

Matthieu Bloch
Associate Professor
School of Electrical and Computer Engineering
CV Table of Contents

I	Earned Degrees	1
II	Employment	1
III	Teaching	1
IV	Scholarly accomplishments	2
V	Honors and awards	11

I EARNED DEGREES

- 2008 **Georgia Institute of Technology**, Atlanta, GA
Ph.D. in Electrical and Computer Engineering
Dissertation title: *Physical-Layer Security*
- 2006 **Université de Franche-Comté**, Besançon, France
Ph.D. in Engineering Sciences
Dissertation title: *Reconciliation Algorithm and Quantum Key Distribution Methods Adapted for the Frequency Domain*
- 2003 **Georgia Institute of Technology**, Atlanta, GA
M.S. in Electrical and Computer Engineering
- 2003 **Supélec**, Gif-sur-Yvette, France
Diplôme d'Ingénieur (Engineering Degree)

II EMPLOYMENT

- 2015-present **Georgia Institute of Technology**, Atlanta, GA
Associate Professor
- 2013-2015 **Georgia Institute of Technology**, Atlanta, GA
Assistant Professor
- 2009-2013 **Georgia Institute of Technology**, Georgia Tech Lorraine, Metz, France
Assistant Professor
- 2008-2009 **University of Notre Dame**, Notre Dame, IN
Postdoctoral Research Associate
- 2006-2008 **Georgia Institute of Technology**, Atlanta, GA
Graduate Research Assistant
- 2004-2005 **Georgia Institute of Technology**, Georgia Tech Lorraine, Metz, France
Graduate Research Assistant

III TEACHING

III.1 Post-doctoral fellows

- [1] Dr. Anne Savard (October 2015 - August 2016) now Maitre de Conférence at Télécom Lille, France
Wireless information-theoretic security
- [2] Dr. Laura Luzzi (October 2010 - September 2011) now Assistant Professor at ENSEA
Construction and analysis of strongly secure codes

III.2 Ph.D. students

- [1] Alex J. Pierrot (May 2010 - July 2015) now Senior Engineer at Qualcomm
Coding Techniques for Multi-User Physical-Layer Security
Preliminary exam Spring 2010 - **Proposal exam** May 2013 - **Ph.D. Defense** July 2015
- [2] Rémi A. Chou (January 2011 - July 2015) now Assistant Professor at Wichita State University
Information Theoretic Security under Computational, Bandwidth, and Uncertainty Constraints
Preliminary exam Spring 2010 - **Proposal exam** June 2014 - **Ph.D. Defense** July 2015

- [3] Keerthi Arumugam (August 2014 - December 2018) now Senior Engineer at Qualcomm
Multiuser covert communications
Preliminary exam Spring 2014 - **Proposal exam** Summer 2018 - **Ph.D. Defense** Spring 2019
- [4] Mehrdad Tahmasbi (Exp. Fall 2019, Spring 2016 - present)
Secure quantum communications
Preliminary exam Spring 2015 - **Proposal exam** Fall 2018
- [5] Ishaque Ashar Kadampot (Exp. Fall 2019, Spring 2015 - present)
Optimal codes for information-theoretically covert communications
Preliminary exam Spring 2015 - **Proposal exam** May 2019
- [6] Meng-Che Chang (Fall 2018 - present) *Uniformity and secrecy*
- [7] Nathan Blinn (Fall 2018 - present) *Machine Learning for Wireless Communications*

IV SCHOLARLY ACCOMPLISHMENTS

IV.1 Published books and parts of books

- [1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, October 2011.

IV.1.1 Refereed book chapters

- [1] M. R. Bloch, *Physical Layer Security in Wireless Communications*, ser. Wireless Networks and Mobile Communications. CRC Press, 2013, ch. Fundamentals of Physical-Layer Security, pp. 1–26.
- [2] J. Hou, G. Kramer, and M. Bloch, “Effective secrecy: Reliability, confusion and stealth,” in *Information Theoretic Security and Privacy of Information Systems*, H. Boche, A. Khisti, H. V. Poor, and R. Schaefer, Eds. Cambridge University Press, 2017, pp. 3–20.

