Information Theoretic Security

Information Theoretic Security

Yingbin Liang

University of Hawaii
Honolulu, HI 96822
USA
yingbinl@hawaii.edu

H. Vincent Poor

Princeton University
Princeton, NJ 08544
USA
poor@princeton.edu

Shlomo Shamai (Shitz)

Technion — Israel Institute of Technology
Haifa, 32000
Israel
sshlomo@ee.technion.ac.il

now
the essence of knowledge
Boston – Delft

Full text available at: http://dx.doi.org/10.1561/0100000036

Foundations and Trends® in Communications and Information Theory

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is Y. Liang, H. V. Poor and S. Shamai (Shitz), Information Theoretic Security, Foundations and Trends® in Communications and Information Theory, vol 5, nos 4–5, pp 355–580, 2008

ISBN: 978-1-60198-240-7
© 2009 Y. Liang, H. V. Poor and S. Shamai (Shitz)

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The 'services' for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1-781-871-0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in
Communications and Information Theory
Volume 5 Issues 4–5, 2008

Editorial Scope

Foundations and Trends® in Communications and Information Theory will publish survey and tutorial articles in the following topics:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication system design
- Cryptology and data security
- Data compression
- Data networks
- Demodulation and Equalization
- Denoising
- Detection and estimation
- Information theory and statistics
- Information theory and computer science
- Joint source/channel coding
- Modulation and signal design
- Multiuser detection
- Multiuser information theory
- Optical communication channels
- Pattern recognition and learning
- Quantization
- Quantum information processing
- Rate-distortion theory
- Shannon theory
- Signal processing for communications
- Source coding
- Storage and recording codes
- Speech and Image Compression
- Wireless Communications

Information for Librarians

Foundations and Trends® in Communications and Information Theory, 2008, Volume 5, 6 issues. ISSN paper version 1567-2190. ISSN online version 1567-2328. Also available as a combined paper and online subscription.

Foundations and Trends® in
Communications and Information Theory
Vol. 5, Nos. 4–5 (2008) 355–580

DOI: 10.1561/0100000036

Information Theoretic Security

Yingbin Liang[1], **H. Vincent Poor**[2]
and Shlomo Shamai (Shitz)[3]

[1] *University of Hawaii, Department of Electrical Engineering, Holmes Hall 483, 2540 Dole Street, Honolulu, HI 96822, USA, yingbinl@hawaii.edu*
[2] *Princeton University, Department of Electrical Engineering, E-Quad, Olden Street, Princeton, NJ 08544, USA, poor@princeton.edu*
[3] *Technion — Israel Institute of Technology, Department of Electrical Engineering, Technion City, Haifa, 32000, Israel, sshlomo@ee.technion.ac.il*

Abstract

The topic of information theoretic security is introduced and the principal results in this area are reviewed. The basic wire-tap channel model is considered first, and then several specific types of wire-tap channels are considered, including Gaussian, multi-input multi-output (MIMO), compound, and feedback wire-tap channels, as well as the wire-tap channel with side information. Practical code design techniques to achieve secrecy for wire-tap channels are also introduced. The wire-tap formalism is then extended to the basic channels of multi-user networks, including broadcast channels, multiple-access channels (MACs), interference channels, relay channels and two-way channels. For all of these models, results on the fundamental communication limits under secrecy constraints and corresponding coding schemes are reviewed. Furthermore, several related topics including key agreement through common randomness, secure network coding, authentication, cross-layer design, and secure source coding are discussed.

Contents

1 Introduction 1

1

Introduction

1.1 Confidentiality and Encryption

Security is one of the most important issues in communications. Security issues arising in communication networks include confidentiality, integrity, authentication, and nonrepudiation. Confidentiality guarantees that legitimate recipients successfully obtain source information intended for them, while eavesdroppers are not able to interpret this information. Integrity guarantees that original source information is not modified by malicious actors during its transmission. Authentication ensures that a recipient of information is able to identify the sender from which that information has been sent. Nonrepudiation guarantees that a sender of information is not able to deny having transmitted that information and the recipient is not able to deny having received the information.

Attacks on the security of communication networks can be divided into two basic types: *passive attacks* and *active attacks*. An active attack corresponds to the situation in which a malicious actor intentionally disrupts the system. Alternatively, a passive attack corresponds to the situation in which a malicious actor attempts to interpret source

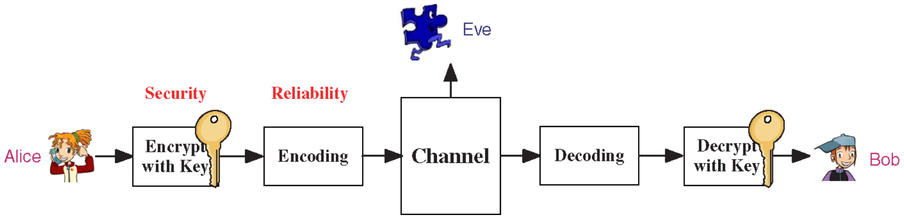

Fig. 1.1 Illustration of encryption with channel coding.

information without injecting any information or trying to modify the information; i.e., passive attackers listen to the transmission without modifying it. This paper focuses primarily on confidentiality issues, and passive attacks are of primary concern in this context.

