Security of Encryption Schemes in Weakened Random Oracle Models
(Extended Abstract)

Akinori Kawachi, Akira Numayama, Keisuke Tanaka, and Keita Xagawa

Department of Mathematical and Computing Sciences, Tokyo Institute of Technology,
W8-55, 2-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan
{kawachi,numayam4,keisuke,xagawa5}@is.titech.ac.jp

Abstract. Liskov proposed several weakened versions of the random oracle model, called *weakened random oracle models* (WROMs), to capture the vulnerability of ideal compression functions, which are expected to have the standard security of hash functions, i.e., collision resistance, second-preimage resistance, and one-wayness properties. The WROMs offer additional oracles to break such properties of the random oracle. In this paper, we investigate whether public-key encryption schemes in the random oracle model essentially require the standard security of hash functions by the WROMs. In particular, we deal with four WROMs associated with the standard security of hash functions; the standard, collision tractable, second-preimage tractable, first-preimage tractable ones (ROM, CT-ROM, SPT-ROM, and FPT-ROM, respectively), done by Numayama et al. for digital signature schemes in the WROMs. We obtain the following results: (1) The OAEP is secure in all the four models. (2) The encryption schemes obtained by the Fujisaki-Okamoto conversion (FO) are secure in the SPT-ROM. However, some encryption schemes with FO are insecure in the FPT-ROM. (3) We consider two artificial variants wFO and dFO of FO for separation of the WROMs in the context of encryption schemes. The encryption schemes with wFO (dFO, respectively) are secure in the CT-ROM (ROM, respectively). However, some encryption schemes obtained by wFO (dFO, respectively) are insecure in the SPT-ROM (CT-ROM, respectively). These results imply that standard encryption schemes such as the OAEP and FO-based one do not always require the standard security of hash functions. Moreover, in order to make our security proofs complete, we construct an efficient sampling algorithm for the binomial distribution with exponentially large parameters, which was left open in Numayama et al.'s paper.

Keywords: public-key encryption schemes, weakened random oracle models, OAEP, Fujisaki-Okamoto conversion.

1 Introduction

Background. In order to design new cryptographic schemes, we often follow the random oracle methodology [1]. First, we analyze the security of cryptographic schemes, by idealizing hash functions as truly random functions called the *random oracle*. When it comes to implementations of these schemes, we replace the random oracles by cryptographic hash functions such as MD5 [2] and SHA-1 [3]. This replacement is called an instantiation of the random oracle.

P.Q. Nguyen and D. Pointcheval (Eds.): PKC 2010, LNCS 6056, pp. 403–419, 2010.

The random oracle methodology causes a trade-off between efficiency and provable security. The schemes proven secure in the random oracle model (ROM) are in general more efficient than those proven secure in the standard model. However, the security proofs in the ROM do not directly guarantee the security in the standard model, i.e., an instantiation of the random oracle might make the cryptographic schemes insecure. Even worse, several recent works [4,5,6] showed that some schemes secure in the ROM have no secure instantiation.

There are several properties of the ROM to prove the security of cryptographic properties. In particular, the ROM is expected to satisfy the one-wayness, second-preimage resistance, and collision resistance properties. We call these properties as the *standard security of hash functions*. These properties are indeed critical in many schemes for their security proofs. For example, the security of the Full-Domain-Hash (FDH) signature schemes (e.g., [7]), which are secure in the ROM, relies on the collision-resistance property of the ROM. That is, if we can obtain two distinct messages m, m' such that $H(m) = H(m')$ and the signature $\sigma = \mathsf{Sig}(H(m))$, then we can obtain a valid forgery (m', σ), where H is a hash function and Sig is a signing algorithm. Leurent and Nguyen also presented the attacks extracting the secret keys on several *hash-then-sign* type signature schemes and identity-based encryption schemes if the underlying hash functions are not collision resistant [8].

Recent progress on the attacks against cryptographic hash functions such as MD5 and SHA-1 raises the question on the assumption that hash functions are collision resistant and one-way (e.g.,[9,10,11]). Therefore, it is significant to investigate whether the collision resistance property (as well as the one-wayness and second-preimage resistance properties, which are weaker notions than the collision resistance one) of the ROM is essential to prove the security of the schemes or not. More generally, it is worth classifying the schemes by the first-preimage, second-preimage, and collision resistance properties of the ROM that their security essentially requires.

Weak versions of random oracle models. Several works recently highlighted some specific properties of the ROM for secure cryptographic constructions in the ROM.

Nielsen proposed the *non-programmable* random oracle model where the random oracle is not *programmable* [12]. In this model, one cannot set the values that the random oracle answers to some convenient values. It was showed in [12] that a non-interactive non-committing encryption scheme exists in the ROM (assuming that trapdoor permutations exists), but not in the *non-programmable* random oracle model.

Unruh proposed a ROM with *oracle-dependent* auxiliary inputs [13]. In this setting, adversaries obtain an auxiliary input that contains information with respect to the random oracle (e.g. collisions). He showed that the RSA-OAEP encryption scheme [14] is secure in the ROM even under the presence of *oracle-dependent* auxiliary inputs.

Liskov proposed several weakened versions of the random oracle model, called *weakened random oracle models* (WROMs), which offer additional oracles to break some properties of the random oracle [15]. These model captures the situation that adversaries are given an attack algorithm for breaking some specific property of the functions. For example, the first-preimage tractable random oracle model offers the random oracle and the first-preimage oracle associated with the random oracle, which returns a first-preimage of the random oracle to adversaries. This first-preimage oracle

then corresponds to the attack to the first preimage property of a hash function. We can replace the additional oracle to others such as the second-preimage and collision ones that correspond to the attack to the properties. Thus, the WROMs can capture vulnerability of hash functions even if the parties are allowed to utilize ideal ones as in the ROM. By using WROMs, Liskov constructed hash functions based on weak ideal compression functions and proved it is indifferentiable from the random oracle.

Several results already analyzed the security in the WROMs. Hoch and Shamir applied Liskov's idea to prove the indifferentiability of another hash construction [16]. Pasini and Vaudenay also applied Liskov's idea to the security analysis of digital signature schemes [17]. They considered the security of *hash-then-sign* type signature schemes in the first-preimage tractable random oracle model. Numayama, Isshiki, and Tanaka formalized the WROMs, which allows us to formally analyze the security of the schemes [18]. By using these models, they classified several digital signature schemes by the properties of the ROM. Fischlin and Lehmann also proposed a weakened random oracle model in a similar way to Liskov's one in the context of secure combiners [19].

Our contributions. In this paper, we investigate whether public-key encryption schemes constructed in the ROM essentially require the standard security of hash functions by further extending the direction originated from Liskov. In particular, we consider their security in the standard, collision tractable, second-preimage tractable, and first-preimage tractable random oracle models (ROM, CT-ROM, SPT-ROM, and FPT-ROM, respectively for short). Note that they are ordered according to their strengths, i.e., the security of encryption schemes in the FPT-ROM implies that in the SPT-ROM and such implications hold between each adjacent two models.

