11-2013

Efficient lossy trapdoor functions based on subgroup membership assumptions

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

Bao LI

Xianhui LU

Dingding JIA

Yamin LIU

Efficient Lossy Trapdoor Functions Based on Subgroup Membership Assumptions*

Haiyang Xue[1,2], Bao Li[1,2], Xianhui Lu[1,2], Dingding Jia[1,2], and Yamin Liu[1,2]

[1] Institute of Information Engineering of Chinese Academy of Science, Beijing, China
[2] The Data Assurance and Communication Security Research Center of Chinese Academy of Sciences, Beijing, China
{hyxue12,lb,xhlu,ddjia,ymliu}@is.ac.cn

Abstract. We propose a generic construction of lossy trapdoor function from the subgroup membership assumption. We present three concrete constructions based on the k-DCR assumption over $\mathbb{Z}^*_{N^2}$, the extended p-subgroup assumption over $\mathbb{Z}^*_{N^2}$, and the decisional RSA subgroup membership assumption over $\mathbb{Z}^*_N$. Our constructions are more efficient than the previous construction from the DCR assumption over $\mathbb{Z}^*_{N^s}(s \geq 3)$.

Keywords: Lossy Trapdoor Functions, DCR Assumption, p-subgroup Assumption, Decisional RSA Assumption.

1 Introduction

Peikert and Waters [1] proposed the notion of lossy trapdoor function (LTDF) in STOC 2008. LTDF implies cryptographic primitives such as classic one-way trapdoor function [2], collision resistant hash function [3], oblivious transfer protocol [4], chosen ciphertext secure (CCA) public key encryption scheme[1], deterministic public key encryption scheme [5], OAEP based public key encryption scheme [6], and selective opening secure public key encryption scheme [7]. LTDFs can be constructed based on many assumptions, especially lattice-based assumptions.

Peikert and Waters [1] proposed two constructions of LTDFs, based on the Decisional Diffie-Hellman (DDH) assumption and the Learning with Errors assumption respectively. But the two constructions are not efficient since they both require a function index of size $\mathcal{O}(n^2)$. Boyen *et al.* [8] shrank the function index of the DDH-based construction from $\mathcal{O}(n^2)$ to $\mathcal{O}(n)$ with common reference string and pairing. But their method can only be applied to bilinear groups and their algorithm requires computing pairing, which is an expensive operation. Freeman *et al.* [9], [10] proposed a construction based on the d-linear

* Supported by the National Basic Research Program of China (973 project)(No.2013CB338002), the National Nature Science Foundation of China (No.61070171, No.61272534, No.61272035), the Strategic Priority Research Program of Chinese Academy of Sciences under Grant XDA06010702 and IIE's Cryptography Research Project (No. Y3Z0027103, No.Y3Z0024103, No. Y3Z002A103).

M. Abdalla, C. Nita-Rotaru, and R. Dahab (Eds.): CANS 2013, LNCS 8257, pp. 235–250, 2013.

assumption which is a generalization of the DDH assumption. This construction is not efficient since the size of the function index is $\mathcal{O}(n^2)$.

Under the quadratic residuosity (QR) assumption, two distinct constructions of LTDFs were given in [9], [11]. The construction of [9] only loses one bit of the input information. In the construction of [11], the inversion algorithm does not use the factorization of N but performs a coordinated ElGamal decryption and learns one bit at one time. Joye *et al.* [12] proposed the 2^k-QR assumption, which is a generalization of the QR assumption, and proved that it is implied by the QR assumption. They proposed a LTDF based on DDH and 2^k-QR assumptions which is slightly different from Hemenway-Ostrovsky's [11] method. In their construction, the factorization of N is the trapdoor and the inversion algorithm processes k bits at one time. With a well-chosen k, only a 18×18 matrix over $\mathbb{Z}_N^*$ is needed which highly reduces the length of the output. But the length of output and the function index is also too long for practical application.

The constructions above belong to the matrix based framework proposed by Peikert and Waters [1]. More efficient constructions of LTDFs based on different techniques were proposed. Kiltz *et al.* [6] showed that the RSA permutation provides a lossy property under the Φ-hiding assumption. A efficient LTDF based on the decisional composite residuosity (DCR) assumption over $\mathbb{Z}_{N^s}^*$, for $s \geq 3$, was proposed in [9], [10] and Wee [13] described a generic construction of LTDFs by using dual hash proof systems.

In the construction of Freeman *et al.* [9], the message is embeded into a subgroup generated by $(1 + N) \mod N^s$ with order N^{s-1} and the image is the group of N-th residuosity with order $\phi(N)$ in lossy mode, s must be larger than 2 in order to make lossiness. It is a very interesting question if we could make lossiness when $s \leq 2$.

1.1 Our Contribution

We propose a generic construction of LTDFs based on the subgroup membership assumption. For a finite cyclic group G with a non-trivial subgroup K, the subgroup membership problem asserts that it is difficult to decide whether an element is in K or $G \backslash K$. To construct LTDFs, two special properties are needed. Firstly, the subgroup discrete logarithm over G/K is easy to compute with the help of a trapdoor. Secondly, the size of G/K is significantly larger than that of K. The construction in [9] based on the DCR assumption over $\mathbb{Z}_{N^s}^*(s \geq 3)$ can be seen as a concrete example of our generic construction. According to our generic construction, $G = Z_{N^s}^*$ and K is the group of N^{s-1}-th residuosity.

We also present three concrete constructions over $\mathbb{Z}_{N^2}^*$ or $\mathbb{Z}_N^*$ which are more efficient. The main idea is to shrink the size of K. Briefly, our constructions can be described as follows.

- **k-DCR based construction.** We extend the 2^k-QR problem from $\mathbb{Z}_N^*$ to $\mathbb{Z}_{N^2}^*$ and get a new assumption named as k-DCR assumption. We prove that the k-DCR assumption over $\mathbb{Z}_{N^2}^*$ is implied by the DCR assumption and the QR assumption. We propose an efficient construction of $(\log N + k, 3k)$-LTDF based on the k-DCR assumption. This construction is more efficient

than the DCR based construction [9] and the 2^k-QR based construction [12]. With a well-chosen parameter k, we can get a $(\frac{9}{8}\log N, \frac{3}{8}\log N)$-LTDF. To our best knowledge, this is the first index independent LTDF over $\mathbb{Z}^*_{N^2}$. We can generalize this construction and get $((s-1)\log N+k, (s-2)\log N+3k)$-LTDFs over $\mathbb{Z}^*_{N^s}$, for $s \geq 2$.

