Multiterminal Secrecy by Public Discussion

Prakash Narayan
University of Maryland, College Park
prakash@umd.edu

Himanshu Tyagi
Indian Institute of Science, Bangalore
htyagi@ece.iisc.ernet.in

the essence of knowledge
Boston — Delft

Foundations and Trends® in Communications and Information Theory

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
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

P. Narayan and H. Tyagi. *Multiterminal Secrecy by Public Discussion*. Foundations and Trends® in Communications and Information Theory, vol. 13, no. 2-3, pp. 129–275, 2016.

This Foundations and Trends® issue was typeset in LaTeX using a class file designed by Neal Parikh. Printed on acid-free paper.

ISBN: 978-1-68083-187-0

Foundations and Trends® in Communications and Information Theory

Volume 13, Issue 2-3, 2016

Editorial Board

Editorial Scope

Topics

Foundations and Trends® in Communications and Information Theory publishes 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, 2016, Volume 13, 4 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. 13, No. 2-3 (2016) 129–275

DOI: 10.1561/0100000072

the essence of knowledge

Multiterminal Secrecy by Public Discussion

Prakash Narayan
University of Maryland, College Park
prakash@umd.edu

Himanshu Tyagi
Indian Institute of Science, Bangalore
htyagi@ece.iisc.ernet.in

Contents

Abstract

This monograph describes principles of information theoretic secrecy generation by legitimate parties with public discussion in the presence of an eavesdropper. The parties are guaranteed secrecy in the form of independence from the eavesdropper's observation of the communication.

Part I develops basic technical tools for secrecy generation, many of which are potentially of independent interest beyond secrecy settings. Various information theoretic and cryptographic notions of secrecy are compared. Emphasis is placed on central themes of interactive communication and common randomness as well as on core methods of balanced coloring and leftover hash for extracting secret uniform randomness. Achievability and converse results are shown to emerge from "single shot" incarnations that serve to explain essential structure.

Part II applies the methods of Part I to secrecy generation in two settings: a multiterminal source model and a multiterminal channel model, in both of which the legitimate parties are afforded privileged access to correlated observations of which the eavesdropper has only partial knowledge. Characterizations of secret key capacity bring out inherent connections to the data compression concept of omniscience and, for a specialized source model, to a combinatorial problem of maximal spanning tree packing in a multigraph. Interactive common information is seen to govern the minimum rate of communication needed to achieve secret key capacity in the two-terminal source model. Furthermore, necessary and sufficient conditions are analyzed for the secure computation of a given function in the multiterminal source model.

Based largely on known recent results, this self-contained monograph also includes new formulations with associated new proofs. Supplementing each chapter in Part II are descriptions of several open problems.

P. Narayan and H. Tyagi. *Multiterminal Secrecy by Public Discussion*. Foundations and Trends® in Communications and Information Theory, vol. 13, no. 2-3, pp. 129–275, 2016.
DOI: 10.1561/0100000072.

1

Introduction

Information theoretic cryptography is founded on the principle of guaranteeing legitimate users provable data security from an adversary with unlimited computational power. Such an unconditional guarantee of security assures secrecy in the form of statistical independence (or near-independence) from the adversary's observations. This is accomplished, however, by giving the legitimate users a hearty leg up. By comparison, most existing cryptosystems for data security are based on the concept of computational complexity. The latter form of security rests on the infeasibility of existing mathematical and computational techniques in solving "hard" underlying computational problems, for instance, inverting specific functions.

Information theoretic perfect secrecy, introduced by Claude Shannon [72], constitutes the strongest definition of data security. It requires independence of a secret from the adversary's observations. A practically acceptable relaxation to near-independence ensures negligible information leakage to the adversary. Taken together with resources for the legitimate parties that lend them a decided advantage over the adversary, it leads to a rich theory raring for application.

In this monograph, we consider secrecy generation with public communication by multiple legitimate parties in two settings: a multiterminal source model and a multiterminal channel model. In both models, the legitimate parties are given privileged access to correlated observations that are only partially available to the eavesdropper. Our primary focus is on the former model.

