BRENT WATERS

University of Texas at Austin
Department of Computer Sciences
2317 Speedway, Stop D9500
Austin TX 78712

phone: 512 232 7464
email: bwaters@cs.utexas.edu
web: www.cs.utexas.edu/~bwaters

Research Interests

Cryptography and computer security

Experience

Professor, University of Texas at Austin, (9/2018 – present)
Associate Professor, University of Texas at Austin, (9/2013 – 8/2018)
Assistant Professor, University of Texas at Austin, (9/2008 – 8/2013)
Computer Scientist, SRI International, Computer Science Lab, (9/2005 – 8/2008)
Postdoc, Stanford University, Computer Science Department, (8/2004 – 8/2005)

Education

Ph. D. Computer Science, Princeton University, 2004 (Advisers: Ed Felten, Amit Sahai)
B. S. Computer Science, UCLA, 2000 (Graduated Summa Cum Laude)

Honors and Awards

FOCS Test-of-Time Award (2023)
CRYPTO Test-of-Time Award (2023)
ACM Fellow (2021)
Eurocrypt Test-of-Time Award (2020)
Simons Investigator (2019)
ACM CCS Test-of-Time Award (2016)
ACM Grace Murray Hopper Award (2015)
Presidential Early Career Award for Scientists and Engineers (PECASE) (2011)
Packard Fellowship (2011)
Microsoft Research Faculty Fellow (2011)
Sloan Research Fellowship (2010)
NSF CAREER Award (2010)

Conference Publications

- B. Waters and D. Wichs. Universal amplification of KDM security: From 1-key circular to multi-key KDM. In *CRYPTO*, pp. 674–693, 2023.
- D. Abram, B. Waters, and M. Zhandry. Security-preserving distributed samplers: How to generate any CRS in one round without random oracles. In *CRYPTO*, 2023.
- C. Freitag, B. Waters, and D. J. Wu. How to use (plain) witness encryption: Registered abe, flexible broadcast, and more. In *CRYPTO*, 2023.
- R. Garg, D. Khurana, G. Lu, and B. Waters. On non-uniform security for black-box non-interactive CCA commitments. In *EUROCRYPT*, pp. 173–204, 2023.
- S. Hohenberger, G. Lu, B. Waters, and D. J. Wu. Registered attribute-based encryption. In C. Hazay and M. Stam, eds., *EUROCRYPT*, pp. 511–542, 2023.
- P. Datta, I. Komargodski, and B. Waters. Fully adaptive decentralized multi-authority ABE. In *EURO-*

CRYPT, pp. 447–478, 2023.

