SCIS 2012 The 29th Symposium on
Cryptography and Information Security
Kanazawa, Japan, Jan. 30 - Feb. 2, 2012
The Institute of Electronics,
Information and Communication Engineers

Instantiating the Random Oracle Using a Random Real

Kohtaro Tadaki * Norihisa Doi *

Abstract— In modern cryptography, the random oracle model is widely used as an *imaginary* framework in which the security of a cryptographic scheme is discussed. Since the random oracle is an imaginary object, even if the security of a cryptographic scheme is proved in the random oracle model, the random oracle has to be instantiated using a concrete cryptographic hash function such as the SHA hash functions if we want to use the scheme in the real world. However, it is not clear how much the instantiation can maintain the security originally proved in the random oracle model, nor is it clear whether the random oracle can be instantiated somehow while keeping the original security. In the present paper we investigate this problem, and consider the instantiation of the random oracle by a random real. Here, a *random real* is an individual infinite binary string which is classified as "random", and not a random variable. It plays a central role in the field of *algorithmic randomness*. Algorithmic randomness enables us to classify an individual infinite binary string into random or not. We show that the security proved in the random oracle model is firmly maintained after instantiating it by a random real. The results of this paper are based only on the definition of the security of a cryptographic scheme, and do not depend on specific schemes.

Keywords: random oracle model, provable security, instantiation, algorithmic randomness, algorithmic information theory, random real, Martin-Löf randomness

1 Introduction

In modern cryptography, *the random oracle model* is widely used as an *imaginary* framework in which the security of a cryptographic scheme is discussed. In the random oracle model, the cryptographic hash function used in a cryptographic scheme is formulated as a random variable uniformly distributed over all possibility of the function, called *the random oracle*, and the legitimate users and the adversary against the scheme are modeled so as to get the values of the hash function not by evaluating it in their own but by querying the random oracle [1]. Since the random oracle is an imaginary object, even if the security of a cryptographic scheme is proved in the random oracle model, the random oracle has to be instantiated using a concrete cryptographic hash function such as the SHA hash functions if we want to use the scheme in the real world. Once it is instantiated, however, the security proof is spoiled and goes back to square one. Actually, it is not clear how much the instantiation can maintain the security originally proved in the random oracle model, nor is it clear whether the random oracle can be instantiated somehow while keeping the original security.

In the present paper we investigate this problem, and consider the instantiation of the random oracle by a random real. Here, a *random real* is an individual infinite binary string which is classified as "random", and plays a central role in the field of *algorithmic randomness*. Algorithmic randomness, also known as *algorithmic information theory*, originated in the groundbreaking works of Solomonoff, Kolmogorov, and Chaitin in the mid-1960s. They independently introduced the notion of *program-size complexity*, also known as *Kolmogorov complexity*, in order to quantify the randomness of an individual object. Around the same time, Martin-Löf [8] introduced a measure theoretic approach to characterize the randomness of an individual infinite binary string. This approach, called *Martin-Löf randomness* nowadays, is one of the major notions in algorithmic randomness as well as program-size complexity. Later on, in the 1970s Schnorr [10] and Chaitin [2] showed that Martin-Löf randomness is equivalent to the randomness defined by program-size complexity in characterizing random infinite binary strings. In the 21st century, algorithmic randomness makes remarkable progress through close interaction with recursion theory [9, 4].

In cryptography, the randomness is just a probability distribution or its family. Namely, the true randomness in cryptography is a uniform probability distribution such as the random oracle, while the pseudorandomness is a family of probability distributions which has a certain computational complexity-theoretic property. Thus, cryptology has had no concern with the randomness of an individual object so far. In algorithmic randomness, on the other hand, a random real, i.e., a random infinite binary string, is not a random variable, unlike in cryptography. Algorithmic randomness enables us to classify an individual infinite binary string into random or not.

* Research and Development Initiative, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan. E-mail: tadaki@kc.chuo-u.ac.jp, doi@doi.ics.keio.ac.jp WWW: http://www2.odn.ne.jp/tadaki/

In this paper we show that the security proved in the random oracle model is firmly maintained after instantiating it by a random real. Actually, we give an equivalent condition for an individual oracle instantiating the random oracle to maintain the security in the random oracle model, in terms of certain variants of Martin-Löf randomness. The results of this paper are based only on the definition of the security of a cryptographic scheme, and do not depend on specific schemes.

The paper is organized as follows. We begin in Section 2 with some preliminaries to algorithmic randomness. In Section 3 we investigate the instantiation of the random oracle by a random real in public-key encryption schemes, and present an equivalent condition for an individual oracle instantiating the random oracle to maintain the security in the random oracle model. We then show in Section 4 that the same holds for the full-domain hash signature schemes in a general form. In Section 5 we present the instantiation by concrete random reals. We conclude this paper with a mention of the future direction of this work in Section 6.

2 Preliminaries

We start with some notation about numbers and strings which will be used in this paper. $\#S$ is the cardinality of S for any set S. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of natural numbers, and $\mathbb{N}^+$ is the set of positive integers. $\mathbb{Q}$ is the set of rational numbers.

$\{0,1\}^* = \{\lambda, 0, 1, 00, 01, 10, 11, 000, 001, 010, \dots\}$ is the set of finite binary strings where λ denotes the *empty string*, and $\{0,1\}^*$ is ordered as indicated. We identify any string in $\{0,1\}^*$ with a natural number in this order. For any $x \in \{0,1\}^*$, $|x|$ is the *length* of x. For any $n \in \mathbb{N}$, we denote by $\{0,1\}^n$ and $\{0,1\}^{\leq n}$ the sets $\{\, x \mid x \in \{0,1\}^* \ \&\ |x| = n\}$ and $\{\, x \mid x \in \{0,1\}^* \ \&\ |x| \leq n\}$, respectively. For any $n, m \in \mathbb{N}$, we denote by Func_n^m and $\mathsf{Func}_{\leq n}^m$ the set of all functions mapping $\{0,1\}^n$ to $\{0,1\}^m$ and the set of all functions mapping $\{0,1\}^{\leq n}$ to $\{0,1\}^m$, respectively. A subset S of $\{0,1\}^*$ is called *prefix-free* if no string in S is a prefix of another string in S.