- **Extended p-subgroup based construction.** We extend the p-subgroup problem from $\mathbb{Z}^*_N$ to $\mathbb{Z}^*_{N^2}$ and get an extended p-subgroup assumption. We propose a construction of $(\log N, \frac{2}{3}\log N)$-LTDF over $\mathbb{Z}^*_{N^2}$. This construction can also be generalized to $\mathbb{Z}^*_{N^s}$, for $s \geq 2$.
- **Decisional RSA subgroup based construction.** The decisional RSA subgroup assumption over Z^*_N for $N = (2p'r_p + 1)(2q'r_q + 1)$ was proposed by Groth [14], where p', q' are primes and r_p, r_q consist of distinct odd prime factors smaller than some low bound B. According to our generic construction, we get a LTDF based on the decisional RSA subgroup assumption.

Kiltz *et al.* [6] proposed an efficient LTDF based on the Φ-hiding assumption over $\mathbb{Z}^*_N$. They utilized a factor of $\phi(N)$ as the public key e in lossy mode. It seems difficult to construct an ALL-But-One (ABO) LTDF for CCA application following their steps. Our generic construction can easily be extended to the ABO LTDF. We will describe the extension in section 3.

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 subgroup membership problem. In Sect. 3, we present the generic construction of LTDF. In Sect. 4, we present concrete constructions of LTDF based on the k-DCR assumption, the extended p-subgroup assumption, and the decisional RSA subgroup assumption, respectively. In Sect. 5, we compare our work with the precious constructions. In Sect. 6, we conclude this paper.

2 Preliminaries

2.1 Notation

If S is a set, we denote its size by $|S|$ 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 Lossy Trapdoor Function

A collection of lossy trapdoor functions consists of two families of functions. Functions in the first family are injective and can be inverted with the trapdoor,

while functions in the second are lossy, meaning that the size of their image is significantly smaller than the size of their preimage. For CCA applications, it is convenient to work with the All-But-One lossy trapdoor function. In the following, we recall the definition of lossy trapdoor functions and All-But-One lossy trapdoor function.

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 $\sigma \in \{0,1\}^*$.*
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 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 $f_\sigma : \{0,1\}^m \to \{0,1\}^*$ 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.

Definition 2 (All-But-One Lossy Trapdoor Functions). *A collection of (m, l)-All-But-One lossy trapdoor functions are 4-tuple of PPT algorithms $(B, S, F_{ltdf}, F_{ltdf}^{-1})$ such that:*

1. Sample a branch B. *On input 1^n, B outputs a value $b \in \{0,1\}^*$.*
2. Sample a function S. *For every value b produced by B, the algorithm S outputs a triple $(\sigma, \tau, \beta) \in \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^*$ where σ is a function index, τ is a trapdoor, and β is a set of lossy branch.*
3. Evaluation algorithm F_{ltdf}. *For any b^* and b produced by $B(1^n)$, every σ, τ, β produced by $S(1^n, b^*)$, the algorithm $F_{ltdf}(\sigma, b, \cdot)$ computes a function $f_{\sigma,b} : \{0,1\}^m \to \{0,1\}^*$ with one of the two following properties:*
   - *Lossy: If $b = b^*$, then the image of f_σ has size at most 2^{m-l}.*
   - *Injective: If $b \neq b^*$, then the function f_σ is injective.*
4. Inversion algorithm F_{ltdf}^{-1}. *For any b^* and b produced by $B(1^n)$ and every (σ, τ, β) produced by $S(1^n, b^*)$ and every $x \in \{0,1\}^m$, we have*

$$F_{ltdf}^{-1}(\tau, F_{ltdf}(\sigma, b, x)) = x.$$

- *In the above algorithms, the two ensembles $\{\sigma, (\sigma, \tau, \beta) \leftarrow S(1^n, b)\}$ and$\{\sigma, (\sigma, \tau, \beta) \leftarrow S(1^n, b^*)\}$ are computationally indistinguishable.*
- *Any PPT algorithm A that receives as input (σ, b^*), where $b^* \leftarrow B(1^n)$ and $(\sigma, \tau, \beta) \leftarrow S(1^n, b^*)$, has only a negligible probability of outputting an element $b \in \beta \setminus \{b^*\}$.*

2.3 Subgroup Membership Assumption

Gjϕsteen [15] discussed the subgroup membership problem. A subgroup membership problem considers a group G with a non-trivial subgroup K. The problem asserts that it is hard to distinguish elements of K from elements of $G \backslash K$. Brown [16] analysed instances of subgroup membership problems and concrete schemes obtained by following the Cramer-Shoup framework [17]. Brown gave the constructions of CCA secure scheme based on the GBD subgroup membership assumption [18] , the r-th residuosity assumption [19], and the p-subgroup assumption [20]. Groth [14] proposed another example of the subgroup membership assumption, the decisional RSA subgroup assumption. Paillier and Pointcheval [21] discussed the subgroup variant of DCR-based encryption. The DCR assumption over this subgroup variant is also a subgroup membership assumption.

Definition 3 (Subgroup Membership Assumption). *Let G be a finite cyclic group G with subgroup K. Let g(resp. h) be a generator of group G (resp. K). The subgroup membership problem $SM_{(G,K)}$ asserts that, for any PPT distinguisher D, the adavantage*

$$Adv_D^{SM_{(G,K)}} = |\Pr[A(G,K,x) = 1 | x \leftarrow K] - \Pr[A(G,K,x) = 1 | x \leftarrow G \setminus K]|.$$

is negligible, where the probability is taken over coin tosses.

There are three interesting subgroup membership problems. We illustrate them here since they are useful for our construction of LTDFs.

The 2^k-QR assumption. Joye *et al.* [12] proposed the 2^k-QR assumption. Let $N = pq$ be the product of two large primes p and q with $p = 2^k p' + 1, q = 2^k q' + 1$, where p', q' are primes. The internal direct product of $\mathbb{Z}_N^*$ is: $\mathbb{Z}_N^* \cong G_{p'q'} \cdot G_{2^k} \cdot K_{2^K}$. The decomposition is unique except for the choice of K_{2^k}. Let $G = G_{p'q'} \cdot G_{2^k}$ and $K = G_{p'q'}$, the 2^k-QR assumption asserts that it is infeasible to distinguish elements of $G \setminus K$ from that of K.

