Fang Song

✉ fang.song@pdx.edu
🌐 https://fangsong.info
G https://scholar.google.com/citations?hl=en&user=A6C3geAAAAAJ

Research Interests

Quantum-safe cryptography ◇ quantum provable security, quantum cryptography, zero-knowledge proofs;

Quantum computing ◇ quantum algorithms, quantum complexity theory, quantum pseudorandomness.

Employment

09/2016 – ◇ **Assistant Professor, Portland State University**, Portland, OR, USA.
Computer Science Department.

09/2018 – 02/2020 ◇ **Assistant Professor, Texas A&M University**, College Station, TX, USA.
Department of Computer Science and Engineering.
(On leave from Portland State University)

09/2013 – 08/2016 ◇ **Postdoctoral Fellow, University of Waterloo**, Waterloo, ON, Canada.
Institute for Quantum Computing (IQC),
and Department of Combinatorics & Optimization.
Mentors: Andrew Childs, Debbie Leung, Michele Mosca.

Education

08/2008 – 08/2013 ◇ **Ph.D., Pennsylvania State University**, University Park, PA, USA.
Computer Science and Engineering.
Thesis: *Quantum Computing: A Cryptographic Perspective*.
Advisor: Sean Hallgren

09/2004 – 06/2008 ◇ **B.Sc., University of Sci. and Tech. of China (USTC)**, Hefei, Anhui, China.
Department of Information Security.
Thesis: Primitives on Quantum Anonymous Communications
Advisors: Liusheng Huang & Baosen Shi

Honors & Awards

03/2022 ◇ Sony Faculty Innovation Award.

01/2021 ◇ Long **Plenary** talk (equivalent to **Best Paper**) at *QIP'21*.

04/2020 ◇ **NSF CAREER Award**.

01/2020 – 05/2020 ◇ Research fellowship at **Simons Institute for the Theory of Computing**,
Lattices: Algorithms, Complexity, and Cryptography.

08/2018 ◇ Appreciation to mentor at Saturday Academy's K-12 Apprenticeship program.

01/2015 ◇ **Plenary** talk (equivalent to **Best Paper**) at *QIP'15*.

Honors & Awards (continued)

09/2013 – 08/2016 ◇ Research funded by **Cryptoworks21**, Ontario Research Fund (**ORF**), Natural Sciences and Engineering Research Council of Canada (**NSERC**).

05/2012 ◇ Outstanding Teaching Assistant Award, Pennsylvania State University.

08/2008 ◇ College of Engineering Fellowship, Pennsylvania State University.

07/2008 ◇ Outstanding Undergraduate Thesis Award, USTC.

Funding

10/2022 – 09/2024 ◇ US National Science Foundation (NSF) Award #2224131, **$299,549**.
Collaborative Research: FET: Small: Minimum Quantum Circuit Size Problems, Variants, and Applications.

03/2022 – 03/2023 ◇ Sony Corporation of America. Sony Faculty Innovation Award, **$100,000**.
Post-Quantum Blockchains – Formal Analysis and Applications..
PI: Fang Song. Co-PI (subawardee): Juan Garay, Texas A&M University.

04/2020 – 03/2025 ◇ US National Science Foundation (NSF) **CAREER** Award #2054758, **$559,775**.
FET: CAREER: Algorithms, cryptography and complexity meet quantum reductions.

10/2018 - 09/2022 ◇ US National Science Foundation (NSF) Award #1816869 (#2041841), **$283,852**.
AF: Small: Quantum Computational Pseudorandomness with Applications.

08/2018 - 07/2022 ◇ US National Science Foundation (NSF) Award #1764042 (#2042414), **$274,752**.
AF: Medium: Collaborative Research: Quantum-Secure Cryptography and Fine-Grained Quantum Query Complexity.
10/2021 - 07/2022 REU supplement, $16,000.