$\{0,1\}^\infty$ is the set of infinite binary strings, where an infinite binary string is infinite to the right but finite to the left. For any $\alpha \in \{0,1\}^\infty$ and any $n \in \mathbb{N}$, we denote by $\alpha\restriction_n \in \{0,1\}^*$ the first n bits of α. For any function f, the *domain of definition* of f is denoted by $\operatorname{dom} f$. We write "r.e." instead of "recursively enumerable."

2.1 Algorithmic Randomness

In the following we concisely review some definitions and results of algorithmic randomness [2, 3, 9, 4].

The idea in algorithmic randomness is to think of a real, i.e., an infinite binary string, as random if it is in no *effective null set*. To specify an algorithmic randomness notion, one has to specify a type of effective null set, which is usually done by introducing a test concept. Failing the test is the same as being in the null set. In this manner, various randomness notions, such as 2-randomness, weak 2-randomness, Demuth randomness, Martin-Löf randomness, Schnorr randomness, Kurtz randomness, have been introduced so far, and a hierarchy of algorithmic randomness notions has been developed (see [9, 4] for the detail).

Among other randomness notions, *Martin-Löf randomness* is a central one. This is because in many respects, Martin-Löf randomness is well-behaved, in that the main properties of Martin-Löf random infinite strings do match our intuition of what random infinite string should look like. Moreover, the concept of Martin-Lof randomness is robust in the sense that it admits various equivalent definitions that are all natural and intuitively meaningful, as we will see in what follows. Martin-Löf randomness is defined as follows based on the notion of *Martin-Löf test*.

Definition 2.1 (Martin-Löf [8])**.** *A subset $\mathcal{C}$ of $\mathbb{N}^+ \times \{0,1\}^*$ is called a* Martin-Löf test *if $\mathcal{C}$ is an r.e. set and there exists a total recursive function $f\colon \mathbb{N}^+ \to \mathbb{Q} \cap (0, \infty)$ such that $\lim_{n\to\infty} f(n) = 0$ and for every $n \in \mathbb{N}^+$,*

$$\sum_{x \in \mathcal{C}_n} 2^{-|x|} \leq f(n),$$

where $\mathcal{C}_n = \{\, x \mid (n, x) \in \mathcal{C} \,\}$. For any $\alpha \in \{0,1\}^\infty$, we say that α is Martin-Löf random *if for every Martin-Löf test $\mathcal{C}$, there exists $n \in \mathbb{N}^+$ such that, for every $k \in \mathbb{N}^+$, $\alpha\restriction_k \notin \mathcal{C}_n$.*[1] □

One of the equivalent variants of Martin-Löf randomness is Solovay randomness, which plays a major role in this paper, as well as Martin-Löf randomness (see Chaitin [3] for the historical detail of Solovay randomness).

Definition 2.2. *A subset $\mathcal{C}$ of $\mathbb{N}^+ \times \{0,1\}^*$ is called a* Solovay test *if $\mathcal{C}$ is an r.e. set and*

$$\sum_{(n,x) \in \mathcal{C}} 2^{-|x|} < \infty,$$

where the sum is over all pairs $(n, x) \in \mathcal{C}$. For any $\alpha \in \{0,1\}^\infty$, we say that α is Solovay random *if for every Solovay test $\mathcal{C}$, there exists $N \in \mathbb{N}^+$ such that, for every $n > N$ and every $k \in \mathbb{N}^+$, $\alpha\restriction_k \notin \mathcal{C}_n$.* □

The robustness of Martin-Löf randomness is mainly due to the fact that it admits characterizations based on the notion of *program-size complexity*, as shown in Theorem 2.3. A *prefix-free machine* is a partial recursive function $M\colon \{0,1\}^* \to \{0,1\}^*$ such that $\operatorname{dom} M$ is a prefix-free set. For each prefix-free machine M and each $x \in \{0,1\}^*$, $K_M(x)$ is defined by $K_M(x) = \min\{\, |p| \mid p \in \{0,1\}^* \,\&\, M(p) = x \,\}$ (may be ∞). A prefix-free machine U is said to be *optimal* if for each prefix-free machine M there exists $d \in \mathbb{N}$ with the following property; if $p \in \operatorname{dom} M$, then there is $q \in \operatorname{dom} U$

[1] Normally, Martin-Löf random is defined with fixing the total recursive function $f\colon \mathbb{N}^+ \to \mathbb{Q} \cap (0, \infty)$ to the form $f(n) = 2^{-n}$. However, the relaxation of the function f as in Definition 2.1 does not alter the class of Martin-Löf random infinite binary strings.

for which $U(q) = M(p)$ and $|q| \leq |p|+d$. It is then easy to see that there exists an optimal prefix-free machine. We choose a particular optimal prefix-free machine U as the standard one for use, and define $K(x)$ as $K_U(x)$, which is referred to as the *program-size complexity* of x or the *Kolmogorov complexity* of x.

Theorem 2.3 (Schnorr [10] and Chaitin [3])**.** *For every $\alpha \in \{0,1\}^\infty$, the following conditions are equivalent:*

(i) α *is Martin-Löf random.*

(ii) α *is Solovay random.*

(iii) There exists $c \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $n - c \leq K(\alpha\restriction_n)$.

(iv) $\lim_{n\to\infty} K(\alpha\restriction_n) - n = \infty$. □

The condition (iii) means that the infinite binary string α is incompressible.

We denote by MLR the set of all infinite binary strings which are Martin-Löf random. Since there are only countably infinitely many algorithms and every Martin-Löf test induces an effective null set, it is easy to show the following.

Theorem 2.4 (Martin-Löf [8])**.** $\mathcal{L}(\mathsf{MLR}) = 1$ *where $\mathcal{L}$ is Lebesgue measure on $\{0,1\}^\infty$.* □

3 Public-Key Encryption

Let $\ell(n)$ be a polynomial. An *ℓ-function* is a function $H\colon \{0,1\}^* \to \{0,1\}^*$ such that $|H(x)| = \ell(|x|)$ for every $x \in \{0,1\}^*$. For each ℓ-function H and each $n \in \mathbb{N}$, we define a function $H|_n\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ by the condition that $H|_n(x) = H(x)$ for every $x \in \{0,1\}^n$.