IV.1.2 Other Parts of Books

IV.1.3 Edited volumes

IV.2 Refereed publications

IV.2.1 Published and accepted journal articles

- [1] S. Donnet, A. Thangaraj, M. Bloch, J. Cussey, J.-M. Merolla, and L. Larger, “Security of Y-00 under heterodyne measurement and fast correlation attack,” *Physics Letters A*, vol. 356, no. 6, pp. 406–410, August 2006.
- [2] M. Bloch, S. W. McLaughlin, F. Patois, and J.-M. Merolla, “Frequency-coded quantum key distribution,” *Optics Letters*, vol. 32, no. 3, pp. 301–303, February 2007.
- [3] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, “Quantum key distribution over 25 km with an all-fiber continuous-variable system,” *Physical Review A*, vol. 76, pp. 042 305/1–10, October 2007.
- [4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.
- [5] M. Bloch, R. Narasimha, and S. W. McLaughlin, “Network security for client-server architecture using wiretap codes,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 404–413, September 2008.
- [6] T. F. Wong, M. Bloch, and J. M. Shea, “Secret sharing over fast-fading MIMO wiretap channels,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 506 973/1–17, 2009.

- [7] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, “Wireless secrecy regions with friendly jamming,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.
- [8] A. Subramanian, A. Thangaraj, M. Bloch, and S. McLaughlin, “Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 585–594, September 2011.
- [9] A. J. Pierrot and M. R. Bloch, “Strongly secure communications over the two-way wiretap channel,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 595–605, September 2011.
- [10] F. Renna, M. R. Bloch, and N. Laurenti, “Semi-blind key-agreement over MIMO fading channels,” *IEEE Transactions on Communications*, vol. 61, no. 2, pp. 620–627, February 2013.
- [11] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, “Coding for secrecy: An overview of error-control coding techniques for physical-layer security,” *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41–50, September 2013.
- [12] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, “Cooperative security at the physical layer: A summary of recent advances,” *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, September 2013.
- [13] M. R. Bloch and J. N. Laneman, “Exploiting partial channel state information for secrecy over wireless channels,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1840–1849, September 2013.
- [14] M. R. Bloch and J. N. Laneman, “Strong secrecy from channel resolvability,” *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8077–8098, December 2013.
- [15] R. A. Chou and M. R. Bloch, “Separation of reliability and secrecy in rate-limited secret key-distillation,” *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4941–4957, August 2014.
- [16] N. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan, “Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser,” *Optics Express*, vol. 22, no. 6, pp. 6634–6646, March 2014.
- [17] V. Tan and M. Bloch, “Information spectrum approach to strong converse theorems for degraded wiretap channels,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1891–1904, September 2015.
- [18] R. A. Chou, M. R. Bloch, and E. Abbe, “Polar coding for secret-key generation,” *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6213–6237, November 2015.
- [19] M. R. Bloch, M. Hayashi, and A. Thangaraj, “Error-control coding for physical-layer secrecy,” *Proceedings of IEEE*, vol. 103, no. 10, pp. 1725–1746, October 2015.
- [20] M. R. Bloch, “Covert communication over noisy channels: A resolvability perspective,” *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.
- [21] R. A. Chou and M. R. Bloch, “Polar coding for the broadcast channel with confidential messages: A random binning analogy,” *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.
- [22] R. A. Chou, B. N. Vellambi, M. R. Bloch, and J. Kliewer, “Coding schemes for achieving strong secrecy at negligible cost,” *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1858–1873, Mar. 2017.
- [23] G. Frèche, M. Bloch, and M. Barret, “Polar codes for covert communications over asynchronous discrete memoryless channels,” *Entropy*, vol. 20, no. 1, p. 3, Dec. 2017.
- [24] B. N. Vellambi, J. Kliewer, and M. R. Bloch, “Strong coordination over multi-hop line networks using channel resolvability codebooks,” *IEEE Transactions on Information Theory*, vol. 64, no. 2, pp. 1132–1162, Feb. 2018.
- [25] R. A. Chou, M. R. Bloch, and J. Kliewer, “Empirical and strong coordination via soft covering with polar codes,” *IEEE Transactions on Information Theory*, vol. 64, no. 7, pp. 5087–5100, Jul. 2018.

- [26] B. Laroousse, S. Lasaulce, and M. Bloch, “Coordination in distributed networks via coded actions with application to power control,” *IEEE Transactions on Information Theory*, vol. 64, no. 5, pp. 3633–3654, May 2018.
- [27] M. Tahmasbi and M. R. Bloch, “First and second order asymptotics in covert communication,” *IEEE Transactions on Information Theory*, vol. 65, no. 4, pp. 2190–2212, Apr. 2019.
- [28] K. S. K. Arumugam and M. R. Bloch, “Embedding covert information in broadcast communications,” accepted to *IEEE Transactions on Information Forensics and Security*, Mar. 2019.
- [29] M. Tahmasbi and M. R. Bloch, “Framework for covert and secret key expansion over classical-quantum channels,” *Physical Review A*, vol. 99, p. 052329, May 2019.

