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

Full text available at: http://dx.doi.org/10.1561/0100000072
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.
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

1 Introduction 2

1 Basic Tools 7

2 Notions of Secrecy and Their Relationships 8
  2.1 Information theoretic secrecy 8
  2.2 Secrecy of a key 10
  2.3 Secrecy of a message 15
  2.4 Secure transmission with one-time pad 19
  2.5 Story of results 21

3 Interactive Communication and Common Randomness 23
  3.1 Interactive communication and properties 24
  3.2 Common randomness 27
  3.3 Story of results 30

4 Secret Key Generation 32
  4.1 Multiterminal secret key 33
  4.2 Upper bounds for secret key length 35
  4.3 Story of results 46
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.

DOI: 10.1561/0100000072.

Full text available at: http://dx.doi.org/10.1561/0100000072
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 \( m \geq 2 \) 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, \( 1 \leq k \leq m - 1 \), 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 commu-
nication 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 in-
formation 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 \( m \geq 2 \) 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


[53] U. M. Maurer. Provably secure key distribution based on independent

[54] U. M. Maurer. Secret key agreement by public discussion from common

[55] M. Mukherjee, C. Chan, N. Kashyap, and Q. Zhou. Bounds on the com-
unication rate needed to achieve SK capacity in the hypergraphical

[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 pub-
lic communication needed to achieve SK capacity in the multiterminal

[58] A.C.A. Nascimento and A. Winter. On the oblivious transfer capacity
of noisy correlations. Proc. IEEE International Symposium on Infor-

[59] S. Nitinawarat and P. Narayan. Perfect omniscience, perfect secrecy,
6500, December 2010.

2012.

generation for a pairwise independent network model. IEEE Trans.

[62] A. Orlitsky. Worst-case interactive communication I: Two messages are
1990.


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

communications via physical-layer and information-theoretic tech-
niques. Proc. the IEEE, 103(10), October 2015.


