Privacy Amplification Secure Against an Adversary with Selectable Knowledge[1]

Robert König Ueli Maurer
Renato Renner
Department of Computer Science
ETH Zürich, Switzerland
{rkoenig,maurer,renner}@inf.ethz.ch

Abstract — **We introduce the concept of *selectable knowledge*, which models the information stored in an arbitrary (e.g., quantum mechanical) device. We then analyze a situation where an entity $\mathcal{A}$ holds selectable knowledge about some random variable X and quantify the information $\mathcal{A}$ has about the output $H(X)$ of a randomly chosen function H applied to X. This generalizes the setting of privacy amplification by universal hashing. In particular, our result can be used to prove that privacy amplification remains secure even if the enemy possesses quantum instead of classical information.**

I. Modeling Knowledge and Storage

We say that an entity $\mathcal{A}$ has *selectable knowledge* $\mathbf{W}$ if $\mathcal{A}$ can learn the value of exactly *one* arbitrarily chosen random variable W from a set of random variables $\mathbf{W}$, thereby irrevocably loosing access to the values $W' \in \mathbf{W}$ for $W' \not\equiv W$. This is for instance the case if $\mathcal{A}$ holds a quantum state ρ and can apply an arbitrary measurement strategy to obtain classical information W from ρ.

The knowledge of $\mathcal{A}$ about a random variable Z can be quantified using the statistical distance $d(Z)$ from the uniform distribution, called *non-uniformity*, of the random variable Z.

Definition I.1 *The* non-uniformity *of a random variable Z,* given selectable knowledge $\mathbf{W}$*, is*

$$d(Z|\mathbf{W}) := \max_{W \in \mathbf{W}} d(Z|W) \ ,$$

where $d(Z|W) := E_W[d(Z|W = w)]$ denotes the expected non-uniformity of Z given $W = w$.

A (physical) storage device is modeled as a set of channels from a set $\mathcal{S}$ (called *state space*) to a set $\mathcal{W}$. We call such a set $\mathbf{p}$ of channels a *selectable channel*. The *output* $\mathbf{p}[S]$ of a selectable channel $\mathbf{p}$ on input S is the selectable knowledge $\mathbf{p}[S] := \{p[S] : p \in \mathbf{p}\}$ where $p[S]$ denotes the output of p on input S. As an example, a *d-dimensional quantum storage device* is defined as $\mathbf{p}^{\mathcal{Q}_d} := \{p_{\{E_w\}} : \{E_w\} \in \mathrm{POVM}(\mathcal{H}_d)\}$, where $p_{\{E_w\}}$ is a channel describing the measurement process when applying the POVM $\{E_w\}$ on a d-dimensional Hilbert space $\mathcal{H}_d$.

II. Bounds on Knowledge and Privacy Amplification

Consider an entity $\mathcal{A}$ which has selectable knowledge $\mathbf{W}$ about a random variable X. We analyze the amount of information she has about the value $G(X)$ of a randomly chosen function G applied to X, which can naturally be measured in terms of the non-uniformity[2] $d(G(X)|[\mathbf{W}, G])$. In the context of privacy amplification [1], one is particularly interested in settings where G is uniformly chosen from a set of two-universal functions.

In certain instances, e.g., for quantum devices, it is particularly easy to analyze the case where this function is binary. Our main result relates the non-binary case to the binary one. It is proven with the following auxiliary lemma, which is of independent interest.

Lemma II.1 *Let X be a random variable with range $\mathcal{X}$ and let H be uniformly chosen from the set of balanced binary functions on $\mathcal{X}$. Then*

$$d(X) \leq \frac{3}{2}\sqrt{|\mathcal{X}|}\, d(H(X)|H)$$

where $d(H(X)|H) := E_H[d(H(X)|H = h)]$.

Combined with the observation that the concatenation of any two-universal function with a uniform balanced random predicate on its range is itself two-universal, we get the following theorem.

Theorem II.2 *Let X be a random variable with range $\mathcal{X}$ and let $\mathbf{W}$ be selectable knowledge. Then, for any two-universal random function G from $\mathcal{X}$ to $\mathcal{Y}$,*

$$d(G(X)|[\mathbf{W}, G]) \leq \frac{3}{2}\sqrt{|\mathcal{Y}|}\, \max_H d(H(X)|[\mathbf{W}, H]) \ .$$

where the maximum is taken over all binary two-universal random functions H.

This can be used to show security results on privacy amplification in contexts where an adversary has selectable knowledge. For the special case of quantum adversaries, a tight bound on the r.h.s. of the inequality in Theorem II.2 can be derived in the case of quantum storage devices[3]. Interestingly, this can be used to show that privacy amplification remains essentially equally secure even if an adversary has quantum instead of only classical knowledge [2].

References

[1] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[2] R. König, U. Maurer, R. Renner. On the Power of Quantum Memory, May 2003, available at http://arxiv.org/abs/quant-ph/0305154

[1] This work was partially supported by the Swiss National Science Foundation (SNF), project no. 20-66716.01.

[2] Informally, the expression $[\mathbf{W}, G]$ refers to the selectable knowledge which results when the random variable G can be used in the selection process.

[3] i.e., where the selectable knowledge is $\mathbf{W} := \mathbf{p}^{\mathcal{Q}_d}[\rho_X]$ and ρ_X is the (quantum) memory content depending on X.