FANG SONG

CURRICULUM VITAE

fang.song@uwaterloo.ca

Research Interests

- Cryptography (quantum-safe crypto in particular), quantum algorithms, computational complexity, theoretical computer science.

Education

- August 2008 - August 2013: PhD, Computer Science and Engineering
  Pennsylvania State University, University Park, PA, USA
  Thesis: Quantum Computing: A Cryptographic Perspective
  Advisor: Dr. Sean Hallgren
- September 2004 - June 2008: Bachelor of Science, Department of Information Security
  University of Sci. and Tech. of China, Hefei, Anhui, China
  Thesis: Primitives on Quantum Anonymous Communications
  Advisor: Dr. Liusheng Huang & Dr. Baosen Shi

Employment

- September 2013 - present: Postdoctoral Fellow
  Institute for Quantum Computing and Department of Combinatorics & Optimization,
  University of Waterloo, Waterloo, ON Canada
  Supervisors: Andrew Childs, Debbie Leung, Michele Mosca
- January 2009 - July 2013: Research Assistant
  Department of Computer Science and Engineering,
  Pennsylvania State University, University Park, PA USA
- September 2008 - December 2008 & January 2011 - December 2011: Teaching Assistant
  Department of Computer Science and Engineering,
  Pennsylvania State University, University Park, PA USA

Honors & Awards

- January 2015: **Plenary** talk at *QIP'15*, Sydney, Australia. (It's of prestigious honor in quantum community. 6 were chosen out of 197 submissions).
- September 2013 - present: support from Cryptoworks21, Ontario Research Fund (ORF), Natural Sciences and Engineering Research Council of Canada (NSERC).
- May 2012: **Outstanding Teaching Assistant Award**, Department of Computer Science and Engineering, Pennsylvania State University.
- August 2008: College of Engineering Fellowship, Pennsylvania State University.
- July 2008: Outstanding Undergraduate Thesis Award, University of Sci. & Tech. of China.

Publications

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

◇ Publications in Refereed Conferences

1. Mitigating multi-target attacks in hash-based signatures
   Authors: Andreas Hülsing, Joost Rijneveld and Fang Song
   *T*o appear in *19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC)*, March 2016.

2. 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.
   To appear in *27th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, January 2016.

3. 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.

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

5. 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.
   Also accepted as a **plenary** talk at *18th Conference on Quantum Information Processing (QIP)*, January 2015.

6. 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.

7. 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.
   Also accepted as a featured talk at *14th Workshop on Quantum Information Processing (QIP)*, January 2011.

◇ Publications in Refereed Journals

8. 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

9. Zero-knowledge proof systems for QMA
Authors: Anne Broadbent, Zhengfeng Ji, Fang Song and John Watrous
Under Submission, November 2015.

10. 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.
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

◇ Instructor

- Spring 2015: *QIC 890/891 Selected Advanced Topics in Quantum Information*
Module 1 - Quantum Algorithms for Number Theory Problems
Institute of Quantum Computing, University of Waterloo.

◇ Advising

- May 2014 - Aug. 2014: Edward Eaton. *Undergraduate Research Opportunities*,
Institute for Quantum Computing, University of Waterloo.
Now a M.Sc student at University of Waterloo (and collaboration is continuing).
A research paper produced and accepted in *TQC 2015*.

◇ Teaching Assistant

- Fall 2011 & Spring 2011: *CMPSC464 Introduction to Theory of Computation*.
Department of CSE, Pennsylvania State University.
Duties: weekly recitation sessions; help design homework and exam problems; office hours; grading.
Received **Graduate Student Teaching Assistant Award**.
- Fall 2008: *CMPSC311 Introduction to Systems Programming*.
Department of CSE, Pennsylvania State University.
Duties: grading; office hours; lab sessions.

Professional Activities

- April 2015 - present: **founder** of *post-quantum crypto seminar* at University of Waterloo.

- June 2012: helped organize *graduate summer school on cryptography and principles of computer security*, Penn State University.

- JOURNAL REVIEWER FOR: International Journal of Quantum Information; IEEE Transaction on Information Theory.

- CONFERENCE REVIEWER FOR: PQCrypto 2016; ISAAC 2015; QIP 2015; Asiacrypt 2014; QCrypt 2014; TQC 2014; TCC 2014; Crypto 2013; PQCrypto 2013; FOCS 2012; Crypto 2011.
- CONFERENCES ATTENDED: 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

- 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

- 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@uwaterloo.ca`
- Phone: +1 (519) 888-4567 ext. 39048
- Homepage: `http://www.fangsong.info/`
- Address: Quantum-Nano Center 3128, University of Waterloo, Wateloo, ON Canada, N2L 3G1.

☞ References available upon request