Cryptology ePrint Archive: Report 2011/106

Common Randomness and Secret Key Capacities of Two-way Channels

Hadi Ahmadi and Reihaneh Safavi-Naini

Abstract: Common Randomness Generation (CRG) and Secret Key Establishment (SKE) are fundamental primitives that are used in information-theoretic coding and cryptography. We study these two problems over the two-way channel model of communication, introduced by Shannon. In this model, the common randomness (CK) capacity is defined as the maximum number of random bits per channel use that the two parties can generate. The secret key (SK) capacity is defined similarly when the random bits are also required to be secure against a passive adversary. We provide lower bounds on the two capacities. These lower bounds are tighter than those one might derive based on the previously known results. We prove our lower bounds by proposing a two-round, two-level coding construction over the two-way channel. We show that the lower bound on the common randomness capacity can also be achieved using a simple interactive channel coding (ICC) method. We furthermore provide upper bounds on these capacities and show that the lower and the upper bounds coincide when the two-way channel consists of two independent (physically degraded) one-way channels. We apply the results to the case where the channels are binary symmetric.

Category / Keywords: foundations / Two-way channel, wiretap channel, common randomness capacity, secret key capacity.

Publication Info: This is the full version of a paper accepted in ICITS 2011. The original publication is available at www.springerlink.com.

Date: received 3 Mar 2011, last revised 4 Mar 2011

Contact author: hahmadi at ucalgary ca

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Note: The full version includes more details and proofs in the appendix.

Version: 20110305:162954 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]