Paul Cuff

paul.cuff@gmail.com

Education

- **Stanford University** — Palo Alto, CA
  Ph.D. in Electrical Engineering — *2004 - 2009*
  - Advisor: Thomas Cover
  - Ph.D Qualification Exam Ranking: 1/148
  - GPA: 4.0+
- **Brigham Young University** — Provo, UT
  B.S. in Electrical Engineering — *1998 - 2004*
  - Major GPA: 4.0 (Overall: 3.93)
- **Rex Putnam High School** — Milwaukie, OR
  1994 - 1998
  - Valedictorian

Professional Experience

- **Renaissance Technologies** — East Setauket, NY
  Principal Researcher — *2017-present*
- **Princeton University - Electrical Engineering Department** — Princeton, NJ
  Assistant Professor — *2009-2017*
- **Peavey Electronics** — Meridian, MS
  Expert Witness & Consultant — *2010 - 2011*
- **Microsoft Research** — Redmond, WA
  Intern - Theory Group — *Summer 2008*
  - Probability theory research (Markov chain mixing time).
- **Google** — Mountain View, CA
  Intern - Decision Support - Search Quality Analyst — *Summer 2007*
- **Nuova Systems** — Santa Clara, CA
  Intern—Network Congestion-Control Algorithms Researcher — *Spring 2006*
- **Adaptive Hearing Solutions** — Palo Alto, CA
  Co-Founder with Prof. Bernard Widrow — *2005*
  - Designed real-time speech denoising adaptive filter for hearing aids.
  - Secured funding through pitches and demonstrations to investors.
- **L-3 Communications** — Salt Lake City, UT
  Intern - Advanced Communications Group — *Summer 2004*
  - Implemented military comm. systems in C++, including Reed-Solomon encoder and decoder.
- **Electro Scientific Industries** — Beaverton, OR
  Intern - Circuit Design — *Summer 2002*
  - Designed and prototyped power amplifiers for precision control circuits.

Publications

Journal Publications

[J1] A. Bunin, Z. Goldfeld, H. Permuter, S. Shamai, P. Cuff, P. Piantanida, "Key and Message Semantic-Security over State-Dependent Channels," accepted to *IEEE Trans. on Information Forensics and Security*, June, 2018.

[J2] J. Buhler, P. Cuff, A. Hales, R. Stong, "Puzzles in Memory of Solomon Golomb," *IEEE Trans. on Information Theory*, 64(4):2839-43, April, 2018.

[J3] J. Liu, P. Cuff, S. Verdú, "Common Randomness and Key Generation with Limited Interaction," *IEEE Trans. on Information Theory*, 63(11):7358-81, November, 2017.

[J4] J. Liu, P. Cuff, S. Verdú, "E_γ Resolvability," *IEEE Trans. on Information Theory*, 63(5):2629-58, May, 2017.

[J5] T. Moy, L. Huang, W. Rieutort-Louis, C. Wu, P. Cuff, S. Wagner, J. Sturm, N. Verma, "An EEG Acquisition and Biomarker-Extraction System Using Low-Noise-Amplifier and Compressive-Sensing Circuits Based on Flexible, Thin-Film Electronics," *IEEE Journal of Solid State Circuits*, 52(1):309-21, January, 2017.

[J6] Z. Goldfeld, G. Kramer, H. Permuter, P. Cuff, "Strong Secrecy for Cooperative Broadcast Channels," *IEEE Trans. on Information Theory*, 63(1):469-95, January, 2017.

[J7] Z. Goldfeld, P. Cuff, H. Permuter, "Arbitrarily Varying Wiretap Channels with Type Constrained States," *IEEE Trans. on Information Theory*, 62(12):7216-44, December, 2016.

[J8] S. Satpathy, P. Cuff, "Secure Cascade Channel Synthesis," *IEEE Trans. on Information Theory*, 62(11):6081-94, November, 2016.

[J9] Z. Goldfeld, P. Cuff, H. Permuter, "Semantic-Security Capacity for Wiretap Channels of Type II," *IEEE Trans. on Information Theory*, 62(7):3863-79, July, 2016.

[J10] C. Schieler, P. Cuff, "The Henchman Problem: Measuring Secrecy by the Minimum Distortion in a List," *IEEE Trans. on InformationTheory*, 62(6):3436-50, June, 2016.

