cryptography

MDPI

Article

Kolmogorov One-Way Functions Revisited

Filipe Casal [1,2], João Rasga [1,2], André Souto [3,4,5,†,*]

1 Department Matemática, Instituto Superior Técnico, Avenida Rovisco Pais 1, 1049-001 Lisboa, Portugal; filipe.casal@tecnico.ulisboa.pt (F.C.); joao.rasga@tecnico.ulisboa.pt (J.R.)
2 Centro de Matemática, Aplicações Fundamentais e Investigação Operacional (CMAF-CIO), Campo Grande 016, 1749-016 Lisboa, Portugal
3 Department Informática, Faculdade de Ciências, Campo Grande 016, 1749-016 Lisboa, Portugal
4 LASIGE, Faculdade de Ciências, U Lisboa, Portugal; Campo Grande 016, 1749-016 Lisboa, Portugal
5 Instituto de Telecomunicações, Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal
* Correspondence: ansouto@fc.ul.pt
† Current address: Campo Grande 016, 1749-016 Lisboa, Portugal

Received: 29 March 2018 ; Accepted: 25 April 2018; Published: 28 April 2018

Abstract: We study characterizations of one-way functions in terms of time-bounded Kolmogorov complexity. As the main contribution, we propose definitions for strong and weak Kolmogorov one-way functions and show that these are equivalent to classical strong and weak one-way functions, respectively. The new definitions were motivated by the fact that the expected value approach is not able to characterize strong one-way functions as we prove in the paper.

Keywords: Kolmogorov complexity; one-way functions; cryptography; complexity theory

MSC: 68Q30-94A60

1. Introduction

One-way functions are polynomially computable functions that are hard to invert, meaning that, given a set of images, there should not exist an efficient algorithm to compute its pre-image. One-way functions are not known to exist. However, their existence has major consequences in mathematics, as well as in everyone's daily life: on one hand, their existence implies that $\mathsf{P} \neq \mathsf{NP}$ (see [1]); on the other hand, if they do not exist, then most cryptographic protocols and pseudo-random generators are not secure since their security is based on the hardness of several one-way function candidates [2–6].

In the literature, it is possible to find three definitions of one-way functions that essentially differ on the power of the polynomial-time algorithm that is used to invert the function and on its probability of success: deterministic, weak and strong (by increasing order of strength). A function f is a deterministic one-way function if all polynomial-time deterministic algorithms fail to invert at least a polynomial fraction of the inputs; f is a weak one-way function if at least a polynomial fraction of the inputs are resilient to polynomial time probabilistic algorithms; and, finally, f is a strong one-way function if any polynomial-time probabilistic algorithm can only invert a negligible fraction of the inputs. Despite the distinctly different hardness assumptions, it is known that weak one-way functions exist if and only if strong one-way functions exist (see [1] for details).

In Algorithmic Information Theory, the central notion is Kolmogorov complexity, $\mathsf{K}(x)$, proposed independently in [7–9], that measures the information contained in a string x by means of the length of its shortest description. The computational hardness is easily encoded in this information measure by considering its time-bounded version, $\mathsf{K}^t(x)$, where the restriction is that the program describing x must run within time $t(|x|)$.

Here, we are interested in the connection between Kolmogorov complexity and the study of one-way functions, a line of work first considered in [10,11]. In these works, the Kolmogorov complexity of x given $f(x)$, $\mathsf{K}^t(x|f(x))$, is studied as a measure of how hard it is to invert $f(x)$ to obtain x. From this, several variants of $\mathsf{K}^t(x|f(x))$ are analyzed, namely $\mathsf{K}^t_f(x|f(x),r,n)$, where r is a random string $r \in \Sigma^{t(n)}$ used to model access to a random coin and n is the size of x. The authors provided a partial characterization of strong and weak one-way functions based on the expected value of $\mathsf{K}^{t\log t}_f(x|f(x),r,n)$, i.e., of the time-bounded Kolmogorov complexity of the pre-image x of length n given the value of $f(x)$ and a random string r. In particular, they prove that if $\mathbb{E}[\mathsf{K}^{t\log t}_f(x|f(x),r,n)] > c$ for any positive constant c and polynomial t, then f is a weak one-way function, and, if f is a strong one-way function, then $\mathbb{E}[\mathsf{K}^t_f(x|f(x),r,n)] > c\log n$ for every constant c and polynomial t. The converse implications were left open. Furthermore, based on the difference between $\mathsf{K}^t_f(x|r,n)$ and $\mathsf{K}^t_f(x|f(x),r,n)$, they proposed an individual approach characterization to one-way functions. In this paper, we show in Proposition 4 that the expected value approach cannot be used to fully characterize the class of strong one-way functions. Moreover, we provide a sufficient condition under which Kolmogorov one-way functions (as defined in [11]) are weak one-way functions.

