10-2024

On the lossiness of 2k-th power and the instantiability of Rabin-OAEP

Haiyang XUE
Singapore Management University, haiyangxue@smu.edu.sg

Bao LI

Xianhui LU

Kunpeng WANG

Yamin LIU

Citation

XUE, Haiyang; LI, Bao; LU, Xianhui; WANG, Kunpeng; and LIU, Yamin. On the lossiness of 2k-th power and the instantiability of Rabin-OAEP. (2024). *Proceedings of the 13th International Conference on Cryptology and Network Security, CANS 2014, Crete, Greece, October 22-24*. 34-49.
Available at: https://ink.library.smu.edu.sg/sis_research/9198

On the Lossiness of 2^k-th Power and the Instantiability of Rabin-OAEP ⋆

Haiyang Xue[1,2,3], Bao Li[1,2], Xianhui Lu[1,2],
Kunpeng Wang[1,2], and Yamin Liu[1,2]

Data Assurance and Communication Security Research Center,
Chinese Academy of Sciences, Beijing, China
State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
University of Chinese Academy of Sciences, Beijing, China
{hyxue12,lb,xhlu,kpwang,ymliu}@is.ac.cn

Abstract. Seurin (PKC 2014) proposed the 2-Φ/4-hiding assumption which asserts the indistinguishability of Blum Numbers from pseudo Blum Numbers. In this paper, we investigate the lossiness of 2^k-th power based on the 2^k-Φ/4-hiding assumption, which is an extension of the 2-Φ/4-hiding assumption. And we prove that 2^k-th power function is a lossy trapdoor permutation over Quadratic Residuosity group. This new lossy trapdoor function has $2k$-bits lossiness for k-bits exponent, while the RSA lossy trapdoor function given by Kiltz *et al.* (Crypto 2010) has k-bits lossiness for k-bits exponent under Φ-hiding assumption in lossy mode. We modify the square function in Rabin-OAEP by 2^k-th power and show the instantiability of this Modified Rabin-OAEP by the technique of Kiltz *et al.* (Crypto 2010). The Modified Rabin-OAEP is more efficient than the RSA-OAEP scheme for the same secure bits. With the secure parameter being 80 bits and the modulus being 2048 bits, Modified Rabin-OAEP can encrypt roughly 454 bits of message, while RSA-OAEP can roughly encrypt 274 bits.

Keywords: Rabin, OAEP, Lossy trapdoor function, Φ-hiding.

1 Introduction

Lossy Trapdoor Function. Peikert and Waters [25] proposed the notion of lossy trapdoor function (LTDF) in STOC 2008. LTDF implies cryptographic primitives such as classic one-way trapdoor function [8], collision resistant hash function [13], oblivious transfer protocol [14], chosen ciphertext secure public key encryption scheme [25], deterministic public key encryption scheme [3], and selective opening secure public key encryption scheme [17]. LTDFs can be constructed based on many assumptions, such as DDH[25], DCR[11], LWE[25], etc.

⋆ Supported by the National Basic Research Program of China (973 project)(No.2013CB338002), the National Nature Science Foundation of China (No.61070171, No.61272534).

D. Gritzalis et al. (Eds.): CANS 2014, LNCS 8813, pp. 34–49, 2014.

Kiltz *et al.* [22] showed that the RSA function $f : x \to x^e \mod N$ is a $\log e$ lossy trapdoor permutation (LTDP) under the Φ-hiding assumption. The Φ-hiding assumption was firstly proposed by Cachin, Micali and Stadler [5]. Intuitively, this assumption states that given an RSA modulus $N = pq$, it is hard to distinguish primes that divide $\phi(N)$ from those that do not, where ϕ is the Euler function. Kiltz *et al.* [22] then showed that the lossiness of RSA implies that the RSA-OAEP is indistinguishable against chosen plaintext attack (IND-CPA) in the standard model by instantiating the hash with t-wise independent hash. Subsequently, Kakvi and Kiltz [21] gave a tight proof of the security of RSA-FDH using the lossiness of RSA function.

Recently, Seurin [26] extended the Φ-hiding assumption to the 2-Φ/4-hiding assumption and showed that the Rabin function is lossy with two bits over the Quadratic Residuosity subgroup and 1 bit over the integers $1 \leq x \leq (N-1)/2$ with Jacobi symbol 1. The 2-Φ/4-hiding assumption is the indistinguishability of Blum Numbers, *i.e.* $p, q \equiv 3 \mod 4$, from pseudo Blum Numbers *i.e.* $p, q \equiv 1 \mod 4$.They also investigated the Rabin Williams signature and gave a tight proof of the Rabin-FDH by following the steps of Kakvi and Kiltz [21].

On the other line, Joye and Libert [19] investigated the Extended pseudo Blum Number and the Gap-2^k-Res assumption. They proposed an efficient LTDF based on the Gap-2^k-Res assumption and DDH assumption over 2^k-th Residuosity.

Optimal Asymmetric Encryption Padding. Bellare and Rogaway [2] introduced Optimal asymmetric encryption padding (OAEP) as a replacement of they widely used RSA PKCS #1 v1.5 [1]. And they proved that OAEP is secure in the random oracle model. When implementing this scheme in practice, the random oracle is replaced by a cryptographic hash function which is not random. Canetti [6] *et al.* showed that there are schemes which are secure in the random oracle model but not secure in the standard model. Two mostly studied OAEP schemes are the RSA-OAEP and Rabin-OAEP. The first evidence that RSA-OAEP could achieve a standard security notion in the standard model was proposed by Kiltz *et al.* [22] stating that the RSA-OAEP is IND-CPA secure under the Φ-hiding assumption. They proved that OAEP is a randomness extractor, that fools distinguishers with small range output. They also investigated the Multi-prime Φ-hiding assumption in order to improve the lossiness of RSA function. Some subsequent works [16][24] improved the security bound and investigated the regularity over subdomain. In terms of practice, the Rabin-OAEP is a competent substitution of RSA-OAEP. But the security of Rabin-OAEP has not been proven in the standard model under better-understood assumptions. One research direction is using the technique of Kiltz *et al.* [22] with the combination of LTDF and OAEP. But this method requires that the LTDF has enough lossiness. Seurin [26] noticed that one first step in this direction is to consider the multi prime pseudo Blum Numbers, but in order to get m bits lossiness, product of $m/2$ secure primes are required. This method reduces the security level and the computational efficiency.