[J11] E. Song, P. Cuff, V. Poor, "The Likelihood Encoder for Lossy Compression," *IEEE Trans. on Information Theory*, 62(4):1836-49, April, 2016.

[J12] J. Liu, P. Cuff, S. Verdú, "Key Capacity for Product Sources with Application to Stationary Gaussian Processes," *IEEE Trans. on Information Theory*, 62(2):984-1005, February, 2016.

[J13] S. Shang, P. Cuff, P. Hui, S. Kulkarni, "An Upper Bound on the Convergence Time for Quantized Consensus of Arbitrary Static Graphs," *IEEE Trans. on Automatic Control*, 60(4):1127-32, April, 2015.

[J14] C. Schieler, P. Cuff, "Rate-Distortion Theory for Secrecy Systems," *IEEE Trans. on Information Theory*, 60(12):7584-605, December, 2014.

[J15] E. Song, E. Soljanin, P. Cuff, V. Poor, K. Guan, "Rate-Distortion-Based Physical Layer Secrecy in Multimode Fiber," *IEEE Trans. on Communications*, 62(3):1080-90, March, 2014.

[J16] P. Cuff, "Distributed Channel Synthesis," *IEEE Trans. on Information Theory*, 59(11):7071-96, November, 2013.

[J17] P. Cuff, J. Ding, O. Louidor, E. Lubetzky, Y. Peres, A. Sly, "Glauber Dynamics for the Mean-Field Potts Model," *Journal of Statistical Physics*, 149(3):432-477, November, 2012.

[J18] J. Wang, J. Chen, L. Zhao, P. Cuff, H. Permuter, "On the Role of the Refinement Layer in Multiple Description Coding and Scalable Coding," *IEEE Trans. on Information Theory*, 57(3):1443-1456, March, 2011.

[J19] P. Cuff, H. Permuter, T. Cover, "Coordination Capacity," *IEEE Trans. on Information Theory*, 56(9):4181-4206, September, 2010.

[J20] H. Permuter, P. Cuff, B. Van Roy, T. Weissman, "Capacity of the Trapdoor Channel with Feedback," *IEEE Trans. on Information Theory*, 54(7):3150-65, July, 2008.

Submitted Journal Publications:

[J21] S. Yagli, P. Cuff, "Exact Exponent for Soft Covering," submitted to *IEEE Trans. on Information Theory*, September, 2018.

[J22] J. Liu, T. Courtade, P. Cuff, S. Verdú, "Smoothing Brascamp-Lieb Inequalities and Strong Converses of Coding Theorems," submitted to *IEEE Trans. on Information Theory*, April, 2017.

[J23] Z. Goldfeld, P. Cuff, H. Permuter, "Wiretap Channels with Random States Non-Causally Available at the Encoder," submitted to *IEEE Trans. on Information Theory*, August, 2016.

Books and Chapters

[B1] P. Cuff, C. Schieler, "Secure Source Coding," Chapter 3 in *Information Theoretic Security and Privacy of Information Systems*, Cambridge University Press, 2017.

[B2] P. Cuff, "Communication in Networks for Coordinating Behavior." Ph.D. dissertation, Stanford University, August, 2009.

Conference Publications

[C1] S. Wagh, P. Mittal, P. Cuff, "Differentially Private Oblivious RAM," *Privacy Enhancing Technologies Symp. (PETS)*, Barcelona, Spain, July, 2018.

[C2] S. Yagli, P. Cuff, "Exact Soft-Covering Exponent," *IEEE Int'l. Symp. Inf. Theory (ISIT)*, Vail, Colorado, June, 2018.

[C3] A. Bunin, Z. Goldfeld, H. Permuter, S. Shamai, P. Cuff, P. Piantanida, "Key-Message Security over State-Dependent Wiretap Channels," *IEEE Int'l. Symp. Inf. Theory (ISIT)*, Vail, Colorado, June, 2018.

[C4] L. Yu, P. Cuff, "The Shannon Cipher System with a Guessing Eavesdropper," *IEEE Int'l. Symp. Inf. Theory (ISIT)*, Aachen, Germany, June, 2017.