IV.2.2 Conference presentation with proceedings (refereed)

- [1] J. Cussey, M. Bloch, A. Thangaraj, J.-M. Merolla, and S. W. McLaughlin, “Direct-modulation scheme for free-space quantum cryptography,” in *Proc. European Conference on Optical Communication*, Stockholm, Sweden, Sep. 2004.
- [2] J. Cussey, M. Bloch, A. Thangaraj, J.-M. Merolla, and S. W. McLaughlin, “Integrated direct-modulation based quantum cryptography system,” in *Proc. Optical Network and Technologies*, ser. IFIP International Federation for Information Processing. Pisa, Italy: IFIP, Oct. 2004, pp. 390–395.
- [3] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, “LDPC-based Gaussian key reconciliation,” in *Proc. IEEE Information Theory Workshop*, Punta del Este, Uruguay, March 2006, pp. 116–120, arXiv:cs.IT/0509041.
- [4] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, “LDPC-based secret key agreement over the Gaussian wiretap channel,” in *Proc. IEEE International Symposium on Information Theory*, Seattle, USA, July 2006, pp. 1179–1183.
- [5] S. Donnet, A. Thangaraj, M. Bloch, J. Cussey, J.-M. Merolla, and L. Larger, “Cryptanalysis of Y-00 under heterodyne measurement and fast correlation attack,” in *Proc. European Conference on Optical Communication*, Cannes, France, September 2006, pp. 1–2.
- [6] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “An opportunistic physical-layer approach to secure wireless communications,” in *Proc. 44th Allerton Conference on Communication Control and Computing*, Monticello, IL, September 2006, pp. 849–854.
- [7] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “LDPC-based secure wireless communication with imperfect knowledge of the eavesdropper’s channels,” in *Proc. IEEE Information Theory Workshop*, Chengdu, China, October 2006, pp. 155–159.
- [8] S. Kaimalettu, A. Thangaraj, M. Bloch, and S. W. McLaughlin, “Constellation shaping using LDPC codes,” in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 2366–2370.
- [9] M. Bloch, J. Barros, and S. W. McLaughlin, “Practical information-theoretic commitment,” in *Proc. 45th Allerton Conference on Communication Control and Computing*, Monticello, IL, September 2007, pp. 1035–1039.
- [10] M. Bloch, R. Narasimha, and S. W. McLaughlin, “Client-server architecture design based on wiretap codes,” in *Proc of the 2008 International Zurich Seminar on Communications*, Zurich, Switzerland, March 2008, pp. 44–47.
- [11] S. Fossier, J. Lodewyck, E. Diamanti, M. Bloch, T. Debuisschert, R. Tualle-Brouiri, and P. Grangier, “Quantum key distribution over 25 km using a fiber setup based on continuous variables,” in *Proc. of CLEO/QELS*, San Jose, CA, May 2008, pp. 1–2.
- [12] M. Bloch and A. Thangaraj, “Confidential messages to a cooperative relay,” in *Proc. of the IEEE Information Theory Workshop*, Porto, Portugal, May 2008, pp. 154–158.
- [13] M. Bloch and J. N. Laneman, “On the secrecy capacity of arbitrary wiretap channels,” in *Proceedings of 46th Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2008, pp. 818–825.