The instantiability of Rabin-OAEP and concrete analysis of the security are interesting questions. The problem is to find a well-understood assumption, construct LTDF with enough lossiness and reduce the security to this assumption in the standard model. As shown above, Seurin [26] investigated the 2-Φ/4-hiding assumption and showed that Rabin fucntion loses 2 bits over QR group. The 2-Φ/4-hiding assumption asserts that it is hard to tell if $N = (2^2s' + 2^2 - 1)(2^2t' + 2^2 - 1)$ or $N = (2^2p' + 1)(2^2q' + 1)$ for some s', t', p' and q'. Inspired by Joye and Libert' scheme [19], a natural extension is the 2^k-Φ/4-hiding assumption and the 2^k-th power function. The 2^k-th power function loses about $2k$ bits which is enough for the instantiability of OAEP given by Kiltz *et al.*[22].

1.1 Our Contributions

In this paper, we consider the problem of reducing the security of Rabin-OAEP to a well-understood assumption. Inspired by Joye and Libert' scheme [19], we first extend the 2-Φ/4-hiding assumption to 2^k-Φ/4-hiding assumption. Then we show that the 2^k-th power is lossy over the Quadratic Residuosity (QR) group under the 2^k-Φ/4-hiding assumption. We also modify the classic Rabin-OAEP with 2^k-th power and prove that it is IND-CPA secure in the standard model using the lossiness of 2^k-th power. In the following, we explain our result with more details.

Lossiness of 2^k-th Power. In order to prove the lossiness of 2^k-th power, we firstly proposed the 2^k-Φ/4-hiding assumption. Intuitively, this assumption is that, given k, it is hard to distinguish RSA modulus N which is the product of two primes with the least significant $k+1$ bits being all 1 from those which is the product of two primes with the least significant $k+1$ bits being all 0 except the last one. The 2^k-Φ/4-hiding assumption asserts that, given (N, k) where N is product of two primes and $k \leq (\frac{1}{4} - \varepsilon) \log N$, it is hard to tell if $N = (2^{k+1}s' + 2^{k+1} - 1)(2^{k+1}t' + 2^{k+1} - 1)$ or $N = (2^{k+1}p' + 1)(2^{k+1}q' + 1)$ for some s', t', p' and q'. We call the numbers of the first kind the Extended Blum Numbers and those of the second kind the Extended pseudo Blum Numbers. Note that it is actually the 2-Φ/4-hiding assumption when $k = 1$. For an Extended Blum Number N, the 2^k-th power is a trapdoor permutation over QR group. For Extended pseudo Blum Number N, the 2^k-th power is a 2^{2k}-to-1 map over QR. Thus we attain new efficient lossy trapdoor permutation. One problem of the QR group is that it is not efficiently recognizable, but the Signed QR subgroup can be recognized efficiently according to [10][26]. We also investigate the 2^k-th power over Signed QR group in the Appendix.

Modified Rabin-OAEP. We modify the Rabin-OAEP and call it Modified Rabin-OAEP. The one way function after OAEP is the 2^{k+1}-th power function. The security proof of our Modified Rabin-OAEP follows by extending Kiltz *et al.*'s proof of RSA-OAEP. Under the same security bits, the 2^k-th power loses about 2 times of the RSA function, and hence the Modified Rabin-OAEP can encrypt longer message. Precisely, for 80 bits security, let $n = 2048$, then $k = 432$.

Our Modified Rabin-OAEP can encrypt 454 bits at once while the RSA-OAEP for the same security bits can encrypt 274 bits only. Assuming the regularity of 2^{k+1}-th power on certain subdomains, message of 534 bits can be encrypted.

1.2 Outline

This paper is organized as follows. In Sect. 2, we introduce the notations and recall the definition of lossy trapdoor function and OAEP. In Sect. 3, we present 2^k-$\Phi/4$-hiding assumption and analyse the lossiness of 2^k-th power. In Sect. 4, we present a construction of LTDF based on the 2^k-$\Phi/4$-hiding assumption and compare it with previous LTDFs. In Sect. 5, we propose the Modified Rabin-OAEP scheme and show the instantiability of this encryption scheme. In Sect. 6, we conclude this paper.

2 Preliminaries

2.1 Notations

If S is a set, we denote by $|S|$ the cardinality of S, and denote by $x \leftarrow S$ the process of sampling x uniformly from S. If A is an algorithm, we denote by $z \leftarrow A(x, y, \cdots)$ the process of running A with input $x, y, \cdots$ and output z. For an integer n, we denote by $[n]$ the set of $\{0, 1, \cdots, n-1\}$. A function is *negligible* if for every $c > 0$ there exists a λ_c such that $f(\lambda) < 1/\lambda^c$ for all $\lambda > \lambda_c$.

2.2 Definitions

Definition 1 (Lossy Trapdoor Functions). *A collection of (m, l)-lossy trapdoor functions are 4-tuple of probabilistic polynomial time (PPT) algorithms $(S_{inj}, S_{loss}, F_{ltdf}, F_{ltdf}^{-1})$ such that:*

1. Sample Lossy Function $S_{loss}(1^n)$. *Output a function index $\sigma \in \{0,1\}^*$ with implicitly understood domain $\mathcal{D}$ of size 2^m.*
2. Sample Injective Function $S_{inj}(1^n)$. *Output a pair $(\sigma, \tau) \in \{0,1\}^* \times \{0,1\}^*$ where σ is a function index with domain $\mathcal{D}$ of size 2^k and τ is a trapdoor.*
3. Evaluation algorithm F_{ltdf}. *For every function index σ produced by either S_{loss} or S_{inj}, the algorithm $F_{ltdf}(\sigma, \cdot)$ computes a function $f_\sigma : \mathcal{D} \to \{0,1\}^*$ with one of the two following properties:*
   - *Lossy: If σ is produced by S_{loss}, then the image of f_σ has size at most 2^{m-l}.*
   - *Injective: If σ is produced by S_{inj}, then the function f_σ is injective.*
4. Inversion algorithm F_{ltdf}^{-1}. *For every pair (σ, τ) produced by S_{inj} and every $x \in \{0,1\}^m$, we have $F_{ltdf}^{-1}(\tau, F_{ltdf}(\sigma, x)) = x$.*

In the above algorithms, the two ensembles $\{\sigma, \sigma \leftarrow S_{loss}(1^n)\}$ and $\{\sigma, (\sigma, \tau) \leftarrow S_{inj}(1^n)\}$ are computationally indistinguishable.

