Stanford

Dan Boneh

Cryptography Professor, Professor of Electrical Engineering and Senior Fellow at the Freeman Spogli Institute for International Studies

Computer Science

CONTACT INFORMATION

- **Administrator**

  Ruth Harris - Administrative Associate

  Email rharris3@stanford.edu

  Tel (650) 723-1658

Bio

BIO

Professor Boneh heads the applied cryptography group and co-direct the computer security lab. Professor Boneh's research focuses on applications of cryptography to computer security. His work includes cryptosystems with novel properties, web security, security for mobile devices, and cryptanalysis. He is the author of over a hundred publications in the field and is a Packard and Alfred P. Sloan fellow. He is a recipient of the 2014 ACM prize and the 2013 Godel prize. In 2011 Dr. Boneh received the Ishii award for industry education innovation. Professor Boneh received his Ph.D from Princeton University and joined Stanford in 1997.

ACADEMIC APPOINTMENTS

- Professor, Computer Science
- Professor, Electrical Engineering
- Senior Fellow, Freeman Spogli Institute for International Studies

HONORS AND AWARDS

- ACM prize, ACM (2015)
- Simons investigator, Simons foundation (2015)
- Godel prize, ACM (2013)
- IACR fellow, IACR (2013)
- Horizon Award, Computerworld (2006)
- Packard Fellow and Sloan Fellow, Packard (present)

PROFESSIONAL EDUCATION

- PhD, Princeton (1996)

LINKS

- http://crypto.stanford.edu/~dabo: http://crypto.stanford.edu/~dabo

Teaching

COURSES

2021-22

- Computer and Network Security: CS 155 (Spr)
- Cryptocurrencies and blockchain technologies: CS 251 (Aut)
- Introduction to Cryptography: CS 255 (Win)

2020-21

- Computer and Network Security: CS 155 (Spr)
- Cryptocurrencies and blockchain technologies: CS 251 (Aut)
- Introduction to Cryptography: CS 255 (Win)

2019-20

- Computer and Network Security: CS 155 (Spr)
- Cryptocurrencies and blockchain technologies: CS 251 (Aut)
- Introduction to Cryptography: CS 255 (Win)

2018-19

- Computer and Network Security: CS 155 (Spr)
- Cryptocurrencies and blockchain technologies: CS 251 (Aut)
- Elements of Quantum Computer Programming: CS 269Q (Spr)
- Introduction to Cryptography: CS 255 (Win)

STANFORD ADVISEES

Doctoral Dissertation Reader (AC)

Jason Anderson, Charis Charitsis, Mehrad Moradshahi, Joachim Neu, Luke Sammarone, Kavya Sreedhar, Srivatsan Sridhar

Postdoctoral Faculty Sponsor

Ronald Robertson, Lior Rotem Benvenisty

Doctoral Dissertation Advisor (AC)

Ben Fisch, Tina White

Orals Evaluator

Ben Fisch

Doctoral Dissertation Co-Advisor (AC)

Keller Blackwell, Alex Ozdemir

Master's Program Advisor

Michel Dellepere, Christie Di, Ayelet Drazen, Ophir Horovitz, Abel Ribbink, Simon Tao, Felix Wang, Federico Zalcberg

Doctoral (Program)

Benedikt Bünz, Trisha Datta, Ben Fisch, Wilson Nguyen, Aditi Partap, Neil Perry, Megha Srivastava

Publications

PUBLICATIONS

- **Falcon — A Flexible Architecture For Accelerating Cryptography** *2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*
  Kiningham, K., Levis, P., Anderson, M., Boneh, D., Horowitz, M., Shih, M.
  2019
- **Stickler: Defending against Malicious Content Distribution Networks in an Unmodified Browser** *IEEE SECURITY & PRIVACY*
  Levy, A., Corrigan-Gibbs, H., Boneh, D.
  2016; 14 (2): 22-28
- **Computing on Authenticated Data** *JOURNAL OF CRYPTOLOGY*
  Jae Hyun Ahn, J. H., Hohenberger, S., Boneh, D., Camenisch, J., Shelat, A., Waters, B.
  2015; 28 (2): 351-395
- **An Experimental Study of TLS Forward Secrecy Deployments** *IEEE INTERNET COMPUTING*
  Huang, L., Adhikarla, S., Boneh, D., Jackson, C.
  2014; 18 (6): 43-51
- **Neuroscience Meets Cryptography: Crypto Primitives Secure Against Rubber Hose Attacks** *COMMUNICATIONS OF THE ACM*
  Bojinov, H., Sanchez, D., Reber, P., Boneh, D., Lincoln, P.
  2014; 57 (5): 110-118
- **Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits** *33rd Annual International Association for Cryptologic Research Eurocrypt Conference on the Theory and Applications of Cryptographic Techniques*
  Boneh, D., Gentry, C., Gorbunov, S., Halevi, S., Nikolaenko, V., Segev, G., Vaikuntanathan, V., Vinayagamurthy, D.
  SPRINGER-VERLAG BERLIN.2014: 533–556
- **Privacy-Preserving Ridge Regression on Hundreds of Millions of Records** *34th IEEE Symposium on Security and Privacy (SP)*
  Nikolaenko, V., Weinsberg, U., Ioannidis, S., Joye, M., Boneh, D., Taft, N.
  IEEE.2013: 334–348
- **Privacy-Preserving Ridge Regression on Hundreds of Millions of Records.**
  Nikolaenko, V., Weinsberg, U., Ioannidis, S., Joye, M., Boneh, D., Taft, N.
  2013
- **Message-Locked Encryption for Lock-Dependent Messages.**
  Abadi, M., Boneh, D., Mironov, I., Raghunathan, A., Segev, G.
  2013
- **Key Homomorphic PRFs and Their Applications.**
  Boneh, D., Lewi, K., Montgomery, H., Raghunathan, A.
  2013
- **Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation.** *Cryptology ePrint Archive: Report*
  Boneh, D., Zhandry, M.
  2013: 642
- **Quantum-Secure Message Authentication Codes.**
  Boneh, D., Zhandry, M.
  2013
- **Function-Private Identity-Based Encryption: Hiding the Function in Functional Encryption.**
  Boneh, D., Raghunathan, A., Segev, G.
  2013
- **Private Database Queries Using Somewhat Homomorphic Encryption.**
  Boneh, D., Gentry, C., Halevi, S., Wang, F., Wu, D.

