possibly random *process* of (1) uniformly and independently choosing element x from set y, or (2) uniformly and independently drawing x according to distribution y, or (3) setting object x equal to object y, or (4) setting object x equal to the output of the (possibly probabilistic) algorithm y (in which case we specify also the input to y). By $\text{Prob}[R_1; \ldots; R_n : E]$ we denote the probability of event E, after the ordered execution of possibly random processes $R_1, \ldots, R_n$.

We define negligible functions as functions that tend to zero smaller than any inverse of a polynomial.

Definition 1. *A function δ is* negligible *if for all positive constants c there exists an integer n_c such that $\delta(n) < n^{-c}$, for all $n \geq n_c$.*

Intuitively, events with a negligible probability should not be noticed by probabilistic polynomial-time algorithms when the input sizes are large enough. We now are ready to formally define one-way functions.

Definition 2. *A function $f : \{0,1\}^* \to \{0,1\}^*$ is* one-way *if*

1. *there exists an efficient algorithm C that, on input x, returns $f(x)$;*
2. *for any efficient algorithm A, the following probability is negligible in n:*

$$\text{Prob}[x \leftarrow \{0,1\}^n; y \leftarrow f(x); x' \leftarrow A(1^n, y) : f(x') = f(x)].$$

We also define collections of one-way functions.

Definition 3. *A* collection of functions $F = \{f_n : n \in \mathcal{N}, f_n : \{0,1\}^n \to \{0,1\}^n\}$ *is* one-way *if*

1. *there exists an efficient algorithm C that, on input n, x, returns $f_n(x)$, and if*
2. *for any efficient algorithm A, the following probability is negligible in n:*

$$\text{Prob}[x \leftarrow \{0,1\}^n; y \leftarrow f_n(x); x' \leftarrow A(1^n, y) : f_n(x') = f_n(x)].$$

It is possible to prove that one-way functions exist if and only if collections of one-way functions exist. We note that the definition of one-way function essentially implies that almost all inputs to the function produce an output that is hard to invert. A natural relaxation of this intuition is that only a large fraction of the inputs produce inputs that are hard to invert. These functions are called "weak one-way" and will be discussed later in greater detail.

We now recall the definition of "trapdoor" functions as one-way function with the additional property that there exists some information that allows its owner (and only her) to invert the function.

Definition 4. *A* trapdoor function $f : \{0,1\}^* \to \{0,1\}^*$ *is a one-way function for which there exists an efficient algorithm E and a polynomial p such that, for any n, there exists a string t_n such that $|t_n| \leq p(n)$ and for all $x \in \{0,1\}^*$, $E(f(x), t_n) = x'$ and $f(x) = f(x')$.*

2.3. Weak vs. Strong One-Way Functions

We now formally define "weak" one-way functions and will also refer to (previously defined) one-way functions as "strong" one-way functions. Informally, weak one-way function represent a relaxation of one-way function as they only require that no efficient adversary can invert the function for at least a noticeable fraction of the inputs.

Definition 6. *Let p be a polynomial. A function $f : \{0,1\}^* \to \{0,1\}^*$ is a* p-weak one-way function *if*

1. *there exists an efficient algorithm C that, on input x, returns $f(x)$*
2. *for any efficient algorithm A, it holds that for all sufficiently large n,*

$$\text{Prob}\,[\, x \leftarrow \{0,1\}^n; y \leftarrow f(x); x' \leftarrow A(1^n, y) \,:\, f(x') \neq f(x)\,] \geq 1/p(n).$$

Similarly as before, we can define a *collection of weak one-way functions*. The following theorem was first stated in the oral presentation of [52].

Theorem 1. *A weak one-way function exists if and only if a strong one-way function exists.*

As one-way functions are believed to represent a very minimal notion of cryptographic hardness, this theorem seems to suggest that cryptographic hardness can be amplified from a low (but sufficiently noticeable) level to a high (and sufficiently close to the maximum possible) level.

Proof. We start the proof by recalling the transformation from weak to strong one-way functions from [52]. Intuitively, the strong one-way function is the concatenation of sufficiently many application of the weak one-way function. This is reminiscent of analogue theorems in Information Theory; interestingly, as we will see, the proof of this theorem is significantly harder.

More formally, given a p-weak collection of one-way functions $F = \{f_n : n \in \mathcal{N}\}$, where $f_n : \{0,1\}^n \to \{0,1\}^n$, we define a collection $G = \{g_m : m \in \mathcal{N}\}$, where $g_m : \{0,1\}^m \to \{0,1\}^m$, for $m = 2n^2p(n)$, is defined as

$$g_m(x_1, \ldots, x_{2np(n)}) = (f_n(x_1) \circ \cdots \circ f_n(x_{2np(n)})).$$

We now prove that G is a collection of strong one-way functions. Assume (towards contradiction) that this is not the case. Then there exists an efficient adversary A and a polynomial q such that for infinitely many m, it holds that

$$\text{Prob}\,[\, x \leftarrow \{0,1\}^m; y \leftarrow g_m(x); x' \leftarrow A(1^n, y) \,:\, g_m(x') = g_m(x)\,] \geq 1/q(m).$$

If we present an efficient adversary A' that, using A, can invert f_n with probability at least $1 - 1/p(n)$ then we contradict the assumption that F is a collection of p-weak one-way functions. Consider the following algorithm A'.