[C5] Z. Goldfeld, P. Cuff, H. Permuter, "The Gelfand-Pinsker Wiretap Channel: Higher Secrecy Rates via a Novel Superposition Code," *IEEE Int'l. Symp. Inf. Theory (ISIT)*, Aachen, Germany, June, 2017.

[C6] A. Bunin, Z. Goldfeld, H. Permuter, S. Shamai, P. Cuff and P. Piantanida, "Semantically-Secured Message-Key Trade-off over Wiretap Channels with Random Parameters," *Eurocrypt (WCS, Workshop on Communication Security)*, Paris, France, April, 2017.

[C7] Z. Goldfeld, P. Cuff, H. Permuter, "Arbitrarily Varying Wiretap Channels with Type Constrained States," *IEEE Global Communications Conf. (Globecom)*, Washington D.C., December, 2016.

[C8] Z. Goldfeld, P. Cuff, H. Permuter, "Wiretap Channels with Random States Non-Causally Available at the Encoder," *IEEE Int'l. Conf. on the Science of Electrical Engineering (ICSEE)*, Eilat, Israel, November, 2016.

[C9] P. Cuff, L. Yu, "Differential Privacy as a Mutual Information Constraint," *ACM Conf. on Computer and Communication Security (CCS)*, Vienna, Austria, October, 2016.

[C10] Z. Goldfeld, P. Cuff, H. Permuter, "Semantic-Security Capacity for Wiretap Channels of Type II," *IEEE Int'l. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, July, 2016.

[C11] P. Cuff, "Soft Covering with High Probability," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Barcelona, Spain, July, 2016.

[C12] J. Liu, P. Cuff, S. Verdú, "Key Generation with Limited Interaction," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Barcelona, Spain, July, 2016.

[C13] J. Liu, T. Courtade, P. Cuff, S. Verdú, "Brascamp-Lieb Inequality and Its Reverse: An Information Theoretic View," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Barcelona, Spain, July, 2016.

[C14] J. Liu, T. Courtade, P. Cuff, S. Verdú, "Smoothing Brascamp-Lieb Inequalities and Strong Converses for Common Randomness Generation," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Barcelona, Spain, July, 2016.

[C15] Z. Goldfeld, P. Cuff, H. Permuter, "Semantic-Security Capacity for the Physical Layer via Information Theory," *IEEE Int'l. Conf. on Software Science, Technology, and Engineering (SwSTE)*, Be'er Sheva, Israel, June, 2016.

[C16] Z. Goldfeld, G. Kramer, H. Permuter, P. Cuff, "Strong Secrecy for Cooperative Broadcast Channels," *Int'l. Zurich Seminar on Communications (IZS)*, Zurich, Switzerland, March, 2016.

[C17] P. Cuff, "A Stronger Soft-Covering Lemma and Applications," *IEEE Conf. on Communications and Network Security (CNS, Workshop on Physical-layer Methods for Wireless Security)*, Florence, Italy, September, 2015.

[C18] S. Satpathy, P. Cuff, "Gaussian Secure Source Coding and Wyner's Common Information," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Hong Kong, June, 2015.

[C19] J. Liu, P. Cuff, S. Verdú, "One-Shot Mutual Covering Lemma and Marton's Inner Bound with a Common Message," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Hong Kong, June, 2015. **(Semi-plenary Talk)**

[C20] J. Liu, P. Cuff, S. Verdú, "Secret Key Generation with One Communicator and a One-Shot Converse via Hypercontractivity," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Hong Kong, June, 2015.

[C21] J. Liu, P. Cuff, S. Verdú, "Resolvability in E_γ with Applications to Lossy Compression and Wiretap Channels," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Hong Kong, June, 2015.

[C22] E. Song, P. Cuff, V. Poor, "Joint Source-Channel Secrecy Using Hybrid Coding," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Hong Kong, June, 2015.

[C23] E. Song, P. Cuff, V. Poor, "A Rate-Distortion Based Secrecy System with Side Information at the Decoders," *Allerton Conf. on Communication, Control, and Computing (Allerton)*, Monticello, Illinois, October, 2014.

[C24] S. Satpathy, P. Cuff, "Secure Coordination with a Two-Sided Helper," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Honolulu, Hawaii, July, 2014.

[C25] E. Song, P. Cuff, V. Poor, "The Likelihood Encoder for Lossy Source Compression," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Honolulu, Hawaii, July, 2014.