2013

- **Ensuring high-quality randomness in cryptographic key generation.**
  Corrigan-Gibbs, H., Mu, W., Boneh, D., Ford, B.
  2013
- **Function-Private Subspace-Membership Encryption and Its Applications.**
  Boneh, D., Raghunathan, A., Segev, G.
  2013
- **OSS: Using Online Scanning Services for Censorship Circumvention.**
  Fifield, D., Nakibly, G., Boneh, D.
  2013
- **Constrained Pseudorandom Functions and Their Applications.**
  Boneh, D., Waters, B.
  2013
- **Privacy-preserving matrix factorization.**
  Nikolaenko, V., Ioannidis, S., Weinsberg, U., Joye, M., Taft, N., Boneh, D.
  2013
- **Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World.**
  Boneh, D., Zhandry, M.
  2013
- **Attribute-Based Encryption for Arithmetic Circuits.** *Cryptology ePrint Archive: Report*
  Boneh, D., Nikolaenko, V., Segev, G.
  2013: 669
- **Functional Encryption: A New Vision for Public-Key Cryptography** *COMMUNICATIONS OF THE ACM*
  Boneh, D., Sahai, A., Waters, B.
  2012; 55 (11): 56-64
- **Privacy and Cybersecurity: The Next 100 Years** *PROCEEDINGS OF THE IEEE*
  Landwehr, C., Boneh, D., Mitchell, J. C., Bellovin, S. M., Landau, S., Lesk, M. E.
  2012; 100: 1659-1673
- **StegoTorus: a camouflage proxy for the Tor anonymity system.**
  Weinberg, Z., Wang, J., Yegneswaran, V., Briesemeister, L., Cheung, S., Wang, F., Boneh, D.
  2012
- **Persistent OSPF Attacks.**
  Nakibly, G., Kirshon, A., Gonikman, D., Boneh, D.
  2012
- **SessionJuggler: Secure Web Login From an Untrusted Terminal Using Session Hijacking.**
  Bursztein, E., Soman, C., Boneh, D., Mitchell, J.
  2012
- **Towards Short-Lived Certificates.**
  Topalovic, E., Saeta, B., Huang, L., S., Jackson, C., Boneh, D.
  2012
- **Computing on Authenticated Data.**
  Ahn, J., H., Boneh, D., Camenisch, J., Hohenberger, S., Shelat, A., Waters, B.
  2012
- **The case for prefetching and prevalidating TLS server certificates.**
  Stark, E., Huang, L., S., Israni, D., Jackson, C., Boneh, D.

2012

- **Who Killed My Battery: Analyzing Mobile Browser Energy Consumption**
  Thiagarajan, N., Aggarwal, G., Nicoara, A., Boneh, D., Singh, J.
  2012
- **The most dangerous code in the world: validating SSL certificates in non-browser software.**
  Georgiev, M., Iyengar, S., Jana, S., Anubhai, R., Boneh, D., Shmatikov, V.
  2012
- **Evading Censorship with Browser-Based Proxies**
  Fifield, D., Hardison, N., Ellithorpe, J., Stark, E., Boneh, D., Dingledine, R.
  2012
- **Neuroscience Meets Cryptography: Designing Crypto Primitives Secure Against Rubber Hose Attacks**
  Bojinov, H., Sanchez, D., Reber, P., Boneh, D., Lincoln, P.
  2012
- **Targeted malleability: homomorphic encryption for restricted computations.**
  Boneh, D., Segev, G., Waters, B.
  2012
- **Efficient Selective Identity-Based Encryption Without Random Oracles** *JOURNAL OF CRYPTOLOGY*
  Boneh, D., Boyen, X.
  2011; 24 (4): 659-693
- **Finding composite order ordinary elliptic curves using the Cocks-Pinch method** *JOURNAL OF NUMBER THEORY*
  Boneh, D., Rubin, K., Silverberg, A.
  2011; 131 (5): 832-841
- **Random Oracles in a Quantum World** *17th Annual International conference on the Theory and Application of Cryptology and Information Security*
  Boneh, D., Dagdelen, O., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.
  SPRINGER.2011: 41–69
- **Functional encryption: definitions and challenges.**
  Boneh, D., Sahai, A., Waters, B.
  2011
- **Homomorphic Signatures for Polynomial Functions.**
  Boneh, D., Freeman, D.
  2011
- **Location privacy via private proximity testing.**
  Narayanan, A., Thiagarajan, N., Lakhani, M., Hamburg, M., Boneh, D.
  2011
- **Random Oracles in a Quantum World.**
  Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.
  2011
- **OpenConflict: preventing real time map hacks in online games.**
  Bursztein, E., Hamburg, M., Lagarenne, J., Boneh, D.
  2011
- **Functional Encryption: Definitions and Challenges** *8th Theory Cryptography Conference*
  Boneh, D., Sahai, A., Waters, B.
  SPRINGER-VERLAG BERLIN.2011: 253–273
- **Homomorphic Signatures for Polynomial Functions** *30th Annual International Conference on the Theory and Applications of Cryptographic Techniques*
  Boneh, D., Freeman, D. M.