Conventional techniques for achieving confidentiality in communication networks are based on cryptographic encryption [122, 148], which is depicted in Figure 1.1. In encryption, a transmitter (Alice) uses a key to encrypt source information, i.e., *plaintext*, to convert it into *ciphertext*. The intended receiver (Bob) extracts the original plaintext from the ciphertext by a corresponding key. If an eavesdropper (Eve) has access to the ciphertext, but it does not know the corresponding decryption key, then it cannot obtain the source information. As a practical matter, the eavesdropper can be assumed to have limited time or limited computational resources so that it cannot test all possible keys to extract the source information. This process is illustrated in Figure 1.1, in which additional encoding and decoding steps, which involve physical layer techniques to combat channel transmission errors, are also shown.

Encryption includes two principal types of algorithms: *secret-key encryption* algorithms and *public-key encryption* algorithms. Secret-key encryption is also referred to as *symmetric key encryption*, because the transmitter and the receiver share a common secret key. The transmitter encrypts the plaintext and the receiver decrypts the ciphertext with the same key. For public-key encryption, which is also referred to as *asymmetric key encryption*, the transmitter and the receiver have different keys for encryption and decryption. The transmitter encrypts the plaintext by a public key, which is known publicly to all potential users of the network, including any eavesdroppers. The intended receiver maintains a private key corresponding to the public key, with which the receiver can extract the plaintext encrypted by the public key. It is in general mathematically difficult (almost computationally impossible) for other users to derive this private key with only the information about the public key. Hence, in practice, an eavesdropper can obtain no source information without the private key.

As compared to public-key algorithms, secret-key algorithms are computationally efficient, and result in higher data throughput, while presenting challenges for key management, such as secure key storage and distribution [7, 15, 20, 35, 38, 65, 100, 134, 167, 181, 184, 185]. Public-key algorithms are simple in terms of key management, but require considerable computational resources [122]. Hence, hybrid cryptosystems [26, 31] are employed in practice, to facilitate key management and achieve high efficiency, in which a secret key is distributed by public-key algorithms, and encryption and decryption can then use secret-key algorithms. However, several disadvantages of public-key algorithms are of serious concern for hybrid cryptosystems. Besides high computational cost, public-key algorithms are not provably perfectly secure and are vulnerable to the so-called man-in-the-middle attack [122]. Moreover, using public-key algorithms to distribute secret keys adds another layer of complexity in the design of networks.

In addition to these general considerations, providing secure communication over *wireless* networks using cryptographic approaches presents further significant challenges due to: (1) the open nature of the wireless medium, which allows eavesdroppers and attackers to intercept information transmission (in particular, transmission of secret keys) or to degrade transmission quality; (2) the lack of infrastructure in decentralized networks, which makes key distribution difficult; and (3) the dynamic topology of mobile networks (e.g., mobile *ad hoc* networks), which makes key management expensive.

The information theoretic approach to achieving secure communication opens a promising new direction toward solving wireless networking security problems. Such an approach was initiated by Wyner [169] and by Csiszár and Körner [27] in the 1970's, who demonstrated that *confidential messages* can be transmitted securely without using an encryption key. Study of the related topic of *secret-key agreement* (including generation and distribution) via information theoretic analysis was later proposed in Maurer's work [115, 116] and in Ahlswede and Csiszár's work [4], which demonstrate that two or multiple legitimate nodes can agree on a key (for encryption later on) kept secret from an eavesdropper. More recently, the emergence and increasing ubiquity of wireless networks, and in particular of networks with minimal infrastructure, have spurred considerable interest in this area. In particular, the promise of this potentially very powerful approach for use in mobile and other wireless networks has been brought to the attention of the wireless networking community.

1.2 Information Theoretic Analysis of Cryptosystems

Information theoretic analysis of secrecy was initiated by Shannon in [145], in which a cryptosystem (see Figure 1.2) was considered. In Shannon's model, a source message W is encrypted to a ciphertext E by a key K shared by the transmitter and receiver. An eavesdropper, which knows the family of encryption functions (keys) and the probability of choosing keys, may intercept the ciphertext E. The system is considered to be *perfectly secure* if the *a posteriori* probabilities of W given E are equal to the *a priori* probabilities of W for all E, i.e., $P_{W|E} = P_W$. It was shown in [145] that the number of different keys must be at least as large as the number of messages to achieve perfect secrecy.

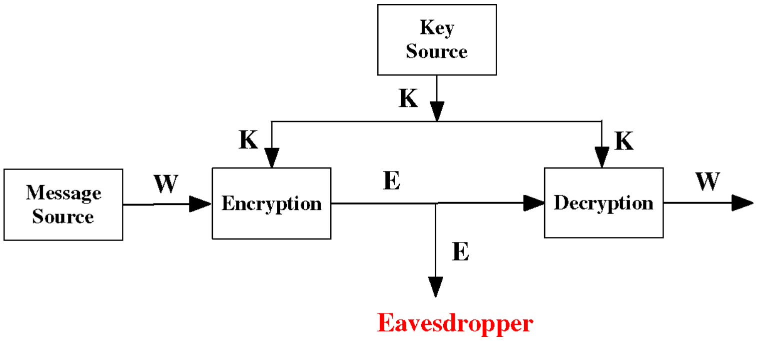

Fig. 1.2 A cryptosystem.

