References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, April 1949.

[2] R. G. Gallager, *Information Theory and Reliable Communication*. Wiley, 1968.

[3] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd edn. Wiley-Interscience, 2006.

[4] R. W. Yeung, *A First Course in Information Theory*. Springer, 2002.

[5] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Akadémiai Kiadó, 1981.

[6] G. Kramer, *Topics in Multi-User Information Theory*. NOW Publishers, 2008.

[7] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, nos. 7/10, pp. 379–423/623–656, July/October 1948.

[8] G. Kramer, "Capacity results for the discrete memoryless networks," *IEEE Transactions on Information Theory*, vol. 49, no. 1, pp. 4–21, January 2003.

[9] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

[10] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[11] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 1–10, January 1976.

[12] R. Ahlswede, "Multi-way communication channels," in *Proc. International Symposium on Information Theory*, Thakadsor, Armenian SSR, USSR, September 1971, pp. 23–52.

[13] H. Liao, "Multiple access channels," Ph.D. dissertation, University of Hawaii, 1972.

[14] T. M. Cover, "Broadcast channels," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 2–14, January 1972.

[15] P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Transactions on Information Theory*, vol. 19, no. 2, pp. 197–207, March 1973.

[16] R. G. Gallager, "Capacity and coding for degraded broadcast channels," *Problemy Peredachi Informatsii*, vol. 10, no. 3, pp. 3–14, 1974.

[17] T. M. Cover, "Comments on broadcast channels," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2524–2530, October 1998.

[18] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[19] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Transactions of the American Institute of Electrical Engineers*, vol. 45, no. 1, pp. 295–301, January 1926.

[20] G. D. Forney, Jr., "On the role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian channels: Shannon meets Wiener," in *Proc. 41st Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, October 2003, pp. 430–439.

[21] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.

[22] S. Leung-Yan-Cheong, "On a special class of wiretap channels," *IEEE Transactions on Information Theory*, vol. 23, no. 5, pp. 625–627, September 1977.

[23] J. L. Massey, "A simplified treatment of Wyner's wire-tap channels," in *Proc. 21st Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, October 1983, pp. 268–276.

[24] I. Csiszár, "Almost independence and secrecy capacity," *Problemy Peredachi Informatsii*, vol. 32, no. 1, pp. 40–47, January–March 1996.

[25] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channels," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1562–1575, April 2006.

[26] M. Bloch and J. N. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *Proc. 46th Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, September 2008, pp. 818–825.

[27] 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.

[28] J. Körner and K. Marton, "Comparison of two noisy channels," in *Proc. Topics in Information Theory*, Keszthely, Hungary, 1977, pp. 411–423.

[29] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 43, no. 2, pp. 712–714, March 1997.

[30] C. Nair, "Capacity regions of two new classes of 2-receiver broadcast channels," in *Proc. IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009, pp. 1839–1843.

[31] H. Yamamoto, "Rate-distortion theory for the Shannon cipher systems," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[32] S. K. Leung-Yan-Cheong, "Multi-user and wiretap channels including feedback," Ph.D. dissertation, Stanford University, 1976.

[33] R. Ahlswede and N. Cai, "Transmission, identification and common randomness capacities for wire-tap channels with secure feedback from the decoder," in *General Theory of Information Transfer and Combinatorics*. Springer-Verlag, 2006, pp. 258–275.

[34] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353–5361, December 2009.

[35] M. Feder and N. Merhav, "Relations between entropy and error probability," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 259–266, January 1994.

[36] K. Yasui, T. Suko, and T. Matsushima, "An algorithm for computing the secrecy capacity of broadcast channels with confidential messages," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, July 2007, pp. 936–940.

[37] K. R. Gowtham and A. Thangaraj, "Computation of secrecy capacity for more-capable channel pairs," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 529–533.