- [14] B. P. Dunn, M. Bloch, and J. N. Laneman, "Secure bits through queues," in *Proc. IEEE Information Theory Workshop on Networking and Information Theory*, Volos, Greece, June 2009, pp. 37–41.
- [15] M. Bloch, "Channel scrambling for secrecy," in *Proc. of IEEE International Symposium on Information Theory*, Seoul, Korea, July 2009, pp. 2452–2456.
- [16] E. MolavianJazi, M. Bloch, and J. N. Laneman, "Arbitrary jamming can preclude secure communications," in *Proc. 47th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2009, pp. 1069–1075.
- [17] M. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On Gaussian wiretap channels with arbitrary inputs," in *Proc. of European Wireless*, Lucca, Italy, April 2010, pp. 774–781.
- [18] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *Proc. of IEEE International Conference on Communications*, Cape Town, South Africa, May 2010, pp. 1550–3607.
- [19] M. Bloch, "Channel intrinsic randomness," in *Proc. of IEEE International Symposium on Information Theory*, Austin, TX, June 2010, pp. 2607–2611.
- [20] A. T. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, and S. McLaughlin, "Strong secrecy for erasure wiretap channels," in *Proc. IEEE Information Theory Workshop*, Dublin, Ireland, September 2010.
- [21] F. Renna, M. Bloch, and N. Laurenti, "Semi-blind key-agreement over MIMO quasi-static channels," in *Proc. of 2011 NEWCOM/COST Joint Workshop*, Paris, France, March 2011, pp. 1–6.
- [22] F. Renna, M. Bloch, and N. Laurenti, "Semi-blind key-agreement over MIMO fading channels," in *Proc. IEEE International Conference on Communications*, Kyoto, Japan, June 2011, pp. 1–6.
- [23] M. R. Bloch, "Achieving secrecy: capacity vs. resolvability," in *Proc. of IEEE International Symposium on Information Theory*, Saint Petersburg, Russia, August 2011, pp. 632–636.
- [24] R. A. Chou and M. R. Bloch, "One-way rate-limited sequential key-distillation," in *Proc. IEEE International Symp. Information Theory*, Cambridge, MA, July 2012, pp. 1777–1781.
- [25] M. R. Bloch and J. Kliewer, "On secure communication with constrained randomization," in *Proc. IEEE International Symp. Information Theory*, Cambridge, MA, July 2012, pp. 1172–1176.
- [26] A. J. Pierrot and M. R. Bloch, "LDPC-based coded cooperative jamming codes," in *Proc. of IEEE Information Theory Workshop*, Lausanne, Switzerland, September 2012, pp. 462–466.
- [27] M. R. Bloch, L. Luzzi, and J. Kliewer, "Strong coordination with polar codes," in *Proc. of 50th Allerton Conference on Communication, Control, and Computing*, Monticello, IL, October 2012, pp. 565–571.
- [28] F. Renna, N. Laurenti, S. Tomasin, M. Baldi, N. Maturo, M. Bianchi, F. Chiaraluce, and M. Bloch, "Low-power secret key agreement over OFDM," in *Proc. of the 2nd ACM workshop on Hot topics on wireless network security and privacy*, Budapest, Hungary, April 2013, pp. 43–48.
- [29] C. Ling, L. Luzzi, and M. R. Bloch, "Secret key generation from gaussian sources using lattice hashing," in *Proc. IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013, pp. 2621–2625.
- [30] R. A. Chou and M. R. Bloch, "Data compression with nearly uniform output," in *Proc. IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013, pp. 1979–1983.
- [31] M. R. Bloch and J. Kliewer, "Strong coordination over a line network," in *Proc. IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013, pp. 2319–2323.
- [32] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "Experimental aspects of secret-key generation in indoor wireless environments," in *Proc. of Signal IEEE 4th Workshop on Signal Processing Advances in Wireless Communications*, April 2013.

