Victor Shoup

Curriculum Vitae December 9, 2019

Department of Computer Science
Courant Institute of Mathematical Sciences
New York University
251 Mercer Street
New York, NY 10012
Tel: (646) 403-7853; email: victor@shoup.net
URL: http://www.shoup.net

Employment History

Visiting Reseach Scientist, Cryptography Research Group, IBM T. J. Watson Research Lab, Yorktown Heights, New York, April 2012–present.

Professor, Computer Science Dept., Courant Institute of Mathematical Sciences, New York University, Jan. 2007–present.

Associate Professor, Computer Science Dept., Courant Institute of Mathematical Sciences, New York University, Sept. 2002–Jan. 2007.

Research Scientist, Network Security Group, IBM Zurich Research Lab, Feb. 1997–Aug. 2002.

Research Scientist, Security Research Group, Bellcore, Morristown, N. J., June 1995–Jan. 1997.

Alexander von Humboldt research fellow, Universität des Saarlandes, Germany, Sept. 1993–June 1995.

Postdoctoral fellow, Univ. of Toronto, Computer Science Department, Sept. 1990–Aug. 1993.

Postdoctoral fellow, AT&T Bell Laboratories, Murray Hill, N. J., Sept. 1989–Sept. 1990.

Education

Ph. D., Computer Science, Univ. of Wisconsin–Madison, 1989; *advisor:* Eric Bach; *thesis title:* Removing randomness from computational number theory; *areas of study:* programming languages, compilers, operating systems, theory of computing, algebra.

M. S., Computer Science, Univ. of Wisconsin–Madison, 1985.

B. S., Mathematics, Computer Science, Univ. of Wisconsin–Eau Claire, 1983.

Awards and Honors

1. 2016: *IACR Fellow* — "For fundamental contributions to public-key cryptography and cryptographic security proofs, and for educational leadership." (`http://www.iacr.org/fellows/2016/`)
2. 2015: *Richard D. Jenks Memorial Prize for Excellence in Software Engineering Applied to Computer Algebra* — "For NTL: A library for doing number theory." (`http://www.sigsam.org/awards/jenks/awardees/2015/`)
3. 2013: *ESORICS best student paper award* — Practical and Employable Protocols for UC-Secure Circuit Evaluation over Zn, with Jan Camenisch and Robert Enderlein.
4. 2011: *AsiaCrypt best paper award*, and *IBM Pat Goldberg best paper award* — A Framework for Practical Universally Composable Zero-Knowledge Protocols, with Jan Camenisch and Stephan Krenn.
5. 2009: *GI (German Computer Science Association) Innovation Award* — Anonymous Credentials on a JavaCard, with Jan Camenisch and Thomas Gross.

Invited Lectures

1. *Coxeter Lecture Series*, The Fields Institute for Research in Mathematical Sciences, Toronto, Canada, October 2015.
2. *Historical Papers in Cryptography Seminar Series*, Summer 2015 program on Cryptography, Simons Institute, Berkeley, California, August 2015. (`http://simons.berkeley.edu/crypto2015/historical-papers-seminar-series`).
3. The Sixth International Conference on Provable Security, Chengdu, China, September 2012.
4. 5th Workshop on Hot Topics in Privacy Enhancing Technologies, Vigo, Spain, July 2012.
5. Applied Cryptography and Network Security, New York, June 2005.
6. Crypto 2004, Santa Barbara, August 2004.
7. Workshop on the Elliptic Curve Discrete Logarithm Problem, Waterloo, Canada, August 2003.
8. RSA Conference 2002, Cryptographer's Track, February 2002.
9. Workshop on the Elliptic Curve Discrete Logarithm Problem, Waterloo, Canada, September 2001.
10. International Symposium on Symbolic and Algebraic Computation, London, Canada, July 2001.

11. LMS Durham Symposium on Computational Number Theory, Durham, England, August 2000.

12. Conference on The Mathematics of Public-Key Cryptography, Toronto, Canada, June 1999.

13. Workshop on the Elliptic Curve Discrete Logarithm Problem, Waterloo, Canada, November 1997.

14. Fourth Annual Conference on Finite Fields and Applications, Waterloo, Ontario, August 1997.

15. IMACS Symposium on Symbolic Computation, Lille, France, June 1993.

16. Workshop on Number Theory and Algorithms, MSRI, Berkeley, CA, March 1990.

17. Summer Meeting of the AMS—Special Session on Cryptography and Number Theory, Boulder, CO, August 1989.

Books (author)

1. *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, 517 pages, June 2005. Revised second edition, 2008. The electronic version of the book is (and will remain) freely available at `http://www.shoup.net/ntb`.

Books (editor)

1. *Advances in Cryptology – CRYPTO 2005 (LNCS 3621)*, Springer, 568 pages, August 2005.