[C26] C. Schieler, P. Cuff, "The Henchman Problem: Measuring Secrecy by the Minimum Distortion in a List," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Honolulu, Hawaii, July, 2014.

[C27] J. Liu, P. Cuff, S. Verdú, "Key Capacity with Limited One-Way Communication for Product Sources," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Honolulu, Hawaii, July, 2014.

[C28] S. Shang, T. Wang, P. Cuff, S. Kulkarni, "The Application of Differential Privacy for Rank Aggregation: Privacy and Accuracy," *Int'l. Conf. on Information Fusion (Fusion)*, Salamanca, Spain, July, 2014.

[C29] S. Shang, Y. Hui, P. Hui, P. Cuff, S. Kulkarni, "Beyond Personalization and Anonymity: Towards a Group-Based Recommendation System," *Symp. on Applied Computing (SAC)*, Gyeongju, S. Korea, March, 2014.

[C30] P. Cuff, E. Song, "The Likelihood Encoder in Source Coding," *IEEE Information Theory Workshop (ITW)*, Seville, Spain, September, 2013.

[C31] C. Schieler, P. Cuff, "A Connection between Good Rate-distortion Codes and Backward DMCs," *IEEE Information Theory Workshop (ITW)*, Seville, Spain, September, 2013.

[C32] P. Cuff, "Secrecy in Cascade Networks," *IEEE Information Theory Workshop (ITW)*, Seville, Spain, September, 2013.

[C33] C. Schieler, P. Cuff, "Rate-distortion Theory for Secrecy Systems," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Istanbul, Turkey, July, 2013.

[C34] C. Song, P. Cuff, H.V. Poor, "A Bit of Secrecy for Gaussian Source Compression," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Istanbul, Turkey, July, 2013.

[C35] S. Satpathy, P. Cuff, "Secure Cascade Channel Synthesis," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Istanbul, Turkey, July, 2013.

[C36] S. Shang, P. Cuff, P. Hui, S. Kulkarni, "An Upper Bound on the Convergence Time for Quantized Consensus," *IEEE Int'l. Conf. on Computer Communications (Infocom)*, Turin, Italy, April, 2013.

[C37] P. Cuff, "Optimal Equivocation in Secrecy Systems – A Special Case of Distortion-based Characterization," *Information Theory and Applications Workshop (ITA)*, San Diego, California, February, 2013.

[C38] T. Wang, J. Sturm, P. Cuff, S. Kulkarni, "Condorcet Voting Methods Avoid the Paradoxes of Voting Theory," *Allerton Conf. on Communication, Control, and Computing (Allerton)*, Monticello, Illinois, October, 2012.

[C39] C. Schieler, C. Song, P. Cuff, V. Poor, "Source-Channel Secrecy with Causal Disclosure," *Allerton Conf. on Communication, Control, and Computing (Allerton)*, Monticello, Illinois, October, 2012.

[C40] S. Shang, S. Kulkarni, P. Cuff, P. Hui, "A Random Walk Based Model Incorporating Social Information for Recommendations," *IEEE Machine Learning for Signal Processing Workshop (MLSP)*, Santander, Spain, September, 2012.

[C41] S. Shang, P. Cuff, S. Kulkarni, P. Hui, "An Upper Bound on the Convergence Time for Distributed Binary Consensus," *Int'l. Conf. on Information Fusion (Fusion)*, Singapore, July, 2012.

[C42] C. Schieler, P. Cuff, "Secrecy Is Cheap if the Adversary Must Reconstruct," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Boston, Massachusetts, July, 2012.

[C43] T. Wang, P. Hui, S. Kulkarni, P. Cuff, "Cooperative Caching based on File Popularity Ranking in Delay Tolerant Networks," *Extreme Conf. on Communication (ExtremeCom)*, Zurich, Switzerland, March, 2012.

[C44] P. Cuff, "The Source Coding Side of Secrecy," *Int'l. Zurich Seminar on Communications (IZS)*, Zurich, Switzerland, February, 2012.

[C45] P. Cuff, "A Class of Log-optimal Utility Functions," *Information Theory and Applications Workshop (ITA)*, San Diego, California, February, 2012.