- R. Ghosal, A. Sahai, and B. Waters. Non-interactive publicly-verifiable delegation of committed programs. In *PKC*, pp. 575–605, 2023.
- R. Garg, R. Goyal, G. Lu, and B. Waters. Dynamic collusion bounded functional encryption from identity-based encryption. In *EUROCRYPT*, pp. 736–763, 2022.
- B. Waters and D. J. Wu. Batch arguments for np and more from standard bilinear group assumptions. In *CRYPTO*, pp. 433–463, 2022.
- V. Koppula, B. Waters, and M. Zhandry. Adaptive multiparty NIKE. In *TCC*, pp. 244–273, 2022.
- R. Garg, K. Sheridan, B. Waters, and D. J. Wu. Fully succinct batch arguments for np from indistinguishability obfuscation. In *TCC*, pp. 526–555, 2022.
- B. Waters, H. Wee, and D. J. Wu. Multi-authority ABE from lattices without random oracles. In *TCC*, pp. 651–679, 2022.
- R. Goyal, R. Syed, and B. Waters. Bounded collusion ABE for tms from IBE. In *ASIACRYPT*, pp. 371–402, 2021.
- R. Goyal, J. Liu, and B. Waters. Adaptive security via deletion in attribute-based encryption: Solutions from search assumptions in bilinear groups. In *ASIACRYPT*, pp. 311–341, 2021.
- R. Goyal, S. Kim, B. Waters, and D. J. Wu. Beyond software watermarking: Traitor-tracing for pseudorandom functions. In *ASIACRYPT*, pp. 250–280, 2021.
- D. Khurana and B. Waters. On the CCA compatibility of public-key infrastructure. In *PKC*, pp. 235–260, 2021.
- P. Datta, I. Komargodski, and B. Waters. Decentralized multi-authority ABE for dnfs from LWE. In *EUROCRYPT*, pp. 177–209, 2021.
- R. Garg, D. Khurana, G. Lu, and B. Waters. Black-box non-interactive non-malleable commitments. In *EUROCRYPT*, pp. 159–185, 2021.
- W. Quach, B. Waters, and D. Wichs. Targeted lossy functions and applications. In *CRYPTO*, pp. 424–453, 2021.
- R. Goyal, V. Koppula, S. Vusirikala, and B. Waters. On perfect correctness in (lockable) obfuscation. In *TCC*, pp. 229–259, 2020.
- R. Garg, G. Lu, and B. Waters. New techniques in replica encodings with client setup. In *TCC*, pp. 550–583, 2020.
- S. Hohenberger, S. Vusirikala, and B. Waters. PPE circuits: Formal definition to software automation. In *CCS*, pp. 391–408, 2020.
- S. Hohenberger, V. Koppula, and B. Waters. Chosen ciphertext security from injective trapdoor functions. In *CRYPTO*, 2020. **Awarded Best Paper**.
- R. Goyal, S. Vusirikala, and B. Waters. New constructions of hinting prgs, owfs with encryption, and more. In *CRYPTO*, 2020.
- S. Hohenberger and B. Waters. New methods and abstractions for rsa-based forward secure signatures. In *ACNS*, 2020.
- S. Badrinarayanan, R. Fernando, V. Koppula, A. Sahai, and B. Waters. Output compression, mpc, and io for turing machines. In S. D. Galbraith and S. Moriai, eds., *ASIACRYPT*, 2019.
- R. Goyal, S. Kim, N. Manohar, B. Waters, and D. J. Wu. Watermarking public-key cryptographic primitives. In *CRYPTO*, pp. 367–398, 2019.

- V. Koppula and B. Waters. Realizing chosen ciphertext security generically in attribute-based encryption and predicate encryption. In *CRYPTO*, pp. 671–700, 2019.
- J. Gong, B. Waters, and H. Wee. ABE for DFA from k-lin. In *CRYPTO*, pp. 732–764, 2019.
- R. Goyal, W. Quach, B. Waters, and D. Wichs. Broadcast and trace with nˆϵ ciphertext size from standard assumptions. In *CRYPTO*, pp. 826–855, 2019.
- R. Goyal, S. Vusirikala, and B. Waters. Collusion resistant broadcast and trace from positional witness encryption. In *PKC*, pp. 3–33, 2019.
- Y. Chen, V. Vaikuntanathan, B. Waters, H. Wee, and D. Wichs. Traitor-tracing from LWE made simple and attribute-based. In *TCC*, pp. 341–369, 2018.
- S. Badrinarayanan, D. Khurana, A. Sahai, and B. Waters. Upgrading to functional encryption. In *TCC*, pp. 629–658, 2018.
- S. Agrawal, V. Koppula, and B. Waters. Impossibility of simulation secure functional encryption even with random oracles. In *TCC*, pp. 659–688, 2018.
- R. Goyal, V. Koppula, A. Russell, and B. Waters. Risky traitor tracing and new differential privacy negative results. In *CRYPTO*, pp. 467–497, 2018.
- S. Hohenberger and B. Waters. Synchronized aggregate signatures from the RSA assumption. In *EUROCRYPT*, pp. 197–229, 2018.
- R. Goyal, V. Koppula, and B. Waters. Collusion resistant traitor tracing from learning with errors. In *STOC*, pp. 660–670, 2018. **Invited to SIAM Journal of Computing, special issue for top papers of STOC 2018**.
- R. Goyal, V. Koppula, and B. Waters. Lockable obfuscation. In *FOCS*, 2017.
- C. Freitag, R. Goyal, S. Hohenberger, V. Koppula, E. Lee, T. Okamoto, J. Tran, and B. Waters. Signature schemes with randomized verification. In *ACNS*, pp. 373–389, 2017.
- R. Goyal, V. Koppula, and B. Waters. Separating semantic and circular security for symmetric-key bit encryption from the learning with errors assumption. In *EUROCRYPT*, pp. 528–557, 2017.
- R. Goyal, V. Koppula, and B. Waters. Separating IND-CPA and circular security for unbounded length key cycles. In *PKC*, pp. 232–246, 2017.
- V. Koppula, A. Poelstra, and B. Waters. Universal samplers with fast verification. In *PKC*, pp. 525–554, 2017.
- D. Hofheinz, T. Jager, D. Khurana, A. Sahai, B. Waters, and M. Zhandry. How to generate and use universal samplers. In *ASIACRYPT*, pp. 715–744, 2016.
- R. Goyal, V. Koppula, and B. Waters. Semi-adaptive security and bundling functionalities made generic and easy. In *TCC*, pp. 361–388, 2016.
- V. Koppula, O. Pandey, Y. Rouselakis, and B. Waters. Deterministic public-key encryption under continual leakage. In *Applied Cryptography and Network Security ACNS*, pp. 304–323, 2016.
- V. Koppula and B. Waters. Circular security separations for arbitrary length cycles from LWE. In *CRYPTO*, pp. 681–700, 2016.
- A. Deshpande, V. Koppula, and B. Waters. Constrained pseudorandom functions for unconstrained inputs. In *EUROCRYPT*, pp. 124–153, 2016.
- M. Bellare, I. Stepanovs, and B. Waters. New negative results on differing-inputs obfuscation. In *EUROCRYPT*, pp. 792–821, 2016.