- *We call this* lossy trapdoor permutation (LTDP) *if the functions in the injective mode are permutations.*
- *We call the functions* regular *if the functions in the lossy mode are k to 1 for some k.*

Definition 2 (t-wise independent hash function). *Let $H : K \times D \to R$ be a hash function. We say that H is t-wise independent if for all distinct $x_1, \cdots x_t \in D$ and all $y_1, \cdots y_t \in R$*

$$Pr[H(k, x_1) = y_1 \wedge \cdots \wedge H(k, x_t) = y_t : k \leftarrow K] = \frac{1}{|R|^t}.$$

In other words, $H(k, x_1), \ldots, H(k, x_t)$ are all uniformly and independently random.

3 The 2^k-Φ/4-Hiding Assumption and 2^k-th Power

In this section, we first propose the 2^k-Φ/4 assumption, then analyze the properties of 2^k-th power function over QR.

3.1 The 2^k-Φ/4-Hiding Assumption

Intuitively, the assumption is that, given secure parameters n and $k < n/4 - 1$ it is hard to distinguish RSA modulus N which are product of two primes with the least significant $k + 1$ bits being all 1 from those which are product of two primes with the least significant $k + 1$ bits being all 0 except the last one. In both cases, the least significant $k + 1$ bits of the modulus N are all zero except the last one. Formally, we define two distributions:

$$R = \{N : N = pq \text{ with } \log p \approx \log q \approx \lfloor \frac{n}{2} \rfloor \text{ and } p, q \equiv 2^{k+1} - 1 \mod 2^{k+1}\},$$

$$L = \{N : N = pq \text{ with } \log p \approx \log q \approx \lfloor \frac{n}{2} \rfloor \text{ and } p, q \equiv 1 \mod 2^{k+1}\}.$$

The 2^k-Φ/4 assumption asserts that, for a probability polynomial time (PPT) distinguisher D the following advantage is negligible:

$$\mathbf{Adv}_D(n) = \Pr[D(R) = 1] - \Pr[D(L) = 1].$$

In order to enhance the strength of this assumption, we add requirements for p and q. In distribution R, we require that $p = 2^{k+1}s' + 2^{k+1} - 1$ (resp. $q = 2^{k+1}t' + 2^{k+1} - 1$) for odd number s' (resp. t'), we also require that $2^k s' + 2^k - 1$ and $2^k t' + 2^k - 1$ are primes (p, q are strong primes); in distribution L, we require that $p = 2^{k+1}p' + 1$ (resp. $q = 2^{k+1}q' + 1$) for prime number p' (resp. q')

This assumption is an extension of the 2-Φ/4-hiding assumption [26] for $k = 1$. We call the numbers in distribution R the Extended Blum Numbers and those in L the Extended pseudo Blum Numbers. Joye and Libert [19] investigated the

Extended pseudo Blum Number. In their paper, they generalized the Goldwasser-Micali cryptosystem [15] to encrypt many bits at once by using the Extended pseudo Blum Number. The underlying assumption is the Gap-2^k-Res assumption which is implied by the original QR assumption. There is an efficient algorithm [20] for generating Extended pseudo Blum Numbers. We can modify this algorithm to get an efficient algorithm for generating Extended Blum Numbers. The distribution R and L can be chosen efficiently.

Analysis of the 2^k-$\Phi/4$-Hiding Assumption. It is easy to break the 2^k-$\Phi/4$-hiding problem with the factorization of modulus N. However, it seems that there is no known algorithm to break this problem without factoring the modulus N. [27] and [28] investigated the RSA modulus with primes sharing least significant bits. If given the modulus primes p and q sharing the least $k+1$ significant bits (denote it by l), at most 4 candidates l can be computed by solving the equation $x^2 = N \mod 2^{k+1}$. In our case, the equation is $x^2 = 1 \mod 2^{k+1}$, and 1, $2^{k+1} - 1$ are the two candidates of l. It is still difficult to decide which distribution the modulus N belongs to. Joye and Libert [19] have investigated the security parameters for the Extended pseudo Blum Numbers. When k is too large, by Coppersmith's method [7] with LLL algorithm [23], N can be factored in time $poly(n)$ with advantage $O(N^{\varepsilon})$ if $k = n/4 - \varepsilon n - 1$. We have εn bits security here. We now consider Extended Blum Numbers. Pollard's $p-1$ method dose not work. The powerful Coppersmith's method bounds the size of k to $n/4 - \varepsilon n - 1$ for the Extended Blum Numbers too. So we end up with the same upper bound:

$$k \leq \frac{1}{4}n - \varepsilon n - 1,$$

for εn bits security. For example, if $n = 2048$, we set $\varepsilon = 0.04$ (about 80 bits security), k can be about 430.

3.2 2^k-th Power over QR Group

Let $N = pq$ be a product of two distinct $n/2$ bits primes. The group Z_N^* consists of all elements of Z_N that are invertible modulo N. Then Z_N^* has order $\phi(N) = (p-1)(q-1)$. Denote QR the subgroup of Z_N^* of quadratic residues modulo N. Note that QR has order $\phi(N)/4$. We now consider the 2^k-th power over the subgroup QR.

Let N be an Extended Blum Number, then we have that the order of QR is an odd number. In fact the Extended Blum Number is a special case of the Blum Number. The Extended Blum Number has all the properties of the Blum Numbers. The square map is a permutation over QR, thus the 2^k-th power is a permutation over QR.