The multiterminal source model consists of $m \geqslant 2$ terminals with prior access to correlated observations, and the means to communicate interactively among themselves over a public and noiseless broadcast medium of unlimited capacity. In the multiterminal channel model, a subset of k terminals, $1 \leqslant k \leqslant m-1$, govern the inputs of a noisy but secure transmission channel with the remaining $m-k$ terminals receiving the channel outputs. In between transmissions over the secure channel, all the terminals additionally can communicate among themselves publicly as in the source model. In both models, a passive adversary can eavesdrop on the communication among the terminals but cannot tamper with it, *i.e.*, the communication is authenticated. In the setting of each model, the primary goal is to generate a secret key of optimal length for all the m terminals under the requirement of information theoretic secrecy from the eavesdropped communication. We also consider secure function computation by trusted computing parties for a multiterminal source model under a similar secrecy constraint.

We do not address "wiretap channel" secrecy, launched in seminal works [98, 17], that entails secure transmission of messages over insecure channels which are wiretapped by an adversary; this is chronicled in [49, 19, 65]. Also, the classical multiterminal (information theoretically) secure function computation problem where the parties themselves are not trusted is not considered here; it has a substantial literature (cf. [46, 15, 95, 25, 58, 40, 96, 93, 94, 3, 87]).

This self-contained monograph is written in the language of information theory and aims to appeal as well to the cryptographer. To this end, we have strived to emphasize its following distinctive features: Comparison of various information theoretic and cryptographic notions of secrecy; bringing out of the significance – in distributed cooperative secrecy generation – of central themes of interactive communication and the common randomness or shared bits thereby created; and a presentation of "single-shot" results with a minimum of statistical assumptions (beyond knowledge of a joint distribution of pertinent random variables). Such a single-shot analysis, redolent of standard practice in cryptography, lies at the heart of information theoretic coding theorems. Also, by virtue of their lean and not mean but essential form, these results are of potential significance for models beyond those considered here.

Although this monograph largely treats known recent results, adherence to a consistency of themes has engendered also new formulations with associated new proofs. Our effort is to be viewed as a complement to the rich chapter on information theoretic security in [19] as well as jaunts in new directions.

Organization

Part I consists of Chapters 2 - 5 that deal with basic technical tools for secrecy generation. Many of these tools are potentially of independent interest beyond secrecy applications. Part II contains Chapters 6 - 9 that apply the methods of Part I to secrecy generation for the multiterminal source and channel models. In order to maintain a smooth flow of presentation, credits are provided only at the end of each chapter in a story of results a la [19]. The list of references is representative but not exhaustive. Supplementing the credits in Chapters 6 - 9 are descriptions of open problems.

Beginning with rudiments, Chapter 2 describes secrecy indices for a key with their operational meanings, as well as secrecy indices for a message and relationships among the latter. Turning to basic methods, Chapter 3 deals with the central concepts of interactive communication among multiple terminals and the common randomness generated thereby; a fundamental structural property of interactive communication and single-shot converse upper bounds for the ensuing common randomness are derived. The concept of a secret key is introduced formally in Chapter 4, and suitable upper bounds on its length are obtained by means of two different converse techniques: bounding the entropy of common randomness and through the error exponent of conditional independence hypothesis testing. The notion of shared information is introduced as an upper bound for the length of a secret key; shared information has a potential role as a measure of mutual dependence among $m \geqslant 2$ random variables. Chapter 5 describes two achievability approaches – balanced coloring and leftover hash – for extracting uniform randomness from a given random variable with near independence from another random variable. These methods pave the way for extracting a secret key from common randomness by means of public communication.

Chapter 6 addresses secret key generation for the multiterminal source model in which each terminal observes one component of a discrete memoryless multiple source. A single-letter characterization of secret key capacity is obtained on the strength of an inherent link to a data compression problem of "omniscience" without secrecy constraints. This capacity is seen as being equal to shared information, thereby imbuing the latter with an operational meaning. Secret key generation for a special "pairwise independent network" model reveals connections to a combinatorial problem of maximal packing of spanning trees in a multigraph. For the two-terminal source model, the minimum rate of interactive communication needed to generate an optimal rate secret key is addressed in Chapter 7, and is shown to be related to a new interactive variant of Wyner's common information. Chapter 8 examines conditions that enable a special form of secrecy generation for the multiterminal source model: secure function computation in which multiple terminals compute a given function of the collective data at the terminals using public communication that does not reveal the function value. The closing Chapter 9 studies secret key generation for the multiterminal channel model in which one subset of the terminals are connected to the remaining terminals by a secure discrete memoryless multiaccess channel. While a general single-letter characterization of secret key capacity remains open, in the special case of a channel with a single output terminal, interesting connections are shown between secrecy capacity and the transmission capacity region of the multiple access channel with and without feedback.

