ON BLIND COMPRESSION OF ENCRYPTED DATA APPROACHING THE SOURCE (WedAmOR9)

Author(s) :

Daniel Schonberg (UC Berkeley, United States)
Stark Draper (UC Berkeley, United States)
Kannan Ramchandran (UC Berkeley, United States)

Abstract :

Traditional data transmission over an insecure noiseless channel consists of first compressing data for efficiency and then encrypting it for security. Reversing the order of these operations is considered in Johnson et al. The central realization is that while the raw and encrypted data are statistically independent, the encrypted data and key sequence are not. If distributed source coding techniques are used to compress and to jointly decode and decrypt the data, reversing the order need not lead to performance reductions in either communication efficiency or security. In this paper, we build on this work by considering systems that must operate without knowledge of the underlying source statistics. We present and analyze an incremental scheme based on exponentially increasing block lengths that is designed to balance the resolution rate of parameter estimation with the redundancy rate of communication. We show that the redundancy at best declines proportional to the inverse of the square root of the block length. We implement these ideas using low−density parity check (LDPC) codes. In practical tests to transmit a binary source of 100,000 bits, ideally compressible to 17,912 bits with perfect knowledge and an ideal code, required only 26,787 bits.
[continued on the next page]

ON BLIND COMPRESSION OF ENCRYPTED DATA APPROACHING THE SOURCE (WedAmOR9)

* Author(s) :	Daniel Schonberg	(UC Berkeley, United States)
	Stark Draper	(UC Berkeley, United States)
	Kannan Ramchandran	(UC Berkeley, United States)

* Abstract : (cont.)	In comparison, to transmit this source with full knowledge of the source statistics required 21,704 bits.