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

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 Assis tant
2004-2005	**Georgia Institute of Technology - Lorraine**, Metz, France Graduate Research Assistant

III. Scholarly Accomplishments

(Boldfaced name indicates students advised by Matthieu Bloch).

III.A. Published Books and Parts of Books

III.A.1. Books

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

III.A.2. Refereed Book Chapters

No data available.

III.A.3. Other Parts of Books

[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.

III.A.4. Edited Volumes

No data available.

III.B. Refereed Publications

III.B.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, June 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**, M. R. Bloch, and J. Kliewer, "Coding schemes for achieving strong secrecy at negligible cost," accepted to *IEEE Transactions on Information Theory*, October 2016.

III.B.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, September 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, October 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-Brouri, 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*, Budaptest, 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 ouput," 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, July 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*, 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*, March 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*, 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*, July 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*, July 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*, 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, September 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?" accepted to *Allerton 2016*, August 2016.

[55] **R. A. Chou**, M. R. Bloch, and A. Yener, "Universal covertness for discrete memoryless sources," accepted to *Allerton 2016*, August 2016.

III.B.3. Other Refereed Material

No data available.

III.B.4. Submitted Journal Articles

[1] B. Larrousse, S. Lasaulce, and M. Bloch, "Coordination in distributed networks via coded actions with application to power control," submitted to *IEEE Transactions on Information Theory*, October 2014.

[2] B. N. Vellambi, J. Kliewer, and M. R. Bloch, "Strong coordination over multi-hop line networks," submitted to *IEEE Transactions on Information Theory*, April 2016.

[3] S. Salimi, M. Bloch, F. Gabry, M. Skoglund, and P. Papadimitratos, "Strong secrecy in pairwise key agreement over a generalized multiple access channel," submitted to *IEEE Transactions on Information Theory*, March 2016.

[4] **R. A. Chou**, M. R. Bloch, and J. Kliewer, "Empirical and strong coordination via soft covering with polar codes," submitted to *IEEE Transactions on Information Theory*, 2016.

III.C. Other Publications

III.B.5. Submitted Conference Proceedings Papers No data available.

No data available.

III.D. Presentations

III.D.1 Invited talks

[1] **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.

[2] **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.

[3] M. R. Bloch, "Covert communications over noisy channels: partial first and second-order asymptotics," Invited talk at Beyond i.i.d. workshop, July 2016.

III.D.2 Keynote Presentations

[1] M. Bloch, "Mechanisms of physical-layer security," Plenary talk at the 1st International ICST Workshop on Secure Wireless Networks, May 2011.

[2] 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.

[3] 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.

[4] M. R. Bloch, "Covert communications over noisy channels," Keynote at the 3rd Workshop on Physical-Layer Methods for Wireless Security, October 2016.

III.D.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

III.D.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.

III.D.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.

III.E. Other Scholarly Accomplishments

[1] M. Bloch and J.-M. Merolla, "System and method for the secure transmission of binary code by phase and intensity modulation," US Patent 8,472,626, June, 2013, filed in September 2007.

[2] M. Bloch, J. Barros, M. Rodrigues, and S. W. McLaughlin, "Systems and methods for providing opportunistic security for physical communication channels," US Patent 8,213,616, July, 2012, filed in September 2007.

V. Service

Editorial work

Lead Guest Editor for Special Issue of *Journal of Communications and Networks* on Physical Layer Security (2012)
Associate Editor for Shannon Theory of *IEEE Transactions on Information Theory* (2016-present, 11 papers)
Editor for *ELSEVIER Physical Communication* (2012-2015, 4 papers)