The p-subgroup membership assumption. Okamoto and Uchiyama [20] proposed the p-subgroup assumption. Let p, q be primes and set $N = p^2 q$. Let g be a random element of $\mathbb{Z}_N^*$ such that the order of $g_p = g^{p-1} \mod p^2$ is p. Let $h = g^N \mod N$ and $G = \{x = g^m h^r \mod N | m \in \mathbb{Z}_p, r \in \mathbb{Z}_N\}$, $K = \{x = h^r \mod N | r \in \mathbb{Z}_N\}$. The p-subgroup assumption is that it is infeasible to distinguish elements of K from that of $G \setminus K$ given N and g.

The decisional RSA subgroup assumption. Groth [14] described a decisional RSA subgroup assumption over $\mathbb{Z}_N^*$ with semi-smooth order. Let $N = pq = (2p'r_p + 1)(2q'r_q + 1)$, with p, q, p', q' primes and r_p, r_q consists of distinct odd prime factors smaller than some bound B. The internal direct product of $\mathbb{Z}_N^*$ is: $\mathbb{Z}_N^* \cong G_{r_p r_q} \cdot G_{p'q'} \cdot G_2 \cdot T$. Let G be $G_{r_p r_q} \cdot G_{p'q'}$ and $K = G_{p'q'}$. The decisional RSA subgroup assumption asserts the hardness of distinguishing elements in $G \setminus K$ from K.

Gjϕsteen also gave the definition of subgroup discrete logarithm problem which is a generalization of Paillier's [22] partial discrete logarithm problem. In their definition, g is a group element such that its residue class generates

G/K and $\lambda : G \to \mathbb{Z}_{|G/K|}$ is the group homomorphism defined by $\lambda(g) = 1$ with $ker(\lambda) = K$. The subgroup discrete logarithm problem is: given a random $x \in G$, compute $\lambda(x)$. The formal definition follows.

Definition 4 (Subgroup Discrete Logarithm Problem). *Assume that group G has a non-trivial subgroup K and let g be a generator of G. If $\varphi : G \to G/K$ is the canonical epimorphism, then the subgroup discrete logarithm problem $SDL_{(G,K,g)}$ is: given a random $x \in G$, to compute $\log_{\varphi(g)}(\varphi(x))$.*

3 A Generic Construction of LTDF

In order to make lossiness in LTDFs, we assume a generic subgroup assumption having two special properties. The first property (namely SDL property) we assume is that the subgroup discrete logarithm problem is solvable with a trapdoor. For a subgroup membership problem $SM_{(G,K)}$, let τ be the corresponding trapdoor, there is a PPT algorithm to solve $SDL_{(G,K,g)}$ with the trapdoor τ. The second property (namely lossy property) we require is that the length of G/K's order is significantly larger than that of K's order. The input message in $[|G/K|]$ can be embeded into G by computing a pre-image of the map ψ. In the lossy mode, we just compute a pre-image falling into subgroup K. The length of G/K's order should be significantly larger than that of K in order to get lossiness.

In this subsection, we give the generic construction of LTDF based on the subgroup membership assumption with special property. We assume that there is a PPT generator Gen of groups with the subgroup membership assumption. The generator Gen takes the security parameter n and outputs (G, K, g, h, τ), where g (resp. h) is the generator of G (resp. K) and τ is the corresponding trapdoor. The order of G is a polynomial of n.

We construct a $(\log|G/K|,\ \log|G/K| - \log|K|)$-lossy trapdoor function $LTDF_{SM} = (S_{inj},\ S_{loss},\ F_{ltdf},\ F_{ltdf}^{-1})$ as follows:

1. *Sample Injective Function S_{inj}.* On input 1^n, S_{inj} chooses a random $r \in \mathbb{Z}_{|K|}$ and computes $c := gh^r$. The function index is $\sigma = (G, g, h, c)$. The trapdoor is $t = \tau$.
2. *Sample Lossy Function S_{loss}.* On input 1^n, S_{loss} chooses a random $r \in \mathbb{Z}_{|K|}$ and computes $c := h^r$. The function index is $\sigma = (G, g, h, c)$.
3. *Evaluation algorithm F_{ltdf}.* Given a function index $\sigma = (N, g, h, c)$ and input $x \in \{0,1\}^l$ where l is the length of $|G/K|$, the algorithm computes and outputs $z = c^x$.
4. *Inversion algorithm F_{ltdf}^{-1}.* Given a function index (N, g, h, c), the trapdoor $t = \tau$ and a message z, the algorithm recovers x with the algorithm of solving $SDL_{(G,K,g)}(z)$ problem.

Theorem 1. *If the membership assumption holds and the group G has the SDL property and the lossy property, then $LTDF_{SM}$ is an $(\log|G/K|,\ \log|G/K| - \log|K|)$-lossy trapdoor function.*

Proof. The algorithm to solve $SDL_{(G,K,g)}$ guarantees the correctness of inversion algorithm F_{ltdf}^{-1}. The subgroup membership assumption implies that the indices of injective and lossy functions are computationally indistinguishable. The output of the lossy function falls in subgroup K. The size of the lossy function's image is at most $\log|K|$. Consequently, the lossiness is $\log|G/K| - \log|K|$. □

Remark 1. The construction [9] based on the DCR assumption is a concrete example of this generic construction. The DCR construction is over $\mathbb{Z}_{N^s}^*$, where $N = (2p'+1)(2q'+1)$. The group structure of $\mathbb{Z}_{N^s}^*$ is

$$\mathbb{Z}_{N^s}^* \cong G_{N^{s-1}} \cdot G_{n'} \cdot G_2 \cdot T,$$

where G_t is the group of order t, T is a group with $\{-1, 1\}$ and $n' = p'q'$. The decomposition is unique except for the choice of G_2. In their construction, $G = G_{N^{s-1}} \cdot G_{n'} \cdot G_2 \cdot T$, $K = G_{n'} \cdot G_2 \cdot T$ with $(N+1)$ be the generator of $G_{N^{s-1}}$. The injective (resp. lossy) function index is $(1+N)r^{N^{s-1}} \mod N^s$ (resp. $r^{N^{s-1}} \mod N^s$) for randomly chosen $r \in \mathbb{Z}_N^*$. For a randomly chosen $g_0 \in K$, let g be $(1+N)g_0$ and h be a random element in K, then $LTDF_{SM}$ is exactly the DCR construction. The $SDL_{(G,K,(1+N)g_0)}$ problem can be solved with decryption algorithm of [23] and the lossiness property is satisfied. The disadvantage of the DCR construction is that s should be larger than 2.