Furthermore, the *entropy* was introduced to measure the amount of information associated with a message and the amount of uncertainty associated with the possibilities of a key, i.e., $H(W)$ and $H(K)$, respectively. The notion of the *equivocation* was also introduced in [145] to measure the eavesdropper's uncertainty about the message and the key, namely, the conditional entropies $H(W\,|\,E)$ and $H(K\,|\,E)$. (The reader can refer to Appendix A.1 for the definitions and the properties of these quantities.) We note that the entropy of a random variable indicates the average length of a binary sequence (in bits) required to represent the random variable (with small probability of error). Based on the properties of the entropy, we obtain

$$H(K,W) = H(K) + H(W), \tag{1.1}$$

$$H(K,W) = H(K,W,E) = H(K,E) = H(E) + H(K\,|\,E), \tag{1.2}$$

and

$$H(K,W) = H(K,W,E) \geq H(W,E) = H(E) + H(W\,|\,E). \tag{1.3}$$

In the case of perfect secrecy, i.e., $H(W) = H(W\,|\,E)$, (1.1) and (1.3) imply $H(K) \geq H(E)$. Moreover, if $H(E) = H(W)$, then (1.1) and (1.2) imply $H(K) = H(K\,|\,E)$, i.e., no information about the key can be inferred from the ciphertext E. On the other hand, if $H(E) = H(W) + H(K)$, then (1.1) and (1.2) imply $H(K\,|\,E) = 0$, i.e., the key can be determined from E. Hence, the value of $H(E) = H(W) + H(K)$ defines the *unicity distance*, i.e., the minimum length of the ciphertext that guarantees recovery of the key used for encryption.

1.3 Information Theoretic Security

Although the scenarios considered in [145] are cryptosystems, the equivocation, which quantifies how unlikely it is that the eavesdropper can infer source information from its received information, is central to information theoretic security as developed later for systems without using encryption keys [27, 169]. This quantifiable measure also enables secrecy to be jointly considered with the traditional measure of reliability, namely the error probability (at the legitimate receiver), and hence facilitates the application of information theoretic techniques to characterize the fundamental communication limits of communication networks under secrecy constraints.

The basic idea of the information theoretic approach to securely transmit conferential messages (without using an encryption key) to a legitimate receiver is to use the inherent randomness of the physical medium (including noises and channel fluctuations due to fading) and exploit the difference between the channel to a legitimate receiver and the channel to an eavesdropper to benefit the legitimate receiver. In this approach, a transmitter intentionally adds structural randomness (stochastic coding) to prevent potential eavesdroppers and attackers from intercepting useful information while guaranteeing that a legitimate receiver can obtain the information. Figure 1.3 illustrates a system that exploits information theoretic security. In this system, the "encryption" and "encoding" of Figure 1.1 are now combined into a single design block for "secure encoding," which guarantees both reliability, i.e., the receiver can successfully decode source messages, and security, i.e., the source messages are guaranteed to be secret from an eavesdropper.

Compared to contemporary cryptosystems, information theoretic approaches to guarantee secrecy have the advantages of eliminating

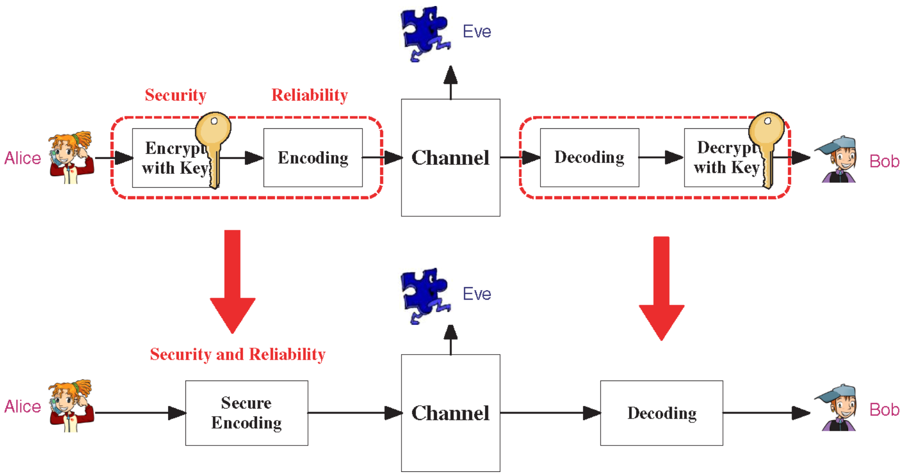

Fig. 1.3 Information theoretic security.

the key management issue, thereby resulting in significantly lower complexity and savings in resources. Furthermore, compared to public-key algorithms for key management in hybrid cryptosystems, the information theoretic security approaches are less vulnerable to the man-in-the-middle attack [78, 113, 114, 141, 146, 162, 171] due to the intrinsic randomness shared by terminals. Moreover, information theoretic security approaches achieve provable security that is robust to powerful eavesdroppers possessing unlimited computational resources, knowledge of the communication strategy employed including coding and decoding algorithms, and access to communication systems either through perfect or noisy channels.

While information theoretic security approaches exploit physical layer attributes of channel randomness for secure communications, and encryption keys are not necessary, these approaches can also be applied to existing cryptosystems to add an additional level of protection for information transmission or to achieve key agreement (including key generation and distribution) for remote terminals. The idea of applying information theoretic approaches to achieve secret-key (SK) agreement exploits initially shared correlated sources (observations) among legitimate terminals or channel transmission between these terminals. In the simplest model [4, 116], two terminals, each observing correlated source sequences, can agree on a key by communicating over a noiseless public channel using Slepian–Wolf coding [23, 147]. This coding scheme also guarantees that the key is kept secret from an eavesdropper that has access to this public communication. It was also shown in [4] that noisy communication channels can also be exploited to create correlated sequences at the two terminals, thereby allowing them to agree on a secret key.