- [33] R. A. Chou, M. R. Bloch, and E. Abbe, “Polar coding for secret-key generation,” in *Proc. of Information Theory Workshop*, Sevilla, Spain, April 2013, pp. 1–5.
- [34] A. J. Pierrot and M. R. Bloch, “Joint channel intrinsic randomness and channel resolvability,” in *Proc. of Information Theory Workshop*, Sevilla, Spain, April 2013, pp. 1–5.
- [35] R. A. Chou and M. R. Bloch, “Secret-key generation with arbitrarily varying eavesdropper’s channel,” in *Proc. of Global Conference on Signal and Information Processing*, Austin, TX, September 2013, pp. 277–280.
- [36] J. J. Boutros, V. Dedeoglu, and M. R. Bloch, “The anti-diversity concept for secure communication on a two-link compound channel,” in *Proc. of International Zurich Seminar on Communications*, Zurich, Switzerland, February 2014.
- [37] N. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. Citrin, and W. Pan, “Ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser,” in *Proc. of CLEO*, San Jose, CA, June 2014, pp. 1–2.
- [38] R. A. Chou, M. R. Bloch, and J. Kliewer, “Low-complexity channel resolvability codes for the symmetric multiple-access channel,” in *Proc. of IEEE Information Theory Workshop*, Hobart, Tasmania, November 2014, pp. 466–470.
- [39] M. R. Bloch and J. Kliewer, “Strong coordination over a three-terminal relay network,” in *Proc. of IEEE Information Theory Workshop*, Hobart, Tasmania, November 2014, pp. 646–650.
- [40] V. Y. F. Tan and M. R. Bloch, “Information spectrum approach to strong converse theorems for degraded wiretap channels,” in *Proc. of 52nd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2014, pp. 747–754.
- [41] R. A. Chou and M. R. Bloch, “Polar coding for the broadcast channel with confidential messages,” in *Proc. IEEE Information Theory Workshop*, Jerusalem, Israel, April 2015, pp. 1–5.
- [42] M. R. Bloch, “A channel resolvability perspective on stealth communications,” in *Proc. of IEEE International Symposium on Information Theory*, Hong Kong, June 2015, pp. 2535–2539.
- [43] R. A. Chou, M. R. Bloch, and J. Kliewer, “Polar coding for empirical and strong coordination via distribution approximation,” in *Proc. of IEEE International Symposium on Information Theory*, Hong Kong, June 2015, pp. 1512–1516.
- [44] B. N. Vellambi, M. R. Bloch, R. A. Chou, and J. Kliewer, “Lossless and lossy source compression with near-uniform outputs: Is common randomness always required?” in *Proc. of IEEE International Symposium on Information Theory*, Hong Kong, June 2015, pp. 2171–2175.
- [45] B. N. Vellambi, J. Kliewer, and M. Bloch, “Strong coordination over multi-hop line networks,” in *Proc. of IEEE Information Theory Workshop*, Jeju, Korea, Jul. 2015, pp. 192–196.
- [46] R. A. Chou and M. R. Bloch, “Using deterministic decisions for low-entropy bits in the encoding and decoding of polar codes,” in *Proc. of 53rd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2015, pp. 1380–1385.
- [47] B. N. Vellambi, J. Kliewer, and M. R. Bloch, “Strong coordination over a line when actions are markovian,” in *Proc. of Annual Conference on Information Science and Systems*, Princeton, NJ, Mar. 2016, pp. 412–417.
- [48] M. Tahmasbi and M. R. Bloch, “Second-order asymptotics of covert communications over noisy channels,” in *Proc. of IEEE International Symposium on Information Theory*, Barcelona, Spain, July 2016, pp. 2224–2228.
- [49] K. S. K. Arumugam and M. R. Bloch, “Keyless covert communication over multiple-access channels,” in *Proc. of IEEE International Symposium on Information Theory*, Barcelona, Spain, Jul. 2016, pp. 2229–2233.
- [50] B. N. Vellambi, J. Kliewer, and M. R. Bloch, “Lossy compression with near-uniform encoder outputs,” in *Proc. of IEEE International Symposium on Information Theory*, Barcelona, Spain, Jul. 2016, pp. 530–534.

- [51] M. Le Treust and M. R. Bloch, “Empirical coordination, state masking and state amplification: Core of the decoder’s knowledge,” in *Proc. of IEEE International Symposium on Information Theory*, Barcelona, Spain, July 2016, pp. 895–899.
- [52] K. S. K. Arumugam and M. R. Bloch, “Keyless asynchronous covert communication,” in *Proc. of IEEE Information Theory Workshop*, Cambridge, United Kingdom, Sep. 2016, pp. 191–195.
- [53] G. Cervia, L. Luzzi, M. R. Bloch, and M. L. Treust, “Polar coding for empirical coordination of signals and actions over noisy channels,” in *Proc. of IEEE Information Theory Workshop*, Cambridge, United Kingdom, September 2016, pp. 81–85.
- [54] M. Tahmasbi and M. R. Bloch, “Second order asymptotics for degraded wiretap channels: How good are existing codes?” in *54th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sept 2016, pp. 830–837.
- [55] R. A. Chou, M. R. Bloch, and A. Yener, “Universal covertness for discrete memoryless sources,” in *54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, August 2016, pp. 516–523.
- [56] M. R. Bloch and S. Guha, “Optimal covert communications using pulse-position modulation,” in *Proc. of IEEE International Symposium on Information Theory*, Aachen, Germany, Jun. 2017, pp. 2835–2839.
- [57] M. Tahmasbi, M. R. Bloch, and A. Yener, “Learning adversary’s actions for secret communication,” in *Proc. of IEEE International Symposium on Information Theory*, Aachen, Germany, Jun. 2017, pp. 2713–2717.
- [58] I. A. Kadampot and M. R. Bloch, “Coordination with clustered common randomness in a three-terminal line network,” in *Proc. of IEEE International Symposium on Information Theory*, Aachen, Germany, Jun. 2017, pp. 1828–1832.
- [59] G. Cervia, L. Luzzi, M. L. Treust, and M. R. Bloch, “Strong coordination of signals and actions over noisy channels,” in *Proc. of IEEE International Symposium on Information Theory*, Aachen, Germany, Jun. 2017, pp. 2845–2849.
- [60] M. Tahmasbi, M. R. Bloch, and V. F. Tan, “Error exponents covert communications,” in *Proc. of IEEE Information Theory Workshop*, Kaohsiung, Taiwan, Nov. 2017, pp. 304–308.
- [61] K. S. K. Arumugam and M. R. Bloch, “Covert communication over broadcast channels,” in *Proc. of IEEE Information Theory Workshop*, Kaohsiung, Taiwan, Nov. 2017, pp. 299–303.
- [62] H. Zivari-Fard, M. Bloch, and A. Nosratinia, “Two-transmitter two-receiver channel with confidential messages,” in *Proc. of Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sep. 2017.
- [63] M. Tahmasbi and M. R. Bloch, “Covert secret key generation,” in *Proc. of IEEE Conference on Communications and Network Security, Workshop on Physical-Layer Methods for Wireless Security*, Las Vegas, NV, Oct. 2017, pp. 540–544.
- [64] I. A. Kadampot, M. Tahmasbi, and M. R. Bloch, “Multilevel-coded pulse position modulation for covert communications,” in *Proc. of IEEE International Symposium on Information Theory*, Vail, CO, Jun. 2018, pp. 1864–1868.
- [65] K. Arumugam, M. R. Bloch, and L. Wang, “Covert communication over a physically degraded relay channel with non-colluding wardens,” in *Proc. of IEEE International Symposium on Information Theory*, Vail, CO, Jun. 2018, pp. 766–770.
- [66] N. Helhal, M. R. Bloch, and A. Nosratinia, “Multiple-access channel resolvability with cribbing,” in *Proc. IEEE International Symposium on Information Theory*, Vail, CO, Jun. 2018, pp. 2052–2056.
- [67] G. Cervia, L. Luzzi, M. Le Treust, and M. R. Bloch, “Strong coordination over noisy channels with strictly causal encoding,” in *Proc. of 56th Annual Allerton Conference on Communication, Control, and Computing*, Oct. 2018, pp. 519–526.