We demonstrate that the security notions in the four WROMs can be strictly separated in the context of encryption schemes. For the separation, we focus on the security of the encryption schemes obtained by the Fujisaki-Okamoto conversion (FO) [20], its two artificial variants (dFO and wFO), and the OAEP [14]. Precisely, we prove the following four statements:

1. OAEP is IND-CCA2 secure in the FPT-ROM.
2. FO is IND-CCA2 secure in the SPT-ROM, but *not* IND-CPA secure in the FPT-ROM.
3. wFO is IND-CCA2 secure in the CT-ROM, but *not* IND-CCA2 secure in the SPT-ROM.
4. dFO is IND-CCA2 secure in the ROM, but *not* IND-CCA2 secure in the CT-ROM.

We summarize the security of four schemes in Table 1.

Table 1. Security of four schemes

scheme/model	ROM	CT-ROM	SPT-ROM	FPT-ROM
OAEP	secure			
FO	secure			insecure
wFO	secure		insecure	
dFO	secure	insecure		

This separation suggests that some public-key encryption schemes essentially require the standard security of hash functions. These notions were also separated in the context of digital signature schemes in [18]. We stress that the role of the collision and second-preimage oracles in encryption schemes is not as clear as that in digital signature schemes. For example, it is easy to see that the collision oracle, breaking the collision resistance property of the random oracle, directly makes a simple scheme vulnerable, but not so easy for the case of encryption schemes. Actually, we need to develop new proof techniques for the (in)security of encryption schemes under additional oracles.

It also suggests that standard encryption schemes such as the OAEP and FO-based ones do not always require the standard security of hash functions for the random oracle. We believe that our results do not only give an example of the first application of the WROMs to encryption schemes, but they are also of independent interest. As far as we know, our results give the first evidence that the OAEP encryption scheme can be used in a practical application even without the first-preimage resistance property, i.e., the one-wayness property. In other words, the OAEP remains secure even if we remove the first-preimage resistance property. This can also be said on FO-based encryption schemes on the second-preimage resistance property.

On the security of the OAEP, Kiltz and Pietrzak recently showed that there is no construction for padding-based encryption schemes including the OAEP that has a black-box reduction from ideal trapdoor permutations to its IND-CCA2 security in [21]. However, they wrote in the paper that the security proof in the ROM can be still a valid argument in practice. We believe so is our security proof in the WROMs.

For the security proof, we explicitly show how to sample approximately in polynomial time from binomial distributions with exponentially large parameters, that is, a polynomial-time sampling algorithm whose output distribution is statistically close to the binomial distribution. For this algorithm, we arrange and combine sampling algorithms that run over real numbers proposed in the field of statistics [22,23,24,25], and give a precise analysis for discretization.

It should be noted that on the security proofs of the digital signature schemes in the WROMs [18], Numayama et al. assumed such an efficient sampling algorithm and thus gave no explicit construction. They left the construction of the sampling algorithm as an open problem. By the sampling algorithm we explicitly show, it is no longer necessary to assume the sampling algorithm in their security proofs of the digital signature schemes [18] as well as those of the public-key encryption scheme in this paper.

The sampling algorithm shown in this paper is adapted for cryptographic use since the statistical closeness to the original distribution is measured by the total variation distance, which is standard in cryptography but not usually required in statistics. The sampling algorithm is useful for other cryptographic tasks as in Numayama et al.'s and this paper.

Comparisons with other models. As mentioned above, a few models that weaken the power of the random oracle were already proposed such as the non-programmable model [12] and the oracle-dependent auxiliary input model [13].

The non-programmable model is not simply comparable with WROMs since the programmability does not imply the collision resistance and vice versa. The target of the oracle-dependent auxiliary input model partially overlaps that of the WROMs.

For a simple comparison, we now focus on the security of the OAEP in both models. Unruh showed a similar result as ours for the OAEP encryption scheme [13]. He proposed a random oracle model where oracle-dependent auxiliary inputs are allowed. In his setting, the adversary of some cryptographic protocol obtains an auxiliary input that contains the information (e.g., collisions) on the random oracle. He showed that the OAEP encryption scheme [14] is still secure in the random oracle model even in his model. This result indicates an important fact that the security of the OAEP encryption scheme does not depend on the collision resistance property since the oracle-dependent auxiliary input can contain a sufficiently long list of collisions.

Our results also present the security of the OAEP in a weak version of the random oracle. However, there are at least two differences between Unruh's result and ours. First, the random oracle model with the oracle-dependent auxiliary input does not completely capture the *adaptive* security of hash functions, and this model still has the second-preimage resistance and the first-preimage resistance properties. Hence, only by his result, we cannot say whether these two properties are necessary or not in order to prove the security of the OAEP encryption scheme. In contrast to Unruh's result, our result clearly shows that the two adaptive securities of hash functions such as the first-preimage resistance and the second-preimage resistance are not necessary to prove the security of the OAEP encryption scheme.

Second, Unruh constructed the reduction algorithm which breaks the partial-domain one-wayness of the underlying trapdoor permutation using the adversary which breaks the IND-CCA2 security of the OAEP encryption scheme. The running time of the reduction algorithm is not bounded by any polynomial. Therefore, he use the security amplification technique for the partial-domain one-wayness. By using this technique, he can avoid employing a stronger assumption that even quasi-polynomial time adversary cannot break the partial-domain one-wayness, and can prove the security under the standard partial-domain one-wayness against polynomial-time adversary.

In contrast to Unruh's result, we construct the polynomial-time reduction algorithm using the adversary, and hence we do not require the security amplification technique for the partial-domain one-wayness, which can be considered as a simplification of Unruh's proof.

Organization. In Section 2, we describe the details of the WROMs and their properties. We also discuss the simulation methods that are applicable to these models. In Section 3, after reviewing the encryption schemes we consider, we show their (in)security in the WROMs. Many technical details will be omitted from this extended abstract. We will describe them in the full version [26].

Notation. Before starting technical parts of this paper, we introduce our notation used in the rest of the paper. For a table $\mathbb{T} = \{(x, y)\}$, we define $\mathbb{T}(y) = \{(x', y') \in \mathbb{T} \mid y' = y\}$. For a distribution D, $x \leftarrow D$ denotes that x is sampled according to D. The function $D(x)$ stands for the probability function of the distribution D.

Let $s \leftarrow S$ denote that s is sampled from the uniform distribution over a finite set S. $\#S$ denotes the number of elements in S. For a probabilistic Turing machine $\mathcal{A}$ and its input x, let $\mathcal{A}(x)$ denote the output distribution of $\mathcal{A}$ on input x.

We usually denote by k a security parameter of a cryptographic scheme in this paper. We also denote by k' length of plaintexts unless it is specified. k' is implicitly assumed

to be polynomially related to the security parameter k, that is, $k' = k^{\Theta(1)}$. We say a function $f(k)$ is negligible in k if $f(k) \leq 2^{-\omega(\log k)}$. For two distributions D_1 and D_2 over a finte set S, we denote the statistical distance (the total variation distance) between them by $\Delta(D_1, D_2)$, defined by $\frac{1}{2}\sum_{s\in S} |D_1(s) - D_2(s)|$. We say two distributions D_1 and D_2 are statistically close if $\Delta(D_1, D_2) \leq 2^{-\omega(\log k)}$.