We note that there is a difference between the two problems of information theoretic security that we mentioned so far, namely, transmission of confidential messages and SK agreement. The latter allows public discussion between legitimate terminals in the process, and secure channel transmission may not be necessary if legitimate terminals share correlated source sequences initially in this latter case. However, there is also a connection between the two problems as secrecy transmission may be used to create a secret key (although without public transmission), and an established secret key helps mitigate conditions required for secrecy transmission by transmitting part of the source information by encryption and only the rest of the information via secrecy transmission.

In this paper, we will focus on the problem of transmission of confidential messages, and will address the problem of SK agreement only in one section to illustrate the main idea. We refer the reader to the corresponding references for further details. We also note that in addition to the two problems mentioned above, information theoretic security covers a variety of other topics that are not included in this paper, for example, the identification problem [6, 32], biometric security [60, 61, 79, 80], and the principle of reciprocity [9, 128, 166].

We finally note that the topics we have included in this paper reflect the subjective views of the authors, and should not be considered as a comprehensive overview of information theoretic security and its applications. Within the page limitations of such a work, we can present only selected topics, and thus we focus on what we consider to be the most timely issues.

1.4 Organization of the Paper

This paper provides an overview of how information theoretic approaches are developed to achieve secrecy for a basic wire-tap channel model as well as for its extensions to multi-user networks. In Section 2, we introduce the basic wire-tap channel and derive the secrecy capacity of this channel. We also describe basic coding techniques that achieve the secrecy capacity and introduce the converse methodology to prove the optimality of these techniques. In Section 3, we consider several special classes of wire-tap channels, and discuss the secrecy capacities for these channels. In Section 4, we introduce practical code design techniques that can achieve secrecy over the wire-tap channel. In Sections 5–8, we address extensions of the basic wire-tap channel to several basic multi-user network models including the broadcast channel, the multiple-access channel (MAC), the interference channel, the relay channel and the two-way channel. In Sections 9 and 10, we review several other topics in information theoretic security, including key agreement through common randomness, secure network coding, authentication, cross-layer design, and secure source coding. In Appendix A, we present basic definitions and properties from information theory that are used in the main text, for the benefit of the reader who is unfamiliar with these notions.

References

[1] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, to appear.

[2] R. Ahlswede, "Multi-way communication channels," in *Proceedings of the 2nd International Symposium on Information Theory (ISIT, 1971)*, pp. 23–52, Tsahkadsor, Armenian S.S.R.: Publishing House of the Hungarian Academy of Sciences, 1973.

[3] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, pp. 1204–1216, July 2000.

[4] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography — Part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, pp. 1121–1132, July 1993.

[5] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography-Part II: CR capacity," *IEEE Transactions on Information Theory*, vol. 44, pp. 225–240, January 1998.

[6] R. Ahlswede and Z. Zhang, "Identification via wire-tap channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, p. 352, Trondheim, Norway, June–July 1994.

[7] N. Asokan and P. Ginzboorg, "Key-agreement in ad hoc networks," *Computer Communications*, vol. 23, no. 17, pp. 1627–1637, 2000.

[8] A. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow," in *Proceedings of the 45th Annual Allerton Conference Communication, Control, and Computing*, Monticello, IL, USA, September 2007.

[9] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 401–410, Alexandria, VA, USA, October–November 2007.

[10] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secure broadcasting: The secrecy rate region," in *Proceedings of the 46th Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, September 2008. Also submitted to *IEEE Transactions on Information Theory*, December 2008.

[11] R. E. Blahut, *Algebraic Codes for Data Transmission.* New York, NY, USA: Cambridge University Press, 2003.

[12] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, pp. 2515–2534, June 2008.

[13] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wire-tap channel," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, to appear.

[14] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, June–July 2009.

[15] M. Cagalj, S. Capkun, and J. P. Hubaux, "Key agreement in peer-to-peer wireless networks," *Proceedings of the IEEE*, vol. 94, pp. 467–478, February 2006.

[16] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wire-tap channels," *Problems of Information Transmission*, vol. 40, no. 4, pp. 318–336, 2004.

[17] N. Cai and R. W. Yeung, "Secure network coding," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, p. 323, Lausanne, Switzerland, June–July 2002.

[18] N. Cai and R. W. Yeung, "A security condition for multi-source linear network coding," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 561–565, Nice, France, June 2007.

[19] G. Caire, G. Taricco, and E. Biglieri, "Optimal power control over fading channels," *IEEE Transactions on Information Theory*, vol. 45, pp. 1468–1489, July 1999.

[20] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of the IEEE Symposium Security and Privacy*, pp. 197–213, Oakland, CA, USA, 2003.

[21] Y. Chen and A. J. H. Vinck, "Wiretap channel with side information," *IEEE Transactions on Information Theory*, vol. 54, pp. 395–402, January 2008.

[22] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, pp. 439–441, May 1983.

[23] T. M. Cover, "A proof of the data compression theorem of Slepian and Wolf for ergodic sources," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 226–228, 1975.

[24] T. M. Cover and A. A. El Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, pp. 572–584, September 1979.

[25] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd Edition. New York, USA: Wiley, 2006.

[26] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," *SIAM Journal on Computing*, vol. 33, no. 1, pp. 167–226, 2004.

[27] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, pp. 339–348, May 1978.

[28] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, pp. 344–366, March 2000.