Journal referee

IEEE Transactions on Information Theory (2007-present, 29 papers)
IEEE Transactions on Wireless Communications (2010-present, 19 papers)
IEEE Transactions on Communications (2010-present, 17 papers)
IEEE Communications Letters (2007-present, 16 papers)
IEEE Transactions on Info. Forensics and Security (2009-present, 14 papers)
IEEE Transactions on Signal Processing (2009-present, 7 papers)
IEEE Journal of Selected Areas in Communications (2012-present, 6 papers)
IEEE Wireless Communications Letters (2014-present, 7 papers)
IEEE Transactions on Vehicular Technology (2009-present, 5 papers)
IEEE Signal Processing Letters (2009-present, 5 papers)
IEEE Communications Magazine 2014, 4 papers)
Proceedings of IEEE (2015-present, 4 papers)
IEEE Journal of Selected Topics in Quantum Electronics (2009, 1 paper)
ELSEVIER Optics Communications (2009-present, 2 papers)
IEICE Fundamentals of Communications (2016-present, 2 papers)
ELSEVIER PHYCOM: Physical Communication (2008, 1 paper)
EURASIP Journal on Wireless Comm. and Networking (2009, 1 paper)
European Transactions on Communications (2011, 1 paper)
Springer Journal of Computer Science and Technology (2012, 1 paper)
International Journal for Ligt and Electron Optics (2016, 1 paper)
International Journal of Information and Coding Theory (2014, 1 paper)

Conference referee

IEEE International Symposium on Information Theory (ISIT)
IEEE Information Theory Workshop (ITW)
IEEE International Conference on Communications (ICC)
IEEE International Conference on Circuits and Systems for Comm. (ICCSC)
IEEE Wireless Communications and Networking Conference (WCNC)
IEEE Global Communications (GLOBECOM)
IEEE International Workshop on Information Forensics and Security (WIFS)
IEEE Workshop on Signal Processing and Wireless Communications (SPAWC)
Eurocrypt

Conference committee

Publicity chair 2008 Information Theory Workshop, Porto, Portugal
Web chair 2009 School of Information Theory, Northwestern, IL, USA
Web chair 2010 School for Information Theory, USC, CA, USA
Web chair 2011 School for Information Theory, UT Austin, TX, USA
Co-Chair ICC 2011 Workshop on Physical-Layer Security
Technical Program Committee 2011 IEEE Information Theory Workshop
Technical Program Committee 2012 IEEE International Conf. on Comm.
Finance Chair 2013 Communication Theory Workshop
Workshop Chair 2013 Globecom
Technical Program Committee 2013 IEEE Information Theory Workshop
Technical Program Committee 2013 IEEE GlobalSIP Conference
Technical Program Committee 2013 International Conference on Information Theoretic Security
Technical Program Committee 2014 IEEE Int. Symp. on Info. Theory
Technical Program Committee 2014 IEEE Information Theory Workshop
Technical Program Committee 2014 Workshop on Trusted Communications with Physical Layer Security, at Globecom 2014
Technical Program Committee 2014 Workshop on Physical-layer Methods for Wireless Security, at IEEE CNS
Technical Program Committee 2015 IEEE Int. Symp. on Info. Theory
Technical Program Committee 2016 IEEE Int. Symp. on Info. Theory
Technical Program Committee 2016 IEEE Information Theory Workshop
Technical Program Committee WCNC'2016 Workshop on Physical-Layer Security
Technical Program Committee 2017 IEEE Int. Symp. on Info. Theory
Technical Program Committee 2017 IEEE International Conf. on Comm.

Professional societies

Chair Online Committee IEEE Information Theory Society (2011-2015)

Board of Governors IEEE Information Theory Society (2016-2018)

Others

Reviewer and Panelist for National Science Foundation (NSF)
Reviewer for Air Force Office of Scientific Research
Reviewer for Army Research Office
Reviewer for French National Research Agency (ANR)
Reviewer for Belgium Fund for Scientific Research (FNRS)
Reviewer for Natural Sciences and Engineering Research Council of Canada
Reviewer for Fonds de recherche du Québec – Nature et technologies
Reviewer for Research Grant Council of Hong Kong
Reviewer for Israel Science Foundation (ISF)

- *IEEE Communications Society and IEEE Information Theory Society 2011 Joint Paper Award*, for the paper authored with João Barros, Miguel Rodrigues and Steven McLaughlin entitled "Wireless Information-Theoretic Security," published in *IEEE Transactions on Information Theory*.
- *2012 Class of 1934 Course Survey Teaching Effectiveness Award* from the Center for the Enhancement of Teaching and Learning.
- *2012 Class of 1969 Teaching Fellow* from the Center for the Enhancement of Teaching and Learning