Professional Activities

Conference Program Committee member

2022 ◇ Quantum Cryptography Workshop (**QCW**), affiliated with IACR Asiacrypt, Taipei, Taiwan.

◇ IACR Asiacrypt (**ASIACRYPT**), Taipei, Taiwan.

◇ Quantum Information Processing (**QIP**), Pasadena, USA. Student Travel Award Committee.

2021 ◇ IACR Cryptology Conference (**CRYPTO**), Santa Barbara, USA.

◇ Information-theoretical Cryptography (**ITC**), Rome, Italy.

◇ Public Key Cryptography (**PKC**), Edinburgh, Scotland.

2020 ◇ Conference on Quantum Cryptography (**QCrypt**), Amsterdam, the Netherlands.

◇ IACR Cryptology Conference (**CRYPTO**), Santa Barbara, USA.

◇ ACM Asia Computer and . . . Security (**AsiaCCS**), Taipei, Taiwan.

2019 ◇ Selected Areas in Cryptography (**SAC**), Waterloo, Canada.

◇ Mathematical Cryptology (**MathCrypt**), Santa Barbara, USA.

◇ Post-quantum Cryptography (**PQC**), Chongqing, China.

Professional Activities (continued)

2018	◇ Mathematical Cryptology (**MathCrypt**), Santa Barbara, USA.
	◇ Theory of Quantum Computing . . . (**TQC**), Sydney, Australia.
	◇ Post-quantum Cryptography (**PQC**), Fort Lauderdale, USA.
2017	◇ IACR Asiacrypt (**ASIACRYPT**), Hong Kong, China.
	◇ Post-quantum Cryptography (**PQC**), Utrecht, the Netherlands.
	◇ Public Key Cryptography (**PKC**), Amsterdam, the Netherlands.
	◇ Quantum Information Processing (**QIP**), Seattle, USA.

Organizing

01/2021 –	◇ *Big Ideas for Small Quantum Computers (BISQC) online seminar series*, founder and organizer, Portland State University.
05/2020	◇ *The 2nd Quantum Computation and Information Workshop*, Texas A&M University.
01/2017	◇ *Quantum day symposium at PDX*, Portland State University.
04/2015 – 08/2016	◇ *Post-quantum crypto seminar*, founder and organizer, University of Waterloo.
06/2012	◇ *Graduate summer school on cryptography and principles of computer security*, local organizer and poster session coordinator, Pennsylvania State University.

Referee

Grant Panelist	◇ NSF MPS/DMR 2022, NSF SaTC 2020, NSF CCF 2020, NSF CCF 2019.
Grant Reviewer	◇ NSF IIP (SBIR) 2021, NSF CCF 2021, NSF SaTC 2021, NSF PHY 2020, NSF SaTC 2019.
Journal reviewer	◇ Algorithmica, IEEE Transaction on Information Theory, International Journal of Quantum Information, Journal of Cryptology, Journal of Mathematical Cryptology, Quantum (open journal for quantum science), Quantum Information and Computation (QIC), Theoretical Computer Science.
Conference reviewer	◇ TCC 2022, Crypto 2022, SODA 2022, Eurocrypt 2022, QIP 2022, QCrypt 2021, PKC 2021, ISIT 2021, Eurocrypt 2021, TCC 2020, Provesec 2020, Asiacrypt 2020, ICALP 2020, Eurocrypt 2020, QIP 2020, FOCS 2019, Crypto 2019, ISIT 2019, STOC 2019, Eurocrypt 2019, FOCS 2018, QCrypt 2018, 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.
Book Reviewer	◇ Princeton University Press (2021), Springer (2020).

Publications

(Note: **alphabetical** authorship order as per common practice in theoretical computer science, unless otherwise specified.)

Publications in Refereed Conferences

2021 ◇ **Quantum Key-length Extension**
Authors: Joseph Jaeger, Fang Song, and Stefano Tessaro
In the *19th Theory of Cryptography Conference* (***TCC***), November 2021.