[29] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, pp. 3047–3061, December 2004.

[30] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, pp. 2437–2452, June 2008.

[31] H. Dennis and E. Kiltz, "Secure hybrid encryption from weakened key encapsulation," in *Proceedings of the 27th Annual International Cryptology Conference (CRYPTO)*, pp. 553–571, Santa Barbara, CA, USA, August 2007.

[32] Y. Desmedt, "Information-theoretic secure identification," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, p. 296, Cambridge, MA, USA, August 1998.

[33] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Taipei, Taiwan, April 2009.

[34] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proceedings of the IEEE Workshop on Statistical Signal Processing*, Cardiff, Wales, UK, August-September 2009.

[35] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," *IEEE Communications Survey and Tutorials*, vol. 3, pp. 62–77, January–March 2006.

[36] A. A. El Gamal, "Capacity of the product and sum of two unmatched broadcast channels," *Problems of Information Transmission*, vol. 16, pp. 1–16, January–March 1980.

[37] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Transactions on Information Theory*, vol. 51, pp. 3401–3416, October 2005.

[38] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47, Washington DC, USA, 2002.

[39] J. Feldman, T. Malkin, R. A. Servedio, and C. Stein, "On the capacity of secure network coding," in *Proceedings of the 42nd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, September 2004.

[40] C. Fragouli and E. Soljanin, "Network coding applications," *Foundations and Trends in Networking*, vol. 2, no. 2, pp. 135–269, 2007.

[41] C. Fragouli and E. Soljanin, "Network coding fundamentals," *Foundations and Trends in Networking*, vol. 2, no. 1, pp. 1–133, 2007.

[42] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[43] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals — Part II: Channel model," *Preprint*, Available at http://www.eecs.berkeley.edu/∼aminzade/Channel Model.pdf. December 2007.

[44] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals — Part I: Source model," *Preprint*, Available at http://www. eecs.berkeley.edu/∼aminzade/Source Model.pdf. December 2007.

[45] A. A. Gohari and V. Anantharam, "Communication for omniscience by a neutral observer and information-theoretic key agreement of multiple terminals," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Nice, France, June 2007.

[46] A. A. Gohari and V. Anantharam, "New bounds on the information-theoretic key agreement of multiple terminals," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, July 2008.

[47] A. Goldsmith and P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Transactions on Information Theory*, vol. 43, pp. 1986–1992, November 1997.

[48] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, pp. 4687–4698, October 2008.

[49] J. Grubb, S. Vishwanath, Y. Liang, and H. V. Poor, "Secrecy capacity of semi-deterministic wire-tap channels," in *Proceedings of the IEEE Information Theory Workshop (ITW) on Information Theory for Wireless Networks*, Bergen, Norway, July 2007.

[50] D. Gündüz, D. R. Brown III, and H. V. Poor, "Secret communication with feedback," in *Proceedings of the International Symposium on Information Theory and Its Applications (ISITA)*, Auckland, New Zealand, December 2008.

[51] D. Gündüz, E. Erkip, and H. V. Poor, "Lossless compression with security constraints," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Canada, July 2008.

[52] D. Gündüz, E. Erkip, and H. V. Poor, "Secure compression with side information," in *Proceedings of the 3rd Workshop on Information Theory and Applications (ITA)*, La Jolla, CA, USA, January–February 2008.

[53] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in *Proceedings of the Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, November 2007.

[54] X. He and A. Yener, "The role of an untrusted relay in secret communication," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, July 2008.

[55] X. He and A. Yener, "K-user interference channels: Achievable secrecy rate and degrees of freedom," in *Proceedings of the IEEE Information Theory Workshop (ITW)*, Volos, Greece, June 2009.

[56] X. He and A. Yener, "A new outer bound for the Gaussian interference channel with confidential messages," in *Proceedings of the Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, USA, March 2009.

[57] T. Ho, R. Koetter, M. Medard, M. Effros, J. Shi, and D. Karger, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, pp. 4413–4430, October 2006.

[58] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problems of Information Transmission*, vol. 9, no. 3, pp. 177–183, 1973.

[59] D. Hughes-Hartogs, "The capacity of the degraded spectral Gaussian broadcast channel," PhD dissertation, Department of Electrical Engineering, Stanford University, Stanford, CA, 1975.

[60] T. Ignatenko and F. Willems, "On privacy in secure biometric authentication systems," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. II 121–II 124, Honolulu, HI, USA, May 2007.

[61] T. Ignatenko and F. Willems, "Privacy leakage in biometric secrecy systems," in *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, September 2008.

[62] J. Jiang, Y. Xin, and H. K. Garg, "Interference channels with common information," *IEEE Transactions on Information Theory*, vol. 54, pp. 171–187, January 2008.

[63] N. Jindal and A. Goldsmith, "Optimal power allocation for parallel Gaussian broadcast channels with independent and common information," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Chicago, IL, USA, June–July 2004.

[64] W. Kang and G. Kramer, "Broadcast channel with degraded source random variables and receiveride information," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, July 2008.

[65] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in *Proceedings of the Symposium on Applications and the Internet Workshops (SAINT)*, pp. 27–31, Orlando, FL, USA, January 2003.

[66] A. Khisti, S. Diggavi, and G. W. Wornell, "Secret key generation with correlated sources and noisy channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, July 2008.

[67] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, pp. 2453–2469, June 2008.