Pursuing the idea of having a full classification of classes of one-way functions using Kolmogorov based measures, we give alternative characterizations of one-way functions based on time-bounded Kolmogorov complexity. As the main contribution of this paper, we define several classes of functions, namely Kolmogorov strong and weak one-way functions and show that these are equivalent to the usual notions of strong and weak one-way functions.

The paper is organized as follows: in Section 2, we recall the definitions of one-way functions and some known results, as well as the basics on Kolmogorov complexity; in Section 3.1, we define Kolmogorov weak/strong one-way functions and show that they are equivalent to weak and strong one-way functions, respectively; in Section 3.2, we show that the expected value of $\mathsf{K}^t_f(x|f(x),r,n)$ is not enough to characterize strong one-way functions; in Section 3.3, we define Kolmogorov Δ-functions and establish their relationship with weak one-way functions; finally, in Section 4, we conclude the paper.

2. Preliminaries

2.1. One-Way Functions

We begin by recalling the usual definitions of honest one-way functions that are used in the literature, and by stating some known results relating these classes of functions. Throughout the paper, we assume one-way functions are honest. Furthermore, we only consider injective one-way functions. We denote by Σ the set with 0 and 1, thus making Σ^* the alphabet of all finite binary strings and Σ^n the set of strings of size n. In the next definitions, we use the adapt the definitions presented in [1] and that were considered in [11].

Definition 1 (Weak one-way function (as in [11])). *A function $f : \Sigma^* \to \Sigma^*$ is a* weak one-way function (wowf) *if the following conditions hold:*

- *There is a deterministic polynomial time algorithm* A *such that on input x,* A *outputs $f(x)$, i.e., $\mathsf{A}(x) = f(x)$.*
- *For any polynomial $t(\cdot)$, there is a polynomial $q(\cdot)$ such that, for any probabilistic t-time bounded algorithm* B *and sufficiently large n,*

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[f(\mathsf{B}(f(x),r,n)) \neq f(x)\right] > \frac{1}{q(n)} \cdot \tag{1}$$

Definition 2 (Strong one-way function (as in [11])). *A function $f : \Sigma^* \to \Sigma^*$ is a* strong one-way function (sowf) *if the following conditions hold:*

- *There is a deterministic polynomial time algorithm* A *such that on input x,* A *outputs $f(x)$, i.e., $\mathsf{A}(x) = f(x)$.*
- *For any polynomial $t(\cdot)$, for every positive polynomial $q(\cdot)$, for any probabilistic t-time bounded algorithm* B*, and for sufficiently large n,*

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[f(\mathsf{B}(f(x),r,n)) = f(x)\right] < \frac{1}{q(n)} \ . \tag{2}$$

The following results are well known: weak one-way functions exist iff strong one-way functions exist; if f is a strong one-way function, then f is a weak one-way function.

2.2. Kolmogorov Complexity

We start by presenting the basics on Kolmogorov complexity that will be used throughout the paper. We refer the reader to [12] for an extensive overview of the topic. Throughout the paper, we assume a fixed prefix-free Turing machine as a model of computation. It is worthwhile mentioning that the choice of such machine only affects the results by constant terms.

Definition 3 (Kolmogorov complexity of a string). *Given a universal Turing machine U with access to an oracle f, for any strings $x, y \in \Sigma^*$, we define the Kolmogorov complexity of x given input y as the length of the smallest program that given y outputs x with access to an oracle f, i.e.,*

$$\mathsf{K}_f(x|y) = \min_p \left\{ |p| : U_f(p,y) = x \right\} \ . \tag{3}$$

For any time constructible function t, the t-time bounded Kolmogorov complexity of x given y with oracle access to f is

$$\mathsf{K}^t_f(x|y) = \min_p \left\{ |p| : U_f(p,y) = x \text{ in at most } t(|x|) \text{ steps} \right\} \ . \tag{4}$$

Intuitively, the larger the term $\mathsf{K}^t_f(x|y)$ is, the harder it is to obtain x given y. This motivates the use of $\mathsf{K}^{\mathsf{poly}}_f(x|f(x))$ to measure how hard it is to invert $f(x)$ and obtain x given polynomial time. Furthermore, in this notion, we can easily mimic the behavior of a stronger adversary, say a probabilistic polynomial time machine, by considering $\mathsf{K}^{\mathsf{poly}}_f(x|f(x),r,n)$, where r is a random string in $\Sigma^{t(n)}$ and n is the size of x.

We recall some results from [11] that already establish connections between strong and weak one-way functions and time-bounded Kolmogorov complexity. There, the authors were able to characterize what happens to $\mathsf{K}^t_f(x|f(x),r)$, on average, when f is a sowf.

Theorem 1 ([11]). *Let f be an injective and polynomial time computable function.*

If f is a strong one-way function, then for every constant c and polynomial $t(\cdot)$, the expected value of $\mathsf{K}^t_f(x|f(x),r,n)$ over pairs $(x,r) \in \Sigma^n \times \Sigma^{t(n)}$ is larger than $c \log n$ for every sufficiently large n.