The generic construction can easily be extended to a ABO LTDF. We describe the extension here and the security proof is similar with that of Theorem 5.4 in [9] and is therefore omitted. We also assume that there is a PPT generator *Gen* of groups with the subgroup membership assumption. The construction of $LTDF_{SM}^{ABO} = (B, S, F_{ltdf}, F_{ltdf}^{-1})$ follows:

1. *Sample a branch B.* On input 1^n, the algorithm B outputs a uniformly distributed $b \in \{0, 1, \ldots, |G|\}$.
2. *Sample a function S.* On input 1^n and a lossy branch b^*, S chooses a random $r \in \mathbb{Z}_{|K|}$ and computes $c := g^{-b^*}h^r$. The function index is $\sigma = (G, g, h, c)$.
3. *Evaluation algorithm F_{ltdf}.* Given a function index $\sigma = (N, g, h, c)$, a branch b and input $x \in \{0,1\}^l$ where l is the length of $|G/K|$, the algorithm computes and outputs $z = (g^b c)^x$.
4. *Inversion algorithm F_{ltdf}^{-1}.* Given a function index (N, g, h, c), the trapdoor $t = \tau$, a branch $b \neq b^*$ and a message z, the algorithm recovers x with the algorithm of solving $SDL_{(G,K,g^{b-b^*})}(z)$ problem.

Theorem 2. *If the membership assumption holds and the group G has the SDL property and the lossy property, then $LTDF_{SM}^{ABO}$ is an* $(\log|G/K|, \log|G/K| - \log|K|)$*-All But One lossy trapdoor function.*

4 Concrete Constructions of LTDF

This section shows new efficient concrete constructions of LTDFs based on three reasonable assumptions: the k-DCR assumption (implied by DCR and QR assumptions), the extended p-subgroup assumption, and the decisional RSA subgroup membership assumption.

4.1 LTDF Based on k-DCR Assumption

Joye *et al.* [12] proposed the 2^k-QR assumption and proved that it is implied by the classical QR assumption. We first review 2^k-QR assumption and DCR assumption, then give the formal definition of k-DCR assumption.

Definition 5 ([12] Definition 1). *Let p be an odd prime and $2^k|p-1$. Then the symbol*

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

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

Let $N = pq$ be the product of two prime numbers, and $p = 2^k p' + 1$, $q = 2^k q' + 1$ with p', q' be primes. Let $J_N := \{a \in Z_N^* | (\frac{a}{N})_2 = 1\}$, $QR_N := \{a \in Z_N^* | (\frac{a}{p})_2 = (\frac{a}{q})_2 = 1\}$ and $QNR_N := J_N \setminus QR_N$.

Definition 6. *Let $N = pq$ be the product of two large primes p and q with $p, q \equiv 1 \mod 2^k$. Define two sets*

$$W_0 := \{x \in QNR_N\},$$

$$W_1 := \{y^{2^k} \mod N | y \in Z_N^*\}.$$

The Gap 2^k Residuosity assumption (2^k-QR) asserts that, for any PPT distinguisher D, the advantage

$$\mathrm{Adv}_D^{2^k\text{-}QR} = |\Pr[D(x, N) = 1 | x \leftarrow W_0] - \Pr[D(x, N) = 1 | x \leftarrow W_1]|$$

is negligible, where the probability is taken over coin tosses.

Definition 7. *Let $N = pq$ be the product of two large primes p and q. Define two sets*

$$P := \{a = x^N \mod N^2 | x \in \mathbb{Z}_N^*\},$$

$$M := \{a = (1+N)^y x^N \mod N^2 | x \in \mathbb{Z}_N^*, y \in \mathbb{Z}_N\}.$$

The Decisional Composite Residuosity (DCR) assumption asserts that, for any PPT distinguisher D, the advantage

$$\mathrm{Adv}_D^{DCR} = |\Pr[D(x, N) = 1 | x \leftarrow P] - \Pr[D(x, N) = 1 | x \leftarrow \mathbb{Z}_{N^2}^*]|$$

is negligible, where the probability is taken over coin tosses.

The 2^k-QR assumption is over the group $\mathbb{Z}_N^*$. We embed $\mathbb{Z}_N^*$ into the group $\mathbb{Z}_{N^2}^*$ and get a k-DCR assumption by combining 2^k-QR and DCR assumptions. We also prove that the k-DCR assumption is implied by QR and DCR assumptions.

Definition 8. *Let $N = pq$ be the product of two large primes p and q with $p = 2^k p' + 1, q = 2^k q' + 1$. For random element $y \in QNR_N$, define two sets*

$$W_0 := \{a = r^{2^k N} \mod N^2 | r \in \mathbb{Z}_N^*\},$$

$$W_1 := \{a = (1+N)^z y^{tN} r^{2^k N} \mod N^2 | r \in \mathbb{Z}_N^*, t \in [2^k], z \in \mathbb{Z}_N\}.$$

The k Decisional Composite Residuosity (k-DCR) assumption asserts that, for any PPT distinguisher D, the advantage

$$\begin{aligned} Adv_D^{k\text{-}DCR} :=& |\Pr[D(x,y,N) = 1 | x \leftarrow W_0, y \leftarrow QNR_N] \\ & - \Pr[D(x,y,N) = 1 | x \leftarrow W_1, y \leftarrow QNR_N]. \end{aligned}$$

is negligible, where the probability is taken over coin tosses.

With overwhelming probability, random element $y \in QNR_N$ has order $2^k p'q'$ in $\mathbb{Z}_N^*$. In detail, let d_1 be the order of y modulo p, we have that d_1 equals to $2^k p'$ or 2^k since that $(\frac{y}{p})_2 \equiv y^{2^{(k-1)}p} \equiv -1 \mod p$. Similarly, the order of y modulo q, d_2, is $2^k q'$ or 2^k. Consequently, the order of random element y in $\mathbb{Z}_N^*$ is $2^k p'q'$ with probability $1 - \frac{1}{p'} - \frac{1}{q'} + \frac{1}{p'q'}$. We decompose $\mathbb{Z}_{N^2}^*$ as an inner direct product

$$\mathbb{Z}_{N^2}^* \cong G_N \cdot G_{2^k} \cdot G_{p'q'} \cdot K_{2^k},$$

where each group G_t is a group of order t. The decomposition is not unique, but if given an element $y^N \mod N^2$ where $y \in QNR_N$ has order $2^k p'q'$, the subgroup $G_N \cdot G_{2^k} \cdot G_{p'q'}$ is unique. Note that the element $(1+N)$ has order N in $\mathbb{Z}_{N^2}^*$, i.e. it generates G_N while $y^N \mod N^2$ has order $2^k p'q'$, i.e. it generates $G_{2^k} \cdot G_{p'q'}$. We have that $(1+N)y^N$ generates the group $G_N \cdot G_{2^k} \cdot G_{p'q'}$ which is actually W_1 in Definition 8. And W_0 in Definition 8 is actually group $G_{p'q'}$.