[38] G. Van Assche, *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2006.
[39] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
[40] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, January 2002.
[41] U. Maurer, R. Renner, and S. Wolf, "Unbreakable keys from random noise," in *Security with Noisy Data*, P. Tuyls, B. Skoric, and T. Kevenaar, Eds. Springer-Verlag, 2007, pp. 21–44.
[42] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[43] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.
[44] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals – part I," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3973–3996, August 2010.
[45] A. A. Gohari and V. Anatharam, "Information-theoretic key agreement of multiple terminals – part II: Channel models," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3997–4010, August 2010.
[46] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and intrinsic conditional information," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 499–514, March 1999.
[47] R. Renner and S. Wolf, "New bounds in secret-key agreement: The gap between formation and secrecy extraction," in *Proc. EUROCRYPT*, 2003, pp. 652–577.
[48] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, March 2000.
[49] A. Khisti, S. N. Diggavi, and G. Wornell, "Secret-key generation with correlated sources and noisy channels," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 1005–1009.
[50] V. Prabhakaran and K. Ramchandran, "A separation result for secure communication," in *Proc. 45th Allerton Conference on Communications, Control and Computing*, Monticello, IL, USA, September 2007, pp. 34–41.
[51] S. Watanabe and Y. Oohama, "Secret key agreement from vector Gaussian sources by rate limited public communications," in *Proc. IEEE International Symposium on Information Theory*, Austin, TX, USA, June 2010, pp. 2597–2601; see also arXiv:1001.3705v1.
[52] M. J. Gander and U. M. Maurer, "On the secret-key rate of binary random variables," in *Proc. IEEE International Symposium on Information Theory*, Trondheim, Norway, June 1994, p. 351.
[53] S. Liu, H. C. A. Van Tilborg, and M. Van Dijk, "A practical protocol for advantage distillation and information reconciliation," *Designs, Codes and Cryptography*, vol. 30, no. 1, pp. 39–62, August 2003.
[54] M. Naito, S. Watanabe, R. Matsumoto, and T. Uyematsu, "Secret key agreement by reliability information of signals in Gaussian Maurer's models," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 727–731.
[55] J. Muramatsu, K. Yoshimura, and P. Davis, "Secret key capacity and advantage distillation capacity," in *Proc. IEEE International Symposium on Information Theory*, Seattle, WA, USA, July 2006, pp. 2598–2602.

[56] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. Advances in Cryptology – Eurocrypt*, T. Helleseth, Ed. Springer-Verlag, May 1993, pp. 411–423.

[57] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Physical Review A*, vol. 67, no. 5, pp. 052 303/1–8, May 2003.

[58] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009, pp. 1879–1883.

[59] G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed Gaussian key," *IEEE Transactions on Information Theory*, vol. 50, no. 2, pp. 394–400, February 2004.

[60] K.-C. Nguyen, G. Van Assche, and N. J. Cerf, "Side-information coding with turbo codes and its application to quantum key distribution," in *Proc. International Symposium on Information Theory and its Applications*, Parma, Italy, October 2004, pp. 1274–1279.

[61] 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; extended report available at arXiv:cs.IT/0509041.

[62] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE International Symposium on Information Theory*, Seattle, WA, USA, July 2006, pp. 2593–2597.

[63] A. Rényi, "On measures of entropy and information," in *Proc. Fourth Berkeley Symposium on Mathematical Statistics and Probability*, vol. 1, Berkeley, CA, USA, 1961, pp. 547–561.

[64] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, November 1995.

[65] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, April 1979.

[66] M. N. Wegman and J. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer Sciences and Systems*, vol. 22, no. 3, pp. 265–279, June 1981.

[67] D. R. Stinson, "Universal hashing and authentication codes," *Designs, Codes and Cryptography*, vol. 4, no. 4, pp. 369–380, October 1994.

[68] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology – Eurocrypt 2000*, B. Preneel, Ed. Springer-Verlag, 2000, p. 351.

[69] S. Vadhan, "Extracting all the randomness from a weakly random source," Massachusetts Institute of Technology, Cambridge, MA, USA, Technical Report, 1998.

[70] C. Cachin, "Entropy measures and unconditional security in cryptography." Ph.D. dissertation, ETH Zürich, Zurich, Switzerland, 1997.

[71] C. Cachin and U. M. Maurer, "Linking information reconciliation and privacy amplification," *Journal of Cryptology*, vol. 10, no. 2, pp. 97–110, March 1997.

