CCIT Report #884 April 2015

A Large Deviations Approach to Secure Lossy Compression

Nir Weinberger and Neri Merhav
Dept. of Electrical Engineering
Technion - Israel Institute of Technology
Technion City, Haifa 3200004, Israel
{nirwein@tx, merhav@ee}.technion.ac.il

Abstract

We consider a Shannon cipher system for memoryless sources, in which distortion is allowed at the legitimate decoder. The source is compressed using a rate distortion code secured by a shared key, which satisfies a constraint on the compression rate, as well as a constraint on the exponential rate of the excess-distortion probability at the legitimate decoder. Secrecy is measured by the exponential rate of the exiguous-distortion probability at the eavesdropper, rather than by the traditional measure of equivocation. We define the perfect secrecy exponent as the maximal exiguous-distortion exponent achievable when the key rate is unlimited. Under limited key rate, we prove that the maximal achievable exiguous-distortion exponent is equal to the minimum between the average key rate and the perfect secrecy exponent, for a fairly general class of variable key rate codes.

Index Terms

Information-theoretic secrecy, Shannon cipher system, secret key, cryptography, lossy compression, rate-distortion theory, error exponent, large-deviations, covering lemmas.

I. Introduction

In his seminal paper [1], Shannon has introduced a mathematical framework for secret communication. The cipher system is considered *perfectly secure* if the cryptogram and the message are statistically independent, and so, an eavesdropper does not gain any information when he observes the cryptogram. To achieve secrecy, the sender and the legitimate recipient share a secret key, which is used to encipher and decipher the message. It is rather apparent from ordinary compression [2] that a necessary and sufficient condition for perfect secrecy is that the available key rate is larger than the information rate required to compress the source (the entropy or rate-distortion function of the source in case of lossless or lossy compression, respectively). Usually, the supply of key bits is a

This work was supported by the Israel Science Foundation (ISF), grant no. 412/12.