John M. Schanck

Email: jmschanck@gmail.com **Phone**: +1 (226) 600 6111 **Web**: https://jmschanck.info

Personal Profile

I am an applied cryptographer with a strong background in mathematics and software engineering. My current goal is to find a position that allows me to conduct research, publish academic articles, and involve myself with standards organizations such as NIST and IETF. My research to date has been in post-quantum cryptography and cryptanalysis, but I am broadly interested in computer security and the analysis of algorithms. I am particularly interested in developing and analyzing algorithms for emerging and unconventional computer architectures.

Education

2016-2020 Ph.D.
Institute for Quantum Computing
Department of Combinatorics and Optimization
University of Waterloo, Waterloo, ON, Canada.

Thesis: *Improving post-quantum cryptography through cryptanalysis* [pdf]

2013-2015 M.Math.
Institute for Quantum Computing
Department of Combinatorics and Optimization
University of Waterloo, Waterloo, ON, Canada.

Thesis: *Practical lattice cryptosystems: NTRUEncrypt and NTRUMLS* [pdf]

2007-2011 B.A.
Hampshire College, Amherst, MA, USA

Thesis: *Classical and Quantum Information Theory* [pdf]

Employment History

Oct. 2011-Jan. 2017 Security Innovation, Wilmington, MA, USA
Senior Cryptographer

I was involved in the design and analysis of cryptographic protocols such as the PASS and pqNTRUSign signature schemes. I also wrote software that was made available through the "NTRU Open Source Project" [www].

Selected publications

- Nina Bindel and John M. Schanck. Decryption failure is more likely after success. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*, pages 206–225. Springer, Heidelberg, 2020. [pdf]
- Samuel Jaques and John M. Schanck. Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 32–61. Springer, Heidelberg, August 2019. **Best Young Researcher Paper Award** [pdf]

- J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367, April 2018. [pdf]
- Andreas Hülsing, Joost Rijneveld, John M. Schanck, and Peter Schwabe. High-speed key encapsulation from NTRU. In Wieland Fischer and Naofumi Homma, editors, *CHES 2017*, volume 10529 of *LNCS*, pages 232–252. Springer, Heidelberg, September 2017. [pdf]
- John M. Schanck, William Whyte, and Zhenfei Zhang. Circuit-extension handshakes for Tor achieving forward secrecy in a quantum world. *PoPETs*, 2016(4):219–236, October 2016. [pdf]
- Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte. Transcript secure signatures based on modular lattices. In Michele Mosca, editor, *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014*, pages 142–159. Springer, Heidelberg, October 2014. [pdf]
- Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte. Practical signatures from the partial fourier recovery problem. In Ioana Boureanu, Philippe Owesarski, and Serge Vaudenay, editors, *ACNS 14*, volume 8479 of *LNCS*, pages 476–493. Springer, Heidelberg, June 2014. [pdf]

A complete list of my publications can be found at: https://jmschanck.info/papers/.

Selected standardization work

- Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2019. [www, zip]
- Cong Chen, Oussama Danba, Jeffrey Hoffstein, Andreas Hülsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, and Zhenfei Zhang. NTRU. Technical report, National Institute of Standards and Technology, 2019. **Principal submitter** [www, zip]

Service

- **Journal submission reviews**
  Designs, Codes, and Cryptography (4 reviews). Journal of Mathematical Cryptology (1 review).
- **Conference submission reviews**
  ACNS (2018). Africacrypt (2017). AsiaCCS (2020). Asiacrypt (2012, 2017, 2018, 2019, 2020). Crypto (2020). Eurocrypt (2019, 2020). Financial Crypto (2019). NuTMiC (2017). PKC (2017, 2018). PQCrypto (2020). ProvSec (2014). QIP (2017, 2018). SAC (2019).
- **Scientific consulting**
  QUANTUM: The Exhibition [www].
- **Summer school teaching**
  Quantum Cryptography School for Young Students (2015, 2016, 2018, 2019) [www].

Patents

- Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William J. Whyte. Digital signature method, Aug. 1, 2017. [pdf]
- Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William J. Whyte. Digital signature technique, Apr. 25, 2017. [pdf]