Definition 3.1. *Let $\ell(n)$ be a polynomial. A* public-key encryption scheme relative to ℓ-functions *is a tuple* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *of probabilistic polynomial-time algorithms such that, for every ℓ-function H,*

1. *The* key generation algorithm Gen *takes as input the security parameter 1^n and outputs a pair of keys (pk, sk). We refer to the first of these as the* public key *and the second as the* private key*. We assume that n can be determined from each of pk and sk.*
2. *The* encryption algorithm Enc *takes as input a public key pk and a message m from some underling plaintext space (that may depend on pk). It is given oracle access to $H|_n(\cdot)$, and then outputs a ciphertext c. We write this as $c \leftarrow \mathsf{Enc}_{pk}^{H|_n(\cdot)}(m)$.*
3. *The* decryption algorithm Dec *takes as input a private key sk and a ciphertext c. It is given oracle access to $H|_n(\cdot)$, and then outputs a message m. We write this as $m := \mathsf{Dec}_{sk}^{H|_n(\cdot)}(c)$.*

It is required that, for all $d \in \mathbb{N}^+$, for all but finitely many n, for all ℓ-function H, for all (pk, sk) output by $\mathsf{Gen}(1^n)$, and for all messages m,

$$\Pr[\mathsf{Dec}_{sk}^{H|_n(\cdot)}(\mathsf{Enc}_{pk}^{H|_n(\cdot)}(m)) \neq m] \leq \frac{1}{n^d}$$

where the probability is taken over the internal coin tosses of the algorithms Enc *and* Dec. □

In this paper we consider the security of public-key encryption schemes against chosen-plaintext attacks as an example. We can show the same results for other security notions, such as the security against chosen-ciphertext attacks.

Consider the following experiment defined for a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ relative to ℓ-functions, a probabilistic polynomial-time adversary $\mathcal{A}$, a parameter n, and a function $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$:

The CPA indistinguishability experiment $\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n, G)$:

1. $\mathsf{Gen}(1^n)$ *is run to obtain keys (pk, sk).*
2. *Adversary $\mathcal{A}$ is given pk as well as oracle access to $G(\cdot)$. The adversary outputs a pair of messages m_0, m_1 of the same length. (These messages must be in the plaintext space associated with pk.)*
3. *A random bit $b \leftarrow \{0,1\}$ is chosen, and then a ciphertext $c \leftarrow \mathsf{Enc}_{pk}^{G(\cdot)}(m_b)$ is computed and given to $\mathcal{A}$.*
4. *$\mathcal{A}$ continues to have access to $G(\cdot)$, and outputs a bit b'.*
5. *The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.*

The CPA-security relative to a specific ℓ-function is defined as follows.

Definition 3.2. *Let H be an ℓ-function. A public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ relative to ℓ-functions has* indistinguishable encryptions under a chosen-plaintext attack *(or is* CPA-secure*)* relative to *H if for all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}^+$ there exists $N \in \mathbb{N}^+$ such that, for all $n > N$,*

$$\Pr[\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n, H|_n) = 1] \leq \frac{1}{2} + \frac{1}{n^d}.$$ □

On the other hand, the CPA-security in the random oracle model is formulated as follows.

Definition 3.3. *A public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ relative to ℓ-functions has* indistinguishable encryptions under a chosen-plaintext attack *(or is* CPA-secure*)* in the random oracle model *if for all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}^+$ there exists $N \in \mathbb{N}^+$ such that, for all $n > N$,*

$$\frac{1}{\#\mathsf{Func}_n^{\ell(n)}} \sum_{G \in \mathsf{Func}_n^{\ell(n)}} \Pr[\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n, G) = 1] \leq \frac{1}{2} + \frac{1}{n^d}.$$

□

We identify the set of all ℓ-functions with $\{0,1\}^\infty$ in the following manner. Each ℓ-function $H\colon \{0,1\}^* \to \{0,1\}^*$ is identified with the infinite binary string

$$H(0)H(1)H(00)H(01)H(10)H(11)H(000)\cdots\cdots.$$

Definition 3.4 (Solovay randomness with respect to an arbitrary set of Solovay tests)**.** *Let S be a set of Solovay tests. For any $\alpha \in \{0,1\}^\infty$, we say that α is* Solovay random with respect to S *if for every Solovay test $\mathcal{C} \in S$, there exists $N \in \mathbb{N}^+$ such that, for every $n > N$ and every $k \in \mathbb{N}^+$, $\alpha\restriction_k \notin \mathcal{C}_n$.* □

Definition 3.5. *Let $\ell(n)$ be a polynomial, and let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme relative to ℓ-functions. We define $\mathsf{S\text{-}TEST}^{\mathsf{cpa}}_\Pi$ as the class of all subsets $\mathcal{C}$ of $\mathbb{N}^+ \times \{0,1\}^*$ for which there exist a probabilistic polynomial-time adversary $\mathcal{A}$ and $d \geq 2$ such that $\mathcal{C}$ is the set of all*

$$(n, xG(0^n)G(0^{n-1}1)G(0^{n-2}10)\cdots G(1^{n-1}0)G(1^n))$$

which have the following properties (i) and (ii):

(i) $x \in \{0,1\}^*$ *and* $|x| = \sum_{k=1}^{n-1} \ell(k)2^k$.

(ii) $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ *and*

$$\Pr[\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n,G) = 1] - \frac{1}{2} > \frac{1}{n^d}.$$ □

Theorem 3.6. *Let $\ell(n)$ be a polynomial. Suppose that a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ relative to ℓ-functions is CPA-secure in the random oracle model. Then $\mathsf{S\text{-}TEST}^{\mathsf{cpa}}_\Pi$ contains only Solovay tests.* □

In order to prove Theorem 3.6, we need the following two lemmas.