For the other direction, it is only known that if the expected value of $\mathsf{K}^{t\log t}_f(x|f(x),r,n)$ is greater than c for any constant c, then f is a wowf.

Theorem 2 ([11]). *Let f be an injective and polynomial time computable function. If, for every polynomial $t(\cdot)$ and for every constant c, the expected value of $\mathsf{K}^{t\log t}_f(x|f(x),r,n)$ over pairs $(x,r) \in \Sigma^n \times \Sigma^{t(n)}$ is larger than c for sufficiently large n, then f is a weak one-way function.*

These results are summarized in the following diagram, where arrows represent known consequences:

$$\begin{aligned} f \text{ is sowf} &\longrightarrow f \text{ is wowf}, \\ f \text{ is sowf} &\longrightarrow \mathbb{E}\left[\mathsf{K}_f^t(x|f(x),r,n)\right] > c\log n, \\ \mathbb{E}\left[\mathsf{K}_f^{t\log t}(x|f(x),r,n)\right] > c &\longrightarrow f \text{ is wowf} \ . \end{aligned}$$

It was left open whether one could use the approach of expected value of $\mathsf{K}_f^t(x|f(x),r,n)$ to fully characterize the classes of weak and strong one-way functions. Here, we provide a partial negative answer, and show that if, for all constants c, $\mathbb{E}[\mathsf{K}_f^t(x|f(x),r,n)] > c\log n$, then this does not imply that f is a strong one-way function, by providing a wowf that is not a sowf that satisfies this requirement.

Furthermore, we show that this result generalizes and show that if a strong one-way function f has $\mathbb{E}[\mathsf{K}_f^t(x|f(x),r,n)] \in \mathcal{O}(p(n))$, for some function $p(\cdot)$, there exists a weak one-way function g (which is not strong one-way) such that $\mathbb{E}[\mathsf{K}_g^t(x|g(x),r,n)] \in \mathcal{O}(p(n))$. These results show that a characterization of strong one-way functions solely based on the expected values should not be possible.

In the sequel, we propose alternative definitions that solve these issues, giving a Kolmogorov complexity characterization of one-way functions. We define Kolmogorov weak and strong one-way functions (Kw and Ks) and Kolmogorov Δ-weak and strong one-way functions (KΔ-w and KΔ-s) and show the following equivalences ($\longleftrightarrow$) and implications ($\longrightarrow$):

$$\begin{aligned} f \text{ is Ks} &\longleftrightarrow f \text{ is sowf} & f \text{ is K}\Delta\text{-s} &\longrightarrow f \text{ is K}\Delta\text{-w} \\ f \text{ is Kw} &\longleftrightarrow f \text{ is wowf} & f \text{ is K}\Delta\text{-w} &\longrightarrow f \text{ is wowf} \ . \end{aligned}$$

3. Results

3.1. Kolmogorov Characterization of One-Way Functions

Here, we propose a definition of classes of functions (Kolmogorov weak and Kolmogorov strong) solely based on the fraction of strings (x,r) for which $\mathsf{K}_f^t(x|f(x),r,n) \leq c$, for a constant c. This is motivated by the fact that if $\mathsf{K}_f^t(x|f(x),r,n) \leq c$, then it is enough to run all programs of size up to c for time $t(n)$ and check (using the oracle for f) which one returns the inverse of $f(x)$. In the sequel, we will show that these classes coincide with the classical classes of weak and strong one-way functions.

Definition 4 (Kolmogorov weak one-way function)**.** *Let $f : \Sigma^* \to \Sigma^*$ be an injective polynomial time computable function. We say that f is a* Kolmogorov weak one-way function *if for every polynomial $t(\cdot)$, there is a polynomial $q(\cdot)$ such that, for all positive integers c and sufficiently large n, we have*

$$\mathbb{P}_{(x,r)\in\Sigma^{n+t(n)}}\left[\mathsf{K}_f^t(x|f(x),r,n) \leq c\right] \leq 1 - \frac{1}{q(n)} \ . \tag{5}$$

This definition is analogous to the one of weak one-way functions, but here we bound the probability that the polynomially time-bounded Kolmogorov complexity of inverting $f(x)$ is a constant.

Proposition 1. *A function f is a Kolmogorov weak one-way function iff f is an injective weak one-way function.*

Proof. ($\to$) Suppose by contraposition that f is not a weak one-way function. Then, there is a polynomial t such that, for all polynomials q, there is a probabilistic t-time bounded algorithm B such that, for infinitely many ns, $\mathbb{P}_{(x,r)\in\Sigma^{n+t(n)}}\left[f(\mathsf{B}(f(x),r,n)) = f(x)\right] > 1 - \frac{1}{q(n)}$.

Let C be the size of the program B. Then, we know that

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}[\mathsf{K}_f^t(x|f(x),r,n) \leq C] > 1 - \frac{1}{q(n),} \tag{6}$$

which means f cannot be a Kolmogorov weak one-way function.