2 The Weakened Random Oracle Models

In this section, we first review the definitions of the WROMs. Next, we present an important property called *weak uniformity* of the WROMs, which is useful for security proofs of encryption schemes. We also discuss the simulation methods of [18] used for the security proofs in the WROMs.

2.1 Definitions of the Weakened Random Oracle Models

To give formal definitions of the WROMs, we define some notation. Let X and Y be finite sets. Let H be a hash function chosen randomly from all of the functions from X to Y. We denote by $\mathbb{T}_H$ the table $\{(x, H(x)) \mid x \in X\}$. We identify the hash function H with the table $\mathbb{T}_H$.

We next define the random oracle and the additional oracles associated with $H : X \to Y$ as follows. (For more details, see [18].)

Random oracle $\mathcal{RO}^H$: Given x, return y such that $(x, y) \in \mathbb{T}_H$.

Collision oracle $\mathcal{CO}^H$: On the query, first pick one entry $(x, y) \in \mathbb{T}_H$ uniformly at random. If there is no other entry $(x', y) \in \mathbb{T}_H$, then answer $\perp$. Otherwise, pick one entry $(x', y) \in \mathbb{T}_H$ satisfying $x \neq x'$ uniformly at random and answer (x, x').

Second-preimage oracle $\mathcal{SPO}^H$: Given (x, y), if $(x, y) \notin \mathbb{T}_H$ answer $\perp$. If there is no other entry $(x', y) \in \mathbb{T}_H$, then answer $\perp$. Otherwise, pick one entry $(x', y) \in \mathbb{T}_H$ satisfying $x \neq x'$ uniformly at random and answer x'.

First-preimage oracle $\mathcal{FPO}^H$: Given y, if there is any entry $(x, y) \in \mathbb{T}_H$ then return such an x uniformly at random. Otherwise return $\perp$.

Remark 1. We usually identify the random oracle and the underlying hash function. However, in this paper as in [18], we explicitly distinguish them by regarding the random oracle as an interface to the underlying hash function. This setting helps us to make the WROMs with an additional oracle well-defined.

The formal definitions of the WROMs are given as follows. The WROMs consist of three components, a hash function h chosen randomly from all of the functions from X to Y, the random oracle, and the additional oracle associated with h. The models are called the CT-ROM, SPT-ROM, and FPT-ROM, if the additional oracle is the collision, second-preimage, and first-preimage oracle, respectively.

Remark 2. The collision oracle may output $\perp$ even if there exists a collision (x, x') in the table. This stems from the simulation method of Numayama et al. [18], and causes no serious problems. Note that the collision oracle outputs $\perp$ with probability

$(1 - 1/\#Y)^{\#X-1}$. In the case where $\#X \geq \#Y$, we can find a collision with polynomially many queries since since $(1 - 1/\#Y)^{\#X-1} \leq \exp(-(\#X - 1)/\#Y)$. In the case where $\#Y = k^{O(1)} \cdot \#X$, we can again find a collision with polynomially many queries $(1 - 1/\#Y)^{\#X-1} \leq 1 - 1/k^{O(1)}$. Finally, in the case where $\#Y = k^{\omega(1)} \cdot \#X$, the following lemma shows that there are no collisions with overwhelming probability.

Lemma 1. *Let $H : X \to Y$ be the hash function, and n_y the number of preimages of y under the function H, that is, $n_y = \#\mathbb{T}_H(y)$. Let BAD denote the event that there is some y such that $n_y > L$. Then for all sufficiently large Y, we have $\Pr_H[\mathsf{BAD}] < \frac{1}{(\#Y)^2}$, where $L = \frac{5 \ln \#Y}{\ln \ln \#Y} \frac{\#X}{\#Y}$ if $\#X \geq \#Y$, or $L = \frac{5 \ln \#Y}{\ln \ln \#Y}$ otherwise.*

The proof is obtained by the standard argument on the balls and bins game by regarding X and Y as sets of balls and bins, respectively. For the details on the game, see a standard textbook (e.g., [27]).

2.2 Difference from the Random Oracle Model

We observe an important difference between the ROM and WROMs by considering the ROM and FPT-ROM. In the both models, the function H, i.e., the table $\mathbb{T}_H$ is uniformly distributed.

In the ROM, if one queries some x that has never been queried to the random oracle, the value of $H(x)$ is uniformly distributed regardless of the past queries. That is, the knowledge of the past queries does not affect the entries not queried in the table. This property of the ROM is called *uniformity*. In contrast to the situation in the ROM, when it comes to the FPT-ROM, this property is not attained. Recall that the first-preimage oracle *uniformly* returns one of the preimages, say x, of queried value y. If the first-preimage oracle leaks a number of preimages of y, the value of $H(x)$ is *not* uniformly distributed for an x not queried yet.

In order to observe this situation, let us consider the following extreme case. Let $y^* = H(x^*)$ for some $x^* \in X$ and suppose that y^* has the unique preimage x^*. Then the first-preimage oracle always returns the same x^* on the input y^*, which convinces us that the number of the preimages of y^* is exactly 1. This implies that the other $x \neq x^*$ does not take a value y^* under H. Therefore, the random oracle no longer has the uniformity in the FPT-ROM. This is a critical difference between the ROM and FPT-ROM since we often make use of the uniformity in the security proofs of the public-key encryption schemes.

We prove the following lemma to overcome this barrier in the WROMs, which states that the WROMs still has weak uniformity instead of the uniformity. The weak uniformity is still useful for the security proofs of the public-key encryption schemes in the WROMs.

Lemma 2 (Weak Uniformity). *In the WROMs, the output distribution of the random oracle is statistically close to the uniform distribution. More formally, it is stated as follows. Let $H : X \to Y$ be the hash function in the WROMs. Let $\mathcal{A}$ be a probabilistic oracle Turing machine that makes at most q queries to the random oracle $\mathcal{RO}^H$ and the additional oracle O^H, where O^H represents one of the additional oracles $\mathcal{CO}^H$, $\mathcal{SPO}^H$, and $\mathcal{FPO}^H$. $V_{\mathcal{A},H}(x)$ denotes the random variable that represents the hash value*

$\mathcal{RO}^H(x)$, where $x \leftarrow \mathcal{A}^{\mathcal{RO}^H,O^H}$ and the correspondence $(x, H(x)) \in \mathbb{T}_H$ is not answered by the two oracles.

Then, for any $\mathcal{A}$, the following holds:

$$\Delta(V_{\mathcal{A},H}(x), U_Y) \leq \begin{cases} \frac{1}{\#Y}\left(5q + 1 + \frac{4q^2}{\#Y} + 20q\frac{\ln \#Y}{\ln\ln \#Y}\right) & \text{if } \#X \geq \#Y, \\ \frac{1}{\#X}\left(5q + 1 + \frac{4q^2}{\#X} + 20q\frac{\ln \#Y}{\ln\ln \#Y}\right) & \text{if } \#X < \#Y. \end{cases}$$

Here, the probability is taken over random choices of the hash function H and the random coin of $\mathcal{A}$.