- N. Bitansky, S. Goldwasser, A. Jain, O. Paneth, V. Vaikuntanathan, and B. Waters. Time-lock puzzles from randomized encodings. In *ACM Conference on Innovations in Theoretical*, pp. 345–356, 2016.
- S. Hohenberger, V. Koppula, and B. Waters. Adaptively secure puncturable pseudorandom functions in the standard model. In *ASIACRYPT*, pp. 79–102, 2015.
- T. Okamoto, K. Pietrzak, B. Waters, and D. Wichs. New realizations of somewhere statistically binding hashing and positional accumulators. In *ASIACRYPT*, pp. 121–145, 2015.
- A. Bishop, S. Hohenberger, and B. Waters. New circular security counterexamples from decision linear and learning with errors. In *ASIACRYPT*, pp. 776–800, 2015.
- B. Waters. A punctured programming approach to adaptively secure functional encryption. In *CRYPTO*, pp. 678–697, 2015.
- S. Hohenberger, V. Koppula, and B. Waters. Universal signature aggregators. In *EUROCRYPT*, pp. 3–34, 2015.
- Y. Rouselakis and B. Waters. Efficient statically-secure large-universe multi-authority attribute-based encryption. In *Financial Cryptography and Data Security*, pp. 315–332, 2015.
- C. Gentry, A. B. Lewko, A. Sahai, and B. Waters. Indistinguishability obfuscation from the multilinear subgroup elimination assumption. In *FOCS*, pp. 151–170, 2015.
- V. Koppula, A. B. Lewko, and B. Waters. Indistinguishability obfuscation for turing machines with unbounded memory. In *STOC*, pp. 419–428, 2015. **Invited to SIAM Journal of Computing, special issue for top papers of STOC 2015 (Invitation was declined)**.
- V. Koppula, K. Ramchen, and B. Waters. Separations in circular security for arbitrary length key cycles. In *TCC*, pp. 378–400, 2015.
- K. Ramchen and B. Waters. Fully secure and fast signing from obfuscation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*, pp. 659–673, 2014.
- D. Boneh, B. Waters, and M. Zhandry. Low overhead broadcast encryption from multilinear maps. In *CRYPTO*, pp. 206–223, 2014.
- C. Gentry, A. B. Lewko, and B. Waters. Witness encryption from instance independent assumptions. In *CRYPTO*, pp. 426–443, 2014.
- T. Calderon, S. Meiklejohn, H. Shacham, and B. Waters. Rethinking verifiably encrypted signatures: A gap in functionality and potential solutions. In *CT-RSA*, pp. 349–366, 2014.
- A. B. Lewko and B. Waters. Why proving HIBE systems secure is difficult. In *EUROCRYPT*, pp. 58–76, 2014.
- S. Hohenberger, A. Sahai, and B. Waters. Replacing a random oracle: Full domain hash from indistinguishability obfuscation. In *EUROCRYPT*, pp. 201–220, 2014.
- S. Hohenberger and B. Waters. Online/offline attribute-based encryption. In *PKC*, pp. 293–310, 2014.
- O. Pandey, K. Ramchen, and B. Waters. Relaxed two-to-one recoding schemes. In *Security and Cryptography for Networks SCN*, pp. 57–76, 2014.
- A. Sahai and B. Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In *STOC*, pp. 475–484, 2014. **Invited to SIAM Journal of Computing, special issue for top papers of STOC 2014**.
- Y. Rouselakis and B. Waters. Practical constructions and new proof methods for large universe attribute-based encryption. In *ACM SIGSAC Conference on Computer and Communications Security*, pp. 463–474, 2013.