[72] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E89-A, no. 7, pp. 2036–2046, July 2006.

[73] S. Nitinawarat, "Secret key generation for correlated Gaussian sources," in *Proc. 45th Allerton Conference on Communications, Control and Computing*, Monticello, IL, USA, September 2007, pp. 1054–1058.

[74] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels – part I. Definitions and a completeness result," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 822–831, April 2003.

[75] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels – part II. The simulatability condition," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 832–838, April 2003.

[76] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels – part III. Privacy amplification," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 839–851, April 2003.

[77] H. Imai, K. Kobara, and K. Morozov, "On the possibility of key agreement using variable directional antenna," in *Proc. 1st Joint Workshop on Information Security*, Seoul, South Korea, September 2006, pp. 153–167.

[78] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, June 2010.

[79] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 205–215, February 2011.

[80] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Letters to Nature*, vol. 421, no. 6920, pp. 238–241, January 2003.

[81] 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.

[82] H. Chabanne and G. Fumaroli, "Noisy cryptographic protocols for low-cost RFID tags," *IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3562–3566, August 2006.

[83] A. Khisti and G. Wornell, "The MIMOME channel," in *Proc. 45th Allerton Conference on Communication, Control and Computing*, Monticello, IL, USA, September 2007, pp. 625–632; available online: http://allegro.mit.edu/pubs/posted/journal/2008-khisti-wornell-it.pdf.

[84] A. Khisti and G. Wornell, "Secure transmission with multiple antennas – II: The MIMOME wiretap channels," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, November 2010.

[85] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[86] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, October 2008.

[87] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channels," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[88] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 370 970/1–8, 2009.

[89] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channels," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 524–528.

[90] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.

[91] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2–2–1 channels," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, September 2009.

[92] M. Gursoy, "Secure communication in the low-SNR regime: A characterization of the energy–secrecy tradeoff," in *Proc. IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009, pp. 2291–2295.

[93] R. Negi and S. Goel, "Secret communication using artificial noise," in *62nd Vehicular Technology Conference (VTC)*, vol. 3, Dallas, TX, USA, September 2005, pp. 1906–1910.

[94] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[95] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channels," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, July 2007, pp. 2471–2475.

[96] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE International Symposium on Information Theory*, Seattle, WA, USA, July 2006, pp. 356–360.

[97] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 1296–1300.

[98] H. Jeon, N. Kim, M. Kim, H. Lee, and J. Ha, "Secrecy capacity over correlated ergodic fading channels," in *Proc. IEEE Military Communications Conference*, San Diego, CA, USA, November 2008, pp. 1–7.

[99] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the k-user Gaussian interference channels," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 384–388.

[100] M. Kobayashi, M. Debbah, and S. S. (Shitz), "Secured communication over frequency-selective fading channels: A practical Vandermonde precoding," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 386 547/1–19, 2009.

[101] M. Bloch and J. N. Laneman, "Information-spectrum methods for information-theoretic security," in *Proc. Information Theory and Applications Workshop*, San Diego, CA, USA, February 2009, pp. 23–28.

[102] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1575–1591, April 2009.

[103] X. Tang, H. Poor, R. Liu, and P. Spasojević, "Secret-key sharing based on layered broadcast coding over fading channels," in *Proc. IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009, pp. 2762–2766.

[104] Y. Liang, L. Lai, H. Poor, and S. Shamai, "The broadcast approach over fading Gaussian wiretap channels," in *Proc. Information Theory Workshop*, Taormina, Italy, October 2009, pp. 1–5.

[105] 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.