Theorem 3. *The k-DCR assumption is implied by the 2^k-QR assumption and QR assumption. It satisfies that,*

$$\mathrm{Adv}_D^{k\text{-}DCR} \leq 2\mathrm{Adv}_B^{2^k\text{-}QR} + \mathrm{Adv}_C^{DCR} \leq 8k\mathrm{Adv}_A^{QR} + \mathrm{Adv}_C^{DCR}.$$

Proof. The complete proof of the theorem can be found in Appendix.

Now, we show a construction of LTDF based on the k-DCR assumption over $\mathbb{Z}_{N^2}^*$. The output of our construction is much shorter, as compared with construction based on the DCR assumption [9] and Joye *et al.*'s construction based on the 2^k-QR assumption [12]. Specifically, the DCR based construction is over $\mathbb{Z}_{N^s}^*$ for $s \geq 3$. The output has $s \log N$ bits for $s \geq 3$. For well-chosen parameters, the output of 2^k-QR construction is a 18×18 matrix over $\mathbb{Z}_N$ with $234 \log N$ bits. Our construction is computed over $\mathbb{Z}_{N^2}^*$. We define $LTDF_{k\text{-}DCR} = (S_{inj}, S_{loss}, F_{ltdf}, F_{ltdf}^{-1})$ as follows

1. *Sample Injective Function* S_{inj}. On input 1^n, S_{inj} chooses an n-bits $N = pq$ where $p = 2^k p' + 1, q = 2^k q' + 1$ and p, q, p', q' are prime numbers. It chooses a random $y \in QNR_N$ and computes $g = y^N \mod N^2$. Then it chooses a random $h_1 \in \mathbb{Z}_N^*$ and compute $h = h_1^{2^k N} \mod N^2$. It chooses a random $r \in [\frac{N}{4^k}]$ and let $c = (1+N)gh^r \mod N^2$. The function index is $\sigma = (N, g, h, c)$. Let $\lambda = (p-1, q-1)$ then the trapdoor is $t = \{\lambda, p\}$.
2. *Sample Lossy Function* S_{loss}. On input 1^n, S_{loss} chooses an n-bits $N = pq$ where $p = 2^k p' + 1, q = 2^k q' + 1$ and p, q, p', q' are prime numbers. It chooses a random $y \in QNR_N$ and computes $g = y^N \mod N^2$. Then it chooses a random $h_1 \in \mathbb{Z}_N^*$ and compute $h = h_1^{2^k N} \mod N^2$. It chooses a random $r \in [\frac{N}{4^k}]$ and let $c = h^r \mod N^2$. The function index is $\sigma = (N, g, h, c)$.
3. *Evaluation algorithm* F_{ltdf}. Given a function index $\sigma = (N, g, h, c)$ and input $x \in [2^k N]$ the algorithm outputs $z = c^x$.
4. *Inversion algorithm* F_{ltdf}^{-1}. Given the function index (N, g, h, c), trapdoor $t = \{\lambda, p\}$ and a message z, the algorithm first computes $x_1 = \frac{z^\lambda - 1}{N} \lambda^{-1} \mod N$, then finds an $x_2 \in [2^k]$ such that the following holds,

$$\left[\left(\frac{g}{p}\right)_{2^k}\right]^{x_2} = \left(\frac{z}{p}\right)_{2^k} \mod p.$$

Finally, it computes x with the Chinese Reminder Theorem:

$$\begin{cases} x = x_1 \mod N, \\ x = x_2 \mod 2^k. \end{cases}$$

Theorem 4. *Under the k-DCR assumption, it holds that* $LTDF_{k\text{-}DCR}$ *is an* $(n+k, 3k)$*-lossy trapdoor function.*

Proof. Let $G = G_N \cdot G_{2^k} \cdot G_{p'q'}$ and $G = G_{2^k} \cdot G_{p'q'}$, the $SM_{G,K}$ is the k-DCR assumption. The decryption algorithms of Paillier's scheme [22] and Joye's scheme [12] solve the $SDL_{(G,K,(1+N)g)}$ problem correctly with the trapdoor. The order of G/K here is $2^k N$ and the order of K is $p'q'$. It's a direct result of Theorem 1. □

Remark 2. Joye *et al.* pointed out that for security parameters n, we can choose $k \leq \frac{1}{4} \log N - n$. If $k = n$, it is sufficient to set $k = \frac{1}{8} \log N$. This construction can be generalized to groups over $Z_{N^s}^*, s \geq 2$ by following the step of [23]. We note that if g is omitted, then $LTDF_{k\text{-DCR}}$ has less lossiness.

4.2 LTDF Based on Extended *p*-Subgroup Assumption

Okamoto and Uchiyama [20] proposed the p-subgroup assumption. with $N = p^2 q$. We restrict p, q to be safe primes for technical reasons. Now we consider the group $\mathbb{Z}_{N^2}^*$ with $N = p^2 q$. The element $(1+N)$ has order N in $\mathbb{Z}_{N^2}^*$. Consider the integer $(1+N)^i \equiv \sum_{j=0}^{i} C_i^j N^j \mod N^2$. The number is 1 modulo N^2 for some i

if and only if $(1+iN) \equiv 1 \mod N^2$. Clearly this is the case $i = aN$ for $a \in \mathbb{N}$, so it follows that the order of $(1+N) \mod N^2$ is N. For random element $y \in Z_N^*$, $g = y^{2N^2}$ has order $p'q'$ modulo N^2 with overwhelming probability. Indeed the order of g modulo p^4 (resp. q^2) is p' (resp. q') with probability $1 - \frac{1}{p'}$ (resp. $1 - \frac{1}{q'}$). The above g has order $p'q'$ modulo N^2 with probability $1 - \frac{1}{p'} - \frac{1}{q'} + \frac{1}{p'q'}$. If the inner direct product of $\mathbb{Z}_{N^2}^*$ is

$$\mathbb{Z}_{N^2}^* \cong G_N \cdot G_p \cdot G_{n'} \cdot K_4,$$

then $(1+N)$ is a generator of G_N and g is a generator of $G_{n'}$ with overwhelming probability. Consequently, $(1+N)g$ is a generator of $G_N \cdot G_{n'}$ with overwhelming probability.