($\leftarrow$) Suppose by contraposition that f is not a Kolmogorov weak one-way function. Then, there is a polynomial $t(\cdot)$ such that, for all polynomials $q(\cdot)$, there is a constant C such that, for infinitely many ns, we have

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\mathsf{K}^t_f(x|f(x),r,n)\leq C\right] > 1-\frac{1}{q(n)}\ . \tag{7}$$

Now, consider the algorithm A that given the inputs $f(x)\in\Sigma^n$, $r\in\Sigma^{t(n)}$ and $n=|x|$ constructs all strings (which are seen as programs) of size C, runs them for time $t(n)$ and then checks using the oracle for f if the obtained result is indeed x. This algorithm runs in time $T(n)=2^C t(n)$ for inputs of size n (which is a polynomial on n) and for infinitely many ns, inverts a fraction of the inputs larger than $1-1/q(n)$. Therefore, by construction,

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{T(n)}}\left[f(\mathsf{A}(f(x),r,n)) \;=\; f(x)\right] > 1-\frac{1}{q(n)}\ , \tag{8}$$

which means that f is not a weak one-way function. □

We now define the class of Kolmogorov strong one-way functions. This class, as we will show, coincides with the class of strong one-way functions.

Definition 5 (Kolmogorov strong one-way function)**.** *Let $f:\Sigma^*\to\Sigma^*$ be an injective polynomial time computable function. We say that f is a* Kolmogorov strong one-way function *if for every polynomials $t(\cdot)$ and $q(\cdot)$, positive integer c and sufficiently large n, we have*

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\mathsf{K}^t_f(x|f(x),r,n)<c\right]\leq\frac{1}{q(n)}\ . \tag{9}$$

Proposition 2. *A function f is a Kolmogorov strong one-way function iff f is a strong one-way function.*

Proof. ($\rightarrow$) Suppose by contraposition that f is not a strong one-way function. Then, there is a probabilistic t-time bounded algorithm B and a polynomial q such that

$$\mathbb{P}_{(x,r)\in\Sigma^{n+t(n)}}\left[f(\mathsf{B}(f(x),r,n)) \;=\; f(x)\right]\geq\frac{1}{q(n)}\ . \tag{10}$$

Thus,

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\mathsf{K}^t_f(x|f(x),r,n)<|B|\right]\geq\frac{1}{q(n)}\ , \tag{11}$$

which means f cannot be a Kolmogorov strong one-way function.

($\leftarrow$) Suppose by contraposition that f is not a Kolmogorov strong one-way function. Then, there are polynomials $t(\cdot),q(\cdot)$ and a constant C such that

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\mathsf{K}^t_f(x|f(x),r,n)<C\right]\geq\frac{1}{q(n)}\ . \tag{12}$$

Now, consider the algorithm A that given $x\in\Sigma^n$ constructs all strings of size C runs them for time $t(n)$ and then checks using the oracle for f if the obtained result is indeed x. This algorithm runs in time $T(n)=2^C t(n)$ for inputs of size n and inverts a fraction of the inputs larger than $1/q(n)$. Thus,

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{T(n)}}\left[f(\mathsf{A}(f(x),r,n)) \;=\; f(x)\right]\geq\frac{1}{q(n)}\ , \tag{13}$$

meaning that f is not a strong one-way function. □

3.2. Expected Value Approach

In this section, we show that a characterization of strong one-way functions via the expected value of $\mathsf{K}^t_f(x|f(x),r,n)$ is not possible. In particular, we show that if a strong one-way function f is such that the expected value of $\mathsf{K}^t_f(x|f(x),r,n)$ is of order $\Omega(p(n))$ for some function p, then there is a weak one-way function g (which is not strong one-way function) such that the expected value of $\mathsf{K}^t_g(x|g(x),r,n)$ is also of order $\Omega(p(n))$.

We will also use the notion of first-bit secure function, which intuitively is a function that inverting, knowing the first-bit of the pre-image, is as hard as inverting the function by itself. In a way, this guarantees that the complexity of inverting strings in the sets $\{0\}\times\Sigma^{n-1}$ and $\{1\}\times\Sigma^{n-1}$ is similar.

