Victor Shoup

Curriculum Vitae

August 16, 2024

Tel: (646) 403-7853; email: victor@shoup.net
URL: http://www.shoup.net

Employment history

Principal Research Scientist, Offchain Labs, Nov. 2023–present.

Principal Researcher, DFINITY, Jan. 2021–Nov. 2023.

Professor Emeritus, Computer Science Dept., Courant Institute of Mathematical Sciences, New York University, Jan. 2023–present.

Visiting Reseach Scientist, Cryptography Research Group, IBM T. J. Watson Research Lab, Yorktown Heights, New York, April 2012–Dec 2020.

Professor, Computer Science Dept., Courant Institute of Mathematical Sciences, New York University, Jan. 2007–Jan. 2023.

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. *Real World Cryptography*, Amsterdam, April 2022.
2. *International Congress on Mathematical Software 2020*, Virtual Conference, July 2020.
3. *Coxeter Lecture Series*, The Fields Institute for Research in Mathematical Sciences, Toronto, Canada, October 2015.
4. *Historical Papers in Cryptography Seminar Series*, Summer 2015 program on Cryptography, Simons Institute, Berkeley, California, August 2015.
5. The Sixth International Conference on Provable Security, Chengdu, China, September 2012.
6. 5th Workshop on Hot Topics in Privacy Enhancing Technologies, Vigo, Spain, July 2012.
7. Applied Cryptography and Network Security, New York, June 2005.
8. Crypto 2004, Santa Barbara, August 2004.
9. Workshop on the Elliptic Curve Discrete Logarithm Problem, Waterloo, Canada, August 2003.
10. RSA Conference 2002, Cryptographer's Track, February 2002.
11. Workshop on the Elliptic Curve Discrete Logarithm Problem, Waterloo, Canada, September 2001.

12. International Symposium on Symbolic and Algebraic Computation, London, Canada, July 2001.

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

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

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

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

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

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

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

Books (author)

1. *A Graduate Course in Applied Cryptography*, with Dan Boneh, verion 0.6 of a free online book, 1116 pages, January 2023. Available at: `http://toc.cryptobook.us/`.

2. *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.

Book chapters

1. Arithmetic software libraries, in *Computational Cryptography*, J. Bos and M. Stam, editors, Cambridge University Press, 2022.

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 `https://libntl.org/`.

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.

Peer reviewed 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 [3], [50], and [56], where all authors are in the order indicated.

1. Sing a song of Simplex, *DISC 2024*.

2. BoLD: Fast and Cheap Dispute Resolution, with M. M. Alvarez, H. Arneson, B. Berger, L. Bousfield, C. Buckland, Y. Edelman, E. W. Felten, D. Goldman, R. Jordan, M. Kelkar, A. Mamageishvili, H. Ng, A. Sanghi, and T. Tsao, *AFT 2024*.

3. Asynchronous consensus without trusted setup or public-key cryptography, by S. Das, S. Duan, S. Liu, A. Momose, L. Ren, and V. Shoup, *ACM CCS 2024*.

4. Fast batched asynchronous distributed key generation, with J. Groth, *Eurocrypt 2024*.

5. Lightweight Asynchronous Verifiable Secret Sharing with Optimal Resilience, with N. Smart, *J. Cryptology 37(3)*, 2024.

6. Internet Computer Consensus, with J. Camenisch, M. Drijvers, T. Hanke, Y.-A. Pignolet, and D. Williams, *PODC 2022*.

7. On the security of ECDSA with additive key derivation and presignatures, with J. Groth, *Eurocrypt 2022*.

8. Bootstrapping for HElib, with S. Halevi, *J. Cryptology 34(7)*, 2021.

9. Security analysis of SPAKE2+. Theory of Cryptography Conference (TCC), 2020.

10. An improved RNS variant of the BFV homomorphic encryption scheme, with S. Halevi and Y. Polyakov, *Topics in Cryptology — CT-RSA 2019*.

11. Doing real work with FHE: the case of logistic regression, with J. L. H. Crawford, C. Gentry, S. Halevi and D. Platt, *WAHC '18 Proceedings of the 6th Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, 2019.

12. Faster Homomorphic Linear Transformations in HElib, with S. Halevi, *CRYPTO 2018*.

13. Implementing BP-Obfuscation Using Graph-Induced Encoding, with S. Halevi, T. Halevi, and N. Stephens-Davidowitz, *ACM CCS 2017*.

14. Bootstrapping for HElib, with S. Halevi, *Eurocrypt 2015*.

15. Algorithms in HElib, with S. Halevi, *Eurocrypt 2014*.

16. Practical and employable protocols for UC-Secure circuit evaluation over $\mathbf{Z}_n$, with J. Camenisch and R. Enderlein. *ESORICS 2013*.

