on NP-hardness using quantum reductions*. Under submission
13. Marko Balogh, Edward Eaton, and Fang Song (2017). *Quantum Collision-Finding in Non-Uniform Random Functions*. IACR Cryptology ePrint Archive, Report 2017/688
14. Jean-François Biasse and Fang Song (September 2015). *On quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in* $\mathbb{Q}(\zeta_{p^n})$. CACR Tech Report CACR2015-12. 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 (and continuing)	Edward Eaton, *Undergraduate Research Opportunities* 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

◇ (Co-)Organizer

- Jan. 2017 — Quantum day symposium at PDX (webpage), 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, International Journal of Quantum Information, IEEE Transaction on Information Theory
- Conference reviewer — 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 — 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, Arhus 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