Definition 6 (First-bit secure function)**.** *We say that a function f is* first-bit secure *if for sufficiently large n and $x\in\Sigma^{n-1}$*

$$\mathsf{K}^t_f(0x|f(0x)) = \mathsf{K}^t_f(1x|f(1x)) \ . \tag{14}$$

We now show that, if we assume the existence of first-bit secure strong one-way functions, there are weak one-way functions that are not strong. To see this, consider the function

$$f \ = \ \lambda x. \begin{cases} 1g(x), & \text{if } x = 1y, \\ x, & \text{if } x = 0y, \end{cases} \tag{15}$$

where g is a strong one-way function that is first-bit secure. Then, f is a weak one-way function but not a strong one-way function since,

- given input x, its output is given either by the identity function or by g, which are both polynomial time computable;
- we can easily deterministically invert half of the inputs and so there is an algorithm, e.g., the first projection $\Pi = \lambda x,y,z.x$ such that,

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[f(\Pi(f(x),r,n)) \ = \ f(x)\right] \geq 1/2 \ , \tag{16}$$

  and thus f is not a strong one-way function;
- on the other hand, since $g(\cdot)$ is a strong one-way function, for any polynomial $q(\cdot)$ and any algorithm B,

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[f(\mathsf{B}(g(x),r,n)) \ = \ g(x)\right] < \frac{1}{q(n)} \, , \tag{17}$$

  and so the same projection algorithm Π is such that

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[f(\Pi(f(x),r,n)) \ = \ f(x)\right] < \frac{1}{2} + \frac{1}{2q(n)} \, , \tag{18}$$

  which means that

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[f(\Pi(f(x),r,n)) \neq f(x)\right] > 1 - \left(\frac{1}{2} + \frac{1}{2q(n)}\right) \ = \ p(n) \ , \tag{19}$$

  and thus, taking $s(n) = 1/p(n)$, $\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[f(\Pi(f(x),r,n)) \neq f(x)\right] > \frac{1}{s(n)}$, i.e., f is a weak one-way function.

Having this construction in mind, we can show the following result:

Proposition 3. *Assuming the existence of one-way functions, there exists a weak one-way function f (which is not a strong one-way function) such that for any constant c and sufficiently large n, $\mathbb{E}\left[\mathsf{K}^t_f\left(x|f(x),r,n\right)\right] > c\log n$.*

Proof. Consider the function f defined above in Label (15). Furthermore, recall from Theorem 1 that, if g is a strong one-way function, then, for any positive integer c and for any sufficiently large n, $\mathbb{E}[\mathsf{K}^t_f(x|g(x),r,n)] > c\log n$, where n is the size of x. In addition, notice that since g in the definition of f is a first-bit secure function, it also holds that $\mathbb{E}[\mathsf{K}^t_f(1y|g(1y),r,n)] > c\log n$ for y of size $n-1$ for sufficiently large ns. Then,

$$\begin{aligned}
\mathbb{E}\left[\mathsf{K}^t_f(x|f(x),r,n)\right] &= \sum_{x\in\Sigma^n} p(x)\mathsf{K}^t_f(x|f(x),r,n) && (20)\\
&= \sum_{x\in\{0\}\times\Sigma^{n-1}} p(x)\mathsf{K}^t_f\left(x|f(x),r,n\right) + \sum_{x\in\{1\}\times\Sigma^{n-1}} p(x)\mathsf{K}^t_f(x|f(x),r,n) && (21)\\
&= \sum_{x\in\{0\}\times\Sigma^{n-1}} p(x)\mathsf{K}^t_f(x|x,r,n) \quad + \sum_{x\in\{1\}\times\Sigma^{n-1}} p(x)\mathsf{K}^t_f(x|g(x),r,n) && (22)\\
&> c+\frac{1}{2}c'\log n && (23)\\
&> (c+1)\log n\ . && (24)
\end{aligned}$$

□

From the discussion above, we derive the following corollary.

Corollary 1. *Let f be such that $\mathbb{E}\left[\mathsf{K}^t_f(x|f(x),r,n)\right] > c\log n$. Then, f is not necessarily a strong one-way function.*

It is worthwhile mentioning that the proof of Proposition 3 can be generalized to a possible characterization of a sowf given by $\mathbb{E}\left[\mathsf{K}^t_f(x|f(x),r,n)\right] \in \Omega(p(n))$:

Proposition 4. *If f is a strong one-way function that is first-bit secure and $\mathbb{E}[\mathsf{K}^t_f(x|f(x),r,n)] \in \Omega(p(n))$ for some function $p(\cdot)$, then there exists a weak one-way function g that is not a strong one-way function such that $\mathbb{E}\left[\mathsf{K}^t_g(x|g(x),r,n)\right] \in \Omega(p(n))$.*

This result implies that the expected value of $\mathsf{K}^t_f(x|f(x),r,n)$ is not enough to fully characterize strong one-way functions that are not weak one-way functions.

3.3. Kolmogorov Δ-Characterization of One-Way Functions

In this section, we provide new results regarding the characterization of one-way functions using the complexity of x versus the complexity of x given $f(x)$. If these terms are very close to each other (i.e., their difference is small), we can conclude that $f(x)$ does not reveal much information about its pre-image x, as one would expect from one-way functions. Results about this notion were proved in [11] where Kolmogorov one-way functions were introduced. We begin by providing a condition under which Kolmogorov one-way functions are weak one-way functions. Following this, we introduce the classes of Kolmogorov Δ-strong and Δ-weak one-way functions and relate them with weak one-way functions.

Recall the following notions introduced in [11].