A note: All the random variables (rvs) throughout this monograph take values in finite sets, with known joint probability mass functions (pmfs). Probabilities of events involving rvs X, Y will be denoted by P_{XY}, $P_{X|Y}$, *etc.*, and by a general $\mathbb{P}$ when appropriate.

References

[1] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography–Part I: Secret sharing. *IEEE Trans. Inf. Theory*, 39(4):1121–1132, July 1993.

[2] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography–Part II: CR capacity. *IEEE Trans. Inf. Theory*, 44(1):225–240, January 1998.

[3] R. Ahlswede and I. Csiszár. On oblivious transfer capacity. *Information Theory, Combinatorics, and Search Theory*, pages 145–166, 2013.

[4] K. Audenaert. A sharp Fannes-type inequality for the von Neumann entropy. *Physical Review A*, 40:8127–8136, 2007. arXiv:quant-ph/0610146.

[5] M. Bellare, S. Tessaro, and A. Vardy. *Semantic Security for the Wiretap Channel*, pages 294–311. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[6] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41(6):1915–1923, November 1995.

[7] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17(2):210–229, 1988.

[8] M. Braverman. Coding for interactive computation: progress and challenges. *Proc. Conference on Communication, Control, and Computing (Allerton)*, pages 1914–1921, October 2012.

[9] N.J. Cerf, S. Massar, and S. Schneider. Multipartite classical and quantum secrecy monotones. *Physical Review A*, 66(4):042309, October 2002.

[10] C. Chan. Generating secret in a network. *Ph. D. Dissertation, Massachussetts Institute of Technology*, 2010.

[11] C. Chan. Linear perfect secret key agreement. In *Proc. Information Theory Workshop (ITW)*, pages 723–726, October 2011.

[12] C. Chan. Agreement of a restricted secret key. *Proc. IEEE International Symposium on Information Theory*, pages 1782–1786, July 2012.

[13] C. Chan and L. Zheng. Mutual dependence for secret key agreement. *Proc. Annual Conference on Information Sciences and Systems (CISS)*, March 2010.

[14] T.A. Courtade and T.R. Halford. Coded cooperative data exchange for a secret key. *IEEE Trans. Inf. Theory*, 62(7):3785–3795, July 2016.

[15] C. Crépeau and J. Kilian. *Weakening Security Assumptions and Oblivious Transfer*, pages 2–7. Springer New York, New York, NY, 1990.

[16] I. Csiszár. Almost independence and secrecy capacity. *Prob. Pered. Inform.*, 32(1):48–57, 1996.

[17] I Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[18] I. Csiszár and J. Körner. Towards a general theory of source networks. *IEEE Trans. Inf. Theory*, 26(2):155–165, March 1980.

[19] I. Csiszár and J. Körner. *Information theory: Coding theorems for discrete memoryless channels. 2nd edition.* Cambridge University Press, 2011.

[20] I. Csiszár and P. Narayan. Common randomness and secret key generation with a helper. *IEEE Trans. Inf. Theory*, 46(2):344–366, March 2000.

[21] I. Csiszár and P. Narayan. Secrecy capacities for multiple terminals. *IEEE Trans. Inf. Theory*, 50(12):3047–3061, December 2004.

[22] I. Csiszár and P. Narayan. Secrecy capacities for multiterminal channel models. *IEEE Trans. Inf. Theory*, 54(6):2437–2452, June 2008.

[23] I. Csiszár and P. Narayan. Secrecy generation for multiaccess channel models. *IEEE Trans. Inf. Theory*, 59(1):17–31, January 2013.

[24] S. Fehr and S. Berens. On the conditional Rényi entropy. *IEEE Trans. Inf. Theory*, 60(11):6801–6810, November 2014.

[25] M. Fitzi, S. Wolf, and J. Wullschleger. *Pseudo-signatures, Broadcast, and Multi-party Computation from Correlated Randomness*, pages 562–578. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[26] A. El Gamal and A. Orlitsky. Interactive data compression. In *Proc. Annual Symposium on Foundations of Computer Science*, pages 100–108, October 1984.

