From Weak to Strong Information-Theoretic Key Agreement

Ueli Maurer [1] Stefan Wolf [1]

Abstract — **In the original definitions of information-theoretic secret-key agreement, the required secrecy condition was too weak. We show, by a generic reduction, that it can be strengthened without any effect on the achievable key-generation rate.**

I. Models of Information-Theoretic Secret-Key Agreement

Motivated by Wyner's wire-tap channel [7], different settings for information-theoretic secret-key agreement have been proposed by Csiszár and Körner [3] and Maurer [5]. Whereas in the model of [3], Alice is connected to Bob and Eve by a noisy broadcast channel characterized by $P_{YZ|X}$ (Alice sends X and Bob and Eve receive Y and Z, respectively), only correlated information, but not insecure communication is regarded as a resource in the model of [5]. Here, the parties Alice and Bob are connected by a noiseless and authentic but otherwise insecure channel and have access to random variables X and Y, respectively, whereas the adversary knows Z.

In both settings, the capability of generating a secret key has been defined asymptotically as the maximal achievable key-generation rate (i.e., the number of resulting key bits per channel use or per realization of the triple XYZ, respectively) such that the adversary obtains information at an arbitrarily small rate only. The corresponding quantities were called the *secrecy capacity* $C_S(P_{YZ|X})$ [3] and the *secret-key rate* $S(X;Y||Z)$ [5], respectively. However, the secrecy condition which only limits the *rate* at which Eve obtains information about the key does not imply that the adversary's information is bounded in an absolute sense, let alone negligibly small. This is clearly unsatisfactory and motivated the definition of strong variants of secrecy capacity $\overline{C_S}(P_{YZ|X})$ [2] and secret-key rate $\overline{S}(X;Y||Z)$ [4], requiring that the adversary's information about the resulting key is small in total.

In [4], a lower bound on $\overline{S}(X;Y||Z)$ was shown, whereas in [2], a result similar to Corollary 2 below was proved (with techniques different from ours). In this note we describe a generic method for strengthening the security of any information-theoretic key agreement by using only a negligible amount of extra communication from Alice to Bob and such that the effective key-generation rate is asymptotically equal to the rate with respect to the weak definition.

II. A General Method for Strengthening the Security

Definition 1. Let $\varepsilon > 0$ be a real number and let N be a positive integer. A *weak key agreement with parameters ε and N* ($KA(\varepsilon, N)$ for short) between two parties Alice and Bob and with respect to an adversary Eve outputs three random variables S_A, S_B, and U, known to Alice, Bob, and Eve, respectively, such that $\mathrm{Prob}\,[S_A \neq S_B] < \varepsilon$, $H(S_A) \geq (1-\varepsilon)N$, and $I(S_A;U) < \varepsilon N$ hold.

Such key agreement is called *strong*, denoted by $\overline{KA}(\varepsilon, N)$, if the random variables S_A, S_B, and U satisfy the following more restrictive conditions. There must exist a string S with $\mathrm{Prob}\,[S = S_A = S_B] > 1-\varepsilon$, $H(S) = \log|\mathcal{S}| \geq (1-\varepsilon)N$, and $I(S;U) < \varepsilon$.

Theorem 1. *Assume that a noiseless channel from Alice to Bob is given to which Eve has perfect read access. Then weak key agreement can be converted into strong key agreement such that the key is generated asymptotically at the same rate and the amount of required extra communication is asymptotically vanishing. More precisely, for every $\varepsilon > 0$ there exists $\alpha > 0$ such that for all sufficiently large M and for all sufficiently large N, $\overline{KA}(\varepsilon, N)$ can be reduced to $K = (1+o(1))N/M$ realizations of $KA(\alpha, M)$ such that the length $\mathrm{len}(C)$ of the message C sent over the insecure channel by Alice is of order $\mathrm{len}(C) = o(N)$.*

The proof idea is as follows. First, weak key agreement is repeated many times. Then, error correction information is sent from Alice to Bob (and hence to Eve), allowing Bob to reconstruct Alice's sequence of weak keys with high probability. Finally, this string is transformed into a highly secret key by *privacy amplification*. Universal hashing, as proposed in [1], is not a good choice for hashing the string in this situation since the required amount of communication, i.e., the specification of a particular function from the universal class, would be too high (thus reducing the achievable key-generation rate in the broadcast-channel model). As a new method in this context, we use *extractors* [6] instead. This allows for keeping the extra communication negligible.

Theorem 1 directly implies that in both models described above, the secrecy requirements can be strengthened without effect on the achievable key-generation rates.

Corollary 2. $\overline{C_S}(P_{YZ|X}) = C_S(P_{YZ|X})$.

Corollary 3. $\overline{S}(X;Y||Z) = S(X;Y||Z)$.

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, Vol. 41, No. 6, pp. 1915–1923, 1995.

[2] I. Csiszár, "Almost independence and secrecy capacity (in Russian)," in *Problems of Information Transmission (PPI)*, Vol. 32, No. 1, pp. 48–57, 1996.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, Vol. 24, No. 3, pp. 339–348, 1978.

[4] U. M. Maurer, "The strong secret key rate of discrete random triples," in *Communication and Cryptography – Two Sides of One Tapestry*, Kluwer Academic Publishers, pp. 271–285, 1994.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.

[6] S. P. Vadhan, "Extracting all the randomness from a weakly random source," *Electronic Colloquium on Computational Complexity*, Tech. Rep. TR98-047, 1998.

[7] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355–1387, 1975.

[1] Department of Computer Science, ETH Zürich, CH–8092 Zürich, Switzerland. E-mail: {maurer,wolf}@inf.ethz.ch