2.3 Simulation Methods

In almost all the security proofs in the ROM, the reduction algorithms simulate the random oracles. When it comes to the security proofs in the WROMs, the reduction algorithms have to simulate both the random and the additional oracle, which makes differences of the simulation methods in the WROMs from those in the ROM.

Numayama et al.'s methods. Numayama et al. proposed the simulation methods for WROMs, but they required an unproven assumption. Let $B_{N,p}$ denote the binomial distribution with parameters N and p whose probability function is $B_{N,p}(x) = \binom{N}{x} p^x(1-p)^{N-x}$ for $x = 0, \ldots, N$, where the parameters N and p take values approximately $\#X$ and $1/\#Y$ for a hash function $H : X \to Y$, say, $(N, p) = (2^{128}, 2^{-128})$. Their simulation methods required the efficient sampler for $B_{N,p}$ with exponentially large N and small p, and they assumed its existence.

Assumption 1. *There is a probabilistic Turing machine $\mathsf{B_N}$ such that the output distribution $\mathsf{B_N}(N, p)$ on inputs N and p is equal to the binomial distribution $B_{N,p}$ and it runs in polynomial time in $\log N$ and $\log p^{-1}$, where N is a positive integer and $0 \leq p \leq 1$ is a rational number.*

Under this assumption, they constructed the simulation algorithms, RO, CO, SPO, and FPO, for the security proofs in the WROMs as given in the following proposition. See [18] for the details of the algorithms.

Proposition 1 (Simulation Method [18]). *We can perfectly simulate the random oracle, the collision oracle, second-preimage oracle, and first-preimage oracle in the* WROM*s under Assumption 1. That is, the output distributions of the random oracle, collision oracle, second-preimage oracle, and first-preimage oracle in the* WROM*s are identical to the output distributions of the algorithms* RO*,* CO*,* SPO*, and* FPO*, under Assumption 1.*

Removing the assumption. For the security proof in the WROMs of digital signature schemes in [18] and encryption schemes in this paper, it is sufficient to utilize a weaker sampling algorithm that generates a distribution *not equal but statistically close* to the binomial distribution $B_{N,p}$. Then, their security proofs can work by just adding negligibly small errors induced by the statistical distance in their analyses.

There are quite many papers (e.g., [25]) on the efficient sampling methods from the binomial distribution in the field of statistics. However, their basic computation model is totally different from the model in the cryptography. As far as the authors' knowledge, all these results are based on the computation model that directly manipulates *real* numbers without errors. If we translate them to those in the bit computation model used in the cryptography, we have to bound the statistical distance between the real distribution and the output distribution generated by the sampling algorithms in the bit computation model rather than the real-number one. Numayama et al. mentioned that they could neither find precise analyses of the statistical distance, nor construct the sampling algorithms by themselves in [18]. Therefore, they had to put the above assumption.

In fact, there is an efficient sampling algorithm appropriate for our purpose in the real-number computation model [25]. We modify the algorithm and rigorously analyze the error bound in the bit computation model. We can finally obtain the following theorem on the sampling algorithm.

Theorem 1. *There is a probabilistic Turing machine* $\mathsf{B_N}$ *such that, for the output distribution* $\mathsf{B_N}(N, p, \epsilon)$ *on inputs* N, p *and* ϵ*, the statistical distance between* $\mathsf{B_N}(N, p, \epsilon)$ *and* $B_{N,p}$ *is at most* ϵ *and it runs in polynomial time in* $\log N, \log p^{-1}$ *and* $\log \epsilon^{-1}$*, where* N *is a positive integer and* $0 \le p \le 1, 0 < \epsilon \le 1$ *are rational numbers.*

Note that the algorithm can control the error parameter ϵ. This property is useful in cryptographic applications for the security proofs even if the other parameters N and p are not sufficiently large. We will put the details of the algorithm and its analysis in the full version.

As a result, we can remove the above assumption and obtain the following theorem.

Theorem 2 (Simulation Method without Assumption 1). *We can statistically simulate the random oracle, collision oracle, second-preimage oracle, and first-preimage oracle in the* WROM*s. That is, the output distributions of the oracles in the* WROM*s are statistically close to the output distributions of the algorithms* RO*,* CO*,* SPO*, and* FPO*, respectively.*

3 The Encryption Schemes and Their Security in the Weakened Random Oracle Models

In this section, we examine the security in the WROMs of the public-key encryption schemes. We particularly discuss separations for notions of ROM, CT-ROM, SPT-ROM, and FPT-ROM by showing (in)security of public-key encryption schemes obtained by the Fujisaki-Okamoto conversion (FO) and its two variants (dFO and wFO), and OAEP.

Public-key encryption schemes. We first give notation and notions for public-key encryption schemes briefly. For details, see standard textbooks, e.g., [28].

A public-key encryption scheme $\mathcal{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a plaintext space $\mathcal{M}$ and a random coin space $\mathcal{R}$ is defined by the following three algorithms. Let k denote the security parameter.

Key Generation: On input 1^k, the key generation algorithm $\mathsf{Gen}(1^k)$ produces a public/secret key pair $(\mathsf{pk}, \mathsf{sk})$.

Encryption: Given a public key pk, a plaintext $m \in \mathcal{M}$, and a random string $r \in \mathcal{R}$, the encryption algorithm $\mathsf{Enc}_{\mathsf{pk}}(m; r)$ outputs a ciphertext c corresponding to the plaintext m.

Decryption: Given a secret key sk and ciphertext c, the decryption algorithm $\mathsf{Dec}_{\mathsf{sk}}(c)$ outputs the plaintext $m \in \mathcal{M}$ or the special symbol $\perp \notin \mathcal{M}$ corresponding to the ciphertext c.

We require the perfect completeness, that is, for every $(\mathsf{pk}, \mathsf{sk})$ generated by $\mathsf{Gen}(1^k)$, every plaintext $m \in \mathcal{M}$, and every random string $r \in \mathcal{R}$, it should be satisfied that $\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(m; r)) = m$.

We only consider three standard security notions for public-key encryption schemes, the one-wayness against chosen-plaintext attack (OW-CPA), the indistinguishability against chosen-plaintext attack (IND-CPA), and the indistinguishability against adaptive chosen-ciphertext attack (IND-CCA2).

For $\gamma = \gamma(k)$, we say $\mathcal{PKE}$ is γ-uniform if for any key pair $(\mathsf{pk}, \mathsf{sk})$ generated by $\mathsf{Gen}(1^k)$, any $m \in \mathcal{M}$, and $c \in \{0,1\}^*$, we have $\Pr_{r \leftarrow \mathcal{R}}[c = \mathsf{Enc}_{\mathsf{pk}}(m; r)] \leq \gamma$. There exists a OW-CPA public-key encryption scheme with γ-uniformity (e.g., the ElGamal encryption scheme).