Publications (continued)

◇ **Oblivious Transfer is in MiniQCrypt**
Authors: Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan
In the *40th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (***EUROCRYPT***), October 2021.
Long plenary talk (equivalent to **Best Paper**) at the *24th Annual Conference on Quantum Information Processing* (***QIP***), January 2021.

2020 ◇ **Quantum-secure message authentication via blind-unforgeability**
Authors: Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song
In the *39th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (***EUROCRYPT***), May 2020.

◇ **A note on the instantiability of the quantum random oracle**
Authors: Edward Eaton and Fang Song
In the *11th International Conference on Post-Quantum Cryptography* (***PQCrypto***), September 2020.

2019 ◇ **General Linear Group Action on Tensors: A Candidate for Post-Quantum Cryptography**
Authors: Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun
In the *17th Theory of Cryptography Conference* (***TCC***), November 2019.
Contributed talk at the *23rd Annual Conference on Quantum Information Processing* (***QIP***), January 2020.

◇ **Quantum security of hash functions and property-preservation of iterated hashing**
Authors: Ben Hamlin and Fang Song
In the *10th International Conference on Post-Quantum Cryptography* (***PQCrypto***), May 2019.

2018 ◇ **Pseudorandom quantum states**
Authors: Zhengfeng Ji, Yi-Kai Liu, and Fang Song
In the *38th International Cryptology Conference* (***CRYPTO***), August 2018.

◇ **Quantum Collision-Finding in Non-Uniform Random Functions**
Authors: Marko Balogh, Edward Eaton, and Fang Song
In the *9th International Conference on Post-Quantum Cryptography* (***PQCrypto***), April 2018.

2017 ◇ **Quantum Security of NMAC and Related Constructions**
Authors: Fang Song and Aaram Yun
In the *37th International Cryptology Conference* (***CRYPTO***), August 2017.

2016 ◇ **Zero-knowledge proof systems for QMA**
Authors: Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous
In the *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.

◇ **Mitigating multi-target attacks in hash-based signatures**
Authors: Andreas Hülsing, Joost Rijneveld, and Fang Song
In the *19th International Conference on the Theory and Practice of Public-Key Cryptography* (***PKC***), March 2016.
Adopted as a guideline in *Internet Research Task Force RFC8391*, May 2018.

◇ **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 the *27th ACM-SIAM Symposium on Discrete Algorithms* (***SODA***), January 2016.
Contributed talk at the *20th Annual Conference on Quantum Information Processing* (***QIP***), January 2017.

Publications (continued)

2015 ◇ **Making existentially unforgeable signatures strongly unforgeable in the quantum-random oracle model**
Authors: Edward Eaton and Fang Song
In the *10th Conference on the Theory of Quantum Computation, Communication and Cryptography (**TQC**)*, May 2015.

2014 ◇ **A note on quantum security for post-quantum cryptography**
Authors: Fang Song
In the *6th International Conference on Post-Quantum Cryptography (**PQCrypto**)*, October 2014.

◇ **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 the *46th Annual ACM Symposium on Theory of Computing (**STOC**)*, June 2014.
Plenary talk (equivalent to **Best Paper**) at *18th Conference on Quantum Information Processing (**QIP**)*, January 2015.

2013 ◇ **Feasibility and completeness of cryptographic tasks in the quantum world**
Authors: Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas
In the *10th Theory of Cryptography Conference (**TCC**)*, March 2013.
Presented at the *6th International Conference on Information Theoretic Security (**ICITS**)*, workshop track, August 2012.

2011 ◇ **Classical cryptographic protocols in a quantum world** Authors: Sean Hallgren, Adam Smith, and Fang Song
In the *31st International Cryptology Conference (**CRYPTO**)*, August 2011.
Feature talk at *14th Workshop on Quantum Information Processing (**QIP**)*, January 2011.