We now consider the Extended pseudo Blum Number $N = pq$ with $p, q \equiv 1 \mod 2^{k+1}$. We recall the definition of the m-th power residue symbol for a divisor m of $p-1$ presented in [19] and [31]. Here we consider the case for $m = 2^i$ for $1 \leq i \leq k+1$.

Definition 3. *Let p be an odd prime and $p \equiv 1 \mod 2^{k+1}$. For $1 \leq i \leq k+1$, the symbol*

$$\left(\frac{a}{p}\right)_{2^i} := a^{\frac{p-1}{2^i}} \mod p,$$

is the 2^i-th power residue symbol modulo p, where $a^{\frac{p-1}{2^i}} \mod p$ is in $[-(p-1)/2, (p-1)/2]$.

Let a and b be two integers coprime to p,

$$\left(\frac{ab}{p}\right)_{2^i} = \left(\frac{a}{p}\right)_{2^i} \left(\frac{b}{p}\right)_{2^i}. \tag{1}$$

Thus, we have

$$\left(\frac{a^2}{p}\right)_{2^i} = \left[\left(\frac{a}{p}\right)_{2^i}\right]^2 = \left(\frac{a}{p}\right)_{2^{i-1}}. \tag{2}$$

For any integer a and any Extended pseudo Blum Number N, we generalize the Jacobi symbol as the product of the m-th power residue Legendre symbol

$$\left(\frac{a}{N}\right)_{2^i} = \left(\frac{a}{p}\right)_{2^i} \left(\frac{a}{q}\right)_{2^i}. \tag{3}$$

Lemma 1. *Let N be the Extended pseudo Blum Number associated with k, then the 2^k-th power map $g : x \to x^{2^k}$ ($x \in QR$)is a 2^{2k}-to-1 map and the 2^{k+1}-th power map $h : x \to x^{2^k}$ ($x \in Z_N^*$) is a $2^{2(k+1)}$-to-1 map.*

Proof. To prove this result, we investigate a sequence of subgroups and square maps on them. Precisely, for $0 \leq s \leq k+1$, we consider the subgroups of Z_N^* denoted by

$$R^s := \{x^{2^s} | x \in Z_N^*\},$$

and define the square map $f_i : y \to y^2$ from R^i to R^{i+1} for $0 \leq i \leq k$. Note that here R^0 is Z_N^* itself. We also define here and in the followings that

$$J^s_{(+,+)} := \{x | x \in R^s, \left(\frac{x}{p}\right)_{2^{s+1}} = 1, \left(\frac{x}{q}\right)_{2^{s+1}} = 1\},$$

$$J^s_{(-,-)} := \{x | x \in R^s, \left(\frac{x}{p}\right)_{2^{s+1}} = -1, \left(\frac{x}{q}\right)_{2^{s+1}} = -1\},$$

$$J^s_{(+,-)} := \{x | x \in R^s, \left(\frac{x}{p}\right)_{2^{s+1}} = 1, \left(\frac{x}{q}\right)_{2^{s+1}} = -1\},$$

$$J^s_{(-,+)} := \{x | x \in R^s, \left(\frac{x}{p}\right)_{2^{s+1}} = -1, \left(\frac{x}{q}\right)_{2^{s+1}} = 1\}.$$

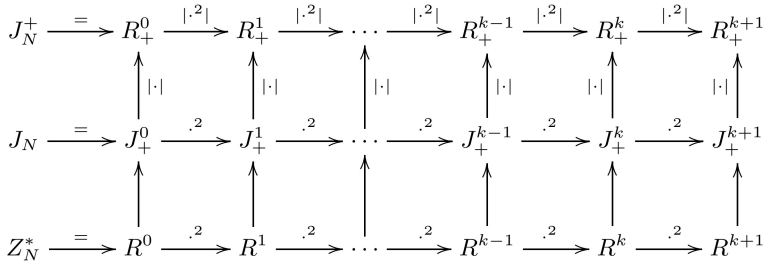
Note that the above sets divide R_s into four parts of the same size. And $J^s_{(+,+)}$ is actually the subgroup R_{s+1}.

We need only to prove that the map f_i is a 4-to-1 map. The map $g = f_k \circ f_{k-2} \cdots \circ f_1$ is 2^{2k}-to-1 naturally. For any element $a \in R_s$, by equation 2,

$$\left(\frac{f_i(a)}{p}\right)_{2^{i+2}} = \left(\frac{a}{p}\right)_{2^{i+1}} \equiv \pm 1 \mod p.$$

It also holds for modulus q. The four preimages of $f_i(a)$ fall into one of $J^i_{\pm 1,\pm 1}$. We have that f_i is a 4-to-1 map. Then we have that 2^k-th power over QR is a 2^{2k}-to-1 map and 2^{k+1}-th power over Z^*_N is a $2^{2(k+1)}$-to-1 map. □

We illustrate the result of Lemma 1 and Lemma 3 in Figure 1.



Here, R^s is the subgroup of Z^*_N with 2^s-th residuocity. J^s_+ is the subset of R^s with Legendre symbal 1. J^+_N is the subset of J^s_+ greater than 0. $\cdot^2$ represents the square map. $|\cdot|$ represents the absolute value and $|\cdot^2|$ is the square map over signed group. R^0 is actually Z^*_N and J^0_+ is J^+_N. It satisfies that $R^0 \supset R^1 \cdots \supset R^{k+1}$, $J^0_+ \supset J^1_+ \cdots \supset J^{k+1}_+$ and $R^0_+ \supset R^1_+ \cdots \supset R^{k+1}_+$. The 2^k-th power over QR is the combination of square maps from R^1 to R^{k+1}. The 2^k-th power over Signed QR is the combination of square maps from R^0_+ to R^k_+. See Appendix for more information about Signed QR group.

Fig. 1. Square map step by step for Extended Blum Number N with associated k

4 LTDP Based on the 2^k-Φ/4-Hiding Assumption

We now give a constructions of 2^{2k}-to-1 lossy trapdoor permutation over the QR group based on the 2^k-Φ/4-hiding assumption. The modulus N is an Extended Blum Number in the injective mode and is an Extended pseudo Blum Number in the lossy mode.