Next, we consider the subgroup problem $SM_{(G_N G_{n'}, G_{n'})}$ over $\mathbb{Z}_{N^2}^*$ and propose another example of the subgroup membership assumption.

Definition 9 (Extended p-subgroup assumption). *With the notions above, let $G = G_N \cdot G_{n'}$ and $K = G_{n'}$. The extended p-subgroup assumption asserts that the subgroup membership problem $SM(G, K)$ is difficult.*

Now, we construct a LTDF based on the extended p-subgroup assumption. We define $LTDF_{E\ p\text{-}sub} = (S_{inj}, S_{loss}, F_{ltdf}, F_{ltdf}^{-1})$ as follows.

1. *Sample Injective Function S_{inj}.* On input security parameter 1^n, S_{inj} chooses $N = p^2 q$ where $p = 2p' + 1, q = 2q' + 1$ and p, q, p', q' are prime numbers. It chooses y randomly in $\mathbb{Z}_N^*$ and computes $h = y^{2N^2} \mod N^2$. S_{inj} chooses a random $r \in \mathbb{Z}_N$ and computes $c = (1+N)h^r \mod N^2$. The function index is $\sigma = (N, h, c)$. The trapdoor is $t = p'q'$.
2. *Sample Lossy Function S_{loss}.* On input security parameter 1^n, S_{loss} chooses $N = p^2 q$ where $p = 2p' + 1, q = 2q' + 1$ and p, q, p', q' are prime numbers. It chooses y randomly in $\mathbb{Z}_N^*$ and computes $h = y^{2N^2} \mod N^2$. S_{loss} chooses a random $r \in \mathbb{Z}_N$ and computes $c = h^r \mod N^2$. The function index is $\sigma = (N, h, c)$.
3. *Evaluation algorithm F_{ltdf}.* Given a function index $\sigma = (N, h, c)$ and input $x \in \mathbb{Z}_N$ the algorithm outputs $z = c^x$.
4. *Inversion algorithm F_{ltdf}^{-1}.* Given the function index (N, g, h, c), trapdoor t and a message z, the algorithm computes $x = \frac{z^t - 1}{N} t^{-1} \mod N$.

Theorem 5. *Under the extended p-subgroup assumption, it holds that $LTDF_{E\ p\text{-}sub}$ is an $(\log N, \frac{1}{3}\log N)$-lossy trapdoor function.*

Proof. Let $G = G_N \cdot G_{n'}$ and $K = G_{n'}$, the inversion algorithm solve the $SDL_{(G, K(1+N)h)}$ correctly. The order of G/K is N and the order of K is n'. It is a direct result of Theorem 1. □

4.3 LTDF Based on the Decisional RSA Subgroup Assumption

Groth [14] described a decisional RSA subgroup assumption over $\mathbb{Z}_N^*$ with semi-smooth order and gave a chosen plaintext secure encryption scheme over this

group. Let $N = pq = (2p'r_p + 1)(2q'r_q + 1)$, where p, q, p', q' are primes and r_p, r_q consist of distinct odd prime factors smaller than some low bound B. The internal direct product of $\mathbb{Z}_N^*$ is:

$$\mathbb{Z}_N^* \cong G_{r_p r_q} \cdot G_{p'q'} \cdot G_2 \cdot T.$$

In fact, $G_{r_p r_q} \cdot G_{p'q'}$ is the quadratic residue group QR_N of $\mathbb{Z}_N^*$. Let g be a generator of QR_N then $h = g^{r_p r_q}$ is a generator of $G_{p'q'}$. The decisional RSA subgroup assumption asserts that it is hard to distinguish elements drawn randomly from QR_N or from $G_{p'q'}$. Let $G = G_{p'q'} \cdot G_{r_p r_q}$ and $K = G_{p'q'}$, then the decisional RSA subgroup assumption is another instance of the subgroup membership assumption.

Let t be the number of distinct primes of $r_p r_q$, and we assume the length l of the prime factors is about $\log B$. Lemma 2 in [14] shows that a randomly chosen g in QR_N has order larger than $p'q'2^{(t-d)(l-1)}$ with overwhelming probability. To encrypt a message with length $(t-d)(l-1)$, where d is an integer smaller than t, we can encrypt m as $c = g^m h^r$. To decrypt c, we compute $c^{p'q'} = g^{p'q'm} \mod N$. The message m can be derived since the order of $g^{p'q'}$ has only small prime factors. The decryption algorithm is efficient with the help of a storage list. Groth gave an example of parameters, where $l_N = 1280$, $l_{p'} = l_{q'} = 160$, $B = 2^{15}$, $t = 64$, $d = 7$. The length of message space is no smaller than 698 with probability higher than $1 - 2^{-80}$. With well chosen parameters, this decisional RSA subgroup assumption can be used to construct efficient LTDF.

Next, we construct a LTDF based on the decisional RSA subgroup assumption. We define $LTDF_{RSA} = (S_{inj}, S_{loss}, F_{ltdf}, F_{ltdf}^{-1})$ as follows.

1. *Sample Injective Function* S_{inj}. On input 1^n, S_{inj} chooses $N = pq$ with $p = 2p'r_p + 1, q = 2q'r_q + 1$ where p, q, p', q' are prime numbers. Let r_p, r_q be B-smooth with distinct prime factors. It chooses $g \in QR_N$ randomly, and chooses a generator h of $G_{p'q'}$. It chooses proper parameters t and d and denotes $l_x = (t-d)(l-1)$. It chooses a random $r \in \mathbb{Z}_N$ and computes $c = gh^r \mod N$. The function index is $\sigma = (N, g, h, c)$. The trapdoor is the factorization of $\varphi(N)$.
2. *Sample Lossy Function* S_{loss}. On input 1^n, S_{loss} chooses $N = pq$ with $p = 2p'r_p + 1, q = 2q'r_q + 1$ where p, q, p', q' are prime numbers. Let r_p, r_q be B-smooth with distinct prime factors. It chooses $g \in QR_N$ randomly, and chooses a generator h of $G_{p'q'}$. It chooses proper parameters t and d and denotes $l_x = (t-d)(l-1)$. It chooses a random $r \in \mathbb{Z}_N$ and computes $c = h^r \mod N$. The function index is $\sigma = (N, g, h, c)$.
3. *Evaluation algorithm* F_{ltdf}. Given a function index $\sigma = (N, g, h, c)$ and the input $x \in \{0,1\}^{l_x}$ the algorithm outputs $z = c^x$.
4. *Inversion algorithm* F_{ltdf}^{-1}. Given the function index (N, g, h, c), the factorization of $\psi(N)$ and the message z, the algorithm invokes the inversion algorithm provided by the decryption algorithm of Groth's scheme. We compute $C_p = z^{p'q'} = (g^{p'q'})^x \mod N$. Since the order of $g^{p'q'}$ is B-smooth, we can derive x by computing discrete log of C_p base $g^{p'q'}$.

