# Generalized Privacy Amplification


Charles H. Bennett
IBM T. J. Watson Research Laboratory,
Yorktown Heights, New York, NY 10598, USA

Gilles Brassard
Département IRO, Université de Montréal,
C.P. 6128, succ. centre-ville, Montréal, Canada H3C 3J7

Claude Crépeau
École Normale Supérieure, Lab. d'Informatique
45 rue d'Ulm, 75230 Paris CEDEX 05, France

Ueli M. Maurer
Inst. for Theoretical Computer Science, ETH Zürich
CH–8092 Zürich, Switzerland



*Abstract* — **This paper provides a general treatment of privacy amplification by public discussion, a concept introduced by Bennett, Brassard and Robert [1] for a special scenario. The results have applications to unconditionally-secure secret-key agreement protocols, quantum cryptography and to a non-asymptotic and constructive treatment of the secrecy capacity of wire-tap and broadcast channels, even for a considerably strengthened definition of secrecy capacity.**


## I. Introduction

This paper is concerned with unconditionally-secure secret-key agreement by two communicating parties Alice and Bob who both know a random variable $W$, for instance a random $n$–bit string, about which an eavesdropper Eve has incomplete information characterized by the random variable $V$ jointly distributed with $W$ according to $P_{VW}$. This distribution may partially be under Eve's control. Alice and Bob know nothing about $P_{VW}$, except that it satisfies a certain constraint. We present protocols by which Alice and Bob can use a public channel, which is totally susceptible to eavesdropping by Eve, to agree on a function $g : \{0,1\}^n \to \{0,1\}^r$ such that Eve, despite her partial knowledge about $W$ and complete knowledge about $g$, almost certainly knows nearly nothing about the secret key $g(W)$. We characterize how the size $r$ of the secret they can safely distill depends on the kind and amount of Eve's partial information on $W$.

## II. Privacy amplification by public discussion

The concept of privacy amplification by public discussion was introduced by Bennett, Brassard and Robert [1]). Their model and results are reviewed and generalized in this paper.

**Definition 1.** [2] A class $G$ of functions $\mathcal{A} \to \mathcal{B}$ is universal if, for any distinct $x_1$ and $x_2$ in $\mathcal{A}$, the probability that $g(x_1) = g(x_2)$ is at most $1/|\mathcal{B}|$ when $g$ is chosen at random from $G$ according to the uniform distribution.

*Example.* Let $a$ be an element of $GF(2^n)$ and also interpret $x$ as an element of $GF(2^n)$. Consider the function $\Sigma^n \to \Sigma^r$ assigning to an argument $x$ the first $r$ bits of the element $ax$ of $GF(2^n)$. The class of such functions for $a \in GF(2^n)$ is a universal class of functions for $1 \le r \le n$.

**Definition 2.** Let $X$ be a random variable with alphabet $\mathcal{X}$ and distribution $P_X$. The *collision entropy* of $X$, also known as the Rényi entropy of order two, is defined as the negative logarithm of its collision probability:

$$H_c(X) = -\log_2 \sum_{x \in X} P_X(x)^2.$$

For an event $\mathcal{E}$, the *collision entropy of $X$ conditioned on $\mathcal{E}$*, $H_c(X|\mathcal{E})$, is defined naturally as the collision entropy of the conditional distribution $P_{X|\mathcal{E}}$.

In many scenarios, Eve's collision entropy is known to be bounded. One such scenario is when Eve is allowed to obtain at most $t$ arbitrary bits of deterministic information about $W$ [1]. Another scenario is that Eve receives $W$ through a binary symmetric channel with certain bit error probability. A third scenario is when Eve can receive the bits of $W$ through individual binary symmetric channels at her choice subject only to a global constraint on the set of individual bit error probabilities. The following theorem demonstrates that in every scenario in which a lower bound on Eve's collision entropy is known, Alice and Bob can generate a secret key $S$.

**Theorem.** *Let $P_{VW}$ be an arbitrary probability distribution. If Eve's collision entropy $H_c(W|V = v)$ about $W$ is known to be at least $t$ and Alice and Bob choose $S = G(W)$ as their secret key, where $G$ is chosen at random from a universal class of hash functions from $\mathcal{W}$ to $\Sigma^r$, then Eve's information about $S$ is exponentially small in the excess compression $r - t$:*

$$H(S|G, V = v) \;\ge\; r - \frac{2^{r-t}}{\ln 2}.$$

In the full version of this paper it is demonstrated that, unlike Shannon entropy, collision entropy can increase when additional information is revealed, and this fact is exploited in privacy amplification by conceptually assuming the existence of an oracle who provides Eve for free with "spoiling knowledge", thus allowing Alice and Bob to distill a secret key that is much longer than suggested at a first glance by the above theorem.

## References


[1] C.H. Bennett, G. Brassard and J.–M. Robert, "Privacy amplification by public discussion", *SIAM Journal on Computing*, Vol. 17, no. 2, April 1988, pp. 210–229.

[2] J.L. Carter and M.N. Wegman, "Universal classes of hash functions", *Journal of Computer and System Sciences*, Vol. 18, 1979, pp. 143–154.