- D. Boneh and B. Waters. Constrained pseudorandom functions and their applications. In *ASIACRYPT*, pp. 280–300, 2013.

- S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, pp. 40–49, 2013.

- C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *CRYPTO*, pp. 75–92, 2013.

- B. Applebaum, Y. Ishai, E. Kushilevitz, and B. Waters. Encoding functions with constant online rate or how to compress garbled circuits keys. In *CRYPTO (2)*, pp. 166–184, 2013.

- S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters. Attribute-based encryption for circuits from multilinear maps. In *CRYPTO (2)*, pp. 479–499, 2013.

- S. Hohenberger, A. Sahai, and B. Waters. Full domain hash from (leveled) multilinear maps and identity-based aggregate signatures. In *CRYPTO (1)*, pp. 494–512, 2013.

- K. Benson, H. Shacham, and B. Waters. The k-bdh assumption family: Bilinear map cryptography from progressively weaker assumptions. In *CT-RSA*, pp. 310–325, 2013.

- S. Hohenberger and B. Waters. Attribute-based encryption with fast decryption. In *Public Key Cryptography*, pp. 162–179, 2013.

- M. Z. Lee, A. M. Dunn, B. Waters, E. Witchel, and J. Katz. Anon-pass: Practical anonymous subscriptions. In *IEEE Symposium on Security and Privacy*, 2013.

- S. Garg, C. Gentry, A. Sahai, and B. Waters. Witness encryption and its applications. In *STOC*, pp. 467–476, 2013.

- A. Luong, M. Gerbush, B. Waters, and K. Grauman. Reconstructing a fragmented face from a cryptographic identification protocol. In *WACV*, pp. 238–245, 2013.

- M. Gerbush, A. B. Lewko, A. O'Neill, and B. Waters. Dual form signatures: An approach for proving security from static assumptions. In *ASIACRYPT*, pp. 25–42, 2012.

- B. Waters. Functional encryption for regular languages. In *CRYPTO*, pp. 218–235, 2012.

- A. B. Lewko and B. Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In *CRYPTO*, pp. 180–198, 2012.

- A. Sahai, H. Seyalioglu, and B. Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In *CRYPTO*, pp. 199–217, 2012.

- M. Bellare, R. Dowsley, B. Waters, and S. Yilek. Standard security does not imply security against selective-opening. In *EUROCRYPT*, pp. 645–662, 2012.

- M. Bellare, E. Kiltz, C. Peikert, and B. Waters. Identity-based (lossy) trapdoor functions and applications. In *EUROCRYPT*, pp. 228–245, 2012.

- S. Hohenberger, A. B. Lewko, and B. Waters. Detecting dangerous queries: A new approach for chosen ciphertext security. In *EUROCRYPT*, pp. 663–681, 2012.

- J. H. Ahn, D. Boneh, J. Camenisch, S. Hohenberger, A. Shelat, and B. Waters. Computing on authenticated data. In *TCC*, pp. 1–20, 2012.

- D. Boneh, G. Segev, and B. Waters. Targeted malleability: homomorphic encryption for restricted computations. In *ITCS*, pp. 350–366, 2012.

- Y. Dodis, A. B. Lewko, B. Waters, and D. Wichs. Storing secrets on continually leaky devices. In *FOCS*, pp. 688–697, 2011.