Brief review for FO. Fujisaki and Okamoto proposed a conversion, called the Fujisaki-Okamoto (FO) conversion, to obtain highly secure public-key encryption schemes in the ROM [20]. Since the standard one-time pad satisfies the requirement of the FO conversion, we fix the one-time pad as the symmetric-key encryption scheme used in the FO conversion for simplicity.

Let $\mathcal{PKE}$ be a OW-CPA secure and γ-uniform public-key encryption scheme over a plaintext space $\mathcal{M}$ and a randomness space $\mathcal{R}$. Then the FO conversion converts $\mathcal{PKE}$ to an IND-CCA2 secure one $\mathcal{PKE}' = \mathrm{FO}(\mathcal{PKE})$ over a plaintext space $\mathcal{M}' = \{0,1\}^{k'}$ and a randomness space $\mathcal{R}' = \mathcal{M}$, where k' denotes the length of plaintexts, which is polynomially related to the security parameter k. The encryption procedure of $\mathcal{PKE}'$ is given as follows: For a plaintext $m \in \mathcal{M}' = \{0,1\}^{k'}$ and a random string $r \in \mathcal{R}' = \mathcal{M}$, the ciphertext is

$$(c_1, c_2) = (\mathsf{Enc}_{\mathsf{pk}}(r; H(m, r)), G(r) \oplus m),$$

where $H : \{0,1\}^{k'} \times \mathcal{M} \to \mathcal{R}$ and $G : \mathcal{M} \to \{0,1\}^{k'}$ are hash functions modeled as the random oracles. The decryption procedure is given as follows: For a given ciphertext (c_1, c_2), decrypt c_1 by sk and obtain r. Then, extract m by $c_2 \oplus G(r)$ and verify $c_1 = \mathsf{Enc}_{\mathsf{pk}}(r; H(m, r))$. If not output $\perp$. Roughly speaking, $H(m, r)$ ensures that if a ciphertext (c_1, c_2) is valid then the encryptor producing (c_1, c_2) knows corresponding m and r.

3.1 The First Variant dFO

We introduce the first artificial variant dFO and show that dFO is secure in the ROM, but not secure in general in the CT-ROM.

The variant dFO converts a public-key encryption scheme $\mathcal{PKE}$ (with the one-time pad) to another public-key encryption scheme $\mathcal{PKE}' = \mathrm{dFO}(\mathcal{PKE})$ similarly to FO. The encryption procedure of $\mathcal{PKE}'$ is defined as follows. For a plaintext $m \in \mathcal{M}' = \{0,1\}^{k'}$ and a random string $r \in \mathcal{R}' = \mathcal{M}$, the ciphertext of $\mathcal{PKE}'$ is

$$(c_1, c_2) = (\mathsf{Enc}_{\mathsf{pk}}(r; H(F(m), r)), G(r) \oplus m),$$

where $F : \{0,1\}^{k'} \to \mathcal{P}$, $G : \mathcal{M} \to \{0,1\}^{k'}$, and $H : \mathcal{P} \times \mathcal{M} \to \mathcal{R}$, for an appropriate set $\mathcal{P}$, are hash functions modeled as the random oracle.

The idea to weaken the conversion is summarized as follows: Recall that $H(m, r)$ in the FO conversion can be considered as encryptor's signature (or a proof of knowledge) on m and r. To make it vulnerable by a collision, we introduce a new random oracle F and replace $H(m, r)$ with $H(F(m), r)$. The replacement does not harm the security in the random oracle model, while it can be exploited by the presence of the collision oracle CO^F.

Formally, we have following theorems on the (in)security. We omit the proof of Theorem 3, which is similar to the original one.

Theorem 3. *Assume that $\mathcal{PKE}$ is a* OW-CPA *secure and γ-uniform public-key encryption scheme for some negligible γ. Then, $\mathcal{PKE}'$ = dFO($\mathcal{PKE}$) is* IND-CCA2 *secure in the* ROM *if $\#\mathcal{P} = 2^{\omega(\log k)}$.*

Theorem 4. *Let $\mathcal{PKE}$ be a public-key encryption scheme. If $\#\mathcal{P} \leq 2^{k'}$ then $\mathcal{PKE}'$ = dFO($\mathcal{PKE}$) is not* IND-CCA2 *secure in the* CT-ROM.

Proof. We construct the adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that breaks the IND-CCA2 security of $\mathcal{PKE}'$, which exploits the collision oracle CO^F of F.

The adversary $\mathcal{A}_1$, on input pk, first queries to CO^F. If the answer is $\perp$, then the adversary flips a random fair coin b', outputs b', and halts. Otherwise, it obtains a collision (m_1, m_2) of F and outputs it as a challenge. The adversary $\mathcal{A}_2$ receives the target ciphertext $(c_1^*, c_2^*) = (\mathsf{Enc}_{\mathsf{pk}}(r; H(F(m_b), r)), G(r) \oplus m_b)$ for some $r \in \mathcal{R}'$. It queries $(c_1', c_2') = (c_1^*, c_2^* \oplus m_0 \oplus m_1)$ to the decryption oracle and obtains m_{1-b}, since

$$c_1' = \mathsf{Enc}_{\mathsf{pk}}(r; H(F(m_0), r)) = \mathsf{Enc}_{\mathsf{pk}}(r; H(F(m_1), r)),$$
$$c_2' = G(r) \oplus m_b \oplus m_0 \oplus m_1 = G(r) \oplus m_{1-b}.$$

Hence, the adversary can answer $b' = b$ correctly.

Finally, we upper-bound the probability that the collision oracle outputs $\perp$, which stems from the definition of the collision oracle. The probability is bounded by $(1 - 1/\#\mathcal{P})^{2^{k'}-1} \leq \exp(-(2^{k'} - 1)/\#\mathcal{P}) \leq 1/\sqrt{e}$. This completes the proof. □

3.2 The Second Variant wFO

We next introduce the second artificial variant wFO and show that the obtained scheme by wFO is secure in the CT-ROM, however not generally secure in the SPT-ROM.

The encryption procedure of $\mathcal{PKE}'$ = wFO($\mathcal{PKE}$) is given as follows. For a plaintext $m \in \mathcal{M}' = \{0,1\}^{k'}$ and random strings $(r, s) \in \mathcal{R}' = \mathcal{M} \times \mathcal{S}$, the ciphertext of $\mathcal{PKE}'$ is

$$(c_1, c_2, c_3) = (\mathsf{Enc}_{\mathsf{pk}}(r; H(F(m, s), r)), G(r) \oplus m, s),$$

where $F : \{0,1\}^{k'} \times \mathcal{S} \to \mathcal{P}$, $G : \mathcal{M} \to \{0,1\}^{k'}$, and $H : \mathcal{P} \times \mathcal{M} \to \mathcal{R}$ are hash functions modeled as the random oracles.

Notice that $(H(F(m, s), r), s)$ is a proof of knowledge on (m, r, s) which resists a collision on F however is vulnerable by a second-preimage attack against F as in Numayama et al. [18].

We can show that the obtained scheme is IND-CCA2 secure in the CT-ROM by using Lemma 2.