[68] A. Khisti and G. Wornell, "The MIMOME channel," in *Proceedings of the 45th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, USA, September 2007.

[69] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," in *Proceedings of the IEEE Informaton Theory Workshop (ITW)*, Taormina, Sicily, Italy, October 2009.

[70] M. Kobayashi, Y. Liang, S. Shamai (Shitz), and M. Debbah, "On the compound MIMO broadcast channels with confidential messages," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, June–July 2009.

[71] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, pp. 782–795, October 2003.

[72] J. Körner and K. Marton, "Comparison of two noisy channels," in *Topics in Information Theory*, (I. Csiszár and P. Elias, eds.), pp. 411–423, 1975. Colloquia Mathamatical Society János Bolyai, Amsterdam: North-Holland Publishers, 1977.

[73] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the K-user Gaussian interference channel," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, July 2008.

[74] G. Kramer, "Topics in multi-user information theory," *Foundations and Trends in Communications and Information Theory*, vol. 4, nos. 4–5, pp. 265–444, 2008.

[75] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Transactions on Information Theory*, vol. 51, pp. 3037–3063, September 2005.

[76] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, pp. 4005–4019, September 2008.

[77] 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, pp. 5059–5067, November 2008.

[78] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE Transactions on Information Theory*, vol. 55, pp. 906–916, February 2009.

[79] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems," in *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 23–26, Monticello, IL, USA, September 2008. Also submitted to *IEEE Transactions on Information Theory,* 2008.

[80] L. Lai, S.-W. Ho, and H. V. Poor, "An information theoretic framework for biometric security systems," in *Proceedings of the 3rd IAPR/IEEE International Conference on Biometrics*, Sassari, Italy, June 2009.

[81] S. Lall, "Advanced topics in computation for control," Lecture notes for Engr210b, Stanford University, Fall, 2004.

[82] S. K. Leung-Yan-Cheong, "On a special class of wire-tap channels," *IEEE Transactions on Information Theory*, vol. 23, pp. 625–627, September 1977.

[83] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, pp. 451–456, July 1978.

[84] L. Li and A. J. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels — Part I: Ergodic capacity," *IEEE Transactions on Information Theory*, vol. 47, pp. 1083–1102, March 2001.

[85] L. Li and A. J. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels — Part II: Outage capacity," *IEEE Transactions on Information Theory*, vol. 47, pp. 1103–1127, March 2001.

[86] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, pp. 371–381, February 2003.

[87] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proceedings of the 44th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, USA, September 2006.

[88] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, July 2008.

[89] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," in *Proceedings of the 45th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, USA, September 2007.

[90] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Recent results on compound wire-tap channels," in *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Cannes, France, September 2008.

[91] Y. Liang and H. V. Poor, "Secure communication over fading channels," in *Proceedings of the 44th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, USA, September 2006.

[92] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, pp. 976–1002, March 2008.

[93] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, pp. 2470–2492, June 2008.

[94] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Physical layer security in broadcast networks," *Security and Communication Networks*, vol. 2, pp. 227–238, Wiley, May–June 2009.

[95] Y. Liang, H. V. Poor, and L. Ying, "Wireless broadcast networks: Reliability, security and stability," in *Proceedings of the 3rd Workshop on Information Theory and Applications (ITA)*, La Jolla, CA, USA, January–February 2008.

[96] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai (Shitz), and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Transactions on Information Theory*, vol. 55, pp. 604–619, February 2009.

[97] Y. Liang, V. V. Veeravalli, and H. V. Poor, "Resource allocation for wireless fading relay channels: Max-min solution," *IEEE Transactions on Information Theory, Special Issue on Models, Theory and Codes for Relaying and Cooperation in Communication Networks*, vol. 53, pp. 3432–3453, October 2007.

[98] H. Liao, "Multiple access channels," Ph.D. thesis, Department of Electrical Engineering, University of Hawaii, Honolulu, HI, 1972.

[99] S. Lin and D. J. Costello, *Error Control Coding*, 2nd Edition. Upper Saddle River, NJ, USA: Pearson Education, Inc., 2004.

[100] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, pp. 52–61, Washington DC, USA, 2003.

[101] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wire-tap channels," in *Proceedings of the IEEE Information Theory Workshop (ITW)*, Lake Tahoe, CA, USA, September 2007.

[102] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian broadcast channels with confidential messages," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, June–July 2009. Also submitted to *IEEE Transactions on Information Theory,* 2009.

[103] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proceedings of the 44th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, USA, September 2006.

[104] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, pp. 2493–2507, June 2008.

[105] R. Liu, I. Maric, R. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Seattle, WA, USA, July 2006.

[106] R. Liu and H. V. Poor, "Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, pp. 1235–1249, March 2009.

[107] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of parallel Gaussian compound wiretap channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, July 2008.

[108] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wire-tap channel," *IEEE Transactions on Information Theory*, vol. 55, pp. 2547–2553, June 2009.

[109] T. Liu and P. Viswanath, "An extremal inequality motivated by multiterminal information-theoretic problems," *IEEE Transactions on Information Theory*, vol. 53, pp. 1839–1851, May 2007.

[110] W. Luh and D. Kundur, "Separate enciphering of correlated messages for confidentiality in distributed networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, Washington DC, USA, November 2007.

[111] H. D. Ly, T. Liu, and Y. Liang, “MIMO broadcasting with common, private and confidential messages,” in *Proceedings of the International Symposium on Information Theory and Its Applications (ISITA)*, Auckland, New Zealand, December 2008.