- [68] W. K. Harrison and M. R. Bloch, “On dual relationships of secrecy codes,” in *Proc. of 56th Annual Allerton Conference on Communication, Control, and Computing*, Oct. 2018, pp. 366–372.
- [69] Q. Zhang, M. Bloch, M. Bakshi, and S. Jaggi, “Undetectable radios: Covert communication under spectral mask constraints,” accepted to *IEEE International Symposium on Information Theory*, Mar. 2019.
- [70] M. Tahmasbi and M. Bloch, “Steganography protocols for quantum channels,” accepted to *IEEE International Symposium on Information Theory*, Mar. 2019.
- [71] M. Tahmasbi, M. Bloch, and A. Yener, “In-band sensing of the adversary’s channel for secure communication in wireless channels,” accepted to *IEEE International Symposium on Information Theory*, Mar. 2019.
- [72] W. Harrison and M. R. Bloch, “Attributes of generator matrices for best finite blocklength wiretap codes,” accepted to *IEEE International Symposium on Information Theory*, Mar. 2019.
- [73] I. A. Kadampot, M. Tahmasbi, and M. R. Bloch, “Codes for covert communication over additive white gaussian noise channels,” accepted to *IEEE International Symposium on Information Theory*, Mar. 2019.

IV.2.3 Submitted journal articles

- [1] K. S. K. Arumugam and M. R. Bloch, “Covert communication over a k-user multiple access channel,” submitted to *IEEE Transactions on Information Theory*, Mar. 2018.
- [2] G. Cervia, L. Luzzi, M. Le Treust, and M. Bloch, “Strong coordination of signals and actions over noisy channels with two-sided state information,” submitted to *IEEE Transactions on Information Theory*, Mar. 2018.
- [3] M. Tahmasbi, M. R. Bloch, and A. Yener, “Learning an adversary’s actions for secret communication,” submitted to *IEEE Transactions on Information Theory*, Jul. 2018.
- [4] R. Chou, M. Bloch, and A. Yener, “Universal covertness for discrete memoryless sources,” submitted to *IEEE Transactions on Information Theory*, Jul. 2018.
- [5] M. Tahmasbi, A. Savard, and M. R. Bloch, “Covert capacity of non-coherent rayleigh-fading channels,” submitted to *IEEE Transactions on Information Theory*, Oct. 2018.
- [6] I. A. Kadampot, M. Tahmasbi, and M. R. Bloch, “Multilevel-coded pulse-position modulation for covert communications over binary-input discrete memoryless channels,” submitted to *IEEE Transactions on Information Theory*, Nov. 2018.
- [7] N. Helhal, M. Bloch, and A. Nosratinia, “Cooperative resolvability and secrecy in the cribbing multiple-access channel,” submitted for *IEEE Transactions on Information Theory*, Nov. 2018.
- [8] H. Zivari-Fard, M. Bloch, and A. Nosratinia, “Secrecy rates for a channel with two senders and two receivers,” submitted to *IEEE Transactions on Information Theory*, Dec. 2018.
- [9] M. Le Treust and M. R. Bloch, “State leakage and coordination of actions: Core of the receiver’s knowledge,” submitted to *IEEE Transactions on Information Theory*, Dec. 2018.
- [10] M. Tahmasbi and M. R. Bloch, “Covert secret key generation with an active warden,” submitted to *IEEE Transactions on Information Forensics and Security*, Jan. 2019.
- [11] M. Tahmasbi and M. R. Bloch, “Covert and secret key expansion over quantum channels under collective attacks,” submitted to *IEEE Transactions on Information Theory*, Jan. 2019.
- [12] E. Shipilova, M. Barret, M. Bloch, J.-L. Boelle, and J.-L. Collette, “Simultaneous seismic sources separation based on matrioshka orthogonal matching pursuit, application in oil and gas exploration,” submitted to *IEEE Transactions on Geoscience and Remote Sensing*, Feb. 2019.