[27] A. Gohari, M.H. Yassaee, and M.R. Aref. Secure channel simulation. In *Information Theory Workshop (ITW)*, pages 406–410, September 2012.

[28] A. A. Gohari and V. Anantharam. Information-theoretic key agreement of multiple terminals - Part I. *IEEE Trans. Inf. Theory*, 56(8):3973 – 3996, August 2010.

[29] A. A. Gohari and V. Anantharam. Information-theoretic key agreement of multiple terminals - Part II: Channel model. *IEEE Trans. Inf. Theory*, 56(8):3997 – 4010, August 2010.

[30] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270 – 299, 1984.

[31] D. Gunduz, E. Erkip, and H.V. Poor. Lossless compression with security constraints. *Proc. IEEE International Symposium on Information Theory*, pages 111–115, July 2008.

[32] Y. Liang H. Zhang, L. lai and H. Wang. The capacity region of the source-type model for secret key and private key generation. *IEEE Trans. Inf. Theory*, 60(10):6389–6398, October 2014.

[33] T. S. Han. *Information-Spectrum Methods in Information Theory [English Translation]*. Series: Stochastic Modelling and Applied Probability, Vol. 50, Springer, 2003.

[34] T. S. Han and K. Kobayashi. A unified achievable rate region for a general class of multiterminal source coding systems. *IEEE Trans. Inf. Theory*, 26(3):277–288, May 1980.

[35] T. S. Han and S. Verdú. Approximation theory of output statistics. *IEEE Trans. Inf. Theory*, 39(3):752–772, May 1993.

[36] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28:12–24, 1999.

[37] M. Hayashi. Exponential decreasing rate of leaked information in universal random privacy amplification. *IEEE Trans. Inf. Theory*, 57(6):3989–4001, June 2011.

[38] M. Hayashi, H. Tyagi, and S. Watanabe. Secret key agreement: General capacity and second-order asymptotics. *Proc. IEEE International Symposium on Information Theory*, pages 1136–1140, July 2014.

[39] M. Hayashi, H. Tyagi, and S. Watanabe. Secret key agreement: General capacity and second-order asymptotics. *IEEE Trans. Inf. Theory*, 62(7), May 2016.

[40] H. Imai, K. Morozov, A. C. Nascimento, and A. Winter. Efficient protocols achieving the commitment capacity of noisy correlations. *Proc. IEEE International Symposium on Information Theory*, pages 1432–1436, 2006.

[41] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proc. ACM Symposium on Theory of Computing*, pages 12–24, 1989.

[42] R. Impagliazzo and D. Zuckerman. How to recycle random bits. In *Proc. Annual Symposium on Foundations of Computer Science*, pages 248–253, November 1989.

[43] M. Iwamoto and K. Ohta. Security notions for information theoretically secure encryptions. *Proc. IEEE International Symposium on Information Theory*, pages 1777–1781, July 2011.

[44] A. H. Kaspi. Two-way source coding with a fidelity criterion. *IEEE Trans. Inf. Theory*, 31(6):735–740, November 1985.

[45] J. Katz and Y. Lindell. *Introduction to Modern Cryptography.* Chapman & Hall/CRC, 2007.

[46] J. Kilian. Founding crpytography on oblivious transfer. In *Proc. Symposium on Theory of Computing*, pages 20–31, 1988.

[47] R. Konig, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory*, 55(9):4337 – 4347, September 2009.

[48] S. K. Leung-Yan-Cheong. Multi-user and wiretap channels including feedback. *Ph. D. Dissertation, Stanford University*, 1976.

[49] Y. Liang, H. V. Poor, and S. Shamai (Shitz). Information theoretic security. *Found. Trends Commun. Inf. Theory*, 5(4-5):355–580, April 2009.

[50] J. Liu, P. Cuff, and S. Verdú. Common randomness and key generation with limited interaction. *CoRR*, abs/1601.00899v2, 2016.

[51] M. Madiman and P. Tetali. Information inequalities for joint distributions, with interpretations and applications. *IEEE Trans. Inf. Theory*, 56(6):2699–2713, June 2010.

[52] J. L. Massey. An introduction to contemporary cryptology. *Proc. the IEEE*, 76(5):533–549, 1988.