[112] K. Marton, “A coding theorem for the discrete memoryless broadcast channel,” *IEEE Transactions on Information Theory*, vol. 25, pp. 306–311, May 1979.

[113] J. L. Massey, “Contemporary cryptology — An introduction,” in *Contemporary Cryptology — The Science of Information Integrity*, (G. J. Simmons, ed.), Piscataway, NJ, USA: IEEE Press, 1992.

[114] U. Maurer, “Authentication theory and hypothesis testing,” *IEEE Transactions on Information Theory*, vol. 46, pp. 1350–1356, July 2000.

[115] U. M. Maurer, “Provably secure key distribution based on independent channels,” in *Proceedings of the IEEE Information Theory Workshop (ITW)*, Veldhoven, The Netherlands, June 1990.

[116] U. M. Maurer, “Secret-key agreement by public discussion based on common information,” *IEEE Transactions on Information Theory*, vol. 39, pp. 733–742, May 1993.

[117] U. M. Maurer and S. Wolf, “From weak to strong information-theoretic key agreement,” in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, p. 18, Sorrento, Italy, June 2000.

[118] U. M. Maurer and S. Wolf, “Information-theoretic key agreement: From weak to strong secrecy for free,” in *Proceedings of the EUROCRYPT 2000 on Advances in Cryptology*, vol. 1807, pp. 352–368, Lecture Notes in Computer Science, Berlin, Germany: Springer, 2000.

[119] U. M. 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, pp. 822–831, April 2003.

[120] U. M. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels — Part II. Privacy amplification,” *IEEE Transactions on Information Theory*, vol. 49, pp. 832–838, April 2003.

[121] U. M. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels — Part III. Privacy amplification,” *IEEE Transactions on Information Theory*, vol. 49, pp. 839–851, April 2003.

[122] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography.* Boca Raton, FL, USA: CRC Press, 1996.

[123] 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, pp. 2181–2190, May 2006.

[124] 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, 2006.

[125] S. Nitinawarat, “Secret-key generation for correlated Gaussian sources,” in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 702–706, Toronto, Ontario, Canada, July 2008.

[126] S. Nitinawarat, "Secret-key generation for correlated Gaussian sources," in *Proceedings of the 45th Annual Allerton Conference on Communication, Control and Computing*, pp. 1054–1058, Monticello, IL, USA, September 2007.

[127] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wire-tap channel," in *Proceedings of the 45th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, USA, September 2007.

[128] T. Ohira, "Secret-key generation exploiting antenna beam steering and wave propagation reciprocity," in *Proceedings of the European Microwave Conference*, Paris, France, October 2005.

[129] Y. Oohama, "Coding for relay channels with confidential messages," in *Proceedings of the IEEE Information Theory Workshop (ITW)*, pp. 87–89, Cairns, Australia, September 2001.

[130] Y. Oohama, "Relay channels with confidential messages," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 926–930, Nice, France, June 2007. Also submitted to *IEEE Transactions on Information Theory,* 2007. Available at http://arxiv.org/PS_cache/cs/pdf/0611/0611125v7.pdf.

[131] P. Oswald and M. Shokrollahi, "Capacity-achieving sequences for the erasure channel," *IEEE Transactions on Information Theory*, vol. 48, pp. 3017–3028, December 2002.

[132] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell System Technical Journal*, vol. 63, pp. 2135–2157, December 1984.

[133] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 2152–2155, Adelaide, Australia, September 2005.

[134] R. D. Pietro, L. V. Mancini, and S. Jajodia, "Efficient and secure keys management for wireless mobile communications," in *Proceedings of the 2nd ACM International Workshop on Principles of Mobile Computing*, pp. 66–73, Toulouse, France, 2002.

[135] V. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels: A secret key-secret message rate trade-off region," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, July 2008.

[136] V. Prabhakaran and K. Ramchandranr, "On secure distributed source coding," in *Proceedings of the IEEE Information Theory Workshop (ITW)*, Lake Tahoe, CA, USA, September 2007.

[137] V. V. Prelov, "Transmission over a multiple-access channel with a special source heirarchy," *Problems of Information Transmission*, vol. 20, pp. 3–10, October–December 1984.

[138] R. Renner and S. Wolf, "New bounds in secret key agreement: The gap between formation and secrecy extraction," in *Proceedings of the EUROCRYPT on Advances in Cryptography*, pp. 562–577, Lecture notes in Computer Science, Springer-Verlag, 2003.

[139] T. Richardson and R. Urbanke, *Modern Coding Theory.* New York, NY, USA: Cambridge University Press, 2008.

[140] T. J. Richardson and R. Urbanke, “Efficient encoding of low-density parity-check codes,” *IEEE Transactions on Information Theory*, vol. 47, pp. 638–656, February 2001.

[141] U. Rosenbaum, “A lower bound on authentication after having observed a sequence of messages,” *Journal of Cryptology*, vol. 6, no. 3, pp. 135–156, 1993.

[142] H. Sato, “An outer bound to the capacity region of broadcast channels,” *IEEE Transactions on Information Theory*, vol. 24, pp. 374–377, May 1978.

[143] A. Schrijver, *Theory of Linear and Integer Programming.* New York, NY, USA: John Wiley and Sons, 1998.

[144] S. Shafiee, N. Liu, and S. Ulukus, “Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel,” *IEEE Transactions on Information Theory*, submitted in 2007.