SPRINGER-VERLAG BERLIN.2011: 149–168

- **Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures** *14th International Conference on Practice and Theory in Public Key Cryptography (PKC 2011)*
  Boneh, D., Freeman, D. M.
  SPRINGER-VERLAG BERLIN.2011: 1–16
- **OpenConflict: Preventing Real Time Map Hacks in Online Games** *32nd IEEE Symposium on Security and Privacy (SP 2011)*
  Bursztein, E., Hamburg, M., Lagarenne, J., Boneh, D.
  IEEE COMPUTER SOC.2011: 506–520
- **Address Space Randomization for Mobile Devices** *4th ACM Conference on Wireless Network Security*
  Bojinov, H., Boneh, D., Cannings, R., Malchev, I.
  ASSOC COMPUTING MACHINERY.2011: 127–137
- **Reliable Location-Based Services from Radio Navigation Systems** *SENSORS*
  Qiu, D., Boneh, D., Lo, S., Enge, P.
  2010; 10 (12): 11369-11389
- **The Emergence of Cross Channel Scripting** *COMMUNICATIONS OF THE ACM*
  Bojinov, H., Bursztein, E., Boneh, D.
  2010; 53 (8): 105-113
- **Kamouflage: Loss-Resistant Password Management** *15th European Symposium on Research in Computer Security*
  Bojinov, H., Bursztein, E., Boyen, X., Boneh, D.
  SPRINGER-VERLAG BERLIN.2010: 286–302
- **Algebraic pseudorandom functions with improved efficiency from the augmented cascade.**
  Boneh, D., Montgomery, H., Raghunathan, A.
  2010
- **Preventing pollution attacks in multi-source network coding.**
  Agrawal, S., Boneh, D., Boyen, X., Freeman, D.
  2010
- **Kamouflage: loss-resistant password management.**
  Bojinov, H., Bursztein, E., Boyen, X., Boneh, D.
  2010
- **Busting frame busting: a study of clickjacking vulnerabilities at popular sites.**
  Rydstedt, G., Bursztein, E., Boneh, D., Jackson, C.
  2010
- **Privacy preserving targeted advertising.**
  Toubiana, V., Narayanan, A., Boneh, D., Nissenbaum, H., Barocas, S.
  2010
- **The case for ubiquitous transport-level encryption**
  Bittau, A., Hamburg, M., Handley, M., Mazieres, D., Boneh, D.
  2010
- **An analysis of private browsing modes in modern browsers.**
  Aggarwal, G., Bursztein, E., Jackson, C., Boneh, D.
  2010
- **Lattice basis delegation in fixed dimension and shorter ciphertext hierarchical IBE**
  Agrawal, S., Boneh, D., Boyen, X.
  2010
- **Framing attacks on smart phones and dumb routers: tap-jacking and geo-localization attacks.**
  Rydstedt, G., Gourdin, B., Bursztein, E., Boneh, D.