Lemma 3.7. *Let $f_1, \ldots, f_N$ be reals. Suppose that $\frac{1}{N}\sum_{i=1}^N f_i \leq \varepsilon$. Then, for every $\alpha > 0$, the number of i for which $\alpha\varepsilon < f_i$ is less than N/α.*

Proof. We prove the contraposition of Lemma 3.7. Assume that the number of i for which $\alpha\varepsilon < f_i$ is at least N/α. Then $\sum_{i=1}^N f_i > \alpha\varepsilon N/\alpha = \varepsilon N$ and therefore $\frac{1}{N}\sum_{i=1}^N f_i > \varepsilon$. □

Lemma 3.8. *Let $d \in \mathbb{N}$ with $d \geq 2$.*

$$\sum_{k=n}^{\infty} \frac{1}{k^d} \leq \frac{1}{(d-1)(n-1)^{d-1}}.$$

Proof. The result follows from the inequality:

$$\sum_{k=n}^{\infty} \frac{1}{k^d} \leq \sum_{k=n}^{\infty} \int_{k-1}^{k} \frac{1}{k^d} = \int_{n-1}^{\infty} \frac{1}{x^d}dx = \frac{1}{(d-1)(n-1)^{d-1}}.$$ □

Proof of Theorem 3.6. Let $\mathcal{C} \in \mathsf{S\text{-}TEST}^{\mathsf{cpa}}_\Pi$. Then there exist a probabilistic polynomial-time adversary $\mathcal{A}$ and $d \geq 2$ such that $\mathcal{C}$ is the set of all

$$(n, xG(0^n)G(0^{n-1}1)G(0^{n-2}10)\cdots G(1^{n-1}0)G(1^n))$$

which have the properties (i) and (ii) in Definition 3.5. Suppose that Π is CPA-secure in the random oracle model. Then it follows from Definition 3.3 that there exists $N \in \mathbb{N}^+$ such that, for all $n > N$,

$$\frac{1}{\#\mathsf{Func}_n^{\ell(n)}} \sum_{G \in \mathsf{Func}_n^{\ell(n)}} \left(\Pr[\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n,G) = 1] - \frac{1}{2} \right) \leq \frac{1}{n^{2d}}.$$

Using Lemma 3.7 with $\varepsilon = 1/n^{2d}$ and $\alpha = n^d$, we see that, for every $n > N$,

$$\#\left\{ G \;\middle|\; \Pr[\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n,G) = 1] - \frac{1}{2} > \frac{1}{n^d} \right\} < \frac{\#\mathsf{Func}_n^{\ell(n)}}{n^d}.$$

It is then easy to see that $\mathcal{C}$ is an r.e. set, since the dyadic rational $\Pr[\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n,G) = 1]$ is computable, given n and $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$. On the other hand, since $\#\mathsf{Func}_n^{\ell(n)} = 2^{\ell(n)2^n}$, it is also easy to see that

$$\sum_{(n,y)\in\mathcal{C}\ \&\ n>N} 2^{-|y|} < \sum_{n>N} \frac{\#\mathsf{Func}_n^{\ell(n)}}{n^d} 2^{-\ell(n)2^n} = \sum_{n>N} \frac{1}{n^d} < \infty,$$

where the first sum is over all pairs $(n,y) \in \mathcal{C}$ with $n > N$, and the last inequality follows from Lemma 3.8. Thus $\mathcal{C}$ is a Solovay test. □

Definition 3.9 (Martin-Löf randomness with respect to an arbitrary set of Martin-Löf tests)**.** *Let S be a set of Martin-Löf tests. For any $\alpha \in \{0,1\}^\infty$, we say that α is* Martin-Löf random with respect to S *if for every Martin-Löf test $\mathcal{C} \in S$, there exists $n \in \mathbb{N}^+$ such that, for every $k \in \mathbb{N}^+$, $\alpha\restriction_k \notin \mathcal{C}_n$.* □

Definition 3.10. *Let $\ell(n)$ be a polynomial, and let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme relative to ℓ-functions. We define $\mathsf{ML\text{-}TEST}^{\mathsf{cpa}}_\Pi$ as the class of all subsets $\mathcal{C}$ of $\mathbb{N}^+ \times \{0,1\}^*$ for which there exists $\mathcal{D} \in \mathsf{S\text{-}TEST}^{\mathsf{cpa}}_\Pi$ such that, for every $n \in \mathbb{N}^+$, $\mathcal{C}_n = \bigcup_{k=n}^\infty \mathcal{D}_k$.* □

Theorem 3.11. *Let $\ell(n)$ be a polynomial. Suppose that a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ relative to ℓ-functions is CPA-secure in the random oracle model. Then $\mathsf{ML\text{-}TEST}^{\mathsf{cpa}}_\Pi$ contains only Martin-Löf tests.*

Proof. Let $\mathcal{C} \in \mathsf{ML\text{-}TEST}^{\mathsf{cpa}}_\Pi$. Then there exists $\mathcal{D} \in \mathsf{S\text{-}TEST}^{\mathsf{cpa}}_\Pi$ such that, for every $n \in \mathbb{N}^+$, $\mathcal{C}_n = \bigcup_{k=n}^\infty \mathcal{D}_k$. Suppose that Π is CPA-secure in the random oracle model. It follows from Theorem 3.6 that $\mathcal{D}$ is a Solovay test. It is then easy to see that $\mathcal{C}$ is an r.e. set, since $\mathcal{D}$ is an r.e. set. On the other hand, since $\mathcal{D} \in \mathsf{S\text{-}TEST}^{\mathsf{cpa}}_\Pi$,

there exist a probabilistic polynomial-time adversary $\mathcal{A}$ and $d \geq 2$ such that $\mathcal{D}$ is the set of all

$$(n, xG(0^n)G(0^{n-1}1)G(0^{n-2}10)\cdots G(1^{n-1}0)G(1^n))$$

which have the properties (i) and (ii) in Definition 3.5. Then, in the same manner as the proof of Theorem 3.6 we can show that there exists $N \in \mathbb{N}^+$ such that, for every $n > N$,

$$\#\left\{ G \;\middle|\; \Pr[\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n, G) = 1] - \frac{1}{2} > \frac{1}{n^d} \right\} < \frac{\#\mathsf{Func}_n^{\ell(n)}}{n^d}.$$