- M. Green, S. Hohenberger, and B. Waters. Outsourcing the decryption of abe ciphertexts. In *USENIX Security*, pp. 523–538, 2011.
- A. Dunn, O. Hoffman, B. Waters, and E. Witchel. Cloaking malware with the trusted platform module. In *USENIX Security*, pp. 395–410, 2011.
- A. O'Neill, C. Peikert, and B. Waters. Bi-deniable public-key encryption. In *CRYPTO*, pp. 525–542, 2011.
- A. B. Lewko, M. Lewko, and B. Waters. How to leak on key updates. In *STOC*, pp. 725–734, 2011.
- A. B. Lewko and B. Waters. Decentralizing attribute-based encryption. In *EUROCRYPT*, pp. 568–588, 2011.
- A. B. Lewko and B. Waters. Unbounded hibe and attribute-based encryption. In *EUROCRYPT*, pp. 547–567, 2011.
- M. Bellare, B. Waters, and S. Yilek. Identity-based encryption secure against selective opening attack. In *TCC*, pp. 235–252, 2011.
- D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. In *TCC*, pp. 253–273, 2011.
- A. B. Lewko, Y. Rouselakis, and B. Waters. Achieving leakage resilience through dual system encryption. In *TCC*, pp. 70–88, 2011.
- B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography*, pp. 53–70, 2011.
- A. B. Lewko and B. Waters. On the insecurity of parallel repetition for leakage resilience. In *FOCS*, pp. 521–530, 2010.
- S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters. Building efficient fully collusion-resilient traitor tracing and revocation schemes. In *ACM Conference on Computer and Communications Security*, pp. 121–130, 2010.
- S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters. Practical leakage-resilient identity-based encryption from simple assumptions. In *ACM Conference on Computer and Communications Security*, pp. 152–161, 2010.
- A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *EUROCRYPT*, pp. 62–91, 2010.
- S. Hohenberger and B. Waters. Constructing verifiable random functions with large input spaces. In *EUROCRYPT*, pp. 656–672, 2010.
- X. Boyen and B. Waters. Shrinking the keys of discrete-log-type lossy trapdoor functions. In *ACNS*, pp. 35–52, 2010.
- A. B. Lewko, A. Sahai, and B. Waters. Revocation systems with very small private keys. In *IEEE Symposium on Security and Privacy*, pp. 273–285, 2010.
- S. Wolchok, O. Hofmann, N. Heninger, E. Felten, J. A. Halderman, C. Rossbach, B. Waters, and E. Witchel. Defeating vanish with low-cost sybil attacks against large dhts. In *NDSS*, 2010.
- A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure hibe with short ciphertexts. In *TCC*, pp. 455–479, 2010.
- A. B. Lewko and B. Waters. Efficient pseudorandom functions from the decisional linear assumption and weaker variants. In *ACM Conference on Computer and Communications Security*, pp. 112–120, 2009.

- S. Hohenberger and B. Waters. Short and stateless signatures from the rsa assumption. In *CRYPTO*, pp. 654–670, 2009.
- B. Waters. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In *CRYPTO*, pp. 619–636, 2009.
- S. Hohenberger and B. Waters. Realizing hash-and-sign signatures under standard assumptions. In *EUROCRYPT*, pp. 333–350, 2009.
- C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In *EUROCRYPT*, pp. 171–188, 2009.
- E. Shen, E. Shi, and B. Waters. Predicate privacy in encryption systems. In *TCC*, pp. 457–473, 2009.
- D. Boneh, D. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding. In *Public Key Cryptography*, pp. 68–87, 2009.
- V. Goyal, S. Lu, A. Sahai, and B. Waters. Black-box accountable authority identity-based encryption. In *ACM Conference on Computer and Communications Security*, pp. 427–436, 2008.
- H. Shacham and B. Waters. Compact proofs of retrievability. In *ASIACRYPT*, pp. 90–107, 2008.
- C. Peikert, V. Vaikuntanathan, and B. Waters. A framework for efficient and composable oblivious transfer. In *CRYPTO*, pp. 554–571, 2008.
- J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT*, pp. 146–162, 2008. **Invited to Journal of Cryptology, special issue for top four papers of Eurocrypt 2008**.
- D. Boneh, P. Papakonstantinou, C. Rackoff, Y. Vahlis, and B. Waters. On the impossibility of basing identity based encryption on trapdoor permutations. In *FOCS*, pp. 283–292, 2008.
- E. Shi and B. Waters. Delegating capabilities in predicate encryption systems. In *ICALP (2)*, pp. 560–578, 2008.
- C. Peikert and B. Waters. Lossy trapdoor functions and their applications. In *STOC*, pp. 187–196, 2008. **Invited to SIAM Journal of Computing, special issue for top papers of STOC 2008**.
- J. Bethencourt, D. Song, and B. Waters. Analysis-resistant malware. In *Network and Distributed System Security Symposium (NDSS)*, 2008.
- J. A. Halderman and B. Waters. Harvesting verifiable challenges from online sources. In *ACM Conference on Computer and Communications Security*, pp. 330–341, 2007.
- R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In *ACM Conference on Computer and Communications Security*, pp. 195–203, 2007.
- J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.
- X. Boyen and B. Waters. Full-domain subgroup hiding and constant-size group signatures. In *Public Key Cryptography*, pp. 1–15, 2007. **Awarded Best Paper**.
- H. Shacham and B. Waters. Efficient ring signatures without random oracles. In *Public Key Cryptography*, pp. 166–180, 2007.
- D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC*, pp. 535–554, 2007.
- J. Bethencourt, D. Boneh, and B. Waters. Cryptographic methods for storing ballots on a voting machine. In *Network and Distributed System Security Symposium (NDSS)*, 2007.