Theorem 6. *Under the decisional RSA subgroup assumption, it holds that* $LTDF_{RSA}$ *is an* $(l_x, l_x - (l_{p'} + l_{q'}))$*-lossy trapdoor function.*

Proof. Let G be the group generated by g and K be the group generated by h, this is a direct result of Theorem 1. □

5 Comparison

In the Table 1, we compare the three constructions instantiated with the generic construction in Section 3 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 a input message in bits and that of lossiness, respectively. The fifth column lists the size of the function index. The last column indicates if there there a direct extension to ABO-LTDF from the construction of LTDF or not.

Table 1. Comparison with existing LTDFs

	Assumption	Input size	Lossiness	Index size	Efficiency	ABO?
[1]	DDH	n	$n - \lvert\mathbb{G}\rvert$	$n^2\mathbb{G}$	n^2 Multi	Yes
[1]	LWE	n	cn	$n(d+w)\mathbb{Z}_q$	$n(d+w)$ Multi	Yes
[9], [10]	d-linear	n	$n - d\lvert\mathbb{G}\rvert$	$n^2\mathbb{G}$	n^2 Multi	Yes
[9], [10]	DCR	$(s-1)\log N$	$(s-2)\log N$	$\mathbb{Z}^*_{N^s}$	1 Modular Exp	Yes
[9], [10]	QR	$\log N$	1	$\mathbb{Z}^*_N$	1 Multi	Yes
[12]	DDH& QR	n	$n - \log N$	$(\frac{n}{k})^2\mathbb{Z}^*_N$	$(\frac{n}{k})^2$ Multi	Yes
[6]	Φ-hiding	$\log N$	$\log e$	$\mathbb{Z}^*_N$	1 Modular Exp	No
Sect.4.1	QR & DCR	$\log N + k$	$3k$	$\mathbb{Z}^*_{N^2}$	1 Modular Exp	Yes
Sect.4.2	E p-sub	$\log N$	$\frac{3}{4}\log N$	$\mathbb{Z}^*_{N^2}$	1 Modular Exp	Yes
Sect.4.3	D RSA	l_x	$l_x - l_{p'} - l_{q'}$	$\mathbb{Z}^*_N$	1 Modular Exp	Yes

In the first and third line, n *is the number of rows used in the matrix. It has to be larger than* $|\mathbb{G}|$*. In the second line,* $0 < C < 1$*,* n *is the rows used in the matrix,* $w = \frac{n}{\log p}$ *with* $p^2 \geq q$ *and* $d < w$*. In the forth line,* s *has to be larger than 2. In the sixth line and the construction in Sect. 4.1,* k *is less than* $\frac{1}{4}\log N - \kappa$ *where* κ *is the security parameter. In the seventh line,* e *is the factor of* $\phi(n)$*. In the last line,* l_x *is the length of the semi-smooth subgroup's order and* $l_{p'}$ *(resp.* $l_{q'}$*) is the length of* p' *(resp.* q'*).*

The LTDFs based on the QR, DCR and Φ-hiding assumptions are efficient. The QR based LTDF in [9], [10] has only one bit lossiness which is useless for some applications. Compared with the DCR based LTDF in [9], [10], our construction in Sect. 4.1 is computed over $\mathbb{Z}^*_{N^2}$ and the LTDF in Sect. 4.3 is computed over $\mathbb{Z}^*_N$. Compared with the Φ-hiding based LTDF in [6], our constructions have a direct extension to ABO-LTDFs.

6 Conclusion

We proposed a generic construction of lossy trapdoor function from the subgroup membership assumption. We presented three concrete constructions based on the k-DCR assumption over $\mathbb{Z}^*_{N^2}$, the extended p-subgroup assumption over $\mathbb{Z}^*_{N^2}$, and the decisional RSA subgroup membership assumption over $\mathbb{Z}^*_N$. Our constructions are more efficient than the previous construction from the DCR assumption over $\mathbb{Z}^*_{N^s}(s \geq 3)$.

Acknowledgments. The authors would like to thank anonymous reviewers for their helpful comments and suggestions.

References

[1] Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: STOC, pp. 187–196 (2008)
[2] Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory 22(6), 644–654 (1976)
[3] Goldreich, O.: The Foundations of Cryptography, Basic Techniques, vol. 1. Cambridge University Press (2001)
[4] Goldreich, O.: The Foundations of Cryptography, Basic Applications, vol. 2. Cambridge University Press (2004)
[5] 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)
[6] 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)
[7] Hofheinz, D.: Possibility and impossibility results for selective decommitments. J. Cryptology 24(3), 470–516 (2011)
[8] Boyen, X., Waters, B.: Shrinking the keys of discrete-log-type lossy trapdoor functions. In: Zhou, J., Yung, M. (eds.) ACNS 2010. LNCS, vol. 6123, pp. 35–52. Springer, Heidelberg (2010)
[9] 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)
[10] 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)
[11] Hemenway, B., Ostrovsky, R.: Lossy trapdoor functions from smooth homomorphic hash proof systems. Electronic Colloquium on Computational Complexity (ECCC) 16, 127 (2009)
[12] 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)
[13] Wee, H.: Dual projective hashing and its applications — lossy trapdoor functions and more. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 246–262. Springer, Heidelberg (2012)