Publications in Refereed Journals

2022 ◇ **Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography**
Authors: J-F Biasse, X. Bonnetain, E Kirshanova, A. Schrottenloher, and F. Song
IET Information Security, 1-39, 2022.

2020 ◇ **On Basing One-way Permutations on NP-hard Problems under Quantum Reductions**
Authors: Nai-Hui Chia, Sean Hallgren, and Fang Song
Quantum, Volume 4, 312, 2020.
Contributed talk at the *8th International Conference on Quantum Cryptography (**QCrypt**)*, September 2018.

◇ **Zero-Knowledge Proof Systems for QMA**
Authors: Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous
SIAM Journal on Computing (**SICOMP**), Volume 49, Issue 2, 245–283, 2020.

2019 ◇ **On the 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
Journal of Mathematical Cryptology, Volume 13, Issue 3-4, Pages 151–168, 2019.
CACR Tech Report CACR2015-12, September 2015.
Poster at *19th Conference on Quantum Information Processing (**QIP**)*, January, 2016.
Highlight in "A Tricky Path to Quantum-Safe Encryption", *Quanta Magazine*, September 9, 2015.

Publications (continued)

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

Manuscripts and Preprints

2021 ◇ **Post-Quantum Blockchain Proofs of Work**
Authors: Alexandru Cojocaru, Juan Garay, Aggelos Kiayias, Fang Song, and Petros Wallden
Preprint quant-ph arXiv:2012.15254v3, December 2021.

Teaching & Advising

Advising

Ph.D.

◇ Mehil Agarwal, 09/2021 –
Portland State University

◇ Nikhil Pappu, 09/2021 –
Portland State University

◇ Chuhan Lu, 06/2020 –
Portland State University
09/2019 – 05/2020 at Texas A&M University

◇ Ben Hamlin, 09/2020 –
Portland State University
09/2018 – 05/2019 at Texas A&M University

◇ Mufeng Xie, 09/2019 – 05/2020
Texas A&M University

◇ Asher Toback, 09/2017 – 08/2018
Portland State University

Undergraduate

◇ Grant VanDomelen, 06/2022 –
Research Experience for Undergraduate (REU)
Sponsored by NSF REU supplement
Portland State University

◇ Felina Kang, 03/2022 –
Research Experience for Undergraduate (REU)
Sponsored by NSF REU supplement
Portland State University

◇ Davis Beilue, 09/2019 – 04/2020
Undergraduate Research Scholars Thesis
Texas A&M University

◇ Darryl Cherian Jacob, 09/2019 – 04/2020
Undergraduate Research Scholars Thesis
Texas A&M University

Teaching & Advising (continued)

◇ Marko Balogh, 09/2016 – 06/2017
Honors Baccalaureate Thesis
Portland State University
A research paper published in *PQCrypto 2018*

◇ Edward Eaton, 05/2014 – 08/2014 (and continuing)
Undergraduate Research Opportunities
Institute for Quantum Computing, University of Waterloo
A research paper published in *TQC 2015*
Awarded *Outstanding Achievement in Graduate Studies* as a M.Sc student at University of Waterloo

K-12 ◇ Sydney Von Arx, Lake Oswego High School
06/2018 – 08/2018, **Saturday academy ASE internship**
Now CS major at Stanford University

◇ Marshal Xu, Lincoln High School
06/2018 – 08/2018, **Saturday academy ASE internship**
Now CS major at University of Pennsylvania

