CCIT Report #800 December 2011

Perfectly Secure Encryption of Individual Sequences *

Neri Merhav

Department of Electrical Engineering
Technion - Israel Institute of Technology
Technion City, Haifa 32000, ISRAEL
E–mail: merhav@ee.technion.ac.il

Abstract

In analogy to the well–known notion of finite–state compressibility of individual sequences, due to Lempel and Ziv, we define a similar notion of "finite–state encryptability" of an individual plaintext sequence, as the minimum asymptotic key rate that must be consumed by finite–state encrypters so as to guarantee perfect secrecy in a well–defined sense. Our main basic result is that the finite–state encryptability is equal to the finite–state compressibility for every individual sequence. This is in parallelism to Shannon's classical probabilistic counterpart result, asserting that the minimum required key rate is equal to the entropy rate of the source. However, the redundancy, defined as the gap between the upper bound (direct part) and the lower bound (converse part) in the encryption problem, turns out to decay at a different rate (in fact, much slower) than the analogous redundancy associated with the compression problem. We also extend our main theorem in several directions, allowing: (i) availability of side information (SI) at the encrypter/decrypter/eavesdropper, (ii) lossy reconstruction at the decrypter, and (iii) the combination of both lossy reconstruction and SI, in the spirit of the Wyner–Ziv problem.

Index Terms: Information–theoretic security, Shannon's cipher system, secret key, perfect secrecy, individual sequences, finite–state machine, compressibility, incremental parsing, Lempel–Ziv algorithm, side information.

1 Introduction

The paradigm of individual sequences and finite–state machines (FSMs), as an alternative to the traditional probabilistic modeling of sources and channels, has been studied and explored quite extensively in several information–theoretic problem areas, including data compression [5], [13], [14], [18], [21], [24], [26], [27], [30], source/channel simulation [9], [15], classification [29], [31],

*This research was supported by ISF grant no. 208/08.