[14] Groth, J.: Cryptography in subgroups of Z_n^*. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 50–65. Springer, Heidelberg (2005)
[15] Gjøsteen, K.: Symmetric subgroup membership problems. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 104–119. Springer, Heidelberg (2005)
[16] Brown, J., González Nieto, J.M., Boyd, C.: Concrete chosen-ciphertext secure encryption from subgroup membership problems. In: Pointcheval, D., Mu, Y., Chen, K. (eds.) CANS 2006. LNCS, vol. 4301, pp. 1–18. Springer, Heidelberg (2006)
[17] Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)
[18] Nieto, J.M.G., Boyd, C., Dawson, E.: A public key cryptosystem based on a subgroup membership problem. Des. Codes Cryptography 36(3), 301–316 (2005)
[19] Kurosawa, K., Katayama, Y., Ogata, W., Tsujii, S.: General public key residue cryptosystems and mental poker protocols. In: Damgård, I.B. (ed.) EUROCRYPT 1990. LNCS, vol. 473, pp. 374–388. Springer, Heidelberg (1991)
[20] Okamoto, T., Uchiyama, S.: A new public-key cryptosystem as secure as factoring. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 308–318. Springer, Heidelberg (1998)
[21] Paillier, P., Pointcheval, D.: Efficient public-key cryptosystems provably secure against active adversaries. In: Lam, K.-Y., Okamoto, E., Xing, C. (eds.) ASIACRYPT 1999. LNCS, vol. 1716, pp. 165–179. Springer, Heidelberg (1999)
[22] Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999)
[23] Damgård, I., Jurik, M.: A generalisation, a simplification and some applications of paillier's probabilistic public key system. Public Key Cryptography (1), 119–136 (2001)

Appendix: Proof of Theorem 3

Proof. Denote by V_0 the set $\{a = r^{2^k} \mod N | r \in \mathbb{Z}_N^*\}$. D is an algorithm which takes x, y, N as input and returns 0 or 1. We shall need the following experiments, **Experiment** i for $i = 1, 2, 3, 4$.

Experiment 1 :
Input: D, N, $y \in QNR_N$

1. $t \leftarrow [2^k]$, $z \leftarrow \mathbb{Z}_N$.
2. $r \leftarrow \mathbb{Z}_N^*$.
3. $b \leftarrow \{0, 1\}$.
4. If $b = 1$, then $x = r^{2^k N} \mod N^2$, otherwise $x = r^{2^k N} y^{tN}(1 + N)^z \mod N^2$.
5. $b' \leftarrow D(N, x, y)$.

Output: If $b' = b$ output 1, otherwise 0.

Experiment 2 :
Input: D, N, $y \in V_0$

1. $t \leftarrow [2^k]$, $z \leftarrow \mathbb{Z}_N$.
2. $r \leftarrow \mathbb{Z}_N^*$.
3. $b \leftarrow \{0, 1\}$.
4. If $b = 1$, then $x = r^{2^k N} \mod N^2$, otherwise $x = r^{2^k N} y^{tN}(1 + N)^z \mod N^2$.
5. $b' \leftarrow D(N, x, y)$.

Output: If $b' = b$ output 1, otherwise 0.

Experiment 3 :
Input: D, N, $y \in V_0$

1. $z \leftarrow \mathbb{Z}_N$.
2. $r \leftarrow \mathbb{Z}_N^*$.
3. $b \leftarrow \{0,1\}$.
4. If $b = 1$, then $x = r^{2^k N} \mod N^2$, otherwise $x = r^{2^k N}(1+N)^z \mod N^2$.
5. $b' \leftarrow D(N, x, y)$.

Output: If $b' = b$ output 1, otherwise 0.

Experiment 4 :
Input: D, N, $y \in QNR_N$

1. $r \leftarrow \mathbb{Z}_N^*$.
2. $b \leftarrow \{0,1\}$.
3. Set $x = r^{2^k N} \mod N^2$.
4. $b' \leftarrow D(N, x, y)$.

Output: If $b' = b$ output 1, otherwise 0.

Let $T_i, i = 1,2,3,4$ denote the event that the Experiment i returns 1. By the definition of k-DCR, Experiment 1 is exactly the k-DCR experiment, and we have

$$\mathrm{Adv}_D^{k-DCR} \leq |2\Pr[T_1] - 1|.$$

Now we consider the Experiment 2, the only difference between Experiment 1 and 2 is that y is sampled from V_0 instead of QNR_N. We have,

$$2|\Pr[T_1] - \Pr[T_2]| \leq \mathrm{Adv}_B^{2^k\text{-}QR}.$$

In Experiment 3, if y is chosen from V_0 uniformly, then Experiment 2 and 3 are identical. We have that, $\Pr[T_2] = \Pr[T_3]$.

Now we consider Experiment 4. The difference between Experiment 4 and 3 is the choice of x and y. Define $X := \{r^{2^k N}(1+N)^z \mod N^2 | r \leftarrow \mathbb{Z}_N^*, z \leftarrow \mathbb{Z}_N\}$ and $L := \{r^{2^k N} \mod N^2 | r \leftarrow \mathbb{Z}_N^*\}$. Given input x of classical DCR problem, if x is chosen uniformly from M (resp. P), then x^{2^k} is uniformly distributed over X (resp. L). The indistinguishability of y in Experiment 3 and 4 is implied by 2^k-QR assumption. Consequently, the difference between Experiment 4 and 3 is bounded by DCR and 2^k-QR assumptions.

$$2|\Pr[T_3] - \Pr[T_4]| \leq \mathrm{Adv}_B^{DCR} + \mathrm{Adv}_B^{2^k\text{-}QR}.$$

The input of D in Experiment 4 includes no information of b, we have that $Pr[T_4] = \frac{1}{2}$. Combining the above, we have

$$\begin{aligned}
\mathrm{Adv}_D^{k\text{-}DCR} &\leq |2\Pr[T_1] - 1| \\
&\leq 2|\Pr[T_1] - \Pr[T_4]| \\
&\leq 2|\Pr[T_1] - \Pr[T_2]| + 2|\Pr[T_2] - \Pr[T_3]| + 2|\Pr[T_3] - \Pr[T_4]| \\
&\leq 2\mathrm{Adv}_B^{2^k\text{-}QR} + \mathrm{Adv}_C^{DCR}.
\end{aligned}$$

With the result of Theorem 2 in [12], $\mathrm{Adv}_B^{2^k\text{-}QR} \leq 4k\mathrm{Adv}_A^{QR}$, we have that

$$\mathrm{Adv}_D^{k\text{-}DCR} \leq 8k\mathrm{Adv}_A^{QR} + \mathrm{Adv}_C^{DCR}.$$

□