CCIT Report No. 374

A Large-Deviations Notion of Perfect Secrecy

Neri Merhav

ABSTRACT

We consider the Shannon cipher system with a variable key rate, and study the necessary and sufficient conditions for perfect secrecy in the sense that the exponential rate of the probability of breaking into the system would not be improved by observing the cryptogram. For a memoryless plaintext source, we derive achievable lower bounds on the number of key bits needed for *almost every plaintext sequence* in every type class. The corresponding minimum achievable average key rate turns out to be the negative logarithm of the probability of the most likely plaintext letter, which is in general, smaller than the entropy.

Index Terms: Shannon cipher system, cryptography, cryptanalysis.