2010

- **Efficient lattice (H)IBE in the standard model.**
  Agrawal, S., Boneh, D., Boyen, X.
  2010
- **Preventing Pollution Attacks in Multi-source Network Coding** *13th International Conference on Practice and Theory in Public Key Cryptography*
  Agrawal, S., Boneh, D., Boyen, X., Freeman, D. M.
  SPRINGER-VERLAG BERLIN.2010: 161–176
- **Protecting Browsers from DNS Rebinding Attacks** *14th ACM Conference on Computer and Communication Security*
  Jackson, C., Barth, A., Bortz, A., Shao, W., Boneh, D.
  ASSOC COMPUTING MACHINERY.2009
- **Signing a Linear Subspace: Signature Schemes for Network Coding.**
  Boneh, D., Freeman, D., Katz, J., Waters, B.
  2009
- **XCS: cross channel scripting and its impact on web applications.**
  Bojinov, H., Bursztein, E., Boneh, D.
  2009
- **Homomorphic MACs: MAC-Based Integrity for Network Coding.**
  Agrawal, S., Boneh, D.
  2009
- **Fast symmetric cryptography in Javascript.**
  Stark, E., Hamburg, M., Boneh, D.
  2009
- **Robust Location Tag Generation from Noisy Location Data for Security Applications** *2009 International Technical Meeting of the Institute-of-Navigation*
  Qiu, D., Boneh, D., Lo, S., Enge, P.
  INST NAVIGATION.2009: 586–597
- **Physical Pseudo Random Function in Radio Frequency Sources for Security** *2009 International Technical Meeting of the Institute-of-Navigation*
  Qiu, D., De Lorenzo, D., Lo, S., Boneh, D., Enge, P.
  INST NAVIGATION.2009: 84–92
- **Pattern Classification for Geotag Generation** *22nd International Technical Meeting of the Satellite Division of the Institute-of-Navigation (ION GNSS-09)*
  Qiu, D., Lo, S., Enge, P., Boneh, D.
  INST NAVIGATION.2009: 1819–1827
- **Homomorphic MACs: MAC-Based Integrity for Network Coding** *7th International Conference on Applied Cryptography and Network Security*
  Agrawal, S., Boneh, D.
  SPRINGER-VERLAG BERLIN.2009: 292–305
- **Symmetric Cryptography in Javascript** *25th Annual Computer Security Applications Conference*
  Stark, E., Hamburg, M., Boneh, D.
  IEEE COMPUTER SOC.2009: 373–381
- **Signing a Linear Subspace: Signature Schemes for Network Coding** *12th International Conference on Practice and Theory in Public Key Cryptograhy*
  Boneh, D., Freeman, D., Katz, J., Waters, B.
  SPRINGER-VERLAG BERLIN.2009: 68–87
- **XCS: Cross Channel Scripting and its Impact on Web Applications** *16th ACM Conference on Computer and Communications Security*
  Bojinov, H., Bursztein, E., Boneh, D.
  ASSOC COMPUTING MACHINERY.2009: 420–431
- **Short signatures without random oracles and the SDH assumption in bilinear groups** *JOURNAL OF CRYPTOLOGY*
  Boneh, D., Boyen, X.

2008; 21 (2): 149-177

- **Overshadow: A virtualization-based approach to retrofitting protection in commodity operating systems** *13th International Conference on Architectural Support for Programming Languages and Operating Systems*
  Chen, X., Garfinkel, T., Lewis, E. C., Subrahmanyam, P., Waldspurger, C. A., Boneh, D., Dwoskin, J., Ports, D. R.
  ASSOC COMPUTING MACHINERY.2008: 2–13
- **Generalized Identity Based and Broadcast Encryption Schemes** *14th International Conference on the Theory and Application of Cryptology and Information Security*
  Boneh, D., Hamburg, M.
  SPRINGER-VERLAG BERLIN.2008: 455–470
- **Generalized Identity Based and Broadcast Encryption Schemes.**
  Boneh, D., Hamburg, M.
  2008
- **On The Impossibility of Basing Identity Based Encryption on Trapdoor Permutations.**
  Boneh, D., Papakonstantinou, A., Rackoff, C., Vahlis, Y., Waters, B.
  2008
- **Overshadow: A Virtualization-Based Approach to Retrofitting Protection in Commodity Operating Systems.**
  Chen, M., Subrahmanyam, P., Waldspurger, C., Lewis, E., C., Garfinkel, T., Boneh, D.
  2008
- **Circular-Secure Encryption from Decision Diffie-Hellman.**
  Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R.
  2008
- **Traitor Tracing with Constant Size Ciphertext.**
  Boneh, D., Naor, M.
  2008
- **On The Impossibility of Basing Identity Based Encryption on Trapdoor Permutations** *49th Annual Symposium on Foundations-of-Computer-Science*
  Boneh, D., Papakonstantinou, P. A., Rackoff, C., Vahlis, Y., Waters, B.
  IEEE COMPUTER SOC.2008: 283–292
- **Circular-secure encryption from decision Diffie-Hellman** *28th Annual International Cryptology Conference*
  Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R.
  SPRINGER-VERLAG BERLIN.2008: 108–125
- **Traitor Tracing with Constant Size Ciphertext** *15th ACM Conference on Computer and Communications Security*
  Boneh, D., Naor, M.
  ASSOC COMPUTING MACHINERY.2008: 501–510
- **Public key encryption that allows PIR queries** *27th Annual International Cryptology Conference*
  Boneh, D., Kushilevitz, E., Ostrovsky, R., Skeith, W. E.
  SPRINGER-VERLAG BERLIN.2007: 50–67
- **Public Key Encryption That Allows PIR Queries.**
  Boneh, D., Kushilevitz, E., Ostrovsky, R., Skeith, W.
  2007
- **Transaction Generators: Root Kits for the Web.**
  Jackson, C., Boneh, D., Mitchell, J.
  2007
- **Cryptographic Methods for Storing Ballots on a Voting Machine.**
  Bethencourt, J., Boneh, D., Waters, B.
  2007
- **Covert Channels in Privacy-Preserving Identification Systems.**

Bailley, D., Boneh, D., Goh, E., Juels, A.
2007

- **Conjunctive, subset, and range queries on encrypted data.**
Boneh, D., Waters, B.
2007

- **Exposing private information by timing web applications.**
Bortz, A., Boneh, D., Nandy, P.
2007

- **Space-Efficient Identity Based Encryption Without Pairings.**
Boneh, D., Gentry, C., Hamburg, M.
2007

- **Geoencryption using Loran.**
Qiu, D., Lo, S., Enge, P., Boneh, D.
2007

- **Private Web Search**
Saint-Jean, F., Johnson, A., Boneh, D., Feigenbaum, J.
2007

- **Reducing Shoulder-surfing by Using Gaze-based Password Entry.**
Kumar, M., Garfinkel, T., Boneh, D., Winograd, T.
2007