4.1 LTDP over QR

We define $LTDP_{QR} = (S_{inj}, S_{loss}, f_{QR}, f^{-1}_{QR})$ as follows:

1. *Sample Injective Function S_{inj}.* On input 1^n, S_{inj} chooses a proper k and random N in distribution R and the function index is $\sigma = \{N, k\}$. The trapdoor is $t = (p, q)$.

2. *Sample Lossy Function* S_{loss}. On input 1^n, S_{loss} chooses a proper k and random N in distribution L and the function index is $\sigma = \{N, k\}$.
3. *Evaluation algorithm* f_{QR}. Given a function index $\sigma = \{N, k\}$ and input $x \in QR$ the algorithm outputs $z = x^{2^k} \mod N$.
4. *Inversion algorithm* f_{QR}^{-1}. Given $z \in QR$ compute the 2^k root over Signed QR with the trapdoor p, q.

Remark 1. For Extended Blum Numbers, the order of the QR group is an odd number, we can compute the square root over QR k times to get the root in the injective mode. The trapdoor can be set as the inverse of $2^k \mod \frac{\phi(N)}{4}$. Then, given $z \in QR$, the 2^k root is in fact $z^t \mod N$.

Theorem 1. *If the* 2^k*-*Φ*/4-hiding assumption holds, then* $LTDP_{QR}$ *is an* 2^{2k}*-to-1 lossy trapdoor permutation.*

Proof. The 2^k-Φ/4-hiding assumption guarantees the indistinguishability of the lossy and injective mode. The trapdoor permutation property is a straight forward result. By Lemma 1, any element in f_{QR} has exactly 2^{2k} preimages when N is an Extended pseudo Blum Number. □

4.2 Comparison

In Table 1, we compare the above two lossy trapdoor permutations with previous LTDFs. The second column lists the basic number-theoretic assumptions used for guaranteeing the security. The third and fourth columns show the size of an input message in bits and that of the function index respectively. The fifth column lists the size of lossiness. The sixth column shows the computational complexity of the corresponding function. According to [29], the complexity of multiplication is $O(n)$ here. The last column is the computational complexity for one bit lossiness.

5 Modified Rabin-OAEP

LTDF over Z_N^* can be used to instantiate the Rabin-OAEP. In [22], Kiltz *et al.* gave a generic result of building IND-CPA secure padding based encryption by combining a lossy TDP and a fooling extractor, and they proved that the OAEP is an adaptive fooling extractor with well chosen parameters. Then, they showed the instantitation of RSA-OAEP based on the Φ-hiding assumption. By the technique of Kiltz *et al.*, we prove that the Rabin-OAEP with a slight modification over Z_N^* is IND-CPA in the standard model based on the 2^k-Φ/4-hiding assumption.

We recall a theorem in [22] here. For more details of padding based encryption please refer to [22].

Theorem 2 (Theorem 1 in [22]). *Let* $\mathcal{F}$ *be a lossy trapdoor permutation with residual leakage* s *and the padding transform* $(\pi, \hat{\pi})$ *is a* (s, ε) *adaptive fooling extractor, The padding based encryption by combination of* $\mathcal{F}$ *and* $(\pi, \hat{\pi})$ *is IND-CPA secure.*

Table 1. Comparison with existing LTDFs

	Assumption	Input size	Index size	Lossiness	Complexity	Comp/Loss
[25]	DDH	n	$n^2 \log p$	$n - \log p$	$n^2 \log p$	$n \log p$
[11]	d-linear	n	$n^2 \log p$	$n - d \log p$	$n^2 \log p$	$n \log p$
[25]	LWE	n	$n(d+w) \log q$	cn	$n(d+w) \log q$	$\frac{(d+w) \log q}{c}$
[11]	DCR	$2 \log N$	$2 \log N$	$\log N$	$4 \log^2 N$	$4 \log N$
[11]	QR	$\log N$	$\log N$	1	$3 \log N$	$3 \log N$
[19]	DDH& QR	n	$(\frac{n}{k})^2 \log N$	$n - \log N$	$(\frac{n^2}{k}) \log N$	$\frac{n^2 \log N}{n - \log N}$
[30]	DCR& QR	$\log N + k$	$2 \log N$	$3k$	$2 \log N(\log N + k)$	$\frac{2 \log N(\log N + k)}{3k}$
[22]	Φ-hiding	$\log N$	$\log N$	$\log e$	$\log e \log N$	$\log N$
[26]	2-Φ/4-hiding	$\log N$	$\log N$	2	$\log N$	$(\log N)/2$
4.1	2^k-Φ/4-hiding	$\log N$	$\log N$	$2k$	$k \log N$	$(\log N)/2$

In the first, second and sixth rows, n is the number of rows used in the matrix. In the first and second rows, p is the order of the underlying group. In the third row, $0 < c < 1$, n is the rows used in the matrix, $w = \frac{n}{\log p}$ with $p^2 \geq q$ and $d < w$. In this table, k and e are less than $\frac{1}{4} \log N - \kappa$ where κ is the security parameter.

We recall the description of OAEP for Rabin given by Boneh [4] with keyed hash function and give a full version of the Modified Rabin-OAEP encryption scheme. The OAEP for Rabin is different with the OAEP for RSA since that $x^2 \mod N$ is not a permutation on Z_N^*. Let N be an $n+1$ bits Extended Blum Number, μ, s_0, ρ be security parameters such that $n = \mu + s_0 + \rho$. Let $G : K_G \times \{0,1\}^\rho \to \{0,1\}^{\mu+s_0}$ and $H : K_H \times \{0,1\}^{\mu+s_0} \to \{0,1\}^\rho$ be keyed hash functions.

