Several Theorems on Probabilistic Cryptosystems

Yuliang ZHENG¹, Nonmember, Tsutomu MATSUMOTO†
and Hideki IMAI², Members

SUMMARY This paper proves several theorems on probabilistic cryptosystems. From these theorems it follows directly that a probabilistic cryptosystem proposed by the authors, whose security is based upon the (supposed) infeasibility of $\gamma^n$-Residuosity Problem, is polynomially secure. Techniques developed in the paper are of independent interest.

1. Introduction

The authors proposed in Ref. (7) a probabilistic cryptosystem based upon the intractability of a famous Number-Theoretic problem called $\gamma^n$-Residuosity Problem ($\gamma^n$-RP). This cryptosystem can be viewed as a byte-by-byte generalization of a bit-by-bit probabilistic cryptosystem (the GM cryptosystem) discovered by Goldwasser and Micali in Ref. (4).

Let $m_1$ and $m_2$ be two messages. Intuitively, a cryptosystem is polynomially secure if no polynomial size bounded adversary, when given two encryptions one of which is for $m_1$ and the other for $m_2$, can tell which encryption corresponds to which message.

Under Quadratic Residuosity Assumption, the GM cryptosystem was shown to be polynomially secure²⁴. Benaloh and Yung claimed²⁵ that the theorems proved in Ref. (4), which were concerned with the binary case of $\gamma=2$, can be "directly" generalized to the case of $\gamma>2$. They, however, did not present any hint on how to "directly" generalize the theorems. To the authors' knowledge, no published paper has suggested how to treat the general case of $\gamma>2$. It seems to the authors that it is not so obvious to generalize the theorems proved in Ref. (4).

The main purpose of this paper is to give proofs for several theorems on probabilistic cryptosystems, from which it follows directly that our probabilistic cryptosystem is polynomially secure. Techniques developed in the paper are of independent interest.

The remaining part of the paper is organized as follows. First, we review concisely the notion of polynomial security and our generalized probabilistic cryptosystem based upon $\gamma^n$-RP (Sec. 2). Then we extend the definition of unapproximable trapdoor predicators²⁶ to that of unapproximable trapdoor functions (Sec. 3), and construct a probabilistic cryptosystem $C_{\gamma^n}$ based upon any unapproximable trapdoor function (Sec. 4). We proceed to prove that under $\gamma^n$-Residuosity Assumption, the set of class-index functions $I=\bigcup_k$ is an unapproximable trapdoor function (Theorems 1 and 2, Sect. 5), and the cryptosystem $C_{\gamma^n}^*$ is polynomially secure (Theorem 3, Sect. 6). From Theorems 2 and 3 it follows that under $\gamma^n$-Residuosity Assumption, our generalized cryptosystem is indeed polynomially secure (Theorem 4, Sect. 6).

2. Preliminary

This section briefly reviews the notion of polynomial security and an efficient probabilistic cryptosystem whose security is based upon the intractability of $\gamma^n$-RP. See Refs. (4) and (7) for details.

2.1 Polynomial Security

Denote by $\mathcal{P}$ the set of positive integers. For any $n \in \mathcal{P}$, define $Z_n=(0, 1, \cdots, n-1)$, and $Z^*_{\mathcal{P}}=\{x|x \in Z_n \text{ and } (x, n)=1\}$. The number of elements in a finite set $S$ is denoted by $|S|$, and in particular $|Z^*_{\mathcal{P}}|$ is denoted by $\phi(n)$. The concatenation of two sequences $x$ and $y$ over some alphabet is represented by $x\parallel y$. When we want to emphasize that an algorithm $A$ (circuit $C$, respectively) receives $t$ inputs, we write $A(t)\cdot \chi(t)\cdot \chi(t)$, respectively.

Denote $K$ be the set of all security parameters $\gamma_k$. For simplicity assume that $K$ is an infinite subset of $\mathcal{P}$. We will use a $k\in K$ as an input to a cryptosystem defined below to create a pair of encryption/decryption algorithms. $k$ determines many quantities such as the plaintext length and the security strength of a pair of

* Before us, Benaloh and Yung²⁵ used a probabilistic cryptosystem presented in the appendix of Ref. (2) in constructing an election scheme. The form of this cryptosystem can be viewed as a byte-by-byte generalization of the GM cryptosystem, but as we will mention later in this paper, no proof on the security of the cryptosystem can be found in Ref. (2). Our cryptosystem looks like Benaloh-Yung's (see Ref. (7) for details) but is proved to be polynomially secure under $\gamma^n$-Residuosity Assumption.
encryption/decryption algorithms. For every k ∈ K there is a set Mk called the message space associated with k.