Definition 7 ((t,ε,δ)-secure Kolmogorov one-way function, [11]). *Let $t(\cdot)$ be a polynomial, $f:\Sigma^n\to\Sigma^m$ an injective and polynomial time computable function and $\delta(\cdot)$ a positive function. We say that an instance $x\in\Sigma^n$ is (t,δ)-secure relative to a random string $r\in\Sigma^{t(n)}$ and f if*

$$\mathsf{K}^t_f(x|r,n)-\mathsf{K}^t_f(x|f(x),r,n)\leq\delta(n)\ . \tag{25}$$

Let $\varepsilon(\cdot)$ be a function. We say that f is a (t,ε,δ)-secure Kolmogorov one-way function *if, for sufficiently large n,*

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\mathsf{K}^t_f(x|r,n)-\mathsf{K}^t_f(x|f(x),r,n)>\delta(n)\right]\leq\varepsilon(n)\ . \tag{26}$$

In due course, we will use the following result from [11].

Corollary 2 ([11]). *Let $t(\cdot)$ be a polynomial. If f is a (t,ε,δ)-secure Kolmogorov one-way function such that*

$$\lim_{n\to\infty}((1-\varepsilon(n))\cdot(n-\log n-\delta(n))-2)=+\infty\ ,$$

then f is a weak one-way function.

We also recall the notion of Kolmogorov one-way function from [11].

Definition 8 (Kolmogorov one-way function, [11]). *Let $f:\Sigma^*\to\Sigma^*$ be an injective polynomial time computable function. We say that f is a* Kolmogorov one-way function *if for every polynomial $t(\cdot)$, positive integer c, sufficiently large n, and x of length n,*

$$\mathsf{K}^t_f(x|n)-\mathsf{K}^t_f(x|f(x),n)\leq c\log n\ .$$

In [11], it was shown that, if f is a Kolmogorov one-way function, then it is a deterministic one-way function (which is a weak one-way function where the adversary only has deterministic computational power and is not probabilistic). However, relating this notion to weak or strong one-way functions seems a hard task given that, in the definition of Kolmogorov one-way functions, there is not any randomness parameter.

However, we now show that Kolmogorov one-way functions are indeed weak one-way functions when a condition on the amount of information given by randomness is fulfilled.

Proposition 5. *Let f be a Kolmogorov one-way function. If there is a constant ε with $0<\varepsilon<1$ and a positive function $\gamma(\cdot)$ such that, for sufficiently large n,*

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\mathsf{K}^t_f(x|f(x),n)-\mathsf{K}^t_f(x|f(x),r,n)>n^\varepsilon\right]\leq\gamma(n)\ ,$$

where $\lim_{n\to\infty}\gamma(n)=\ell<1$, then f is a weak one-way function.

Proof. Let f be a Kolmogorov one-way function. Then,

$$\begin{aligned}\mathsf{K}^t_f(x|r,n)-\mathsf{K}^t_f(x|f(x),r,n)&\leq\mathsf{K}^t_f(x|n)-\mathsf{K}^t_f(x|f(x),r,n)\\&\leq\mathsf{K}^t_f(x|n)+\Big(\mathsf{K}^t_f(x|f(x),n)-\mathsf{K}^t_f(x|f(x),n)\Big)-\mathsf{K}^t_f(x|f(x),r,n)\\&\leq c\log n+\mathsf{K}^t_f(x|f(x),n)-\mathsf{K}^t_f(x|f(x),r,n)\\&\leq c\log n+n^\varepsilon\text{ with probability greater than }1-\gamma(n)\ .\end{aligned}$$

This means that

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\mathsf{K}^t_f(x|r,n)-\mathsf{K}^t_f(x|f(x),r,n)>c\log n+n^\varepsilon\right]\leq\gamma(n)\ ,$$

and so we conclude that f is a $(t,\gamma(n),c\log n+n^\varepsilon)$-secure Kolmogorov one-way function.

Using Corollary 2, consider the limit

$$\lim_{n\to\infty}(\underbrace{(1-\gamma(n))}_{\text{goes to } 1-\ell>0}\cdot\underbrace{(n-\log n-c\log n-n^\varepsilon)}_{\text{goes to }\infty}-2)\ ,$$

which goes to infinity. Thus, f is a weak one-way function. □

Corollary 3. *Let f be a Kolmogorov one-way function. If there is a polynomial $q(\cdot)$ and a constant c such that, for sufficiently large n, we have*

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\mathsf{K}^t_f(x|f(x),n)-\mathsf{K}^t_f(x|f(x),r,n)>c\log n\right]\leq\frac{1}{q(n)}\ ,$$

then f is a weak one-way function.

As we have seen, the notion of Kolmogorov one-way function proposed in [11] lacks the link with the probabilistic features of weak and strong one-way functions, and thus we had to impose a condition relative to how much a random input helps when inverting a function.