[106] 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.
[107] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, September 2007.
[108] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008.
[109] H. Jin and T. Richardson, "Block error iterative decoding capacity for LDPC codes," in *Proc. International Symposium on Information Theory*, Adelaide, Australia, 2005, pp. 52–56.
[110] R. G. Gallager, "Low density parity check codes," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, USA, 1963.
[111] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 599–618, February 2001.
[112] S.-Y. Chung, T. J. Richardson, and R. L. Urbanke, "Analysis of sum–product decoding of low-density parity-check codes using a Gaussian approximation," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 657–670, February 2001.
[113] S.-Y. Chung, J. G. D. Forney, T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Communications Letters*, vol. 5, no. 2, pp. 58–60, February 2001.
[114] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 619–637, February 2001.
[115] A. Shokrollahi and R. Storn, "Design of efficient erasure codes with differential evolution," in *Proc. IEEE International Symposium on Information Theory*, Sorrento, Italy, June 2000.
[116] L. H. Ozarow and A. D. Wyner, "Wire tap channel II," *AT&T Bell Laboratories Technical Journal*, vol. 63, no. 10, pp. 2135–2157, December 1984.
[117] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channels," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, August 2007.
[118] 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, 2010, pp. 1–5.
[119] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes," submitted to *IEEE Transactions on Information Forensics and Security*, September 2010. Available online: arXiv:1009.3130.
[120] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Two edge type LDPC codes for the wiretap channels," in *Proc. 43rd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, November 2009, pp. 834–838.
[121] G. Cohen and G. Zemor, "Syndrome-coding for the wiretap channel revisited," in *Proc. IEEE Information Theory Workshop*, Chengdu, China, October 2006, pp. 33–36.
[122] R. Liu, Y. Liang, H. V. Poor, and P. Spasojević, "Secure nested codes for type II wiretap channels," in *Proc. IEEE Information Theory Workshop*, Lake Tahoe, CA, USA, September 2007, pp. 337–342.

[123] E. Verriest and M. Hellman, "Convolutional encoding for Wyner's wiretap channels," *IEEE Transactions on Information Theory*, vol. 25, no. 2, pp. 234–236, March 1979.
[124] V. Wei, "Generalized Hamming weights for linear codes," *IEEE Transactions on Information Theory*, vol. 37, no. 5, pp. 1412–1418, September 1991.
[125] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," in *Proc. IEEE International Symposium on Information Theory*, Austin, TX, USA, June 2010, pp. 913–917. Available online: arXiv:1001.0210v1.
[126] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Communications Letters*, vol. 14, no. 4, pp. 752–754, June 2010.
[127] O. O. Koyluoglu and H. E. Gamal, "Polar coding for secure transmission and key agreement," in *Proc. IEEE International Symposium on Personal Indoor and Mobile Radio Communications*, Istanbul, Turkey, 2010, pp. 2698–2703.
[128] E. Hof and S. Shamai, "Secrecy-achieving polar-coding for binary-input memoryless symmetric wire-tap channels," in *Proc. IEEE Information Theory Workshop*, Dublin, Ireland, 2010, pp. 1–5.
[129] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channels," in *Proc. IEEE Information Theory Workshop*, Taormina, Sicily, October 2009, pp. 95–99.
[130] J.-C. Belfiore and P. Solé, "Unimodular lattices for the Gaussian wiretap channels," in *Proc. IEEE Information Theory Workshop*, Dublin, Ireland, September 2010, pp. 1–5.
[131] J.-C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design," in *Proc. International Symposium on Information Theory and its Applications*, Taichung, Taiwan, October 2010.
[132] A. Wyner, "Recent results in the Shannon theory," *IEEE Transactions on Information Theory*, vol. 20, no. 1, pp. 2–10, January 1974.
[133] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Communications Letters*, vol. 6, no. 10, pp. 440–442, October 2002.
[134] J. Chen, D. He, and A. Jagmohan, "Slepian–Wolf code design via source-channel correspondence," in *Proc. IEEE International Symposium on Information Theory*, Seattle, WA, USA, July 2006, pp. 2433–2437.
[135] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Physical Review A*, vol. 77, no. 4, p. 042325, April 2008.
[136] U. Wachsmann, R. F. H. Fischer, and J. B. Huber, "Multilevel codes: Theoretical concepts and practical design rules," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1361–1391, July 1999.
[137] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 927–946, May 1998.
[138] J. Hou, P. H. Siegel, L. B. Milstein, and H. D. Pfister, "Capacity-approaching bandwidth-efficient coded modulation schemes based on low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 49, no. 9, pp. 2141–2155, September 2003.
[139] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2010.