OAEP for Rabin

The associated padding transform is $(\pi_{K_G,K_H}, \hat{\pi}_{K_G,K_H})$ defined by

Algorithm $\pi_{K_G,K_H}(m)$
$Step1 : r \leftarrow \{0,1\}^\rho$
$Step2 : s \leftarrow m \parallel 0^{s_0} \oplus G_{K_G}(r)$
$Step3 : t \leftarrow r \oplus H_{K_H}(s)$
$Step4 : x \leftarrow s \parallel t$
$Step5 :$ Return x

Algorithm $\hat{\pi}_{K_G,K_H}(x)$
$Step1 : s \parallel t \leftarrow x$
$Step2 : r \leftarrow t \oplus H_{K_H}(s)$
$Step3 : m \parallel v \leftarrow s \oplus G_{K_G}(r)$
$Step4 :$ If $v = 0^{s_0}$ return m
else return$\perp$.

Remark 2. Kiltz *et al.* [22] noted that their result also applies to Simplified OAEP given by Boneh[4] since hash function H_{K_H} in OAEP can be anything in their analysis. We remove the hash function H_{K_H} and use the Simplified OAEP for Rabin in the following. This does not affect the secure proof and parameter bound.

The Modified Rabin-OAEP

KeyGen: On input a security parameters n, choose a k and $n+1$ bits Extended Blum Number $N = pq$ associated with k. Choose a random t-wise indepen-

dent hash function G_{K_G} and a hash function H_{K_H}. Compute the inversion of $2^k \mod \frac{\phi(N)}{4}$ and denote it as d. Let $A \equiv 1 \mod p$ and $A \equiv 0 \mod q$, and $B \equiv 0 \mod p$ and $B \equiv 1 \mod q$, set

$$pk = (N, k, G_{K_G}, H_{K_H}), \quad sk = (p, q, d, A, B).$$

Encryption: On input a massage $m \in \{0,1\}^\mu$,
Step 1: Pick a random $r \in \{0,1\}^\rho$ and compute $\pi_{K_G,K_H}(m)$.
Step 2: Set the ciphertext as $c = y^{2^{k+1}} \mod N$.
Decryption: On input a ciphertext c,
Step 1: Compute $z = c^d \mod N$.
Step 2: Compute $z_p = z^{\frac{p+1}{4}} \mod p$ and $z_q = z^{\frac{q+1}{4}} \mod q$.
Step 3: Set $y_1 = Az_p + Bz_q$ and $y_2 = Az_p - Bz_q$. Four square roots of $z \mod N$ is $\pm y_1, \pm y_2$. Two of them are less than $N/2$ and denote them by y_1, y_2.
Step 4: Compute $\hat{\pi}_{K_G,K_H}(y_1)$ and $\hat{\pi}_{K_G,K_H}(y_2)$. If one of them outputs a message m and the other outputs $\perp$, then return m.

Remark 3. Note that in Step 4, if both $v = 0^{s_0}$ for y_1, y_2, the decryption can not choose between them. Boneh [4] showed that this happens with low probability, namely 2^{s_0} and s_0 is typically chosen to be greater than 128.

Theorem 3. *If G_{K_G} is a t-wise independent hash function and the 2^k-Φ/4-hiding assumption holds, then the Modified Rabin-OAEP is IND-CPA secure*

1. *with advantage $\varepsilon = 2^{-u}$ for $u = \frac{t}{3t+2}(\rho - s - \log t) - \frac{2(\mu+s_0+s)}{3t+2} - 1$.*
2. *with advantage $\varepsilon = 2^{-u}$ for $u = \frac{t}{2t+2}(\rho - s - \log t) - \frac{\mu+s_0+s+2}{t+1} - 1$, if it is regular on OAEP domain.*

This is almost a direct result of the combination of Theorem 1 and Theorem 2 in [22]. We omit the proof here and just point out the different part. The OAEP for Rabin is different with the OAEP for RSA since that $x^2 \mod N$ is not a permutation on Z_N^*. The least significant s_0 bits of message is padded by zero in order to choose the right plaintext from four square roots. There is 2^μ possible $(\mu + s_0, \rho)$-sources $X = (m \| 0^{s_0}, R)$ here while there is $2^{\mu+s_0}$ possible $(\mu + s_0, \rho)$-sources in RSA-OAEP. This just affects the security bound of ε.

5.1 Efficiency of the Modified Rabin-OAEP

Regularity. We have analyzed the regularity of 2^{k+1}-th power over Z_N^* for Extended pseudo Blum Number. Unfortunately, in practice, the domain of Rabin-OAEP is $\{0,1\}^{\mu+s_0+\rho}$ (as integer) where $\mu + s_0 + \rho = n - 16$ (i.e. the most significant two bytes of the output are zeroed out). The 2^{k+1}-th power may not be regular over the subdomain $\{0, 1, \cdots, 2^{\mu+s_0+\rho} - 1\}$. Lewko *et al.* [24] proved the regularity of RSA function over this subdomain. We assume that the 2^{k+1}-th power over this subdomain is regular and leave it as an open problem.

Concrete Parameters. If we do not assume the regularity of 2^k-th power over subdomain, from part 1 in Theorem 3, for $u = 80$ bits of security, messages of roughly $\mu = n - s - s_0 - 3 \cdot 80$ bits can be encrypted for sufficiently large t. For $n = 2048$, then $k = 432$, $s \approx 1184$, and the lossiness is 864 bits. Set $s_0 = 130$, 454 bits message ($t \approx 2000$) can be encrypted at once. Kiltz *et al.* [22] instantiated the RSA-OAEP under the Φ-hiding assumption. 160 bits can be encrypted at once in the RSA-OAEP ($t \approx 400$). Under the investigation of Lewko *et al.* [24] that the RSA function is regular over subdomain, 274 bits can be encrypted at once ($t \approx 2000$).

If we assume the regularity of 2^k-th power over subdomain, from part 2 in Theorem 3, for $u = 80$ bits of security, messages of roughly $\mu = n - s - s_0 - 2 \cdot 80$ bits can be encrypted For $n = 2048$, then $k = 432$, 534 bits message ($t \approx 2000$) can be encrypted at once. But this conjecture is not proved.

In Table 2, we compare the efficiency of the Modified Rabin-OAEP above with RSA-OAEP. The second column lists the basic number-theoretic assumptions used for guaranteeing the security. The following columns show the size of modulus, k or length of e, length of lossiness and encrypted message in bits, respectively. The first row is the RSA-OAEP. The second row is the Rabin-OAEP without the regular assumption ($t \approx 2000$). The last row is the Rabin-OAEP with the regular assumption ($t \approx 2000$).