17. GNUC: A New Universal Composability Framework, with D. Hofheinz. *J. Cryptology*, 2013.

18. Practical chosen ciphertext secure encryption from factoring, with D. Hofheinz and E. Kilz. *J. Cryptology 26(1):102–118*, 2012.

19. A Framework for Practical Universally Composable Zero-Knowledge Protocols, with J. Camensisch and S. Krenn. *Asiacrypt 2011.*

20. Anonymous Credentials on Java Card, with P. Bichsel, J. Camenisch, and T. Gross. *21st Fraunhofer SIT-Smartcard Workshop*, 2011.

21. Credential authenticated identification and key exchange, with J. Camenisch, N. Casati, and T. Gross. *CRYPTO 2010.*

22. Simple and efficient public-key encryption from computational Diffie-Hellman in the standard model, with K. Haralambiev, T. Jager, and E. Kiltz. *PKC 2010*.

23. Anonymous credentials on a standard Java Card, with P. Bichsel, J. Camenisch, and T. Gross. *ACM CCS 2009*.

24. A new and improved paradigm for hybrid encryption secure against chosen-ciphertext attack, with Y. Desmedt, R. Gennaro, and K. Kurosawa. *J. Cryptology 23(1):91-120*, 2010

25. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks, with J. Camenisch and N. Chandran. *Eurocrypt 2009*.

26. Efficient constructions of composable commitments and zero-knowledge proofs, with Y. Dodis and S. Walfish. *CRYPTO 2008*.

27. The Twin Diffie-Hellman problem and applications, with D. Cash and E. Kiltz. *Eurocrypt 2008*.

28. Stateful public-key cryptosystems: how to encrypt with one 160-bit exponentiation, with M. Bellare and T. Kohno. In *Proc. 13th ACM Conf. on Computer and Communications Security*, 2006.

29. Optimistic asynchronous atomic broadcast, with K. Kursawe, in *Proc. ICALP 2005*.

30. Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM, with M. Abe, R. Gennaro, K. Kurosawa, in *Proc. Eurocrypt 2005*.

31. Anonymous identification in *ad hoc* groups, with Y. Dodis, A. Nicolosi, and A. Kiayias, in *Proc. Eurocrypt 2004*.

32. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, with R. Cramer, *SIAM Journal on Computing* 33:167–226, 2003.

33. Practical verifiable encryption of and decryption of discrete logarithms, with J. Camenisch, in *Proc. Crypto 2003.*

34. A secure signature scheme from bilinear maps, with D. Boneh and I. Mironov, in *Proc. RSA CT-2003*.

35. Efficient computation modulo a shared secret with application to the generation of shared safe-prime products, with J. Algesheimer and J. Camenisch, in *Proc. Crypto 2002*.

36. Universal hash proofs and a paradigm for chosen ciphertext secure public key encryption, with R. Cramer, in *Proc. Eurocrypt 2002*.

37. OAEP reconsidered, *Journal of Cryptology* 15(4):223–249, 2002. Extended abstract in *Proc. Crypto 2001.*

38. Secure and efficient asynchronous broadcast protocols, with C. Cachin, K. Kursawe, and F. Petzold, in *Proc. Crypto 2001.*

39. Factorization in $Z[x]$: the searching phase, with J. Abbott and P. Zimmermann, in *Proc. 2000 International Symposium on Symbolic and Algebraic Computation.*

40. Random oracles in Constantinople: practical asynchronous Byzantine agreement using cryptography, with C. Cachin and K. Kursawe, in *Proc. 2000 Principles of Distributed Computing.* To appear, *Journal of Cryptology.*

41. Algorithms for exponentiation in finite fields, with S. Gao, J. von zur Gathen, and D. Panario, *Journal of Symbolic Computation* 29:879–889, 2000.

42. A composition theorem for universal one-way hash functions, in *Proc. Eurocrypt 2000.*

43. Using hash functions as a hedge against chosen ciphertext attack, in *Proc. Eurocrypt 2000.*

44. Practical threshold signatures, in *Proc. Eurocrypt 2000.*

45. Signature schemes based on the Strong RSA Assumption, with R. Cramer, *ACM Transactions on Information and System Security (ACM TISSEC)* 3(3):161–185, 2000. Extended abstract in *Proc. 6th ACM Conf. on Computer and Communications Security*, 1999.

46. Efficient computation of minimal polynomials in algebraic extension of finite fields, in *Proc. 1999 International Symposium on Symbolic and Algebraic Computation.*

47. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, with R. Cramer, in *Proc. Crypto '98.*

48. Optimistic fair exchange of digital signatures, with N. Asokan and M. Waidner, *IEEE Journal on Selected Areas in Communications* 18(4):593–610, 2000. Extended abstract in *Proc. Eurocrypt '98.*

49. Asynchronous protocols for optimistic fair exchange, with N. Asokan and M. Waidner, in *Proc. of the IEEE Symp. on Research in Security and Privacy*, 1998.