It follows that, for each $n > N$,

$$\sum_{y \in \mathcal{C}_n} 2^{-|y|} \leq \sum_{k=n}^{\infty} \sum_{s \in \mathcal{D}_k} 2^{-|s|} < \sum_{k=n}^{\infty} \frac{\#\mathsf{Func}_k^{\ell(k)}}{k^d} 2^{-\ell(k)2^k}$$
$$= \sum_{k=n}^{\infty} \frac{1}{k^d} \leq \frac{1}{(d-1)(n-1)^{d-1}}.$$

Thus $\mathcal{C}$ is a Martin-Löf test. □

Definition 3.12. *Let $\ell(n)$ be a polynomial, and let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme relative to ℓ-functions. We denote by $\mathsf{SecrH}^{\mathsf{cpa}}_{\Pi}$ the set of all ℓ-functions $H\colon \{0,1\}^* \to \{0,1\}^*$ such that Π is CPA-secure relative to H.* □

Theorem 3.13. *Let $\ell(n)$ be a polynomial. Suppose that a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ relative to ℓ-functions is CPA-secure in the random oracle model. Let $H\colon \{0,1\}^* \to \{0,1\}^*$ be an ℓ-function. Then the following conditions are equivalent:*

(i) $H \in \mathsf{SecrH}^{\mathsf{cpa}}_{\Pi}$.

(ii) H is Solovay random with respect to $\mathsf{S\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$.

(iii) H is Martin-Löf random with respect to $\mathsf{ML\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$.

Proof. First we show the equivalence between the conditions (i) and (ii). The negation of the condition (i) is that there exist a probabilistic polynomial-time adversary $\mathcal{A}$ and $d \geq 2$ such that, for infinitely many $n \in \mathbb{N}^+$,

$$\Pr[\mathsf{PubK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n, H|_n) = 1] - \frac{1}{2} > \frac{1}{n^d}.$$

However, it is easy to see that this is equivalent to the condition that there exists $\mathcal{C} \in \mathsf{S\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$ such that, for infinitely many $n \in \mathbb{N}^+$, there exists $k \in \mathbb{N}^+$ such that $H\restriction_k \in \mathcal{C}_n$. This is further equivalent to the condition that H is not Solovay random with respect to $\mathsf{S\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$, since $\mathsf{S\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$ contains only Solovay tests by Theorem 3.6. Thus the conditions (i) and (ii) are equivalent to each other.

Next we show the equivalence between the conditions (ii) and (iii). Suppose that $\mathcal{C} \in \mathsf{ML\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$ and $\mathcal{D} \in \mathsf{S\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$ satisfy that $\mathcal{C}_n = \bigcup_{k=n}^{\infty} \mathcal{D}_k$ for all $n \in \mathbb{N}^+$. Then the condition that for all $n \in \mathbb{N}^+$ there exists $k \in \mathbb{N}^+$ such that $H\restriction_k \in \mathcal{C}_n$ is equivalent to the condition that for infinitely many $n \in \mathbb{N}^+$ there exists $k \in \mathbb{N}^+$ such that $H\restriction_k \in \mathcal{D}_n$. Note here that $\mathsf{ML\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$ contains only Martin-Löf tests by Theorem 3.11, and $\mathsf{S\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$ contains only Solovay tests by Theorem 3.6. Thus, H is not Martin-Löf random with respect to $\mathsf{ML\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$ if and only if H is not Solovay random with respect to $\mathsf{S\text{-}TEST}^{\mathsf{cpa}}_{\Pi}$. This completes the proof. □

Obviously, the following proposition holds.

Proposition 3.14. *Let $\alpha \in \{0,1\}^\infty$.*

(i) For every set S of Martin-Löf tests, if α is Martin-Löf random then α is Martin-Löf random with respect to S.

(ii) For every set S of Solovay tests, if α is Solovay random then α is Solovay random with respect to S. □

Theorem 3.15. *Let $\ell(n)$ be a polynomial. Suppose that a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ relative to ℓ-functions is CPA-secure in the random oracle model. For every ℓ-function H, if H is Martin-Löf random then $H \in \mathsf{SecrH}^{\mathsf{cpa}}_{\Pi}$.*

Proof. The result follows immediately from Theorem 3.13 and Proposition 3.14. □

Theorem 3.16. *Let $\ell(n)$ be a polynomial. Suppose that a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ relative to ℓ-functions is CPA-secure in the random oracle model. Then $\mathcal{L}(\mathsf{SecrH}^{\mathsf{cpa}}_{\Pi}) = 1$, where $\mathcal{L}$ is Lebesgue measure on $\{0,1\}^\infty$.*

Proof. The result follows immediately from Theorem 2.4 and Theorem 3.15. □

4 Signature Schemes

Let $\ell(n)$ be a polynomial. An *ℓ-family* is a family $\{H_n\}_{n \in \mathbb{N}^+}$ such that $H_n\colon \{0,1\}^* \to \{0,1\}^{\ell(n)}$ for all $n \in \mathbb{N}^+$.

Definition 4.1. *Let $\ell(n)$ be a polynomial. A* signature scheme relative to ℓ-families *is a tuple* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ *of three probabilistic polynomial-time algorithms such that, for every ℓ-family $\{H_n\}_{n \in \mathbb{N}^+}$,*

1. *The* key generation algorithm Gen *takes as input a security parameter 1^n and outputs a pair of keys (pk, sk). These are called the* public key *and the* private key*, respectively. We assume that n can be determined from each of pk and sk.*

2. *The* signing algorithm Sign *takes as input a private key sk and a message $m \in \{0,1\}^*$. It is given oracle access to $H_n(\cdot)$, and then outputs a signature σ, denoted as $\sigma \leftarrow \mathsf{Sign}_{sk}^{H_n(\cdot)}(m)$.*

3. *The deterministic* verification algorithm Vrfy *takes as input a public key pk, a massage m, and a signature σ. It is given oracle access to $H_n(\cdot)$, and then outputs a bit b, with $b = 1$ meaning* valid *and $b = 0$ meaning* invalid*. We write this as $b := \mathsf{Vrfy}_{pk}^{H_n(\cdot)}(m, \sigma)$.*