[53] U. M. Maurer. Provably secure key distribution based on independent channels. *IEEE Information Theory Workshop (ITW)*, pages 49–71, June 1990.

[54] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, 39(3):733–742, May 1993.

[55] M. Mukherjee, C. Chan, N. Kashyap, and Q. Zhou. Bounds on the communication rate needed to achieve SK capacity in the hypergraphical source model. *CoRR*, arXiv:1601.05377v2, 2016.

[56] M. Mukherjee and N. Kashyap. On the communication complexity of secret key generation in the multiterminal source model. *Proc. IEEE Symposium on Information Theory*, June 2014.

[57] M. Mukherjee, N. Kashyap, and Y. Sankarasubramaniam. On the public communication needed to achieve SK capacity in the multiterminal source model. *CoRR*, abs/1507.02874, 2015.

[58] A.C.A. Nascimento and A. Winter. On the oblivious transfer capacity of noisy correlations. *Proc. IEEE International Symposium on Information Theory*, pages 1871–1875, July 2009.

[59] S. Nitinawarat and P. Narayan. Perfect omniscience, perfect secrecy, and Steiner tree packing. *IEEE Trans. Inform. Theory*, 56(12):6490 – 6500, December 2010.

[60] S. Nitinawarat and P. Narayan. Secret key generation for correlated Gaussian sources. *IEEE Trans. Inf. Theory*, 58(6):3373–3391, June 2012.

[61] S. Nitinawarat, C. Ye, A.Barg, P. Narayan, and A. Reznik. Secret key generation for a pairwise independent network model. *IEEE Trans. Inform. Theory*, 56(12):6482 – 6489, December 2010.

[62] A. Orlitsky. Worst-case interactive communication I: Two messages are almost optimal. *IEEE Trans. Inf. Theory*, 36(5):1111–1126, September 1990.

[63] A. Orlitsky and A. El Gamal. Communication with secrecy constraints. In *Proc. ACM Symposium on Theory of Computing*, pages 217–224, October 1984.

[64] V. Prabhakaran and K. Ramchandran. On secure distributed source coding. In *IEEE Information Theory Workshop (ITW)*, pages 442–447, September 2007.

[65] P. A. Regalia, A. Khisti, Y. Liang, and S. Tomasin (editors). Secure communications via physical-layer and information-theoretic techniques. *Proc. the IEEE*, 103(10), October 2015.

[66] R. Renner. Security of quantum key distribution. *Ph. D. Dissertation, ETH Zurich*, 2005.

[67] R. Renner and S. Wolf. *New Bounds in Secret-Key Agreement: The Gap between Formation and Secrecy Extraction*, pages 562–577. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[68] R. Renner and S. Wolf. Smooth Rényi entropy and applications. *Proc. IEEE International Symposium on Information Theory*, page 233, June 2004.

[69] R. Renner and S. Wolf. *Simple and Tight Bounds for Information Reconciliation and Privacy Amplification*, pages 199–216. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[70] M. Santha and U. V. Vazirani. Generating quasi-random sequences from slightly-random sources. In *Proc. Annual Symposium on Foundations of Computer Science*, pages 434–440, October 1984.

[71] M. Santha and U. V. Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of Computer and System Sciences*, 33(1):75 – 87, 1986.

[72] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, October 1949.

[73] R. Tandon, S. Ulukus, and K. Ramchandran. Secure source coding with a helper. *Proc. Conference on Communication, Control, and Computing (Allerton)*, pages 1061–1068, October 2009.

[74] H. Tyagi. Distributed computing with privacy. *Proc. IEEE International Symposium on Information Theory*, pages 1157–1161, July 2012.

[75] H. Tyagi. Common information and secret key capacity. *IEEE Trans. Inf. Theory*, 59(9):5627–5640, September 2013.

[76] H. Tyagi. Common randomness principles of secrecy. *Ph. D. Dissertation, Univeristy of Maryland, College Park*, 2013.

[77] H. Tyagi. Distributed function computation with confidentiality. *IEEE Journal on Selected Areas in Communications*, 31(4):691–701, April 2013.

[78] H. Tyagi, N. Kashyap, Y. Sankarasubramaniam, and K. Viswanathan. Fault-tolerant secret key generation. *Proc. IEEE International Symposium on Information Theory*, pages 1787–1791, July 2012.