Theorem 5. *Suppose that $\mathcal{PKE}$ is a* OW-CPA *secure and γ-uniform public-key encryption scheme for some negligible γ. Then, $\mathcal{PKE}' = \mathrm{wFO}(\mathcal{PKE})$ is* IND-CCA2 *secure in the* CT-ROM *if $\#\mathcal{P}^{-1}$ and $\#\mathcal{S}^{-1}$ are negligible in k.*

However, its security is broken under the presence of the second-preimage oracle for F.

Theorem 6. *Let $\mathcal{PKE}$ be a public-key encryption. If $\#\mathcal{P} \leq 2^{k'} \cdot \#\mathcal{S}$, then the scheme $\mathcal{PKE}' = \mathrm{wFO}(\mathcal{PKE})$ is not* IND-CCA2 *secure in the* SPT-ROM.

Proof. We construct the adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that exploits the second-preimage oracle $\mathcal{SPO}^F$ associated to F. The adversary $\mathcal{A}_1$ chooses random distinct plaintexts m_0 and m_1 and queries them to the challenger. The challenger responses

$$(c_1^*, c_2^*, c_3^*) = (\mathsf{Enc}_{\mathsf{pk}}(r; H(F(m_b, s), r)), G(r) \oplus m_b, s).$$

Receiving (c_1^*, c_2^*, c_3^*), the adversary $\mathcal{A}_2$ queries (m_0, s) to the second-preimage oracle $\mathcal{SPO}^F$. If it receives $\perp$ from the second-preimage oracle, then it flips a random fair coin b', outputs b', and halts. Otherwise, it obtains $(m', s') \neq (m_0, s)$ such that $F(m_0, s) = F(m', s')$. So, the adversary queries

$$(c_1', c_2', c_3') = (c_1^*, c_2^* \oplus m_0 \oplus m', s')$$

to the decryption oracle. Notice that, if (c_1^*, c_2^*, c_3^*) is the valid ciphertext of m_0, then we have

$$\begin{aligned} c_1' &= \mathsf{Enc}_{\mathsf{pk}}(r; H(F(m_0, s), r)) = \mathsf{Enc}_{\mathsf{pk}}(r; H(F(m', s'), r)), \\ c_2' &= G(r) \oplus m_0 \oplus m_0 \oplus m' = G(r) \oplus m', \\ c_3' &= s', \end{aligned}$$

and (c_1', c_2', c_3') is a valid ciphertext for m'. On the other hand, if the ciphertext is the encryption of m_1, we have

$$(c_1', c_2', c_3') = (\mathsf{Enc}_{\mathsf{pk}}(r; H(F(m_1, s), r)), G(r) \oplus m_1 \oplus m_0 \oplus m', s').$$

Thus, if $f = F(m_1, s)$ is equal to $F(m_1 \oplus m_0 \oplus m', s')$ the decryption oracle returns $m_1 \oplus m_0 \oplus m' (\neq m')$. Otherwise, the decryption oracle returns $\perp$.

Thus, if the answer is m', then the adversary concludes that (c_1^*, c_2^*, c_3^*) is the ciphertext of m_0, that is, it outputs $b' = 0$. Otherwise, the adversary concludes that it is the ciphertext of m_1, that is, it outputs $b' = 1$. Therefore, $\mathcal{A}$ can output the correct answer unless $\mathcal{A}$ receives $\perp$ from the second-preimage oracle.

We finally bound the probability that the oracle outputs $\perp$. It is bounded by $(1 - 1/\#\mathcal{P})^{2^{k'} \cdot \#\mathcal{S} - 1} \leq \exp(-(2^{k'} \cdot \#\mathcal{S} - 1)/\#\mathcal{P}) \leq 1/\sqrt{e}$ as required. This completes the proof. □

3.3 The Original Fujisaki-Okamoto Conversion

We next show that the obtained scheme by the conversion FO with the one-time pad is secure in the SPT-ROM, but not secure in the FPT-ROM in some parameter setting.

Let $G : \mathcal{M} \to \{0,1\}^{k'}$ and $H : \{0,1\}^{k'} \times \mathcal{M} \to \mathcal{R}$ be hash functions modeled as the random oracles. Recall the encryption procedure of $\mathcal{PKE}' = \mathrm{FO}(\mathcal{PKE})$. For a plaintext $m \in \mathcal{M}' = \{0,1\}^{k'}$ and a random string $r \in \mathcal{R}' = \mathcal{M}$, the ciphertext is $(\mathsf{Enc}_{\mathsf{pk}}(r; H(m,r)), G(r) \oplus m)$.

Modifying the existing proofs, we can show the scheme is secure in the SPT-ROM using Lemma 2.

Theorem 7. *Suppose that $\mathcal{PKE}$ is* OW-CPA *secure and γ-uniform for some negligible γ. Then, $\mathcal{PKE}' = \mathrm{FO}(\mathcal{PKE})$ is* IND-CCA2 *secure in the* SPT-ROM.

However, the presence of the first-preimage oracle for G violates the IND-CPA security of $\mathcal{PKE}'$ in some parameter settings. Note that if m is $0^{k'}$, the second component of the ciphertext is $G(r)$, which is vulnerable the first-preimage oracle of G.

Theorem 8. *Let $C = \#\mathcal{M}/2^{k'}$. Assume that $C = k^{O(1)}$. Then, $\mathcal{PKE}' = \mathrm{FO}(\mathcal{PKE})$ is not* IND-CPA *secure in the* FPT-ROM.

Proof. We prove the theorem by constructing the adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ which exploits the first-preimage oracle of G, $\mathcal{FPO}^G$. The adversary $\mathcal{A}_1$, on input pk, queries $m_0 = 0^{k'}$ and $m_1 = 1^{k'}$ to the challenger. The adversary $\mathcal{A}_2$, on input the target ciphertext (c_1^*, c_2^*), queries c_2^* to the first-preimage oracle of G. If it obtains $\tilde{r}$, it checks that $c_1 = \mathsf{Enc}_{\mathsf{pk}}(\tilde{r}; H(0^{k'}, \tilde{r}))$. If the check passes, the adversary outputs $b' = 0$. Otherwise, it flips a random fair coin b', outputs b', and halts.

It is obvious that if $b = 0$ and $\tilde{r} = r$, the adversary answers correctly, that is, it outputs $b' = b$. If $b = 1$, the preimage of the query $G(r) \oplus 1^{k'}$ never equals to r since $G(r) \neq G(r) \oplus 1^{k'}$. Hence, the adversary's check fails if $b = 1$.

We estimate the probability that the adversary wins. By Lemma 1, with probability at least $1 - 2^{-2k'}$, there is no preimage of size larger than L, where if $C \geq 1$ then $L = 5Ck' \ln 2/(\ln k' + \ln\ln 2) \leq 4Ck'/\ln k'$ and otherwise $L = 5k' \ln 2/(\ln k' + \ln\ln 2) \leq 4k'/\ln k'$ for all sufficiently large k'.