[C46] P. Cuff, L. Zhao, "Coordination using Implicit Communication," *IEEE Information Theory Workshop (ITW)*, Paraty, Brazil, October, 2011.

[C47] S. Shang, P. Hui, S. Kulkarni, P. Cuff, "Wisdom of the Crowd: Incorporating Social Influence in Recommendations Models," *IEEE Int'l. Conf. on Parallel and Distributed Systems (ICPADS, HotPOST Workshop)*, Tainan, Taiwan, December, 2011. **(Best Paper Award)**

[C48] P. Cuff, C. Schieler, "Hybrid Codes Needed for Coordination over the Point-to-Point Channel," *Allerton Conf. on Communication, Control, and Computing (Allerton)*, Monticello, Illinois, September, 2011.

[C49] P. Cuff, T. Cover, G. Kumar, L. Zhao, "A Lattice of Gambles," *IEEE Int'l. Symp. on Information Theory (ISIT)*, St. Petersburg, Russia, August, 2011.

[C50] H. Aftab, N. Raj, P. Cuff, and S. Kulkarni, "Mutual Information Scheduling for Ranking," *Int'l. Conf. on Information Fusion (Fusion)*, Chicago, Illinois, July, 2011.

[C51] P. Cuff, "A Framework for Partial Secrecy," *IEEE Global Communications Conf. (Globecom)*, Miami, Florida, December, 2010.

[C52] P. Cuff, "Using Secret Key to Foil an Eavesdropper," *Allerton Conf. on Communication, Control, and Computing (Allerton)*, Monticello, Illinois, September, 2010.

[C53] P. Cuff, "State Information in Bayesian Games," invited and presented at *Allerton Conf. on Communication, Control, and Computing (Allerton)*, Monticello, Illinois, October, 2009, published at http://arxiv.org/abs/0911.0874.

[C54] P. Cuff, H.-I Su, A. El Gamal, "Cascade Multiterminal Source Coding," *IEEE Int. Symp. on Information Theory (ISIT)*, Seoul, S. Korea, July, 2009.

[C55] L. Zhao, P. Cuff, H. Permuter, "Consolidating Achievable Regions for Multiple Descriptions," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Seoul, S. Korea, July, 2009.

[C56] P. Cuff, "Communication Requirements for Generating Correlated Random Variables," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Toronto, Canada, July, 2008. **(Best Student Paper Award)**

[C57] H. Permuter, P. Cuff, B. Van Roy, and T. Weissman, "Capacity and Zero-Error Capacity of the Chemical Channel with Feedback," *IEEE Int'l. Symp. on Information Theory (ISIT)*, Nice, France, June, 2007.

[C58] H. Permuter, P. Cuff, B. Van Roy, and T. Weissman, "Capacity of the Trapdoor Channel with Feedback," *Allerton Conf. on Communication, Control, and Computing (Allerton)*, Monticello, Illinois, September, 2006.

Invited Talks, Seminars, and Panels

[T1] "Soft Covering Exponent," *Information Theory and Applications Workshop*, February, 2019.

[T2] "Soft Covering Exponent," *Information Theory Forum, Stanford*, January, 2019.

[T3] "Distribution Approximation Techniques for Security, Differential Privacy, and Learning," *EECS Department Seminar, MIT*, May, 2017.

[T4] "Wiretap Channels with Random States," *IEEE Conf. on Information Sciences and Systems*, March, 2017.

[T5] "Differential Privacy as a Mutual Information Constraint," *Information Theory and Applications Workshop*, February, 2017.

[T6] "Part 1: Wiretap Channels with Random States; Part 2: Differential Privacy as a Mutual Information Constraint," *EE Department Seminar, Univ. of Michigan*, November, 2016.

[T7] "Part 1: Wiretap Channels with Random States; Part 2: Differential Privacy as a Mutual Information Constraint," *EE Department Seminar, Univ. of Maryland*, November, 2016.

[T8] "Part 1: Wiretap Channels with Random States; Part 2: Differential Privacy as a Mutual Information Constraint," *Information Theory Forum, Stanford*, September, 2016.

[T9] "Secure Communication through Wiretap Channels," *EE Department Seminar, Pennsylvania State Univ.*, August, 2016.

[T10] "Introduction to Information Theory," *Guest Lecture, Accounting Department, Rutgers Univ.*, June, 2016.