- **Geoencryption Using Loran** *2007 National Technical Meeting of the Institute-of-Navigation*
Qiu, D., Lo, S., Enge, P., Boneh, D., Peterson, B.
INST NAVIGATION.2007: 104–115

- **A brief look at pairings based cryptography** *48th Annual IEEE Symposium on Foundations of Computer Science*
Boneh, D.
IEEE COMPUTER SOC.2007: 19–26

- **Conjunctive, subset, and range queries on encrypted data** *4th Theory of Cryptography Conference*
Boneh, D., Waters, B.
SPRINGER-VERLAG BERLIN.2007: 535–554

- **Private Web Search** *6th ACM Workshop on Privacy in the Electronic Society*
Saint-Jean, F., Johnson, A., Boneh, D., Feigenbaum, J.
ASSOC COMPUTING MACHINERY.2007: 84–90

- **Protecting Browsers from DNS Rebinding Attacks** *14th ACM Conference on Computer and Communication Security*
Jackson, C., Barth, A., Bortz, A., Shao, W., Boneh, D.
ASSOC COMPUTING MACHINERY.2007: 421–431

- **Space-efficient identity based encryption without pairings** *48th Annual IEEE Symposium on Foundations of Computer Science*
Boneh, D., Gentry, C., Hamburg, M.
IEEE COMPUTER SOC.2007: 647–657

- **Covert Channels in Privacy-Preserving Identification Systems** *14th ACM Conference on Computer and Communication Security*
Bailey, D. V., Boneh, D., Goh, E., Juels, A.
ASSOC COMPUTING MACHINERY.2007: 297–306

- **Chosen-ciphertext security from identity-based encryption** *SIAM JOURNAL ON COMPUTING*
Boneh, D., Canetti, R., Halevi, S., Katz, J.
2006; 36 (5): 1301-1328

- **Private encrypted content distribution using private broadcast encryption.**
Barth, A., Boneh, D., Waters, B.

2006

- **On the impossibility of efficiently combining collision resistant hash functions.**
  Boneh, D., Boyen, X.
  2006
- **A collusion resistant broadcast, trace and revoke system.**
  Boneh, D., Waters, B.
  2006
- **Chosen Ciphertext Secure Public Key Threshold Encryption Without Random Oracles.**
  Boneh, D., Boyen, X., Halevi, S.
  2006
- **Strongly Unforgeable Signatures Based on Computational Diffie-Hellman.**
  Boneh, D., Shen, E., Waters, B.
  2006
- **SANE: A protection architecture for enterprise networks.**
  Casado, M., Garfinkel, T., Akella, A., Freedman, M., Boneh, D., McKeown, N.
  2006
- **Secure function evaluation with ordered binary decision diagrams.**
  Kruger, L., Jha, S., Goh, E., Boneh, D.
  2006
- **Fully Collusion Resistant Traitor Tracing With Short Ciphertexts and Private Keys.**
  Boneh, D., Sahai, A., Waters, B.
  2006
- **SANE: A protection architecture for enterprise networks** *15th USENIX Security Symposium*
  Casado, M., Garfinkel, T., Akella, A., Freedman, M. J., Boneh, D., McKeown, N., Shenker, S.
  USENIX ASSOC.2006: 137–151
- **Privacy in encrypted content distribution using private broadcast encryption** *10th International Conference on Financial Cryptography and Data Security*
  Barth, A., Boneh, D., Waters, B.
  SPRINGER-VERLAG BERLIN.2006: 52–64
- **Chosen ciphertext secure public key threshold encryption without random oracles** *Cryptographers Track held at the RSA Conference (CT-RSA)*
  Boneh, D., Boyen, X., Halevi, S.
  SPRINGER-VERLAG BERLIN.2006: 226–243
- **Fully collusion resistant traitor tracing with short ciphertexts and private keys** *24th Annual International Conference on Theory and Applications of Cryptographic Techniques*
  Boneh, D., Sahai, A., Waters, B.
  SPRINGER-VERLAG BERLIN.2006: 573–592
- **Strongly unforgeable signatures based on computational Diffie-Hellman** *9th International Conference on Theory and Practice of Public Key Cryptography*
  Boneh, D., Shen, E., Waters, B.
  SPRINGER-VERLAG BERLIN.2006: 229–240
- **On the impossibility of efficiently combining collision resistant hash functions** *26th Annual International Cryptology Conference*
  Boneh, D., Boyen, X.
  SPRINGER-VERLAG BERLIN.2006: 570–583
- **Remote timing attacks are practical** *COMPUTER NETWORKS*
  Brumley, D., Boneh, D.
  2005; 48 (5): 701-716
- **Oblivious signature-based envelope** *22nd ACM Symposium on Principles of Distributed Computing (PODC 03)*
  Li, N. H., Du, W. L., Boneh, D.