Let Good denote the event that $r \leftarrow \mathcal{FPO}_G(G(r))$. We then have $\Pr[\mathsf{Good}] \geq (1 - 2^{-2k'})/L$. Hence, we obtain that

$$\begin{aligned}
\Pr[b' = b] &= \Pr[b' = 0 \mid b = 0 \wedge \mathsf{Good}] \Pr[b = 0 \wedge \mathsf{Good}] \\
&\quad + \Pr[b' = 0 \mid b = 0 \wedge \neg\mathsf{Good}] \Pr[b = 0 \wedge \neg\mathsf{Good}] \\
&\quad + \Pr[b' = 1 \mid b = 1] \Pr[b = 1] \\
&= 1 \cdot \frac{1}{2} \cdot \Pr[\mathsf{Good}] + \frac{1}{2} \cdot \frac{1}{2} \cdot (1 - \Pr[\mathsf{Good}]) + \frac{1}{2} \cdot \frac{1}{2} \\
&= \frac{1}{2} + \frac{1}{4} \Pr[\mathsf{Good}] \geq \frac{1}{2} + \frac{1 - 2^{-2k'}}{4L}.
\end{aligned}$$

and $4L$ is a polynomial in the security parameter k. This completes the proof. □

As shown above, the FO conversion is not secure in the FPT-ROM, but there is a way to modify it so as to maintain the security in the FPT-ROM. Naito, Wang, and Ohta

Key Generation	Encryption	Decryption
Input: 1^k	Input: $m \in \{0,1\}^{k-k_0-k_1}$, f_{pk}	Input: c, g_{sk}
1: $(f_{\mathsf{pk}}, g_{\mathsf{sk}}) \leftarrow F$	1: $r \leftarrow \{0,1\}^{k_0}$	1: $s \,\|\| \, t \leftarrow g_{\mathsf{sk}}(c)$
Output: $(f_{\mathsf{pk}}, g_{\mathsf{sk}})$	2: $s \leftarrow (m \,\|\| \, 0^{k_1}) \oplus G(r)$	2: $r \leftarrow t \oplus H(s)$
	3: $t \leftarrow H(s) \oplus r$	3: $M \leftarrow s \oplus G(r)$
	4: $c \leftarrow f_{\mathsf{pk}}(s \,\|\| \, t)$	5: If $M = m \,\|\| \, 0^{k_1}$ set $o \leftarrow m$
	Output: c	6: Otherwise set $o \leftarrow \perp$
		Output: o

Fig. 1. OAEP

proposed the conversion method that converts a cryptosystem secure in the ROM to that secure even in the FPT-ROM [29]. In the case of the FO conversion, the public key is (pk, c), where $c \leftarrow \{0,1\}^k$, and the ciphertext is

$$(c_1, c_2) = (\mathsf{Enc}_{\mathsf{pk}}(r; H(c, m, r)), G(c, r) \oplus m),$$

where the domains of H and G are modified. Intuitively, this change makes the first-preimage oracles, $\mathcal{FPO}^H$ and $\mathcal{FPO}^G$, useless.

3.4 OAEP

We finally focus on the OAEP and present its IND-CCA2 security in the FPT-ROM. For the security parameter k, let k_0 and k_1 be functions in k, where $k_0 < k - k_0$. Let F be a family of partial-domain one-way trapdoor permutations of a domain $\{0,1\}^{k-k_0} \times \{0,1\}^{k_0}$. (See [30] for the definition of the partial-domain one-wayness.) Furthermore, let G and H be hash functions such that $G : \{0,1\}^{k_0} \to \{0,1\}^{k-k_0}$ and $H : \{0,1\}^{k-k_0} \to \{0,1\}^{k_0}$. Then, the OAEP encryption scheme based on F is described in Fig. 1.

We obtain the following theorem that states the security of the OAEP encryption scheme in the FPT-ROM.

Theorem 9. *Let F be a family of partial-domain one-way trapdoor permutations. Then, the OAEP encryption scheme based on F is* IND-CCA2 *secure in the* FPT-ROM.

We here only give the sketch of the security proof.

Proof (Sketch). As in the proof of Fujisaki et al. [30], we prove the security by defining a sequence of games and bounding the advantages of the adversary among the games. The games are the almost same as the original ones in [30]. However, we need to pay attention to the following two points. First, as mentioned, we no longer have the uniformity of the ROM because of the first-preimage oracle. Second, the adversary can make use of the first-preimage oracle. These points make the security proofs difficult.

In order to observe the difference between the security proofs in the FPT-ROM and ROM, let us consider the following two games. We will describe the sequence of the games in the full version.

- Game_1: The challenger generates a pair of keys $(f_{\mathsf{pk}}, g_{\mathsf{sk}})$ by using the key-generation algorithm. It next produces $r^+ \leftarrow \{0,1\}^{k_0}$ and obtains $g^+ \leftarrow \mathsf{RO}_G(r^+)$. In generation of the target ciphertext, the challenger generates the random string r^+. The target ciphertext y^* is generated as follows:

$$r^* \leftarrow r^+, \qquad s^* \leftarrow (m_b \,\|\, 0^{k_1}) \oplus g^+, \qquad t^* \leftarrow r^* \oplus \mathsf{RO}_H(s^*),$$
$$x^* \leftarrow (s^*, t^*), \qquad y^* \leftarrow f_{\mathsf{pk}}(x^*).$$

The ciphertext y^* is given to $\mathcal{A}$. Finally, the adversary $\mathcal{A}$ outputs a bit b'.

– Game_2: We modify the above game, by changing the rule for generation of g^+. That is, g^+ is not obtained by the query of the random oracle, but obtained by choosing from $\{0,1\}^{k-k_0}$ uniformly at random. Notice that (r^+, g^+) is not contained in the table $\mathbb{T}_G$.

Let AskG be the event that r^+ is queried to RO_G. The original proof in the ROM showed that, if the value r^+ is not queried to RO_G, the Game_1 and Game_2 are identical.

On the other hand, in our case in the $\mathsf{FPT\text{-}ROM}$, even if the event AskG does not occur, that is, the value r^+ is not queried, we cannot say that Game_1 and Game_2 are identical. Notice that the adversary would distinguish the games by querying g^+ to FPO_G, which leads to a contradiction to the partial-domain one-wayness in the final game. The value g^+ must have the preimage r^+ in Game_1 since (r^+, g^+) is contained in the table $\mathbb{T}_G$. In contrast, the value g^+ has no preimages in Game_2 with high probability if $k - k_0$ is much larger than k_0 since (r^+, g^+) is not inserted in the table $\mathbb{T}_G$ and $\perp \leftarrow \mathsf{FPO}_G(g^+)$ with high probability. We must take care of this event AskG^-. Additionally, it would distinguish between Game_1 and Game_2 by querying $(m_{1-b}\|0^{k_1})\oplus s^*$ to FPO_G, which also leads to contradiction to the partial-domain one-wayness in the final game. This event is denoted by $\mathsf{AskG}^\diamond$. Notice that, conditioned on the above events, AskG, AskG^-, and $\mathsf{AskG}^\diamond$, do not occur, g^+ is almost perfectly uniform in Game_1 by Lemma 2. Hence, we can show two games Game_1 and Game_2 are statistically close if the events do not occur.