50. Securing threshold cryptosystems against chosen ciphertext attack, by V. Shoup and R. Gennaro, *Journal of Cryptology* 15(2):75–96, 2002. Extended abstract in *Proc. Eurocrypt '98.*

51. Fast polynomial factorization over high algebraic extensions of finite fields, with E. Kaltofen, in *Proc. 1997 International Symposium on Symbolic and Algebraic Computation.*

52. Private information storage, with R. Ostrovsky, in *Proc. 29th ACM Symposium on Theory of Computation*, 1997.

53. Lower bounds for discrete logarithms and related problems, in *Proc. Eurocrypt '97.*

54. On fast and provably secure message authentication based on universal hashing, in *Proc. Crypto '96*.

55. On the security of a practical identification scheme, *Journal of Cryptology* 12(4):247–260, 1999. Extended abstract in *Proc. Eurocrypt '96*.

56. Session-key distribution using smart cards, by V. Shoup and A. Rubin, in *Proc. Eurocrypt '96*.

57. Subquadratic-time factorization of polynomials over finite fields, with E. Kaltofen, *Mathematics of Computation* 67(223):1179–1197, 1998. Extended abstract in *Proc. 27th ACM Symposium on Theory of Computation,* 1995.

58. A new polynomial factorization algorithm and its implementation, *Journal of Symbolic Computation* 20:363-397, 1995.

59. Counting the number of points on elliptic curves of characteristic greater than three, with F. Lehmann, M. Mauerer, and V. Mueller, in *Proc. First Algorithmic Number Theory Symposium*, 1994.

60. Primality testing with fewer random bits, with R. Peralta, *Computational Complexity* 3:355–367, 1993.

61. Factoring polynomials over finite fields: asymptotic complexity vs. reality, in *Proc. IMACS Symposium*, Lille, France, 1993.

62. Fast construction of irreducible polynomials over finite fields, *Journal of Symbolic Computation* 17:371–391, 1994. Extended abstract in *Proc. 4th Annual Symposium on Discrete Algorithms*, 1993.

63. Computing Frobenius maps and factoring polynomials, with J. von zur Gathen, *Computational Complexity* 2:187–224, 1992. Extended abstract in *Proc. 24th ACM Symposium on Theory of Computing*, 1992.

64. Smoothness and factoring polynomials over finite fields, *Information Processing Letters* 39:39–42, 1991.

65. A fast deterministic algorithm for factoring polynomials over finite fields of small characteristic, in *Proc. 1991 International Symposium on Symbolic and Algebraic Computation.*

66. Lower bounds for polynomial evaluation and interpolation problems, with R. Smolensky, *Computational Complexity* 6:301–311, 1997. Extended abstract in *Proc. 31st Annual Symposium on Foundations of Computer Science*, 1991.

67. Constructing nonresidues in finite fields and the Extended Riemann Hypothesis, with J. Buchmann, *Mathematics of Computation* 65(215):1311–1326, 1996. Extended abstract in *Proc. 23rd ACM Symposium on Theory of Computation*, 1991.

68. On the deterministic complexity of factoring polynomials over finite fields, *Information Processing Letters* 33:261–267, 1990.

69. Hiding instances in zero-knowledge proof systems, with D. Beaver and J. Feigenbaum, in *Proc. Crypto '90*.

70. Factoring polynomials using fewer random bits, with E. Bach, *Journal of Symbolic Computation* 9:229–239, 1990.

71. Searching for primitive roots in finite fields, *Mathematics of Computation* 58:369-380, 1992. Extended abstract in *Proc. 22nd ACM Symposium on Theory of Computation*, 1990.

72. New algorithms for finding irreducible polynomials over finite fields, *Mathematics of Computation* 54:435–447, 1990. Extended abstract in *Proc. 29th Annual Symposium on Foundations of Computer Science*, 1988.

Research articles that have not been peer reviewed

These are my research articles that have not (yet) 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.

1. MiniCast: Minimizing the Communication Complexity of Reliable Broadcast, with T. Locher. April 2024. `https://eprint.iacr.org/2024/571`

2. The many faces of Schnorr. June 2023. `http://eprint.iacr.org/2023/1019`

3. vetKeys: How a blockchain can keep many secrets, with A. Cerulli, A. Connolly, G. Neven, and F.-S. Preiss. April 2023. `http://eprint.iacr.org/2023/616`

4. Design and analysis of a distributed ECDSA signing service, with J. Groth. April 2022. Revised February 2023. `http://eprint.iacr.org/2022/506`

5. Sequences of games: a tool for taming complexity in security proofs, November 2004; Revised May 2005, January 2006. `http://eprint.iacr.org/2004/332`

6. On formal models for secure key exchange. April 1999. Revised November 1999. `https://eprint.iacr.org/1999/012`