We now consider Kolmogorov Δ-weak one-way functions, which already include probabilistic notions in their definition. For this, let

$$\Delta(x|f(x),r,n):=\mathsf{K}^t_f(x|n)-\mathsf{K}^t_f(x|f(x),r,n)\ .$$

Definition 9 (Kolmogorov Δ-weak one-way function)**.** *Let $f:\Sigma^*\to\Sigma^*$ be an injective polynomial time computable function. We say that f is a* Kolmogorov Δ-weak one-way function *if, for every polynomial $t(\cdot)$, there is a function $\gamma(n)$ and a positive ε with $0<\varepsilon<1$ such that, for sufficiently large n,*

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\Delta(x|f(x),r,n)>n^\varepsilon\right]\leq\gamma(n)\ ,$$

where $\lim_{n\to\infty}\gamma(n)<1$.

With this notion, we are able to prove unconditionally that Kolmogorov Δ-weak one-way functions are indeed weak one-way functions. This is a direct consequence of Proposition 5.

Proposition 6. *If f is a Kolmogorov Δ-weak one-way function, then f is a weak one-way function.*

We can then strengthen this notion by considering a logarithmic bound on the Δ term. The choice of parameters for the Δ-weak one-way function was an immediate consequence of Proposition 5 where we analyzed the minimum probability that the help of randomness could provide describing x from $f(x)$ in order to still have a Kolmogorov weak-one-way function (and therefore a weak-one function). Since any strong one-way function is a weak one-way function, then the condition for Δ-strong one-way function must be stronger and therefore we have to consider reasonable tighter parameter functions.

Definition 10 (Kolmogorov Δ-strong one-way function)**.** *Let $f : \Sigma^* \to \Sigma^*$ be an injective polynomial time computable function. We say that f is a* Kolmogorov Δ-strong one-way function *if, for every polynomial $t(\cdot)$, there is a function $\gamma(n)$ and a constant c such that, for sufficiently large n,*

$$\mathbb{P}_{(x,r)\in\Sigma^n\times\Sigma^{t(n)}}\left[\Delta(x|f(x),r,n) > c\log n\right] \leq \gamma(n) \ , \tag{27}$$

where $\lim_{n\to\infty} \gamma(n) < 1$.

We can easily see that a Kolmogorov Δ-strong one-way function is a Kolmogorov Δ-weak one-way function since

$$\mathbb{P}_{(x,r)}\left[\Delta(x|f(x),r) > n^{\varepsilon}\right] < \mathbb{P}_{(x,r)}\left[\Delta(x|f(x),r) > c\log n\right] \leq \gamma(n) \ . \tag{28}$$

Corollary 4. *If f is a Kolmogorov Δ-strong one-way function, then f is a weak one-way function.*

Despite showing that Kolmogorov Δ-strong one-way functions are indeed stronger than Kolmogorov Δ-weak one-way functions, and that Kolmogorov Δ-weak one-way functions are weak one-way functions, the relationship between Kolmogorov Δ-strong one-way functions and strong one-way functions is not clear.

4. Conclusions

The aim of this work was to use Kolmogorov complexity based measures in order to understand the classes of strong and weak one-way functions. For this, we introduced alternative characterizations of one-way functions based on time-bounded Kolmogorov complexity. In particular, we introduced Kolmogorov Δ-functions and Kolmogorov weak and strong functions. The latter were shown to be equivalent to the class of weak and strong one-way functions, respectively. Furthermore, we showed that we cannot characterize strong one-way functions with the average value of $\mathsf{K}^t_f(x|f(x),r,n)$. We also provided a sufficient condition under which Kolmogorov one-way functions are weak one-way functions. From this, we proposed Kolmogorov Δ-strong and Δ-weak one-way functions that already encompass this condition. We were, however, not able to establish relations between Kolmogorov Δ functions and strong one-way functions, which we find would be an interesting problem to solve as future work.

In [13], the author proposed a unified approach to one-way function and conjectured that, given any one-way function f, the function $g(x,x) = (a, f(x) + ax)$ is also a one way function. In particular, if f is defined over a finite field, then g is a one-way permutation and therefore suitable to be used in the quantum realm. Capitalizing on this approach, de Castro [14] considered for one-way function the function x^2 xor x xor 1 and exploited the quantum properties of such a construction proving that if such function is indeed a one-way function then quantum one-way functions also exist. With this two papers in mind, as a future work, it is interesting to:

1. Develop a specialized Kolmogorov complexity approximation (similar to a zip compressor) that allows the analysis of this function towards the definition proposed in this paper. This would allow to give, not just for this particular function, but also to any other possible proposal for a one-way function, a practical security analysis regarding its one-wayness.
2. The analyses driven in [14] proves that quantum one-way functions exist if and only if classical one-way functions exist and the techniques used to derive the (quantum) security of such functions are different form the classical ones. In the literature, there are several definitions of (bounded) quantum Kolmogorov complexity [15–20] . One can study the adaptation of the results presented in this paper to address directly the characterization of one way-functions that are quantum resilient and provide insight regarding some (quantum) one-way function candidates such as the one presented in [14].