- X. Boyen, H. Shacham, E. Shen, and B. Waters. Forward-secure signatures with untrusted update. In *ACM Conference on Computer and Communications Security*, pp. 191–200, 2006.

- D. Boneh and B. Waters. A fully collusion resistant broadcast, trace, and revoke system. In *ACM Conference on Computer and Communications Security*, pp. 211–220, 2006.

- V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.

- M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. In *ACM Conference on Computer and Communications Security*, pp. 99–112, 2006.

- X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption (without random oracles). In *CRYPTO*, pp. 290–307, 2006.

- X. Boyen and B. Waters. Compact group signatures without random oracles. In *EUROCRYPT*, pp. 427–444, 2006.

- S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters. Sequential aggregate signatures and multisignatures without random oracles. In *EUROCRYPT*, pp. 465–485, 2006.

- D. Boneh, A. Sahai, and B. Waters. Fully collusion resistant traitor tracing with short ciphertexts and private keys. In *EUROCRYPT*, pp. 573–592, 2006.

- A. Barth, D. Boneh, and B. Waters. Privacy in encrypted content distribution using private broadcast encryption. In *Financial Cryptography*, pp. 52–64, 2006.

- D. Boneh, E. Shen, and B. Waters. Strongly unforgeable signatures based on computational diffie-hellman. In *Public Key Cryptography*, pp. 229–240, 2006.

- J. Bethencourt, D. X. Song, and B. Waters. New constructions and practical applications for private stream searching (extended abstract). In *S&P*, pp. 132–139, 2006.

- X. Boyen, Q. Mei, and B. Waters. Direct chosen ciphertext security from identity-based techniques. In *ACM Conference on Computer and Communications Security*, pp. 320–329, 2005.

- D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *CRYPTO*, pp. 258–275, 2005.

- B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT*, pp. 114–127, 2005.

- A. Sahai and B. Waters. Fuzzy identity-based encryption. In *EUROCRYPT*, pp. 457–473, 2005.

- J. A. Halderman, B. Waters, and E. W. Felten. A convenient method for securely managing passwords. In *WWW*, pp. 471–479, 2005.

- B. Waters, A. Juels, J. A. Halderman, and E. W. Felten. New client puzzle outsourcing techniques for dos resistance. In *ACM Conference on Computer and Communications Security*, pp. 246–256, 2004.

- P. Golle, J. Staddon, and B. R. Waters. Secure conjunctive keyword search over encrypted data. In *ACNS*, pp. 31–45, 2004.

- B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters. Building an encrypted and searchable audit log. In *Network and Distributed System Security Symposium (NDSS)*, pp. 16–24, 2004.

- J. A. Halderman, B. R. Waters, and E. W. Felten. Privacy management for portable recording devices. In *WPES*, pp. 16–24, 2004.

- B. R. Waters, E. W. Felten, and A. Sahai. Receiver anonymity via incomparable public keys. In *ACM Conference on Computer and Communications Security*, pp. 112–121, 2003.