[140] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, November 1976.
[141] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, February 1978.
[142] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd edn. Wiley, 1996.
[143] A. Menezes, P. Van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, 5th edn. CRC Press, 2001.
[144] M. Médard, D. Marquis, R. Barry, and S. Finn, "Security issues in all-optical networks," *IEEE Network*, vol. 11, no. 3, pp. 42–48, May–June 1997.
[145] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1350–1356, July 2000.
[146] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proc. 5th ACM Workshop on Wireless Security*, Los Angeles, CA, USA, September 2006, pp. 33–42.
[147] Y. Liang, H. V. Poor, and S. S. (Shitz), *Information-Theoretic Security*. Now Publishers, 2009.
[148] R. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*. Springer-Verlag, 2010.
[149] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.
[150] X. He and A. Yener, "On the role of feedback in two-way secure communications," in *Proc. 42nd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, October 2008, pp. 1093–1097.
[151] M. Bloch, "Channel scrambling for secrecy," in *Proc. of IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009, pp. 2452–2456.
[152] M. Médard, "Capacity of correlated jamming channels," in *Proc. Allerton Conference on Communications, Computing and Control*, Monticello, IL, USA, October 1997.
[153] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference-assisted secret communications," in *Proc. IEEE Information Theory Workshop*, Porto, Portugal, May 2008, pp. 164–168.
[154] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 389–393.
[155] X. He and A. Yener, "Providing secrecy with lattice codes," in *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, September 2008, pp. 1199–1206.
[156] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling," in *Proc. IEEE Global Telecommunications Conference*, Honolulu, HI, USA, December 2009, pp. 1–6.
[157] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 2217–2221.

[158] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," in *Proc. IEEE Information Theory Workshop*, Porto, Portugal, May 2008, pp. 154–158.
[159] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *Proc. IEEE International Conference on Communications*, Cape Town, South Africa, May 2010, pp. 1550–3607.
[160] O. Simeone and A. Yener, "The cognitive multiple access wire-tap channel," in *Proc. 43rd Annual Conference on Information Sciences and Systems*, Baltimore, MD, USA, March 2009, pp. 158–163.
[161] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Transactions on Information Theory*, vol. 55, no. 2, pp. 604–619, February 2009.
[162] C. Mitrpant, A. J. H. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.
[163] G. T. Amariucai and S. Wei, "Secrecy rates of binary wiretapper channels using feedback schemes," in *Proc. 42nd Annual Conference on Information Sciences and Systems*, Princeton, NJ, USA, March 2008, pp. 624–629.
[164] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5059–5067, November 2008.
[165] D. Gündüz, D. R. Brown, and H. V. Poor, "Secret communication with feedback," in *Proc. International Symposium on Information Theory and Its Applications*, Auckland, New Zealand, May 2008, pp. 1–6.
[166] A. El Gamal, O. O. Koyluoglu, M. Youssef, and H. El Gamal, "New achievable secrecy rate regions for the two way wiretap channels," in *Proc. IEEE Information Theory Workshop*, Cairo, Egypt, January 2010, pp. 1–5.
[167] X. He and A. Yener, "A new outer bound for the secrecy capacity region of the Gaussian two-way wiretap channels," in *Proc. IEEE International Conference on Communications*, Cape Town, South Africa, May 2010, pp. 1–5.
[168] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, September 2001, pp. 87–89.
[169] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, September 2008.
[170] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wire-tapper," in *Proc. IEEE Information Theory Workshop*, Lake Tahoe, CA, USA, September 2007, pp. 595–600.
[171] X. He and A. Yener, "Secure communication with a Byzantine relay," in *Proc. IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009, pp. 2096–2100.
[172] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP Journal on Wireless Communication and Networking*, vol. 2009, pp. 305 146/1–13, 2009.
[173] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, August 2010.
[174] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.
[175] Y. Liang, G. Kramer, H. V. Poor, and S. S. (Shitz), "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 142 374/1–12, 2009.