By carefully applying similar arguments, we can show the $\mathsf{IND\text{-}CCA2}$ security for the OAEP encryption scheme in $\mathsf{FPT\text{-}ROM}$. □

4 Future Work

It should be noted that our WROMs are based on a simplified variant, which Numayama et al. [18] and Pasini and Vaudenay [17] also adopted, of the original WROMs of Liskov [15].

The original WROMs consists of the ideal compression function $h : \{0,1\}^{k+k'} \to \{0,1\}^k$ of *fixed input length* and the first-preimage oracle. Then, he discussed the security of the *flexible input-length* hash functions $H^h : \{0,1\}^* \to \{0,1\}^k$ employing h as the component in the context of indifferentiability [31]. A random oracle H is often instantiated by employing a compression h. (See, e.g., the survey in [8, Section 2].) Therefore, his work reflects the attacks against the compression function of MD5 and SHA-1 rather than the construction H.

On the contrary, we (and similarly [18,17]) discussed the *monolithic* random oracle H and the additional oracles associated with H. Hence, our model has a gap from such a realistic instantiation of the random oracle in some sense. We leave filling this gap as future work.

Except for the FO conversion, there are several conversion methods in the ROM, such as REACT [32] and GEM [33]. It would also be interesting as future work to examine the security of these conversion methods in the WROMs.

Acknowledgements

We thank anonymous reviewers for their helpful comments. This research was supported in part by NTT Information Sharing Platform Laboratories, JSPS Global COE program "Computationalism as Foundation for the Sciences," KAKENHI 18300002, KAKENHI 19-55201, and the Japan Science and Technology Agency, Strategic Japanese-French Cooperative Program "Quantum Computer: Theory and Feasibility."

References

1. Bellare, M., Rogaway, P.: Random oracle are practical: A paradigm for designing efficient protocols. In: CCS 1993, pp. 62–73. ACM, New York (1993)
2. Rivest, R.L.: The MD5 message-digest algorithm. Internet Request for Comments, RFC 1321 (April 1992)
3. National Institute of Standards and Technology: Secure hash standard. FIPS 180-2 (August 2002)
4. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. Journal of the ACM 51(4), 557–594 (2004); Preliminary version in STOC 1998 (1998)
5. Goldwasser, S., Kalai, Y.T.: On the (in)security of the Fiat-Shamir paradigm. In: FOCS 2003, pp. 102–113. IEEE Computer Society, Los Alamitos (2003)
6. Bellare, M., Boldyreva, A., Palacio, A.: An uninstantiable random-oracle-model scheme for a hybrid-encryption problem. In: Franklin, M.K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 171–188. Springer, Heidelberg (2004)
7. Bellare, M., Rogaway, P.: The exact security of digital signatures – how to sign with RSA and Rabin. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 399–416. Springer, Heidelberg (1996)
8. Leurent, G., Nguyen, P.Q.: How risky is the random-oracle model? In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 445–464. Springer, Heidelberg (2009), http://eprint.iacr.org/2008/441
9. Wang, X., Yu, H.: How to break MD5 and other hash functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19–35. Springer, Heidelberg (2005)
10. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 17–36. Springer, Heidelberg (2005)
11. Aoki, K., Sasaki, Y.: Preimage attacks on one-block MD4, 63-step MD5 and more. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2008. LNCS, vol. 5381, pp. 103–119. Springer, Heidelberg (2008)
12. Nielsen, J.B.N.: Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 111–126. Springer, Heidelberg (2002)
13. Unruh, D.: Random oracles and auxiliary input. In: [34], pp. 205–223
14. Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 92–111. Springer, Heidelberg (1995)

15. Liskov, M.: Constructing an ideal hash function from weak ideal compression functions. In: Biham, E., Youssef, A.M. (eds.) SAC 2006. LNCS, vol. 4356, pp. 358–375. Springer, Heidelberg (2007)
16. Hoch, J.J., Shamir, A.: On the strength of the concatenated hash combiner when all the hash functions are weak. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008, Part II. LNCS, vol. 5126, pp. 616–630. Springer, Heidelberg (2008)
17. Pasini, S., Vaudenay, S.: Hash-and-sign with weak hashing made secure. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 338–354. Springer, Heidelberg (2007)
18. Numayama, A., Isshiki, T., Tanaka, K.: Security of digital signature schemes in weakened random oracle models. In: Cramer, R. (ed.) PKC 2008. LNCS, vol. 4939, pp. 268–287. Springer, Heidelberg (2008)
19. Fischlin, M., Lehmann, A.: Security-amplifying combiners for collision-resistant hash functions. In: [34], pp. 224–243
20. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (1999)
21. Kiltz, E., Pietrzak, K.: On the security of padding-based encryption schemes (or: Why we cannot prove OAEP secure in the standard model). In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 389–406. Springer, Heidelberg (2009)
22. Devroye, L.D.: Non-Uniform Random Variate Generation. Springer, Heidelberg (1986)
23. Ahrens, J.H., Dieter, U.: Computer methods for sampling from Gamma, Beta, Poisson and Binomial distributions. Computing 12(3), 223–246 (1974)
24. Ahrens, J.H., Dieter, U.: Sampling from Binomial and Poisson distributions: A method with bounded computation times. Computing 25(3), 193–208 (1980)
25. Relles, D.A.: A simple algorithm for generating Binomial random variables when N is large. American Statistical Association 67(339), 612–613 (1972)
26. Kawachi, A., Numayama, A., Tanaka, K., Xagawa, K.: Security of encryption schemes in weakened random oracle models. Cryptology ePrint Archive, Report 2010/122 (2010)
27. Motwani, R., Raghavan, P.: Randomized Algorithms. Cambridge University Press, Cambridge (1995)
28. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. Chapman & Hall/CRC, Boca Raton (2007)
29. Naito, Y., Wang, L., Ohta, K.: How to construct cryptosystems and hash functions in weakenend random oracle models. Cryptology ePrint Archive, Report 2009/550 (2009)
30. Fujisaki, E., Okamoto, T., Pointcheval, D., Stern, J.: RSA-OAEP is secure under the RSA assumption. Journal of Cryptology 17(2), 81–104 (2004)
31. Maurer, U.M., Renner, R., Holenstein, C.: Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 21–39. Springer, Heidelberg (2004)
32. Okamoto, T., Pointcheval, D.: REACT: Rapid enhanced-security asymmetric cryptosystem transform. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 159–175. Springer, Heidelberg (2001)
33. Coron, J.S., Handschuh, H., Joye, M., Paillier, P., Pointcheval, D., Tymen, C.: Gem: A Generic chosen-ciphertext secure Encryption Method. In: Preneel, B. (ed.) CT-RSA 2002. LNCS, vol. 2271, pp. 175–184. Springer, Heidelberg (2002)
34. Menezes, A. (ed.): CRYPTO 2007. LNCS, vol. 4622. Springer, Heidelberg (2007)