SPRINGER.2005: 293–302

- **Improved efficiency for CCA-secure cryptosystems built using identity-based encryption** *Cryptographers Track held at the RSA Conference (CT-RSA)*
  Boneh, D., Katz, J.
  SPRINGER-VERLAG BERLIN.2005: 87–103
- **Evaluating 2-DNF Formulas on Ciphertexts.**
  Boneh, D., Goh, E., Nissim, K.
  2005
- **Stronger Password Authentication Using Browser Extensions.**
  Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J.
  2005
- **Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity Based Encryption.**
  Boneh, D., Katz, J.
  2005
- **Collusion resistant broadcast encryption with short ciphertexts and private keys** *25th Annual International Cryptology Conference*
  Boneh, D., Gentry, C., Waters, B.
  SPRINGER-VERLAG BERLIN.2005: 258–275
- **Hierarchical identity based encryption with constant size ciphertext** *24th Annual International Conference on Theory and Applications of CryptographicTechniques*
  Boneh, D., Boyen, X., Goh, E. J.
  SPRINGER-VERLAG BERLIN.2005: 440–456
- **Evaluating 2-DNF formulas on ciphertexts** *2nd Theory of Cryptography Conference (TCC 2005)*
  Boneh, D., Goh, E. J., Nissim, K.
  SPRINGER-VERLAG BERLIN.2005: 325–341
- **Stronger password authentication using browser extensions** *14th USENIX Security Symposium*
  Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J. C.
  USENIX ASSOC.2005: 17–31
- **Short signatures from the Weil pairing** *JOURNAL OF CRYPTOLOGY*
  Boneh, D., Lynn, B., Shacham, H.
  2004; 17 (4): 297-319
- **Short group signatures** *24th Annual International Cryptology Conference*
  Boneh, D., Boyen, X., Shacham, H.
  SPRINGER-VERLAG BERLIN.2004: 41–55
- **On the Effectiveness of Address-Space Randomization**
  Shacham, H., Page, M., Pfaff, B., Goh, E., Modadugu, N., Boneh, D.
  2004
- **Efficient Selective Identity-Based Encryption Without Random Oracles.**
  Boneh, D., Boyen, X.
  2004
- **Short Group Signatures.**
  Boneh, D., Boyen, X., Shacham, H.
  2004
- **Secure Identity Based Encryption Without Random Oracles.**
  Boneh, D., Boyen, X.
  2004
- **Group Signatures with Verifier-Local Revocation.**
  Boneh, D., Shacham, H.

2004

- **Public key encryption with keyword search.**
  Boneh, D., Crescenzo, G., Di, Ostrovsky, R., Persiano, G.
  2004
- **Short Signatures Without Random Oracles.**
  Boneh, D., Boyen, X.
  2004
- **Public key encryption with keyword search** *23rd Annual Eurocrypt Conference*
  Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.
  SPRINGER-VERLAG BERLIN.2004: 506–522
- **Short signatures without random oracles** *23rd Annual Eurocrypt Conference*
  Boneh, D., Boyen, X.
  SPRINGER-VERLAG BERLIN.2004: 56–73
- **Secure identity based encryption without random oracles** *24th Annual International Cryptology Conference*
  Boneh, D., Boyen, X.
  SPRINGER-VERLAG BERLIN.2004: 443–459
- **Efficient selective-ID secure identity-based encryption without random oracles** *23rd Annual Eurocrypt Conference*
  Boneh, D., Boyen, X.
  SPRINGER-VERLAG BERLIN.2004: 223–238
- **Identity-based encryption from the Weil pairing** *SIAM JOURNAL ON COMPUTING*
  Boneh, D., Franklin, M.
  2003; 32 (3): 586-615
- **SiRiUS: Securing Remote Untrusted Storage.**
  Goh, E., Shacham, H., Modadugu, N., Boneh, D.
  2003
- **Remote timing attacks are practical.**
  Boneh, D., Brumley, D.
  2003
- **Oblivious Signature-Based Envelope.**
  Li, N., Du, W., Boneh, D.
  2003
- **A Survey of Two Signature Aggregation Techniques.** *In CryptoBytes*
  Boneh, D., Gentry, C., Lynn, B., Shacham, H.
  2003; 6 (2)
- **Aggregate and Verifiably Encrypted Signatures from Bilinear Maps.**
  Boneh, D., Gentry, C., Shacham, H., Lynn, B.
  2003
- **The Design and Implementation of Protocol-based Hidden Key Recovery.**
  Goh, E., Boneh, D., Golle, P., Pinkas, B.
  2003
- **Flexible OS support and applications for trusted computing.** *In the 9th Hot Topics in Operating Systems (HOTOS-IX)*
  Garfinkel, T., Rosenblum, M., Boneh, D.
  2003
- **Applications of Multilinear Forms to Cryptography.** *Contemporary Mathematics, American Mathematical Society*
  Boneh, D., Silverberg, A.