Author Contributions: A.S. and F.C. conceived the example proving that the expected value cannot be used to characterise strong one-way functions. F.C. and J.R and A.S. discussed and propose the new definitions and the equivalence results. F.C. and J.R. wrote the rigorous arguments proving the equivalence to classical definitions. F.C. and A.S. wrote all the rest of the paper. All the authors revised the manuscript.

Acknowledgments: This work was partially supported by funds granted to Instituto de Telecomunicações, namely PEst-OE/EEI/LA0008/2013 and UID/EEA/50008/2013, by funds granted to LASIGE Research Unit, ref. UID/CEC/00408/2013 and by way of grant UID/MAT/04561/2013 to Centro de Matemática, Aplicações Fundamentais e Investigação Operacional of Universidade de Lisboa (CMAF-CIO). F.C. acknowledges the support from the Doctoral Programme in the Physics and Mathematics of Information: Foundations of Future Information Technologies and FCT (Portugal) through scholarship SRFH/BD/52243/2013 and A.S. acknowledges the FCT Post-Doc grant SFRH/BPD/76231/2011 and grants of FCT project Confident PTDC/EEI-CTP/4503/2014.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Goldreich, O. *Foundations of Cryptography*; Cambridge University Press: Cambridge, UK, 2001.
2. Blum, M.; Micali, S. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM J. Comput.* **1984**, *13*, 850–864. [CrossRef]
3. Goldwasser, S.; Micali, S.; Rivest, R. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.* **1988**, *17*, 281–308. [CrossRef]
4. Impagliazzo, R.; Luby, M. One-way functions are essential for complexity based cryptography. In Proceedings of the Symposium on Foundations of Computer Science '89, Research Triangle Park, NC, USA, 30 October–1 November 1989.
5. Impagliazzo, R.; Levin, L.; Luby, M. Pseudo-random generation from one-way functions. In Proceedings of the Symposium on Theory of Computing '89 ACM, Seattle, WA, USA, 14–17 May 1989; pp. 22–24.
6. Rompel, J. One-way functions are necessary and sufficient for secure signatures. In Proceedings of the Symposium on Theory of Computing '90 ACM, Baltimore, MD, USA, 13–17 May 1990; pp. 387–394.
7. Kolmogorov, A. Three approaches to the quantitative definition of information. *Probl. Inf. Transm.* **1965**, *1*, 1–7. [CrossRef]
8. Solomonoff, R. A formal theory of inductive inference, part I. *Inf. Control* **1964**, *7*, 1–22. [CrossRef]
9. Chaitin, G. On the length of programs for computing finite binary sequences. *J. ACM* **1966**, *13*, 547–569. [CrossRef]
10. Souto, A.; Teixeira, A.; Pinto, A. One-way functions using Kolmogorov complexity. *Proc. of CiE* **2010**, 346–356.
11. Antunes, L.; Matos, A.; Pinto, A.; Souto, A.; Teixeira, A. One-Way Functions Using Algorithmic and Classical Information Theories. *Theory Comput. Syst.* **2013**, *52*, 162–178. [CrossRef]
12. Li, M.; Vitányi, P. *An Introduction to Kolmogorov Complexity and its Applications*; Springer: Berlin, Germany, 2013.
13. Levin, L.A. The Tale of One-Way Functions. *Probl. Inf. Trans.* **2003**, *39*, 92–103, doi:10.1023/A:1023634616182. [CrossRef]
14. De Castro, A. Quantum one-way permutation over the finite field of two elements. *Quantum Inf. Process.* **2017**, *16*, 149, doi:10.1007/s11128-017-1599-6. [CrossRef]
15. Vitányi, P. Quantum Kolmogorov complexity based on classical descriptions. *IEEE Trans. Inf. Theory* **2001**, *47*, 2464–2479. [CrossRef]
16. Berthiaume, A.; Dam, W.; Laplante, S. Quantum Kolmogorov complexity. *J. Comput. Syst. Sci.* **2001**, *63*, 201–221. [CrossRef]
17. Gács, P. Quantum algorithmic entropy. *J. Phys. A Math. Gen.* **2001**, *34*, 6859. [CrossRef]
18. Mora, C.; Briegel, H. Algorithmic Complexity and Entanglement of Quantum States. *Phys. Rev. Lett.* **2005**, *95*, 200503. [CrossRef] [PubMed]

19. Müller, M. Strongly Universal Quantum Turing Machines and Invariance of Kolmogorov Complexity. *IEEE Trans. Inf. Theory* **2008**, *54*, 763–780. [CrossRef]
20. Mateus, P.; Sernadas, A.; Souto, A. Universality of quantum Turing machines with deterministic control. *J. Log. Comput.* **2017**, *27*, 1–19. [CrossRef]