It is required that, for every $n \in \mathbb{N}^+$, for every ℓ-family $\{H_n\}_{n\in\mathbb{N}^+}$, for every (pk, sk) output by $\mathsf{Gen}(1^n)$, and for every $m \in \{0,1\}^*$,

$$\mathsf{Vrfy}_{pk}^{H_n(\cdot)}(m, \mathsf{Sign}_{sk}^{H_n(\cdot)}(m)) = 1. \qquad \square$$

Let $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a signature scheme relative to ℓ-families, and consider the following experiment for a probabilistic polynomial-time adversary $\mathcal{A}$, a parameter n, and a function G mapping a superset of $\{0,1\}^{\leq q(n)}$ to $\{0,1\}^{\ell(n)}$ where $q(n)$ is the maximum value between the running time of $\mathcal{A}$ and the running time of Sign on the parameter n:

The signature experiment $\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(n, G)$:

1. *$\mathsf{Gen}(1^n)$ is run to obtain keys (pk, sk).*
2. *Adversary $\mathcal{A}$ is given pk and oracle access to $\mathsf{Sign}_{sk}^{G(\cdot)}(\cdot)$ and $G(\cdot)$. (The first oracle returns a signature $\mathsf{Sign}_{sk}^{G(\cdot)}(m)$ for any message m of the adversary's choice.) The adversary then outputs (m, σ). Let $\mathcal{Q}$ denotes the set of messages whose signatures were requested by $\mathcal{A}$ during its execution.*
3. *The output of the experiment is defined to be 1 if and only if* **(1)** *$m \notin \mathcal{Q}$, and* **(2)** *$\mathsf{Vrfy}_{pk}^{G(\cdot)}(m, \sigma) = 1$.*

The existential unforgeability of signature schemes under adaptive chosen-message attacks relative to a specific ℓ-family is defined as follows.

Definition 4.2. *Let $\{H_n\}_{n\in\mathbb{N}^+}$ be an ℓ-family. A signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-families is* existentially unforgeable under an adaptive chosen-message attack relative to $\{H_n\}_{n\in\mathbb{N}^+}$ *if for all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}^+$ there exists $N \in \mathbb{N}^+$ such that, for all $n > N$,*

$$\Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(n, H_n) = 1] \leq \frac{1}{n^d}. \qquad \square$$

On the other hand, the existential unforgeability of signature schemes under adaptive chosen-message attacks in the random oracle model is formulated as follows.

Definition 4.3. *A signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-families is* existentially unforgeable under an adaptive chosen-message attack in the random oracle model *if for all probabilistic polynomial-time adversaries $\mathcal{A}$ and all $d \in \mathbb{N}^+$ there exists $N \in \mathbb{N}^+$ such that, for all $n > N$,*

$$\frac{1}{\#\mathsf{Func}_{\leq q(n)}^{\ell(n)}} \sum_{G\in\mathsf{Func}_{\leq q(n)}^{\ell(n)}} \Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(n, G) = 1] \leq \frac{1}{n^d},$$

where $q(n)$ is the maximum value between the running time of $\mathcal{A}$ and the running time of Sign on the parameter n. $\square$

We identify the set of all ℓ-families with $\{0,1\}^\infty$ in the following manner: We choose a particular bijective total recursive function $b\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ with $b(k) = (b_1(k), b_2(k))$ as the standard one for use throughout the rest of this paper. We assume for convenience that, for every $k, l \in \mathbb{N}$, if $b_1(k) = b_1(l)$ and $k < l$ then $b_2(k) < b_2(l)$. For example, the inverse function of a function $c\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with $c(m, n) = (m + n)(m + n + 1)/2 + n$ can serve as such a function b. Then each ℓ-family $\{H_n\}_{n\in\mathbb{N}^+}$ is identified with the infinite binary string

$$H_{b_1(0)}(b_2(0))H_{b_1(1)}(b_2(1))H_{b_1(2)}(b_2(2))\cdots\cdots. \quad (1)$$

Recall here that we identify $\{0,1\}^*$ with $\mathbb{N}$, and therefore each $b_2(k)$ is regarded as a finite binary string in (1).

Definition 4.4. *Let $\ell(n)$ be a polynomial, and let $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a signature scheme relative to ℓ-families. We define $\mathsf{S\text{-}TEST}_\Pi^{\mathsf{acma}}$ as the class of all subsets $\mathcal{C}$ of $\mathbb{N}^+ \times \{0,1\}^*$ for which there exist a probabilistic polynomial-time adversary $\mathcal{A}$ and $d \geq 2$ such that $\mathcal{C}$ is the set of all*

$$(n, x_0 G(\lambda) x_1 G(0) x_2 G(1) x_3 \cdots x_{f(n)} G(1^{q(n)}))$$

which have the following properties (i), (ii), and (iii):

(i) $q(n)$ is the maximum value between the running time of $\mathcal{A}$ and the running time of Sign on the parameter n, and $f(n) = 2^{q(n)+1} - 1$.

(ii) For each $i = 0, \ldots, f(n)$, $x_i \in \{0,1\}^*$ and

$$|x_0 G(\lambda) x_1 G(0) x_2 G(1) x_3 \cdots x_i| = \sum_{k<k_i} \ell(b_1(k)),$$

where k_i is a natural number such that $b(k_i) = (n, i)$.

(iii) $G\colon \{0,1\}^{\leq q(n)} \to \{0,1\}^{\ell(n)}$ and

$$\Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(n, G) = 1] > \frac{1}{n^d}. \qquad \square$$

Theorem 4.5. *Let $\ell(n)$ be a polynomial. Suppose that a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-families is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. Then $\mathsf{S\text{-}TEST}_\Pi^{\mathsf{acma}}$ contains only Solovay tests.*

Proof. Let $\mathcal{C} \in \mathsf{S\text{-}TEST}_\Pi^{\mathsf{acma}}$. Then there exist a probabilistic polynomial-time adversary $\mathcal{A}$ and $d \geq 2$ such that $\mathcal{C}$ is the set of all

$$(n, x_0 G(\lambda) x_1 G(0) x_2 G(1) x_3 \cdots x_{f(n)} G(1^{q(n)}))$$

which have the properties (i), (ii), and (iii) in Definition 4.4. Suppose that a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-families is existentially unforgeable under an adaptive chosen-message attack in

the random oracle model. Then it follows from Definition 4.3 that there exists $N \in \mathbb{N}^+$ such that, for all $n > N$,

$$\frac{1}{\#\mathsf{Func}^{\ell(n)}_{\le q(n)}} \sum_{G \in \mathsf{Func}^{\ell(n)}_{\le q(n)}} \Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(n, G) = 1] \le \frac{1}{n^{2d}}.$$