Table 2. Comparison with RSA-OAEP

Scheme	Assumption	$\lfloor \log N \rfloor$	k or $\log e$	Lossiness	Message
RSA-OAEP [22][24]	Φ-hiding	2048	432	432	274
Rabin-OAEP	2^k-Φ/4-hiding	2048	432	864	454
Rabin-OAEP	2^k-Φ/4-hiding, Regular	2048	432	864	534

6 Conclusion

In this paper, we investigate the lossiness of 2^k-th power based on the 2^k-Φ/4-hiding assumption, which is an extension of the 2-Φ/4-hiding assumption. And we prove that 2^k-th power function is a lossy trapdoor permutation over Quadratic Residuosity group. We instantiate Modified Rabin-OAEP by the technique of Kiltz *et al.*. Our Modified Rabin-OAEP is more efficient than the RSA-OAEP scheme for the same secure bits.

References

1. RSA public-key cryptography standards, `ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1`
2. Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 92–111. Springer, Heidelberg (1995)

3. Boldyreva, A., Fehr, S., O'Neill, A.: On notions of security for deterministic encryption, and efficient constructions without random oracles. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 335–359. Springer, Heidelberg (2008)
4. Boneh, D.: Simplified OAEP for the RSA and Rabin Functions. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 275–291. Springer, Heidelberg (2001)
5. Cachin, C., Micali, S., Stadler, M.: Computationally private information retrieval with polylogarithmic communication. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 402–414. Springer, Heidelberg (1999)
6. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. J. ACM 51(4), 557–594 (2004)
7. Coppersmith, D.: Small solutions to polynomial equations, and low exponent rsa vulnerabilities. J. Cryptology 10(4), 233–260 (1997)
8. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory 22(6), 644–654 (1976)
9. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 523–540. Springer, Heidelberg (2004)
10. Fischlin, R., Schnorr, C.P.: Stronger security proofs for rsa and rabin bits. J. Cryptology 13(2), 221–244 (2000)
11. Freeman, D.M., Goldreich, O., Kiltz, E., Rosen, A., Segev, G.: More constructions of lossy and correlation-secure trapdoor functions. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 279–295. Springer, Heidelberg (2010)
12. Freeman, D.M., Goldreich, O., Kiltz, E., Rosen, A., Segev, G.: More constructions of lossy and correlation-secure trapdoor functions. J. Cryptology 26(1), 39–74 (2013)
13. Goldreich, O.: The Foundations of Cryptography. Basic Techniques, vol. 1. Cambridge University Press (2001)
14. Goldreich, O.: The Foundations of Cryptography. Basic Applications, vol. 2. Cambridge University Press (2004)
15. Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. 28(2), 270–299 (1984)
16. Herrmann, M.: Improved cryptanalysis of the multi-prime ϕ - hiding assumption. In: Nitaj, A., Pointcheval, D. (eds.) AFRICACRYPT 2011. LNCS, vol. 6737, pp. 92–99. Springer, Heidelberg (2011)
17. Hofheinz, D.: Possibility and impossibility results for selective decommitments. J. Cryptology 24(3), 470–516 (2011)
18. Hofheinz, D., Kiltz, E.: The group of signed quadratic residues and applications. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 637–653. Springer, Heidelberg (2009)
19. Joye, M., Libert, B.: Efficient cryptosystems from 2^k-th power residue symbols. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 76–92. Springer, Heidelberg (2013)
20. Joye, M., Paillier, P.: Fast generation of prime numbers on portable devices: An update. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 160–173. Springer, Heidelberg (2006)
21. Kakvi, S.A., Kiltz, E.: Optimal security proofs for full domain hash, revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 537–553. Springer, Heidelberg (2012)
22. Kiltz, E., O'Neill, A., Smith, A.: Instantiability of rsa-oaep under chosen-plaintext attack. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 295–313. Springer, Heidelberg (2010)

23. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen 261, 515–534 (1982)
24. Lewko, M., O'Neill, A., Smith, A.: Regularity of lossy rsa on subdomains and its applications. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 55–75. Springer, Heidelberg (2013)
25. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: STOC, pp. 187–196 (2008)
26. Seurin, Y.: On the lossiness of the rabin trapdoor function. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 380–398. Springer, Heidelberg (2014)
27. Steinfeld, R., Zheng, Y.: On the security of rsa with primes sharing least-significant bits. Appl. Algebra Eng. Commun. Comput. 15(3-4), 179–200 (2004)
28. Sun, H.M., Wu, M.E., Steinfeld, R., Guo, J., Wang, H.: Cryptanalysis of short exponent rsa with primes sharing least significant bits. IACR Cryptology ePrint Archive 2008, 296 (2008)
29. von zur Gathen, J., Gerhard, J.: Modern Computer Algebra, 3rd edn. Cambridge University Press (2013)
30. Xue, H., Li, B., Lu, X., Jia, D., Liu, Y.: Efficient lossy trapdoor functions based on subgroup membership assumptions. In: Abdalla, M., Nita-Rotaru, C., Dahab, R. (eds.) CANS 2013. LNCS, vol. 8257, pp. 235–250. Springer, Heidelberg (2013)
31. Yan, S.Y.: Number Theory for Computing, 2nd edn. Springer (2002)

Appendix: Signed QR Group

In this appendix, we investigate the 2^k-th power over Signed QR group, and propose another version of Rabin-OAEP. This version of OAEP is not used in practice, but this is one solution of constructing OAEP-like CPA secure encryption.

2^k-th Power over Signed QR Group

We first recall the definition of Signed QR group and the group operation. Let N be an integer, we represent Z_N^* in $[-(N-1)/2, (N-1)/2]$. For $x \in Z_N^*$, define $|x|$ as the absolute value of x. we denote J_N the subgroup of Z_N^* with Jacobi symbol 1, and QR the group of quadratic residue. The signed quadratic residues is defined as the group $QR_N^+ = \{|x| : x \in QR_N\}$, and $J_N^+ := \{|x| : x \in J_N\}$. For elements g, h and the integer x, the group operation is defined by

$$g \circ h = |g \cdot h \mod N|,\ g^{\underline{x}} = |\underbrace{g \cdot g \cdots g}_{x \text{ times}}| = |g^x \mod N|.$$

In fact, the Extended Blum Number is over a subset of Blum Numbers $N = pq$, $(p \equiv q \equiv 3 \mod 4)$. They have all the properties of Blum Numbers.