[79] H. Tyagi and P. Narayan. How many queries will resolve common randomness? *IEEE Trans. Inf. Theory*, 59(9):5363–5378, September 2013.

[80] H. Tyagi and P. Narayan. How many queries will resolve common randomness? *Proc. IEEE International Symposium on Information Theory*, pages 3165–3169, July 2013.

[81] H. Tyagi, P. Narayan, and P. Gupta. Secure computing. *Proc. IEEE International Symposium on Information Theory*, pages 2612–2616, June 2010.

[82] H. Tyagi, P. Narayan, and P. Gupta. When is a function securely computable? *Proc. IEEE International Symposium on Information Theory*, pages 2876–2880, August 2011.

[83] H. Tyagi, P. Narayan, and P. Gupta. When is a function securely computable? *IEEE Trans. Inf. Theory*, 57(10):6337–6350, October 2011.

[84] H. Tyagi and S. Watanabe. Secret key capacity for multiple access channel with public feedback. *Proc. Conference on Communication, Control, and Computing (Allerton)*, pages 1–7, October 2013.

[85] H. Tyagi and S. Watanabe. *A Bound for Multiparty Secret Key Agreement and Implications for a Problem of Secure Computing*, pages 369–386. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.

[86] H. Tyagi and S. Watanabe. Unpublished notes. 2014.

[87] H. Tyagi and S. Watanabe. Converses for secret key agreement and secure computing. *IEEE Trans. Inf. Theory*, 61:4809–4827, September 2015.

[88] S. P. Vadhan. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science*, 7:1–336, 2012.

[89] S. Vembu and S. Verdú. Generating random bits from an arbitrary source: Fundamental limits. *IEEE Trans. Inf. Theory*, 41(5):1322–1332, Sep. 1995.

[90] J. von Neumann. Various techniques used in connection with random digits. 1963.

[91] Y. Wang and P. Ishwar. On unconditionally secure multi-party sampling from scratch. *Proc. IEEE Symposium on Information Theory (ISIT)*, pages 1782–1786, July 2011.

[92] S. Watanabe and Y. Oohama. Secret key agreement from vector Gaussian sources by rate limited public communication. *Information Forensics and Security, IEEE Transactions on*, 6(3):541–550, September 2011.

[93] S. Winkler and J. Wullschleger. *On the Efficiency of Classical and Quantum Oblivious Transfer Reductions*, pages 707–723. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[94] S. Winkler and J. Wullschleger. On the efficiency of classical and quantum secure function evaluation. *IEEE Trans. Inf. Theory*, 60(6):3123–3143, June 2014.

[95] A. Winter, A.C.A. Nascimento, and H. Imai. *Commitment Capacity of Discrete Memoryless Channels*, pages 35–51. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[96] S. Wolf and J. Wullschleger. New monotones and lower bounds in unconditional two-party computation. *IEEE Trans. Inf. Theory*, 54(6):2792–2797, June 2008.

[97] A. D. Wyner. Recent results in the Shannon theory. *IEEE Trans. Inf. Theory*, 20(1):2–10, January 1974.

[98] A. D. Wyner. The wiretap channel. *Bell System Technical Journal*, 54(8):1355–1367, October 1975.

[99] A. D. Wyner, J. K. Wolf, and F. M. J. Willems. Communicating via a processing broadcast satellite. *IEEE Trans. Inf. Theory*, 48(6):1243–1249, June 2002.

[100] A. C. Yao. Some complexity questions related to distributive computing. *Proc. Annual Symposium on Theory of Computing*, pages 209–213, 1979.

[101] C. Ye and P. Narayan. The secret key-private key capacity region for three terminals. *Proc. IEEE International Symposium on Information Theory*, pages 2142–2146, September 2005.

[102] C. Ye and P. Narayan. Secret key and private key constructions for simple multiterminal source models. *IEEE Trans. Inf. Theory*, 58(2):639–651, February 2012.

[103] C. Ye and A. Reznik. Group secret key generation algorithms. *Proc. IEEE International Symposium on Information Theory*, pages 2596–2600, June 2007.

[104] Z. Zhang. Estimating mutual information via Kolmogorov distance. *IEEE Trans. Inf. Theory*, 53(9):3280–3282, September 2007.