2003; 324

- **Terra: A Virtual Machine-Based Platform for Trusted Computing.**
  Garfinkel, T., Pfaff, B., Chow, J., Rosenblum, M., Boneh, D.
  2003
- **The design and implementation of protocol-based hidden key recovery** *6th International Information Security Conference (ISC 2003)*
  Goh, E. J., Boneh, D., Pinkas, B., Golle, P.
  SPRINGER-VERLAG BERLIN.2003: 165–179
- **Remote timing attacks are practical** *12th USENIX Security Symposium*
  Brumley, D., Boneh, D.
  USENIX ASSOC.2003: 1–13
- **A secure signature scheme from bilinear maps** *Cryptographers Track held at the RSA Conference (CT-RSA)*
  Boneh, D., Mironov, I., Shoup, V.
  SPRINGER-VERLAG BERLIN.2003: 98–110
- **Aggregate and verifiably encrypted signatures from bilinear maps** *International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT 2003)*
  Boneh, D., Gentry, C., Lynn, B., Shacham, H.
  SPRINGER-VERLAG BERLIN.2003: 416–432
- **Finding smooth integers in short intervals using CRT decoding** *32nd Annual ACM Symposium on Theory of Computing*
  Boneh, D.
  ACADEMIC PRESS INC ELSEVIER SCIENCE.2002: 768–84
- **Attacking an obfuscated cipher by injecting faults** *2nd Workshop on Digital Rights Management*
  Jacob, M., Boneh, D., Felten, E.
  SPRINGER-VERLAG BERLIN.2002: 16–31
- **Attacking an obfuscated cipher by injecting faults.**
  Jacob, M., Boneh, D., Felten, E.
  2002
- **Fast variants of RSA.** *CryptoBytes*
  Boneh, D., Shacham, H.
  2002; 5 (1): 1-9
- **Almost entirely correct mixing with applications to voting.**
  Boneh, D., Golle, P.
  2002
- **Optimistic mixing for exit-polls** *8th International Conference on the Theory and Application of Cryptology and Information Security*
  Golle, P., Zhong, S., Boneh, D., Jakobsson, M., Juels, A.
  SPRINGER-VERLAG BERLIN.2002: 451–465
- **Efficient generation of shared RSA keys** *JOURNAL OF THE ACM*
  Boneh, D., Franklin, M.
  2001; 48 (4): 702-722
- **On the importance of eliminating errors in cryptographic computations** *JOURNAL OF CRYPTOLOGY*
  Boneh, D., DeMillo, R. A., LIPTON, R. J.
  2001; 14 (2): 101-119
- **Where genetic algorithms excel** *EVOLUTIONARY COMPUTATION*
  Baum, E. B., Boneh, D., Garrett, C.
  2001; 9 (1): 93-124
- **Lower bounds for multicast message authentication** *International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 2001)*
  Boneh, D., Durfee, G., Franklin, M.

SPRINGER-VERLAG BERLIN.2001: 437–452

- **Lower Bounds for Multicast Message Authentication.**
  Boneh, D., Durfee, G., Franklin, M.
  2001
- **Simplified OAEP for the RSA and Rabin functions.**
  Boneh, D.
  2001
- **The Modular Inversion Hidden Number Problem.**
  Boneh, D., Halevi, S., Howgrave-Graham, N.
  2001
- **On the importance of checking cryptographic protocols for faults.** *Journal of Cryptology, Springer-Verlag*
  Boneh, D., DeMillo, R., Lipton, R.
  2001; 14 (2): 101-119
- **Improving SSL Handshake Performance via Batching.**
  Boneh, D., Shacham, H.
  2001
- **On the Unpredictability of Bits of the Elliptic Curve Diffie--Hellman Scheme.**
  Boneh, D., Shparlinski, I.
  2001
- **Improving SSL handshake performance via batching** *Cryptographers Track held at the RSA Conference (CT-RSA)*
  Shacham, H., Boneh, D.
  SPRINGER-VERLAG BERLIN.2001: 28–43
- **A method for fast revocation of public key certificates and security capabilities** *10th USENIX Security Symposium*
  Boneh, D., Ding, X. H., Tsudik, G., Wong, C. M.
  USENIX ASSOC.2001: 297–308
- **Architectural support for copy and tamper resistant software** *9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS_IX)*
  Lie, D., Thekkath, C., Mitchell, M., Lincoln, P., Boneh, D., Mitchell, J., Horowitz, M.
  ASSOC COMPUTING MACHINERY.2000: 168–77
- **Cryptanalysis of RSA with private key d less than N-0.292** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  Boneh, D., Durfee, G.
  2000; 46 (4): 1339-1349
- **Why textbook ElGamal and RSA encryption are insecure - (Extended abstract)** *6th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2000)*
  Boneh, D., Joux, A., Nguyen, P. Q.
  SPRINGER-VERLAG BERLIN.2000: 30–43
- **Why Textbook ElGamal and RSA Encryption are Insecure.**
  Boneh, D., Joux, A., Nguyen, P.
  2000
- **Generating RSA Keys on a Handheld Using an Untrusted Server.**
  Modadugu, N., Boneh, D., Kim, M.
  2000
- **Timed commitments** *20th Annual International Cryptology Conference*
  Boneh, D., Naor, M.
  SPRINGER-VERLAG BERLIN.2000: 236–254
- **Breaking generalized Diffie-Hellman modulo a composite is no easier than factoring** *INFORMATION PROCESSING LETTERS*