Lemma 2 (Lemma 1 in [18]). *Let N be an Extended Blum Number, then*

1. *$(QR_N^+, \circ)$ is a group of order $\phi(N)/4$.*
2. *$QR_N^+ = J_N^+$, and QR_N^+ is efficiently recognizable.*
3. *The map $QR_N \mapsto QR_N^+$ is a group isomorphism.*

The order of the Signed QR is odd, the 2^k-th power is a permutation. If the factorization of N or the inverse of 2^k modulo $\phi(N)/4$ is given, the preimage of 2^k-th power is computable. The 2^k-th power is a trapdoor permutation.

Lemma 3. *Let N be an Extended pseudo Blum Number associated with k, then*

1. *$(J_N^+, \circ)$ is a group of order $\phi(N)/4$.*
2. *$\left(\frac{-1}{p}\right)_{2^k} = 1, \left(\frac{-1}{q}\right)_{2^k} = 1$.*
3. *The 2^k-th power map over J_N^+ is 2^{2k} or 2^{2k-1}-to-1.*

Proof. The map $|\cdot|$ from J_N to J_N^+ has kernel $\{\pm 1\}$, so ord $(J_N^+) = \phi(N)/4$. By the definition of 2^k residue symbol. Items 2 holds. Item 2 implies that -1 belongs to

$$J^{k-1}_{(-,-)}$$

. We define $J_+^s = J^s_{+,+} \cup J^s_{-,-}$ to be the subset of R^s with Legendre symbol 1. To prove the third item, we investigate a sequence of subgroups and square maps on them. Precisely, for $0 \leq s \leq k+1$, we consider the subgroups of Z_N^* denoted by

$$R_+^s := \{x^{\underline{2^s}} | x \in J_N^+\},$$

and for $0 \leq i \leq k$ define the square map $f_i : y \to y^{\underline{2}}$ from R_+^{i-1} to R_+^i. Note that R_+^0 is J_N^+ itself. We first prove that the map f_i is a regular 4-to-1 map for $0 \leq i \leq k-1$. Then we show that the map f_k is regularly 4-to-1 or 2-to-1 depending on whether $-1 \in J_+^k$ or not. The combination map $g = f_k \circ f_{k-1} \cdots \circ f_1$ is regularly 2^{2k} or 2^{2k-1}-to-1 naturally. We divide the map f_i into two parts. The first part is the square map and the second part is the absolute map. From part two, -1 belongs to J_+^{k-1}, the surjective map from subset R_+^{i-1} to J_+^i is a 2-to-1 map $(1 \leq i \leq k)$, and the map from J_+^j to R_+^j is a 2 tot 1 map $(1 \leq j \leq k-1)$. The absolute value is a surjective homomorphism from J_+^k to R_+^k with kernel $\{1\}$ if $-1 \notin J_+^k$ and with kernel $\{\pm 1\}$ if $-1 \in J_+^k$. □

LTDP over Signed QR

We define $LTDP_{SQR} = (S_{inj}, S_{loss}, f_{SQR}, f_{SQR}^{-1})$ as follows:

1. *Sample Injective Function S_{inj}.* On input 1^n, S_{inj} chooses a proper k and random N in distribution R and the function index is $\sigma = \{N, k\}$. The trapdoor is $t = (2^k)^{-1} \mod \frac{\phi(N)}{4}$.
2. *Sample Lossy Function S_{loss}.* On input 1^n, S_{loss} chooses a proper k and random N in distribution L and the function index is $\sigma = \{N, k\}$.
3. *Evaluation algorithm f_{SQR}.* Given a function index $\sigma = \{N, k\}$ and input $x \in J_N^+$, the algorithm outputs $z = x^{\underline{2^k}} \mod N$.
4. *Inversion algorithm f_{SQR}^{-1}.* Given $z \in J_N^+$ and trapdoor t, compute and output $z^{\underline{t}} \mod N$.

Theorem 4. *If the 2^k-$\Phi/4$-hiding assumption holds, then $LTDP_{SQR}$ is an 2^{2k} or 2^{2k-1}-to-1 lossy trapdoor permutation.*

Another Modified Rabin-OAEP

The following scheme is another modification of Rabin-OAEP. The 2^k-th power is computed over Signed QR group. In this scheme, one needs to resample the output of OAEP until it falls into Signed QR group. The Leftover hash lemma guarantees that OAEP falls into Signed QR with probability about $\frac{1}{4}$. However, we have to admit that this is NOT done in practice.

KeyGen: On input a security parameters n, choose a k and n bits Extended Blum Number N associated with k. Choose a random t-wise independent hash function G_{K_G} and a hash function H_{K_H}. Compute the inversion of 2^k mod $\frac{\phi(N)}{4}$ and denote it as d.

$$pk = (N, k, G_{K_G}, H_{K_H}), \quad sk = d.$$

Encryption: On input a massage $m \in \{0,1\}^\mu$,
Step 1: Pick a random $r \in \{0,1\}^\rho$ for $\rho = n - \mu$.
Step 2: Set $s = m \parallel G_{K_G}(r)$.
Step 3: set $t = r \parallel H_{K_H}(s)$.
Step 4: Set $y = s \parallel t$ and view y as an integer. If $y \notin J_N^+$ goto step 1, otherwise set the ciphertext as $c = y^{\underline{2^k}} \mod N$.

Decryption: On input a ciphertext c,
Step 1: If $c \notin J_N^+$ output $\perp$, otherwise $y = c^{\underline{d}} \mod N$.
Step 2: For $y = s \parallel t$, set $r = t \oplus H_{K_H}(s)$.
Step 3: Compute and output $m = s \oplus G_{G_K}(r)$.