[T11] "The Next 50 Years," *IEEE Conf. on Information Sciences and Systems*, March, 2016. **(Panel)**

[T12] "Semantic Security in Wiretap Channels," *AFOSR Information Operations and Security Program Review*, April, 2016.

[T13] "Semantic Security using a Stronger Soft-Covering Lemma," *Int'l. Zurich Seminar on Communications*, March, 2016.

[T14] "Estimation of Smoothed Entropy," *Information Theory and Applications Workshop*, February, 2016.

[T15] "Semantic Security using a Stronger Soft-Covering Lemma," *EE Systems Seminar, Caltech*, November, 2015.

[T16] "Semantic Security using a Stronger Soft-Covering Lemma," *Information Theory Forum, Stanford*, November, 2015.

[T17] "Semantic Security using a Stronger Soft-Covering Lemma," *EE Department Seminar, UC Berkeley*, November, 2015.

[T18] "Semantic Security using a Stronger Soft-Covering Lemma," *EE Department Seminar, USC*, November, 2015.

[T19] "Semantic Security using a Stronger Soft-Covering Lemma," *EE Department Seminar, UC Irvine*, November, 2015.

[T20] "Semantic Security using a Stronger Soft-Covering Lemma," *IEEE CNS Workshop on Physical-layer Methods for Wireless Security*, September, 2015. **(Keynote Talk)**

[T21] "Semantic Security using a Stronger Soft-Covering Lemma," *Science of Information Day, Princeton*, September, 2015.

[T22] "Embedded Coordination for Signals," *IEEE Communication Theory Workshop*, May, 2015.

[T23] "Zero-Delay Distortion-Inducing Secure Source Coding," *IEEE Information Theory Workshop*, April, 2015.

[T24] "The Third Way," *IEEE Information Theory Workshop*, April, 2015.

[T25] "Secret Key Agreement with Rate-Limited Communication Among Three Nodes," *Information Theory and Applications Workshop*, February, 2015.

[T26] "Provable Security of Communication for Protecting Information Flow in Distributed Systems," *AFOSR Cybersecurity and Information Science Program Review*, January, 2015.

[T27] "Secure Rate-Limited Feedback for Control," *Allerton Conference*, October, 2014.

[T28] "Source Coding (secrecy and embedding)," *Edgestream Partners*, September, 2014.

[T29] "Rate-Distortion Theory for Secrecy Systems," *Int'l. Conf. on Signal Processing and Communications*, July, 2014. **(Tutorial)**

[T30] "The Likelihood Encoder," *Int'l. Zurich Seminar on Communications*, February, 2014.

[T31] "The Henchman Problem — Secrecy measured by minimum distortion in a list," *Information Theory and Applications Workshop*, February, 2014.

[T32] "Rate-distortion Theory for Secrecy Systems," *EE Department Seminar, Cornell*, October, 2013.

[T33] "Rate-distortion Theory for Secrecy Systems," *EE Department Seminar, BYU*, October, 2013.

[T34] "Rate-distortion Theory for Communication in Games," *EE Department Seminar, Yale*, October, 2013.

[T35] "Secrecy Aspects of Communication for Distributed Systems," *AFOSR Information Operations and Security Annual PI Meeting*, August, 2013.

[T36] "Information Theory and Log-optimal Trading," *Process Driven Trading*, July, 2013.

[T37] "Rate-distortion Theory for Secrecy Systems," *NIKSUN World Wide Security and Mobility Conference*, June, 2013.

[T38] "Rate-distortion Theory for Secrecy Systems," *Communications Seminar, UIUC*, April, 2013.

[T39] "How Structure Affects Information Transfer," *What is Information? Workshop*, January, 2013.

[T40] "Requirements for Fair and Robust Voting Systems," *NIPS Workshop on Social Choice: Theory and Practice*, December, 2012.

[T41] "Secrecy Aspects of Communication for Distributed Systems," *AFOSR Information Operations and Security Annual PI Meeting*, October, 2012.

[T42] "Secure Communication of Signals," *Mathematics Colloquium, Bell Labs*, September, 2012.

[T43] "Secure Communication of Signals," *EE Department Seminar, UC Berkeley*, August, 2012.

[T44] "Secure Communication of Signals," *ISL Colloquium, Stanford*, August, 2012.