Journal Publications

- R. Goyal, V. Koppula, and B. Waters. Collusion resistant traitor tracing from learning with errors. *SIAM J. Comput.*, 49(5), 2020.
- S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Hiding secrets in software: a cryptographic approach to program obfuscation. *Commun. ACM*, 59(5):113–120, 2016.
- S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM J. Comput.*, 45(3):882–929, 2016.
- B. Applebaum, Y. Ishai, E. Kushilevitz, and B. Waters. Encoding functions with constant online rate, or how to compress garbled circuit keys. *SIAM J. Comput.*, 44(2):433–466, 2015.
- J. H. Ahn, D. Boneh, J. Camenisch, S. Hohenberger, A. Shelat, and B. Waters. Computing on authenticated data. *J. Cryptology*, 28(2):351–395, 2015.
- M. Z. Lee, A. M. Dunn, J. Katz, B. Waters, and E. Witchel. Anon-pass: Practical anonymous subscriptions. *IEEE Security & Privacy*, 12(3):20–27, 2014.
- H. Shacham and B. Waters. Compact proofs of retrievability. *J. Cryptology*, 26(3):442–483, 2013.
- S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters. Sequential aggregate signatures, multisignatures, and verifiably encrypted signatures without random oracles. *J. Cryptology*, 26(2):340–373, 2013.
- J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *J. Cryptology*, 26(2):191–224, 2013.
- C. Peikert and B. Waters. Lossy trapdoor functions and their applications. *SIAM J. Comput.*, 40(6):1803–1844, 2011.
- M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. *Journal of Computer Security*, 18(5):799–837, 2010.
- J. Bethencourt, D. Song, and B. Waters. New techniques for private stream searching. *ACM Trans. Inf. Syst. Secur.*, 12(3), 2009.

Journal Boards and Program Chair

Associate Editor, International Journal of Applied Cryptography (2006– present)
Program Co-Chair, Pairings (2009)
Program Co-Chair, TCC (2021)

Program Committee Service

TCC 2009,2016-A, 2021 **(Program Co-Chair)**
Eurocrypt 2007, 2008, 2017,2019
CRYPTO 2008,2010,2014, 2024
Computer and Communications Security (CCS) 2010,2011, 2013
IEEE Symposium on Security and Privacy 2009, 2010,2011
Africacrypt 2010
Conference on Public Key Cryptography 2010
PODC 2009
Pairings 2009 **(Program Co-Chair)**
Electronic Voting Technology (EVT) Workshop 2008
WWW Conference: Security, Privacy, and Ethics Track 2006, 2007, 2008
Asiacrypt 2007
Applied Cryptography and Network Security (ACNS) 2006,2007
RSA Cryptographer's Track 2007
ACM CCS Industry and Government Track 2006

Workshop on Privacy in the Electronic Society (WPES) 2005
European Symposium on Research in Computer Security (ESORICS) 2005
Network and Distributed System Security Symposium (NDSS) 2005

Volunteer Service

Member of Travis County Elections Study Group (2009)

Teaching

University of Texas at Austin, CS346: Cryptography – Undergraduate (Spring 2022)
University of Texas at Austin, CS346: Cryptography – Undergraduate (Fall 2018)
University of Texas at Austin, CS388H: Cryptography (Spring 2017)
University of Texas at Austin, CS346: Cryptography – Undergraduate (Fall 2016)
University of Texas at Austin, CS388H: Cryptography (Fall 2015)
University of Texas at Austin, CS346: Cryptography – Undergraduate (Spring 2015)
University of Texas at Austin, CS395T: Special Topic — Obfucation in Cryptography (Fall 2014)
University of Texas at Austin, CS346: Cryptography – Undergraduate (Spring 2013)
University of Texas at Austin, CS388H: Cryptography (Fall 2012)
University of Texas at Austin, CS346: Cryptography – Undergraduate (Spring 2012)
University of Texas at Austin, CS388H: Cryptography (Fall 2011)
University of Texas at Austin, CS336H: Analysis of Programs Honors (Spring 2011)
University of Texas at Austin, CS395T: Advanced Cryptography (Fall 2010)
University of Texas at Austin, CS346: Cryptography – Undergraduate (Spring 2010)
University of Texas at Austin, CS388H: Cryptography (Fall 2009)
University of Texas at Austin, CS395T: Advanced Cryptography (Spring 2009)
Stanford University, CS255: Introduction to Cryptography (Fall 2004), Co-Instructor with Dan Boneh

Ph.D. Student Advising

Rishab Goyal, UT Austin (Ph.D. Candidate)
Venkata Koppula, UT Austin (Ph.D. 2018)
Yannis Rouselakis, UT Austin (Ph.D. 2013)
Allison Bishop, UT Austin (Ph.D. 2012)