IV.3 Presentations

IV.3.1 Invited talks

- [1] M. R. Bloch, “Covert communications over noisy channels: partial first and second-order asymptotics,” Invited talk at Beyond i.i.d. workshop, July 2016.
- [2] M. R. Bloch, “Secure and covert communications over noisy channels,” Invited talk at the Nexus of Information and Computation Theories - Secrecy and Privacy Theme, Paris, France, March 2016.
- [3] R. A. Chou, M. R. Bloch, and J. Kliewer, “Wiretap codes from channel resolvability codes,” invited talk at the *Conference on Information Science and Systems*, Princeton, NJ, March 2014.

IV.3.2 Keynote presentations

- [1] M. R. Bloch, “Covert communications over noisy channels,” Keynote at the 3rd Workshop on Physical-Layer Methods for Wireless Security, October 2016.
- [2] M. R. Bloch, “Towards a unified information theoretic approach to physical-layer security,” Keynote at the ICC’16 workshop on wireless physical layer security, May 2016.
- [3] M. R. Bloch, “What can physical-layer security do for you ?” Keynote at the Globecom 2013 Workshop on Trusted Communications with Physical-Layer Security, December 2013.
- [4] M. Bloch, “Mechanisms of physical-layer security,” Plenary talk at the 1st International ICST Workshop on Secure Wireless Networks, May 2011.

IV.3.3 Conference presentations with non-refereed proceedings

- [1] J. Lodewyck, M. Bloch, S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, “Distribution quantique de clé a 25 km au moyen d’un dispositif fibré utilisant des variables continues,” in *10eme Colloque sur les Lasers et l’Optique Quantique*, Grenoble, France, July 2007.
- [2] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, “Quantum key distribution device with coherent states,” in *Proc. of SPIE Optics East*, vol. 6780, Boston, MA, USA, September 2007, pp. 67 800Z/1–14, (invited).
- [3] J. Barros and M. Bloch, “Strong secrecy for wireless channels,” in *Information Theoretic Security*, ser. Lecture Notes in Computer Science. Calgary, Canada: Springer Berlin / Heidelberg, August 2008, pp. 40–53, (invited).
- [4] M. Bloch and J. N. Laneman, “Information-spectrum methods for information-theoretic security,” in *Proc. Information Theory and Applications Workshop*, San Diego, CA, February 2009, pp. 23–28, (invited).
- [5] A. Subramanian, A. T. Suresh, A. Thangaraj, M. Bloch, and S. McLaughlin, “Strong and weak secrecy in wiretap channels,” in *Proc. of 6th International Symposium on Turbo Codes and Iterative Information Processing*, Brest, France, September 2010, pp. 30 – 34, (invited).
- [6] L. Luzzi and M. R. Bloch, “Capacity-based random codes cannot achieve strong secrecy over symmetric wiretap channels,” in *Proc. of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools*, Cachan, France, May 2011, pp. 641–647, (invited). [Online]. Available: <http://dl.acm.org/citation.cfm?id=2151688.2151767>
- [7] R. A. Chou and M. R. Bloch, “Uniform distributed source coding for the multiple access wiretap channel,” in *Proc. of IEEE Conference on Communications and Network Security*, San Francisco, CA, October 2014, pp. 127–132.
- [8] G. Frèche, M. R. Bloch, and M. Barret, “Polar codes for covert communications over asynchronous discrete memoryless channels,” in *Proc. of 51st Annual Conference on Information Sciences and Systems*, Baltimore, MD, Mar. 2017, pp. 1–1.