[T45] "Toward a Secure Data-rate Theorem," *IEEE Conf. on Information Sciences and Systems*, March, 2012.

[T46] "Secure Communication for Distributed Systems," *Colloquium, Institute for Defense Analysis – Center for Communications Research*, November, 2011.

[T47] "Secure Communication for Distributed Systems," *Communications Seminar, UIUC*, November, 2011.

[T48] "Secure Communication for Distributed Systems," *EE Department Colloquium, Syracuse*, November, 2011.

[T49] "Information Theory—Aggregating Information," *Princeton Stats Symposium*, 2011.

[T50] "Causal Secrecy: An Informed Eavesdropper," *Information Theory and Applications Workshop*, February, 2011.

[T51] "Secure Communication for Distributed Systems," *HP Seminar, MIT*, November, 2010.

[T52] "Information Theory for Secrecy and Control," *EE Department Seminar, Univ. of Utah*, August, 2010.

[T53] "Information Theory for Secrecy and Control," *EE Department Seminar, BYU*, August, 2010.

[T54] "When Research is Puzzling, and Puzzling is Research," *MIRTHE & PCCM REU Guest Lecture*, June, 2010.

[T55] "Efficient Communication for Control in Games and Networks," *Information Sciences and Systems Seminar*, October, 2009.

[T56] "Investigating the Fundamental Communication Burden of Cooperation," *Information Theory and Applications Workshop*, February, 2009.

[T57] "The Golden Ratio in Communication—Blackwell's Trapdoor Channel and Task Assignment," *HP Seminar, MIT*, November, 2008.

[T58] "Coordination via Communication," *Allerton Conference*, September, 2008.

[T59] "Coordination via Communication," *School of Information Theory*, May, 2008.

[T60] "Entropy Rates of Hidden Markov Processes emerge from Blackwell's Trapdoor Channel," *BIRS Workshop on Entropy Rate of Hidden Markov Processes and Connections to Dynamical Systems*, October, 2007.

Awards and Honors

- **Engineering Commendation List for Outstanding Teaching (Princeton)** 2016 - 2017
- **Young Investigator Program Award (AFOSR YIP)** 2015
- **CAREER Award (NSF)** 2014
- **Best Paper Award (ICPADS, HotPOST Workshop)** 2011
- **Best Student Paper Award (ISIT)** 2008
- **National Defense Science and Engineering Graduate Fellowship** 2005 - 2008
- **Numerical Technologies Fellowship (Stanford)** 2005
- **Outstanding Teaching Assistant (Stanford IEEE-WIE)** 2005
- **Entrepreneurial Challenge: 1st Place (Stanford BASES)** 2005
- **Micron Scholarship (BYU)** 2002 - 2004
- **Tau Beta Pi (BYU)** 2002 - 2004
- **Dean's List (BYU)** 2001 - 2004
- **Academic Full Scholarship (BYU)** 1998 - 2002

Academic Community Involvement

- Technical Program Committee, *IEEE Information Theory Workshop*, Jerusalem, Israel, 2015.
- Invited-Session Organizer, "Security of Information," *IEEE CISS*, Princeton, New Jersey, 2014.
- Technical Program Committee, *IEEE Information Theory Workshop*, Seville, Spain, 2013.
- Technical Program Co-Chair, *School of Information Theory*, Ithaca, NY, 2012.
- General Co-Chair, *IEEE Conf. on Information Sciences and Systems*, Princeton, New Jersey, 2012.
- Finance and Sponsorship Co-Chair, *IEEE WiOpt*, Princeton, New Jersey, 2011.
- Technical Program Committee, *IEEE Information Theory Workshop*, Cairo, Egypt, 2010.
- Mentor and Advisor (three interns), *NSF MIRTHE Center REU*, 2010 and 2012.
- Manuscript Reviewer (45 journal reviews), *IEEE Journals*, 2010-present.
- Proposal Reviewer and 3x Panelist, *NSF and AFOSR.*
- Member, *IEEE*, 2009-present.

