CCIT Report #604
November 2006

# Shannon's Secrecy System With Informed Receivers and its Application to Systematic Coding for Wiretapped Channels

Neri Merhav

November 23, 2006

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

### Abstract

Shannon's secrecy system is studied in a setting, where both the legitimate decoder and the wiretapper have access to side information sequences correlated to the source, but the wiretapper receives both the coded information and the side information via channels that are more noisy than the respective channels of the legitmate decoder, which in turn, also shares a secret key with the encoder. A single–letter characterization is provided for the achievable region in the space of five figures of merit: the equivocation at the wiretapper, the key rate, the distortion of the source reconstruction at the legitimate receiver, the bandwidth expansion factor of the coded channels, and the average transmission cost (generalized power). Beyond the fact that this is an extension of earlier studies, it also provides a framework for studying fundamental performance limits of systematic codes in the presence of a wiretap channel. The best achievable performance of systematic codes is then compared to that of a general code in several respects, and a few examples are given.

**Index Terms:** wiretap channel, encryption, Shannon's cipher system, separation theorem, systematic codes.