Biham, E., Boneh, D., Reingold, O.
1999; 70 (2): 83-87

- **Experimenting with electronic commerce on the PalmPilot** *3rd International Financial Cryptography Conference (FC 99)*
  Daswani, N., Boneh, D.
  SPRINGER-VERLAG BERLIN.1999: 1–16
- **Twenty years of attacks on the RSA cryptosystem.** *Notices of the American Mathematical Society (AMS)*
  Boneh, D.
  1999; 46 (2): 203-213
- **Factoring N=prq for large r.**
  Boneh, D., Durfee, G., Howgrave-Graham, N.
  1999
- **Breaking generalized Diffie-Hellman modulo a composite is no easier than factoring.**
  Biham, E., Boneh, D., Reingold, O.
  1999
- **Experimenting with Shared Generation of RSA keys.**
  Malkin, M., Wu, T., Boneh, D.
  1999
- **Experimenting with electronic commerce on the PalmPilot.**
  Boneh, D., Daswani, N.
  1999
- **Building intrusion tolerant applications.**
  Wu, T., Malkin, M., Boneh, D.
  1999
- **An efficient public key traitor tracing scheme.**
  Boneh, D., Franklin, M.
  1999
- **Anonymous authentication with subset queries.**
  Boneh, D., Franklin, M.
  1999
- **Cryptanalysis of RSA with private key d less than N-0.292** *International Conference on the Theory and Application of Cryptographic Techniques*
  Boneh, D., Durfee, G.
  SPRINGER-VERLAG BERLIN.1999: 1–11
- **Building intrusion tolerant applications** *8th USENIX Security Symposium (Security 99)*
  Wu, T., Malkin, M., Boneh, D.
  USENIX ASSOC.1999: 79–91
- **Collusion-secure fingerprinting for digital data** *IEEE TRANSACTIONS ON INFORMATION THEORY*
  Boneh, D., Shaw, J.
  1998; 44 (5): 1897-1905
- **Breaking RSA may not be equivalent to factoring (Extended abstract)** *International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 98)*
  Boneh, D., Venkatesan, R.
  SPRINGER-VERLAG BERLIN.1998: 59–71
- **An attack on RSA given a small fraction of the private key bits.**
  Boneh, D., Durfee, G., Frankel, Y.
  1998

- **Breaking RSA may not be equivalent to factoring.**
  Boneh, D., Venkatesan, R.
  1998
- **Cryptanalysis of RSA with private key d less than N0.292.**
  Boneh, D., Durfee, G.
  1998
- **The decision Diffie-Hellman problem.**
  Boneh, D.
  1998
- **Generating a Product of Three Primes With an Unknown Factorization.**
  Boneh, D., Horwitz, J.
  1998
- **A generalized wallet architecture.**
  Daswani, N., Boneh, D., Gracia-Molina, H., Ketchpel, S., Paepcke, A.
  1998
- **An attack on RSA given a small fraction of the private key bits** *International Conference on the Theory and Application of Cryptology and Information Security*
  Boneh, D., Durfee, G., Frankel, Y.
  SPRINGER-VERLAG BERLIN.1998: 25–34
- **SWAPEROO: A simple wallet architecture for payments, exchanges, refunds, and other operations** *3rd USENIX Workshop on Electronic Commerce*
  Daswani, N., Boneh, D., Garcia-Molina, H., KETCHPEL, S., Paepcke, A.
  USENIX ASSOC.1998: 121–139
- **Revocation of unread E-mail in an untrusted network.**
  Rubin, A., Boneh, D., Fu, K.
  1997
- **Rounding in lattices and its cryptographic applications.**
  Boneh, D., Venkatesan, R.
  1997
- **Effect of operators on straight line complexity.**
  Boneh, D., Lipton, R.
  1997
- **On the importance of checking cryptographic protocols for faults.**
  Boneh, D., DeMillo, R., Lipton, R.
  1997
- **A revocable backup system.**
  Boneh, D., Lipton, R.
  1996
- **Running dynamic programming algorithms on a DNA computer.**
  Baum, E., Boneh, D.
  1996
- **Algorithms for black box fields and their application to cryptography.**
  Boneh, D., Lipton, R.
  1996
- **Making DNA computers error resistant.**
  Boneh, D., Lipton, R.
  1996

- **Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes.**
  Boneh, D., Venkatesan, R.
  1996
- **On the computational power of DNA.** *In Discrete Applied Mathematics, Special Issue on Computational Molecular Biology*
  Boneh, D., Dunworth, C., Lipton, R., Sgall, J.
  1996; 71: 79-94
- **Collusion secure fingerprinting for digital data.**
  Boneh, D., Shaw, J.
  1995
- **Quantum cryptanalysis of hidden linear forms.**
  Boneh, D., Lipton, R.
  1995
- **Breaking DES using a molecular computer.**
  Boneh, D., Dunworth, C., Lipton, R.
  1995
- **Learning using group representations.**
  Boneh, D.
  1995
- **Amplification of weak learning over the uniform distribution.**
  Boneh, D., Lipton, R.
  1993
- **A Secure Signature Scheme from Bilinear Maps.**
  Boneh, D., Mironov, I., Shoup, V.
- **Protecting Browsers from DNS Rebinding Attacks.**
  Jackson, C., Barth, A., Bortz, A., Shao, W., Boneh, D.
  2009, 2007
- **Client side caching for TLS.** *ACM Trans. Info. and Sys. Security*
  Boneh, D., Shacham, H., Rescrola, E.
  2,004; 4 (7): 553-75
- **Protecting Browser State from Web Privacy Attacks.**
  Jackson, C., Bortz, A., Boneh, D., Mitchell, J.
- **Hierarchical Identity Based Encryption with Constant Size Ciphertext.**
  Boneh, D., Goh, E., Boyen, X.
- **A Method for Fast Revocation of Public Key Certificates and Security Capabilities.**
  Boneh, D., Ding, X., Tsudik, G., Wong, M.
- **Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys.**
  Boneh, D., Gentry, C., Waters, B.