Computer Science > Information Theory

The Sender-Excited Secret Key Agreement Model: Capacity, Reliability and Secrecy Exponents

Tzu-Han Chou, Vincent Y. F. Tan, Stark C. Draper

(Submitted on 21 Jul 2011 (v1), last revised 26 May 2012 (this version, v3))

We consider the fundamental limits of the secret key generation problem when the sources are randomly excited by the sender and there is a noiseless public discussion channel. In many practical communication settings, the sources or channels may be influenced by some parties involved. Similar to recent works on probing capacity and channels with action-dependent states, our system model captures such a scenario. We derive single-letter expressions for the secret key capacity. Our coding strategy involves a key generation scheme and wiretap channel coding. We show that the secret key capacity is composed of both source- and channel-type randomness. By assuming that the eavesdropper receives a degraded version of the legitimate receiver's observation, we also obtain a capacity result that does not involve any auxiliary random variables, and thus it is amenable to numerical evaluation. By evaluating the capacity for several degraded channels, we show that there is a fundamental interplay between the portion of the secret key rate that is due to that from source-type and that from channel-type randomness. In addition, we derive lower bounds on the achievable reliability and secrecy exponents, i.e., the exponential rates at which the probability of decoding error and the information leakage decay. These exponents allow us to determine the set of "strongly-achievable" secret key rates. Our exponents explicitly capture the twin effects of the channel and the source in the model. The exponents can be specialized to previously known results. We also demonstrate that there is an inherent tradeoff between the achievable reliability and secrecy exponents.

Comments:	Submitted to the IEEE Transactions on Information Theory; Corrections to and explanations of some results
Subjects:	**Information Theory (cs.IT)**; Cryptography and Security (cs.CR)
Cite as:	**arXiv:1107.4148 [cs.IT]**
	(or **arXiv:1107.4148v3 [cs.IT]** for this version)

Submission history

From: Vincent Tan [view email]

[v1] Thu, 21 Jul 2011 02:35:47 GMT (1186kb)

[v2] Thu, 15 Dec 2011 04:47:55 GMT (1189kb)
[v3] Sat, 26 May 2012 17:08:11 GMT (1264kb)

Which authors of this paper are endorsers?