

BENNETT
BRASSARD
ROBERTS

Desk Copy

PRIVACY AMPLIFICATION BY PUBLIC DISCUSSION*

CHARLES H. BENNETT†, GILLES BRASSARD‡ AND JEAN-MARC ROBERT§

Abstract. In this paper, we investigate how the use of a channel with perfect authenticity but no privacy can be used to repair the defects of a channel with imperfect privacy but no authenticity. More precisely, let us assume that Alice and Bob wish to agree on a secret random bit string, and have at their disposal an imperfect private channel and a perfect public channel. The private channel is imperfect in various ways: transmission errors can occur, and partial information can leak to an eavesdropper, Eve, who also has the power to suppress, inject, and modify transmissions arbitrarily. On the other hand, the public channel transmits information accurately, and these transmissions cannot be modified or suppressed by Eve, but their entire contents becomes known to her. We consider the situation in which a random bit string x has already been transmitted from Alice to Bob over the private channel, and we describe interactive public channel protocols that allow them, with high probability: (1) to assess the extent to which the private channel transmission has been corrupted by tampering and channel noise; and (2) if this corruption is not too severe, to repair Bob's partial ignorance of the transmitted string and Eve's partial knowledge of it by distilling from the transmitted and received versions of the string another string, in general shorter than x , upon which Alice and Bob have perfect information, while Eve has nearly no information (or in some cases exactly none), except for its length. These protocols remain secure against unlimited computing power.

Key words. cryptography, error-correcting codes, information theory, key exchange, privacy, randomness, universal hashing, t -resilient functions, wiretap channel

AMS(MOS) subject classifications. 94A60, 94A40

1. Introduction. Alice and Bob wish to agree on a secret random bit string. In order to achieve this goal, they have at their disposal an imperfect private channel and an authenticated public channel. The private channel is imperfect in various ways: transmission errors can occur, and partial information can leak to Eve, the eavesdropper, who also can modify the transmissions arbitrarily, as explained below. The only limitation we impose on Eve is the knowledge by Alice and Bob of an upper bound on the amount of partial information that can leak to her when she eavesdrops on a private channel transmission.

We allow Eve to tamper arbitrarily with the private channel transmissions. For instance, she can suppress the transmission of selected bits, perhaps to replace them with bits of her choice, to inject new bits, to toggle transmitted bits or to jumble them around. We allow her to introduce as much malicious noise as she wishes. In this paper, we granted Eve unlimited tampering power even though probably no real channel performs quite this badly, so that our results will hold true in any circumstance.

The quantum channel of [BB1], [BB2] is a prime example of an imperfect private channel, and this paper effectively allows the removal of its previous defects. Indeed,

* Received by the editors October 28, 1985; accepted for publication (in revised form) March 9, 1987. Part of this work was presented at CRYPTO 85 under the title, "How to Reduce your Enemy's Information."

† IBM T. J. Watson Research Laboratory, Yorktown Heights, New York 10598.

‡ Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, C.P. 6128, Succ. "A" Montréal, Québec, Canada H3C 3J7. The work of this author was supported in part by the Natural Sciences and Engineering Research Council of Canada under grant A4107 and National Science Foundation grant MCS-8204506. Part of this research was conducted while the author was at the University of California, Berkeley, California 94720.

§ School of Computer Science, McGill University, 805 Sherbrooke St. West, Montréal, Québec, Canada H3A 2K6. This work was partially supported by Natural Sciences and Engineering Research Council of Canada grant A4107. This research was conducted while this author was at the Université de Montréal, Montréal, Québec, Canada H3C 3J7.