Funding

- **Air Force Office of Scientific Research FA9550-15-1-0180** 2015-2018
  Performance-based Security for Encoding of Information Signals *$360,000*
- **National Science Foundation CCF-1350595** 2014-2019
  CAREER: Digital Encoding of Information Signals for Security with Limited Resources *$450,000*
- **Air Force Office of Scientific Research FA9550-12-1-0196** 2012-2015
  Provable Security of Comm. for Protecting Information Flow in Distributed Systems *$450,000*
- **National Science Foundation CCF-1116013** 2011-2015
  Causal Secrecy: A Theoretical Basis for Secrecy of Signals *$490,000*
- **National Science Foundation CCF-1017431 (transfer from R. Calderbank)** 2011-2013
  Collaborative Research: Compressed Sensing for High-Resolution Image Inversion *$142,131.95*

Research Advising

Ph.D.

- Lanqing Yu (third year)
- Jingbo Liu (fifth year), co-advised S. Verdú
- Sanket Satpathy – Squarepoint Capital 2016
- Eva Song – Huawei, co-advised H. V. Poor 2015
- Tiance Wang – Goldman Sachs, co-advised S. Kulkarni 2015
- Shang Shang – Amazon, co-advised S. Kulkarni 2014
- Curt Schieler – Lincoln Labs 2014

Undergraduate Research

- 32 semester research projects: 2010-2017
- Kevin Wang (junior independent work) 2016
- Peter Park (junior independent work) 2015-16
- Michael Freyberger (junior independent work) 2015
- Timothy Seah (junior independent work) 2015
- Aaron Himelman (junior independent work) 2014
- Yuan Chen (junior and senior independent work) 2012-13
- Jennifer Tang (junior and senior independent work) 2011-13
- Hamza Aftab (summer research and junior independent work) 2010
- Florina Yezril (senior independent work) 2010
- Nevin Raj (summer research earned best talk award) 2010

Princeton University Involvement

- Chair, *Faculty Advisory Committee on Athletics and Campus Recreation*, 2013-14.
  - Committee Member, 2011-14, 2015-16.
- Committee Member, *Program in Robotics and Intelligent Systems*, 2014-present.
- Committee Member, *ELE Undergraduate Committee*, 2010-present.
- Committee Member, *ELE Graduate Committee*, 2011-14, 2015-present.
- Committee Member, *ELE Faculty Hiring Committee*, 2010-11, 2015-present.
- Course Redesign and Teaching, required undergraduate course, *ELE 201, Info. Signals*, 2013.
- Course Redesign (committee of five), required undergraduate project course, *ELE 302*, 2010.
- Dissertation Reader (15 dissertations), *Ph.D Examination Committee*, 2011-present.
- Associated Faculty, *Center for Information Technology Policy*, 2009-present.
- Faculty Fellow, *Football Team*, 2011-present.
- Faculty Fellow, *Volleyball Team*, 2014-present.
- Faculty Fellow, *Butler College*, 2011-present.

Teaching

- **Information Theory (ELE 528)** 2015
  Princeton University
- **Quantum Information Theory (ELE 538B)** 2014
  Princeton University
- **Information Theoretic Security (ELE 538)** 2013, 2016
  Princeton University
- **Information Signals (ELE 201)** 2013 - 2016
  Princeton University
- **Signals and Systems (ELE 301)** 2011
  Princeton University
- **Theory of Detection and Estimation (ELE 530)** 2010 - 2012, 2015
  Princeton University
- **Graduate Course in Statistical Signal Processing (EE 278)** Summer 2009
  Stanford University
  - Taught this course at department request during last term of Ph.D.
- **Teaching Assistant**
  Stanford University
  - Information Theory (Prof. Cover)
  - Signal Processing and Linear Systems I and II **(TA Award)** — taught five lectures.
  - Introduction to Electronics

Personal Details

Name: Paul W. Cuff
Email: cuff@princeton.edu
Address: B316 E-Quad
Princeton, NJ 08544, USA
Tel: +1 609-258-7946
Homepage: http://www.princeton.edu/∼cuff/

Interests and Adventures

- Four Children 2005 - 2012
- Minor League Football — Golden Coast Football League — Wide Receiver 2006 - 2008
- International Folk Dance Team — Brigham Young University 2003 - 2004
- Japanese — Two years as volunteer missionary in Japan 1999 - 2001
- Wrestling Intramural Champion 1999
- Jazz Band — Alto Saxophone 1994 - 1998
- Eagle Scout 1993 - 1998

Last updated: February 25, 2019