[176] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, December 2004.
[177] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.
[178] I. Csiszár and P. Narayan, "Secrecy generation for multiple input multiple output channel models," in *Proc. IEEE International Symosium on Information Theory*, Seoul, South Korea, July 2009, pp. 2447–2451.
[179] S. Nitinawarat, A. Barg, P. Narayan, C. Ye, and A. Reznik, "Perfect secrecy, perfect omniscience and Steiner tree packing," in *Proc. IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009, pp. 1288–1292.
[180] S. Nitinawarat and P. Narayan, "Perfect secrecy and combinatorial tree packing," in *Proc. IEEE International Symposium on Information Theory*, Austin, TX, USA, June 2010, pp. 2622–2626.
[181] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 539–543.
[182] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. 11th IEEE Singapore International Conference on Communication Systems*, Guangzhou, Singapore, November 2008, pp. 974–979.
[183] E. Perron, S. Diggavi, and E. Telatar, "On noise insertion strategies for wireless network secrecy," in *Proc. Information Theory and Applications Workshop*, San Diego, CA, USA, February 2009, pp. 77–84.
[184] R. Ahlswede, N. Cai, S. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.
[185] S. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, February 2003.
[186] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, October 2003.
[187] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, October 2006.
[188] P. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. 41st Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, October 2003.
[189] C. Gkantsidis and P. Rodriguez, "Network coding for large scale content distribution," in *Proc. 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Miami, FL, USA, March 2005, pp. 2235–2245.
[190] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air: practical wireless network coding," in *Proc. Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Pisa, Italy, August 2006, pp. 243–254.
[191] N. Cai and R. Yeung, "Secure network coding," in *Proc. IEEE International Symposium on Information Theory*, Lausanne, Switzerland, July 2002, p. 323.
[192] L. Ozarow and A. Wyner, "Wire-tap channel II," *AT&T Bell Labs Technical Journal*, vol. 63, no. 10, pp. 2135–2157, December 1984.
[193] S. Rouayheb and E. Soljanin, "On wiretap networks II," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 551–555.
[194] K. Bhattad and K. Narayanan, "Weakly secure network coding," in *Proc. First Workshop on Network Coding, Theory, and Applications (NetCod)*, Riva del Garda, Italy, February 2005.

[195] L. Lima, M. Médard, and J. Barros, "Random linear network coding: A free cipher?" in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 546–550.
[196] J. Vilela, L. Lima, and J. Barros, "Lightweight security for network coding," in *Proc. IEEE International Conference on Communications*, Beijing, China, May 2008, pp. 1750–1754.
[197] L. Lima, S. Gheorghiu, J. Barros, M. Médard, and A. Toledo, "Secure network coding for multi-resolution wireless video streaming," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 3, pp. 377–388, April 2010.
[198] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient network coding in the presence of Byzantine adversaries," in *IEEE INFOCOM*, May 2007.
[199] C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," in *IEEE INFOCOM*, Barcelona, Spain, April 2006.
[200] N. Cai and R. Yeung, "Network error correction," in *Proc. IEEE International Symposium on Information Theory*, Kanagawa, Japan, July 2003, p. 101.
[201] R. Koetter and F. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, August 2008.
[202] M. Kim, L. Lima, F. Zhao, J. Barros, M. Médard, R. Koetter, T. Kalker, and K. Han, "On counteracting Byzantine attacks in network coded peer-to-peer networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 692–702, June 2010.
[203] P. F. Oliveira, R. A. Costa, and J. Barros, "Mobile secret key distribution with network coding," in *Proc. International Conference on Security and Cryptography*, Barcelona, Spain, July 2007, pp. 1–4.
[204] M. J. Kim, J. Barros, M. Médard, and R. Koetter, "An algebraic watchdog for wireless network coding," in *Proc. IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009, pp. 1159–1163.
[205] T. Ho and D. Lun, *Network Coding: An Introduction*. Cambridge University Press, 2008.
[206] C. Fragouli and E. Soljanin, "Network coding fundamentals," *Foundations and Trends in Networking*, vol. 2, no. 1, pp. 1–133, 2007.
[207] C. Fragouli and E. Soljanin, "Network coding applications," *Foundations and Trends in Networking*, vol. 2, no. 2, pp. 135–269, 2007.