IV.3.4 Conference presentations without proceedings

- [1] M. Bloch, J.-M. Merolla, S. W. McLaughlin, and J.-P. Goedgebuer, “Long distance continuous variable transmission system using sideband detection method,” in *First Russian-French Laser Physics Workshop for Young Scientists (RFLPW-YS)*, St. Petersburg, Russia, July 2004.
- [2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Information theoretic security for wireless channels - theory and practice,” in *Proc. 2007 Information Theory and Application Workshop*, San Diego, CA, USA, February 2007, (invited).
- [3] E. Diamanti, S. Fossier, J. Lodewyck, M. Bloch, R. Garcia-Patron, E. Karpov, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, “Implementation of an all-fiber continuous variables quantum key distribution system,” in *International Conference on Quantum Information Processing and Communication*, Barcelona, Spain, October 2007.
- [4] M. Bloch, “Channel intrinsic randomness,” talk given at *Information Theory and Applications Workshop*, February 2010, (invited).
- [5] A. J. Pierrot and M. R. Bloch, “Key generation over the Gaussian two-way wiretap channel,” talk given at *Information Theory and Applications Workshop*, February 2011, (invited).
- [6] A. J. Pierrot and M. R. Bloch, “Polar codes for secure communications over the two-way wiretap channel,” invited talk at *IEEE Information Theory Workshop*, September 2012.
- [7] A. J. Pierrot and M. R. Bloch, “Exponents of channel intrinsic randomness,” talk given at *Information Theory and Applications Workshop*, February 2013.
- [8] M. R. Bloch and J. Kliewer, “Coordination over a line network,” talk given at *Information Theory and Applications Workshop*, February 2013.
- [9] N. Li, B. Kim, V. N. Chizhevsky, A. Locquet, M. Bloch, D. S. Citrin, and W. Pan, “Chaotic semiconductor lasers for ultrafast random bit generation,” talk given at *DynamicDays US*, January 2014.
- [10] A. J. Pierrot, R. A. Chou, and M. R. Bloch, “Practical limitations of secret key generation in real wireless environments,” talk given at *Information Theory and Applications Workshop*, February 2014.
- [11] M. R. Bloch and J. Kliewer, “Coordination over broadcast and multiple-access networks,” talk given at *Information Theory and Applications Workshop*, February 2014.
- [12] M. Tahmasbi and M. Bloch, “Covert key generation over a classical-quantum channel,” talk given at *Information Theory and Applications Workshop*, Feb. 2018.
- [13] M. Tahmasbi and M. Bloch, “A framework for covert secret key generation over quantum channels,” talk given at *Information Theory and Applications Workshop*, Feb. 2019.
- [14] H. ZivariFard, M. Bloch, and A. Nosratinia, “Multicasting with confidential messages: From weak to strong secrecy,” talk given at *Information Theory and Applications Workshop*, Feb. 2019.

IV.3.5 Seminar presentations

- [1] M. Bloch, “Physical-Layer Security,” six-hour invited tutorial given at Newcom++ Emerging Technology Workshop, September 2009, Padova, Italy.
- [2] M. Bloch, “Physical-Layer Security,” eight-hour invited course at Indian Institute of Science Bangalore, May 2010, Bangalore, India.
- [3] M. Bloch, “Harnessing randomness in information theory,” twelve-hour invited course at University of Padova, February 2011.
- [4] M. Bloch, “Physical-layer security,” twelve-hour invited course at Korean Advanced Institute for Science and Technology, June 2011, Daejeon, South Korea.

- [5] M. Bloch, “Physical-layer security,” Six-hour invited course at the Digicosme Spring School, May 2014, Supélec, Gif-sur-Yvette France.

V HONORS AND AWARDS

- [1] IEEE Communications Society and IEEE Information Theory Society Joint Paper Award (2011) for the paper authored with João Barros, Miguel Rodrigues and Steven McLaughlin entitled “Wireless Information-Theoretic Security,” published in the *IEEE Transactions on Information Theory*
- [2] Class of 1934 Course Survey Teaching Effectiveness Award (2012) from the Center for the Enhancement of Teaching and Learning (Georgia Tech)
- [3] Class of 1969 Teaching Fellow (2012) from the Center for the Enhancement of Teaching and Learning (Georgia Tech)
- [4] Hesburgh Award Teaching Fellows (2017) from the Center for the Enhancement of Teaching and Learning (Georgia Tech)
- [5] Richard M. Bass/Eta Kappa Nu Outstanding Teacher Award (2018) (Georgia Tech, ECE)
- [6] ECE Outstanding Junior Faculty Member Award (2019) (Georgia Tech, ECE)