[145] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[146] G. J. Simmons, “Authentication theory/coding theory,” in *Proceedings of the CRYPTO’84 on Advances in Cryptography*, pp. 411–431, Lecture Notes in Computer Science, New York, NY, USA: Springer-Verlag, 1985.

[147] D. Slepian and J. K. Wolf, “Noiseless coding of correlated information sources,” *IEEE Transactions on Information Theory*, vol. IT-19, pp. 471–480, 1973.

[148] W. Stallings, *Cryptography and Network Security Principles and Practices.* Upper Saddle River, NJ, USA: Prentice Hall, 3rd ed., 2003.

[149] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, “Interference-assisted secret communication,” in *Proceedings of the IEEE Information Theory Workshop (ITW)*, Porto, Portugal, May 2008.

[150] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, “On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels,” *IEEE Transactions on Information Theory*, vol. 55, pp. 1575–1591, April 2009.

[151] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, “Secret-key sharing based on layered broadcast coding over fading channels,” in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, June–July 2009.

[152] L. Tassiulas and A. Ephremides, “Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks,” *IEEE Transactions on Automatic Control*, vol. 37, no. 12, pp. 1936–1948, 1992.

[153] E. Tekin and A. Yener, “The Gaussian multiple access wire-tap channel,” *IEEE Transactions on Information Theory*, vol. 54, pp. 5747–5755, December 2008.

[154] E. Tekin and A. Yener, “The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming,” *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, pp. 2735–2751, June 2008.

[155] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, “Application of LDPC codes to the wiretap channel,” *IEEE Transactions on Information Theory*, vol. 53, pp. 2933–2945, August 2007.

[156] D. Tse, "A deterministic model for wireless channels and its applications," in *Proceedings of the IEEE Information Theory Workshop (ITW)*, Lake Tahoe, CA, USA, September 2007.

[157] D. N. Tse, "Optimal power allocation over parallel Gaussian broadcast channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, p. 27, Ulm, Germany, June 1997.

[158] E. C. van der Meulen, "Three-terminal communication channels," *Advances in Applied Probability*, vol. 3, pp. 120–154, 1971.

[159] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 43, pp. 712–714, March 1997.

[160] S. Venkatesan and V. Anantharam, "The common randomness capacity of a pair of independent discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 44, pp. 215–224, January 1998.

[161] S. Venkatesan and V. Anantharam, "The common randomness capacity of a network of discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 46, pp. 367–387, March 2000.

[162] M. Walker, "Information theoretic bounds for authentication schemes," *Journal of Cryptology*, vol. 2, no. 3, pp. 131–143, 1990.

[163] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Nice, France, June 2007.

[164] H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, and P. Viswanath, "The capacity region of the degraded MIMO compound broadcast channel," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Nice, France, June 2007.

[165] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Transactions on Information Theory*, vol. 52, pp. 3936–3964, September 2006.

[166] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Transactions on Information Forensics and Security*, pp. 364–375, 2007.

[167] B. Wu, J. Wu, E. B. Ernandez, M. Ilyas, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 30, pp. 937–954, August 2007.

[168] A. D. Wyner, "Recent results in the Shannon theory," *IEEE Transactions on Information Theory*, vol. 20, pp. 2–10, January 1974.

[169] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, October 1975.

[170] A. D. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications: Part I," *IEEE Transactions on Information Theory*, vol. 19, pp. 769–777, November 1973.

[171] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 1520–1524, Beijing, China, May 2008.

[172] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, Submitted in May 2008.

[173] H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Transactions on Information Theory*, vol. 35, pp. 572–578, May 1989.

[174] H. Yamamoto, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Transactions on Information Theory*, vol. 37, pp. 634–638, May 1991.

[175] R. D. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Toronto, Ontario, Canada, July 2008.

[176] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 2133–2137, Adelaide, Australia, September 2005.

[177] C. Ye and P. Narayan, "The secret key-private key capacity region for three terminals," in *Proceedings of the 39th Annual Conference on Information Scienes and Systems (CISS)*, Baltimore, MD, USA, 2005.

[178] C. Ye and P. Narayan, "The secret key-private key capacity region for three terminals," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 2142–2146, Adelaide, Australia, September 2005.

[179] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, "Network coding theory: Multiple sources," *Foundations and Trends in Communications and Information Theory*, vol. 2, no. 5, pp. 241–381, 2005.

[180] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, "Network coding theory: Single sources," *Foundations and Trends in Communications and Information Theory*, vol. 2, no. 4, pp. 241–381, 2005.

[181] S. Yi and R. Kravets, "Composite key management for ad hoc networks," in *Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous)*, pp. 52–61, Boston, MA, USA, August 2004.

[182] R. Zamir, S. Shamai (Shitz), and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Transactions on Information Theory*, vol. 48, pp. 1250–1276, June 2002.

[183] Y. Zhong, F. Alajaji, and L. L. Campbell, "Error exponents for asymmetric two-user discrete memoryless source-channel coding systems," *IEEE Transactions on Information Theory*, vol. 55, pp. 1497–1518, April 2009.

[184] B. Zhu, F. Bao, R. H. Deng, M. S. Kankanhalli, and G. Wang, "Efficient and robust key management for large mobile ad hoc networks," *Computer Networks*, vol. 48, pp. 657–682, July 2005.

[185] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach," in *Proceedings of the 11th IEEE International Conference on Network Protocols*, pp. 326–335, Atlanta, GA, USA, November 2003.