Input for Algorithm A': $y \in \{0,1\}^n$, where $y = f_n(x)$, for a randomly chosen x.

Instructions for Algorithm A':

1. repeat $4n^2p(n)q(m)$ times:
   for $i = 1, \ldots, 2np(n)$
   randomly choose $x_j \in \{0,1\}^n$, for $j = 1, \ldots, i-1, i+1, \ldots, 2np(n)$
   compute $y_j = f_n(x_j)$, for $j = 1, \ldots, i-1, i+1, \ldots, m$
   if A successfully inverts $(y_1, \ldots, y_{i-1}, y, y_{i+1}, \ldots, y_{2np(n)})$ then
   let $(x_1, \ldots, x_{2np(n)}) = A(y_1, \ldots, y_{i-1}, y, y_{i+1}, \ldots, y_{2np(n)})$
   return: x_j and halt
2. return: 'failure to invert'.

We define the subset BAD $\subseteq \{0,1\}^n$ of x such that the probability, over the randomness used by A', that in a single iteration of its repeat loop A' returns $f_n^{-1}(f_n(x))$ is less than $1/4np(n)q(m)$.

We now show that the probability, over the randomness used by A' and the random choice of x, that A' is not successful is 'essentially' the probability that x is BAD. More precisely, we define event $e(A', x)$ as the event that A' does not invert $y = f_n(x)$, when x is randomly chosen, and A' is run on $f_n(x)$. Then we have that

$$\begin{aligned}
\text{Prob}[\, e(A',x)\,] &= \text{Prob}[\, e(A',x) \,|\, x \in \text{BAD}\,] \cdot \text{Prob}[\, x \in \text{BAD}\,] \\
&\quad + \text{Prob}[\, e(A',x) \,|\, x \notin \text{BAD}\,] \cdot \text{Prob}[\, x \notin \text{BAD}\,] \\
&\leq 1 \cdot \text{Prob}[\, x \in \text{BAD}\,] + (1 - 1/4np(n)q(m))^{4n^2p(n)q(m)} \cdot 1 \\
&\leq \text{Prob}[\, x \in \text{BAD}\,] + e^{-n}
\end{aligned}$$

If we show that $\text{Prob}[\, x \in \text{BAD}\,] \leq 1/2p(n)$ then we have that $\text{Prob}[\, e(A', x)\,] \leq 1/2p(n) + e^{-n} < 1/p(n)$, which brings us to contradicting the assumption that f_n is a weak one-way function. To show that $\text{Prob}[\, x \in \text{BAD}\,] \leq 1/2p(n)$, assume (towards contradiction) that this is not the case. Then let $\vec{x} = (x_1, \ldots, x_{2np(n)})$ and define the event $e(A, \vec{x})$ as the event that A successfully inverts $\vec{y} = g_m(\vec{x})$, when $\vec{x}$ is uniformly chosen. Then we have that the probability of event $e(A, \vec{x})$ is

$$\begin{aligned}
&= \text{Prob}\left[\, e(A,\vec{x}) \,|\, \vee_{i=1}^{2np(n)}\, x_i \in \text{BAD}\,\right] \cdot \text{Prob}\left[\, \vee_{i=1}^{2np(n)} x_i \in \text{BAD}\,\right] \\
&\quad + \text{Prob}\left[\, e(A,\vec{x}) \,|\, \wedge_{i=1}^{2np(n)}\, x_i \notin \text{BAD}\,\right] \cdot \text{Prob}\left[\, \wedge_{i=1}^{2np(n)} x_i \notin \text{BAD}\,\right] \\
&\leq \Sigma_{i=1}^{2np(n)} \text{Prob}[\, e(A,\vec{x}) \,|\, x_i \in \text{BAD}\,] \cdot \text{Prob}[\, x_i \in \text{BAD}\,] \\
&\quad + \text{Prob}\left[\, e(A,\vec{x}) \,|\, \wedge_{i=1}^{2np(n)}\, x_i \notin \text{BAD}\,\right] \cdot \text{Prob}\left[\, \wedge_{i=1}^{2np(n)} x_i \notin \text{BAD}\,\right] \\
&\leq (2np(n)) \cdot \left(\frac{1}{4np(n)q(m)}\right) \cdot 1 \;+\; 1 \cdot (1 - 1/2p(n))^{2np(n)} \\
&\leq \left(\frac{1}{2q(m)}\right) \;+\; e^{-n} \\
&< \left(\frac{1}{q(m)}\right)
\end{aligned}$$

which negates our original assumption and therefore gives us a contradiction. □