Courses

Fall 2022	◇ *CS 581 Theory of computation*, Portland State University.
	◇ *CS 410/510 Intro to Quantum Computing*, Portland State University.
Winter 2022	◇ *CS 485/585 Introduction to Cryptography*, Portland State University.
Fall 2021	◇ *CS 581 Theory of computation*, Portland State University.
	◇ *CS 410/510 Foundations of emerging technologies*, Portland State University.
Winter 2021	◇ *CS 510/610 Topic: probalistic graphical models*, Portland State University.
	◇ *CS 584/684 Algorithm Design And Analysis*, Portland State University.
Spring 2020	◇ *CS 410/510 Introduction to Quantum Computing*, Portland State University.
Fall 2019	◇ CSCE 629 Analysis of Algorithms, Texas A&M University.
Spring 2019	◇ *CSCE 440/640 Quantum Algorithms*, Texas A&M University.
Fall 2018	◇ *CSCE 689 Foundations of Post-Quantum Cryptography*, Texas A&M University.
Spring 2018	◇ *CS 410/510 Introduction to Quantum Computing*, Portland State University.
Winter 2018	◇ *CS 485/585 Introduction to Cryptography*, Portland State University.
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*, Pennsylvania State University. Received Outstanding Teaching Assistant Award.
Fall 2008	◇ *CMPSC311 Introduction to Systems Programming*, Pennsylvania State University.

Selected Talks

2022 ◇ **Introduction to Quantum Information**
Invited lectures at the *IPAM Graduate Summer School on Post-quantum and Quantum Cryptography*, July, 2022.

2021 ◇ **Quantum-secure key-length extension**
Invited Zoom talk at the *EWHA-KMS International Workshop on Cryptography*, June 2021.

2020 ◇ **Unpredictable Functions and Quantum-secure Authentication**
Invited Zoom talk at the *International Joint Conference on Theoretical Computer Science*. (IJTCS), August 2020.

◇ **Cybersecurity in a quantum world**
Invited Zoom talk at the *Portland quantum computing meetup group*, August 2020.

◇ **Cryptography from NP Hardness: can quantum help?**
Simons Institute for the Theory of Computing, Berkeley, February, 2020.
Invited talk at the *2nd IAMCS Quantum Computation and Information Workshop*, TAMU, May 13-15, 2019.

2019 ◇ **Zero-knowledge proofs meet quantum computing**
Invited tutorial at the *9th International Conference on Quantum Cryptography (**QCrypt**)*, Montreal, Canada, August 2019.

◇ **Pseudorandom quantum states**
Invited talk at the *AMS Spring Central and Western Joint Sectional Meeting*, University of Hawaii at Manoa, Honolulu, HI, March 22-24, 2019.
Invited talk at the *1st IAMCS Quantum Computation and Information Workshop*, TAMU, TX, September 20-22, 2018.

2018 ◇ **Pseudorandom quantum states**
Crypto 2018, Santa Barbara, CA, August 2018.

2017 ◇ **Zero-knowledge proof systems for QMA**
QIP 2017, Seattle, WA. January 2017.
FOCS 2016, New Brunswick, NJ. October 2016.

2016 ◇ **Quantum computing and post-quantum computation**
Invited talk at the *2nd PQC Asia Forum*, Seoul, Korea. November 2016.

◇ **Zero-knowledge proof systems for QMA**
QUICS, University of Maryland, College Park, MD. October 2016.

2015 ◇ **A quantum algorithm for computing the unit group in a number field of arbitrary degree**
QIP 2015, **plenary** talk, Sydney, Australia. January 2015.

2014 ◇ **Quantum security for post-quantum cryptography: quantum-friendly reductions**
PQCrypto 2014, Waterloo, Canada. October 2014.

◇ **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.
Quantum complexity seminar, IQC. December 2013.

2013 ◇ **Cryptography in a quantum world**
Institute for Quantum Computing. February 2013.
Cryptography seminar, Arhus University. January 2013.

Selected Talks (continued)

2012 ◇ **Feasibility and completeness of cryptographic tasks in the quantum world**
Poster at *STOC 2012*, New York, NY. June 2012.

2011 ◇ **Classical cryptographic protocols in a quantum world**
CRYPTO 2011, Santa Barbara, CA. August 2012.
QIP 2011, **featured** talk, Singapore. January 2011.