Using Lemma 3.7 with $\varepsilon = 1/n^{2d}$ and $\alpha = n^d$, we see that, for every $n > N$,

$$\#\left\{ G \;\middle|\; \Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(n, G) = 1] > \frac{1}{n^d} \right\} < \frac{\#\mathsf{Func}^{\ell(n)}_{\le q(n)}}{n^d}.$$

It is then easy to see that $\mathcal{C}$ is an r.e. set, since the dyadic rational $\Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(n, G) = 1]$ is computable, given n and $G\colon \{0,1\}^{\le q(n)} \to \{0,1\}^{\ell(n)}$. On the other hand, since $\#\mathsf{Func}^{\ell(n)}_{\le q(n)} = 2^{\ell(n)(2^{q(n)+1}-1)}$, it is also easy to see that, for each $n > N$,

$$\begin{aligned}\sum_{(n,y)\in\mathcal{C}\ \&\ n>N} 2^{-|y|} &< \sum_{n>N} \frac{\#\mathsf{Func}^{\ell(n)}_{\le q(n)}}{n^d} 2^{-\ell(n)(2^{q(n)+1}-1)} \\ &= \sum_{n>N} \frac{1}{n^d} < \infty,\end{aligned}$$

where the first sum is over all pairs $(n, y) \in \mathcal{C}$ with $n > N$, and the last inequality follows from Lemma 3.8. Thus $\mathcal{C}$ is a Solovay test. □

Definition 4.6. *Let $\ell(n)$ be a polynomial, and let $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a signature scheme relative to ℓ-families. We define $\mathsf{ML\text{-}TEST}^{\mathsf{acma}}_{\Pi}$ as the class of all subsets $\mathcal{C}$ of $\mathbb{N}^+ \times \{0,1\}^*$ for which there exists $\mathcal{D} \in \mathsf{S\text{-}TEST}^{\mathsf{acma}}_{\Pi}$ such that, for every $n \in \mathbb{N}^+$, $\mathcal{C}_n = \bigcup_{k=n}^{\infty} \mathcal{D}_k$.* □

Theorem 4.7. *Let $\ell(n)$ be a polynomial. Suppose that a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-families is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. Then $\mathsf{ML\text{-}TEST}^{\mathsf{acma}}_{\Pi}$ contains only Martin-Löf tests.*

Proof. Let $\mathcal{C} \in \mathsf{ML\text{-}TEST}^{\mathsf{acma}}_{\Pi}$. Then there exists $\mathcal{D} \in \mathsf{S\text{-}TEST}^{\mathsf{acma}}_{\Pi}$ such that, for every $n \in \mathbb{N}^+$, $\mathcal{C}_n = \bigcup_{k=n}^{\infty} \mathcal{D}_k$. Suppose that Π is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. It follows from Theorem 4.5 that $\mathcal{D}$ is a Solovay test. It is then easy to see that $\mathcal{C}$ is an r.e. set, since $\mathcal{D}$ is an r.e. set. On the other hand, since $\mathcal{D} \in \mathsf{S\text{-}TEST}^{\mathsf{acma}}_{\Pi}$, there exist a probabilistic polynomial-time adversary $\mathcal{A}$ and $d \ge 2$ such that $\mathcal{D}$ is the set of all

$$(n, x_0 G(\lambda) x_1 G(0) x_2 G(1) x_3 \cdots x_{f(n)} G(1^{q(n)}))$$

which have the properties (i), (ii), and (iii) in Definition 4.4. Then, in the same manner as the proof of Theorem 4.5 we can show that there exists $N \in \mathbb{N}^+$ such that, for every $n > N$,

$$\#\left\{ G \;\middle|\; \Pr[\mathsf{Sig\text{-}forge}_{\mathcal{A},\Pi}(n, G) = 1] > \frac{1}{n^d} \right\} < \frac{\#\mathsf{Func}^{\ell(n)}_{\le q(n)}}{n^d}.$$

It follows that, for each $n > N$,

$$\begin{aligned}\sum_{y\in\mathcal{C}_n} 2^{-|y|} &\le \sum_{k=n}^{\infty} \sum_{s\in\mathcal{D}_k} 2^{-|s|} \\ &< \sum_{k=n}^{\infty} \frac{\#\mathsf{Func}^{\ell(k)}_{\le q(k)}}{k^d} 2^{-\ell(k)(2^{q(k)+1}-1)} \\ &= \sum_{k=n}^{\infty} \frac{1}{k^d} \le \frac{1}{(d-1)(n-1)^{d-1}}.\end{aligned}$$

Thus $\mathcal{C}$ is a Martin-Löf test. □

Definition 4.8. *Let $\ell(n)$ be a polynomial, and let $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a signature scheme relative to ℓ-families. We denote by $\mathsf{ExstUnfrg}^{\mathsf{acma}}_{\Pi}$ the set of all ℓ-families $\{H_n\}_{n\in\mathbb{N}^+}$ such that Π is existentially unforgeable under an adaptive chosen-message attack relative to $\{H_n\}_{n\in\mathbb{N}^+}$.* □

In a similar manner to the proof of Theorem 3.13, we can show the following theorem based on Theorems 4.5 and 4.7.

Theorem 4.9. *Let $\ell(n)$ be a polynomial. Suppose that a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-families is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. Let $\{H_n\}_{n\in\mathbb{N}^+}$ be an ℓ-family. Then the following conditions are equivalent:*

(i) $\{H_n\}_{n\in\mathbb{N}^+} \in \mathsf{ExstUnfrg}^{\mathsf{acma}}_{\Pi}$.

(ii) $\{H_n\}_{n\in\mathbb{N}^+}$ *is Solovay random with respect to* $\mathsf{S\text{-}TEST}^{\mathsf{acma}}_{\Pi}$.

