CCIT Report #530
May 2005

On the Shannon Cipher System with a Capacity–Limited Key–Distribution Channel

Neri Merhav

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

Abstract

We consider the Shannon cipher system in a setting where the secret key is delivered to the legitimate receiver via a channel with limited capacity. For this setting, we characterize the achievable region in the space of three figures of merit: the security (measured in terms of the equivocation), the compressibility of the cryptogram, and the distortion associated with the reconstruction of the plaintext source. Although lossy reconstruction of the plaintext does not rule out the option that the (noisy) decryption key would differ, to a certain extent, from the encryption key, we show, nevertheless, that the best strategy is to strive for perfect match between the two keys, by applying reliable channel coding to the key bits, and to control the distortion solely via rate–distortion coding of the plaintext source before the encryption. In this sense, our result has a flavor similar to that of the classical source–channel separation theorem. Some variations and extensions of this model are discussed as well.

Index Terms: Shannon cipher system, key distribution, encryption, cryptography, source–channel separation.

1 Introduction

In the classical Shannon–theoretic approach to cryptology (see, e.g., [6],[4],[10] and references therein), two assumptions are traditionally made. The first is that the reconstruction of the decrypted plaintext source at the legitimate receiver is distortion–free (or almost distortion–free), and the second, which is related, is that the encryption and the decryption units share identical copies of the same key. Yamamoto [11] has relaxed the first assumption and extended the theory of Shannon secrecy systems into a rate–distortion scenario, allowing lossy reconstruction at the legtimate receiver.