Patents

1. Method for reducing a value modulo a shared secret, with J. Algesheimer, J. Camenisch. US Patent Number 7194089, March 20, 2007.

2. Piggy-backed key exchange protocol for providing secure, low-overhead browser connections when a client requests a server to propose a message encoding scheme, with C. Binding, S. Hild, Y. M. Huang, Y-M., L. O'Connor, S. K. Singhal, M. Steiner. US Patent Number 7039946, May 2, 2006.

3. Agreement and atomic broadcast in asynchronous networks, with C. Cachin, K. Kursawe, F. Petzold. US Patent Number 6931431, August 16, 2005.

4. Method of achieving multiple processor agreement in potentially asynchronous networks, with C. Cachin, K. Kursawe. US Patent Number 6957332, Oct 18, 2005.

5. Piggy-backed key exchange protocol for providing secure low-overhead browser connections from a client to a server using a trusted third party, with C. Binding, S. Hild, Y. M. Huang, Y-M., L. O'Connor, S. K. Singhal, M. Steiner. US Patent Number 6775772, August 10, 2004.

6. Method of achieving optimistic multiple processor agreement in potentially asynchronous networks, with K. Kursawe. US Patent Number 6754845, June 22, 2004.

7. Piggy-backed key exchange protocol for providing secure, low-overhead browser connections to a server with which a client shares a message encoding scheme, with C. Binding, S. Hild, Y. M. Huang, Y-M., L. O'Connor, S. K. Singhal, M. Steiner. US Patent Number 6751731, June 15, 2004.

8. Practical non-malleable public-key cryptosystem, with R. Cramer. US Patent Number 6697488, February 24, 2004.

9. Piggy-backed key exchange protocol for providing secure, low-overhead browser connections when a server will not use a message encoding scheme proposed by a client, with C. Binding, S. Hild, Y. M. Huang, Y-M., L. O'Connor, S. K. Singhal, M. Steiner. US Patent Number 6694431, February 17, 2004.

10. Session key distribution using smart cards, with A. Rubin. US Patent Number 5809140, September 15, 1998.

Standards

1. Editor, ISO/IEC Standard on Encryption Algorithms (18033, Part 2: Asymmetric Encryption).

Software

1. Author and maintainer of *NTL*, a free, high-performance, *C++* library for number theoretic computations. *NTL* consists of approximately 140,000 lines of source code, and has been used and cited in numerous research articles, and in a number of university courses around the world (the software has averaged well over 500 downloads a month for many years, and a quick Google Scholar search reveals several hundred research citations). For more information, visit `http://www.shoup.net/ntl`.

2. Co-author of *HElib*, a library that implements the Brakerski-Gentry-Vaikuntanathan homomorphic encryption scheme. For more information, visit `https://github.com/homenc/HElib`.

Other Professional Activities

1. Program Chair, Crypto 2005.
2. Program committee member:
   - CT-RSA 2020,
   - Crypto 2000, 2003,
   - RSA 2001,
   - Eurocrypt 1999,
   - International Symposium on Symbolic and Algebraic Computation (ISSAC) 1999,
   - Foundations of Computer Science (FOCS) 1994.

Research Articles

These are my research articles that have appeared in journals and/or refereed conferences. They are all available on-line at `http://www.shoup.net/papers`. Authors on multi-author papers are in alphabetical order, except for papers [41] and [47], where all authors are in the order indicated.

1. An improved RNS variant of the BFV homomorphic encryption scheme, with Shai Halevi and Yuriy Polyakov, *Topics in Cryptology — CT-RSA 2019*.
2. Doing real work with FHE: the case of logistic regression, with Jack L. H. Crawford, Craig Gentry, Shai Halevi and Daniel Platt, *WAHC '18 Proceedings of the 6th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, 2019.
3. Faster Homomorphic Linear Transformations in HElib, with Shai Halevi, *CRYPTO 2018*.
4. Implementing BP-Obfuscation Using Graph-Induced Encoding, with Shai Halevi, Tzipora Halevi, and Noah Stephens-Davidowitz, *ACM CCS 2017*.
5. Bootstrapping for HElib, with Shai Halevi, *Eurocrypt 2015*.
6. Algorithms in HElib, with Shai Halevi, *Eurocrypt 2014*.
7. Practical and employable protocols for UC-Secure circuit evaluation over $\mathbf{Z}_n$, with J. Camenisch and R. Enderlein. *ESORICS 2013*.
8. GNUC: A New Universal Composability Framework, with D. Hofheinz. *J. Cryptology*, 2013.
9. Practical chosen ciphertext secure encryption from factoring, with D. Hofheinz and E. Kilz. *J. Cryptology 26(1):102–118*, 2012.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.