(iii) $\{H_n\}_{n\in\mathbb{N}^+}$ *is Martin-Löf random with respect to* $\mathsf{ML\text{-}TEST}^{\mathsf{acma}}_{\Pi}$. □

Theorem 4.10. *Let $\ell(n)$ be a polynomial. Suppose that a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-families is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. For every ℓ-family $\{H_n\}_{n\in\mathbb{N}^+}$, if $\{H_n\}_{n\in\mathbb{N}^+}$ is Martin-Löf random then $\{H_n\}_{n\in\mathbb{N}^+} \in \mathsf{ExstUnfrg}^{\mathsf{acma}}_{\Pi}$.*

Proof. The result follows immediately from Theorem 4.9 and Proposition 3.14. □

Theorem 4.11. *Let $\ell(n)$ be a polynomial. Suppose that a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-families is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. Then $\mathcal{L}(\mathsf{ExstUnfrg}^{\mathsf{acma}}_{\Pi}) = 1$.*

Proof. The result follows immediately from Theorem 2.4 and Theorem 4.10. □

5 Security by Concrete Random Reals

While a real is almost surely Martin-Löf random by Theorem 2.4, only a few concrete examples of random reals are known. Chaitin [2] introduced the halting probability Ω defined by

$$\Omega = \sum_{p\in\operatorname{dom} U} 2^{-|p|}.$$

Recall here that U is an optimal prefix-free machine used to define the notion of program-size complexity $K(x)$. He then showed that the base-two expansion of Ω is Martin-Löf random. On the other hand, Tadaki [11] introduced another type of Martin-Löf random real, called Θ, based on all compressible finite binary strings. It is defined by

$$\Theta = \sum_{K(x) \leq |x|} 2^{-|x|}.$$

The reals Ω and Θ are not a computable real but a left-computable real, i.e., a real which can be approximated from below by a computable increasing sequence of rationals converging to it. By Theorems 3.15 and 4.10 we have Theorems 5.1 and 5.2 below, respectively.

Theorem 5.1. *Let $\ell(n)$ be a polynomial. Suppose that a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ relative to ℓ-functions is CPA-secure in the random oracle model. Then Π is CPA-secure relative to each of Ω and Θ, where Ω and Θ are regarded as an ℓ-function via their base-two expansions.* □

Theorem 5.2. *Let $\ell(n)$ be a polynomial. Suppose that a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ relative to ℓ-families is existentially unforgeable under an adaptive chosen-message attack in the random oracle model. Then Π is existentially unforgeable under an adaptive chosen-message attack relative to each of Ω and Θ, where Ω and Θ are regarded as an ℓ-family via their base-two expansions.* □

6 Concluding Remarks

In this paper we have considered the instantiation of the random oracle. We have derived equivalent conditions for an individual oracle instantiating the random oracle to maintain the security originally proved in the random oracle model, in terms of a variant of Martin-Löf randomness or Solovay randomness. These equivalent conditions depend on the combination of a cryptographic scheme and its security notion being considered.

For example, if a public-key encryption scheme Π is CPA-secure in the random oracle model, the set $\mathsf{SecrH}_{\Pi}^{\mathsf{cpa}}$ of all oracles instantiating the random oracle which maintain CPA-security is characterized in terms of a set $\mathsf{ML\text{-}TEST}_{\Pi}^{\mathsf{cpa}}$ of Martin-Löf tests. In the same manner, if another public-key encryption scheme Π' is CCA-secure in the random oracle model, we can characterize the set $\mathsf{SecrH}_{\Pi'}^{\mathsf{cca}}$ of all oracles which maintain CCA-security, in terms of a set $\mathsf{ML\text{-}TEST}_{\Pi'}^{\mathsf{cca}}$ of Martin-Löf tests. The comparison between the two sets $\mathsf{SecrH}_{\Pi}^{\mathsf{cpa}}$ and $\mathsf{SecrH}_{\Pi'}^{\mathsf{cca}}$ may lead to revealing which is easier to instantiate between the CPA-security of Π and the CCA-security of Π'. Thus, future work may aim at comparing various sets of oracles instantiating the random oracle which maintain the security originally proved in the random oracle model for each combination of cryptographic scheme and security notion, in terms of Martin-Löf tests or Solovay tests. To do so, we may use the techniques developed in algorithmic randomness so far. This effort may develop a hierarchy of sets of oracles in which each set is ordered according to the degree of reality of instantiation.

Note also that our results are valid only if the security in the random oracle model is confirmed already. This may imply that the random oracle model is not necessarily an imaginary framework to discuss the security of a cryptographic scheme, but may have substantial implications for the security of it in the standard model.

Acknowledgments

This work was supported by the Ministry of Economy, Trade and Industry of Japan. The first author was also supported by KAKENHI (23340020) and KAKENHI (23650001), and by CREST from Japan Science and Technology Agency.

References

[1] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," Proceedings of the 1st ACM Conference on Computer and Communications Security, ACM, pp.62–73, 1993.

[2] G. J. Chaitin, "A theory of program size formally identical to information theory," *J. Assoc. Comput. Mach.*, vol. 22, pp. 329–340, 1975.

[3] G. J. Chaitin, *Algorithmic Information Theory*. Cambridge University Press, Cambridge, 1987.

[4] R. G. Downey and D. R. Hirschfeldt, *Algorithmic Randomness and Complexity*. Springer-Verlag, New York, 2010.

[5] O. Goldreich, *Foundations of Cryptography: Volume 1 – Basic Tools*. Cambridge University Press, New York, 2001.

[6] O. Goldreich, *Foundations of Cryptography: Volume 2 – Basic Applications*. Cambridge University Press, New York, 2004.

[7] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman & Hall/CRC Press, 2007.

[8] P. Martin-Löf, "The definition of random sequences," *Information and Control*, vol. 9, pp. 602–619, 1966.

[9] A. Nies, *Computability and Randomness*. Oxford University Press, Inc., New York, 2009.

[10] C.-P. Schnorr, "Process complexity and effective random tests," *J. Comput. System Sci.*, vol. 7, pp. 376–388, 1973.

[11] K. Tadaki, "A Chaitin Ω number based on compressible strings," To appear in *Nat. Comput.*, DOI: 10.1007/s11047-011-9272-y.