A cryptosystem is a polynomial time algorithm C which on input a k ∈ K, outputs a pair (E, D) of encryption/decryption algorithms. Note that generally there are a lot of pairs (E, D) corresponding to a given k, and on input k the algorithm C outputs one of the pairs in a randomized and uniform way. The set of all pairs generated by C on input k is denoted by C(k), and for any (E, D) ∈ C(k), the set of all encryptions of m ∈ Mk is denoted by E(m).

A cryptosystem C is called probabilistic (or randomized) if E is a probabilistic (or randomized) algorithm for all k ∈ K and all C ∈ C(k). Note that for a probabilistic cryptosystem C, E(m) is typically quite large.

The notion of polynomial security is set up by means of two kinds of polynomial size circuits—line tappers and message finders.

A line tapper is a family of polynomial size circuits T = (T(k) ∈ K). Each Tk has one Boolean output and two inputs: one for code(E) with (E, D) ∈ C(k) and the other for an encryption e(E)(m), where m belongs to Mk, and code(E) denotes a suitable encoding of the encryption algorithm E. For any m ∈ Mk, let p(m) denote the probability that Tk outputs 1 on input code(E) and e(E)(m), p(m) is taken over all the encryptions e(E)(m).

A message finder is also a family of polynomial size circuits F = (Fk ∈ K). For each k ∈ K and (E, D) ∈ C(k), the circuit Fk outputs two messages m1, m2 ∈ Mk, on input code(E).

[Definition 1] Let Qk and Q1 be two polynomials. A cryptosystem C is polynomially secure if there is no message finder F such that for infinitely many k ∈ K, for a line tapper T, for any (E, D) ∈ C(k), Fk finds with probability greater than 1/Ω(k) two messages m1, m2 ∈ Mk, such that |

\[ p(m1) - p(m2) \geq \frac{1}{Q(k)} \]

2.2 A Cryptosystem Based on γ^n-RP

Let γ and n be positive integers. An integer x with gcd(x, n) = 1 is called a γ^n-residue modulo n if there exists an integer w such that x ≡ w^γ (mod n), or a γ^n-nonsite modulus n if there doesn’t exist such a w.

Assume that γ is an odd integer with γ ≥ 3. Call n ∈ ℤ a hard integer about k if n ≡ p^2 (mod γ^n) + 1 such that \[ |p - p| - γ = k, \] gcd (r, q, γ) = 1 and the four integers p, q, r, q are all primes. Denote by H(n) the set of all hard integers about k.

Let n = p^2 + 1, and let h_n be primitive roots mod p and mod q, respectively, such that h_n = 1 (mod γ^n) and h_n = 1 (mod p). For any γ ∈ ℤ, we call the triple (n, y, γ) acceptable if y can be written as y = h^n γ, where 0 < γ < γ, gcd(e, γ) = 1, 1 ≤ h ≤ h and 1 ≤ h ≤ h (q).

It is proved in Ref. [7] that for any acceptable triple (n, γ, y), every element x ∈ ℤ can be represented as x = y^n γ (mod n) with a unique 0 ≤ i ≤ γ and some a_i ∈ ℤ. Clearly, from the definition of AI, an element x ∈ ℤ is a γ^n-residue mod n if and only if I(x) = 0.

It is also proved in Ref. [7] that for an acceptable triple (n, γ, y) where γ = O(k^n), the following three closely related problems are polynomially equivalent:

1. γ^n-RP: Given a random selected element e ∈ ℤ, decide whether or not a is a γ^n-residue mod n.
2. Class-Index-Comparing Problem: Given two random selected elements a, p ∈ ℤ, judge whether or not a and p have the same class-index with respect to (n, γ, y).
3. Class-Index-Finding Problem: Given a random selected element e ∈ ℤ, find the class-index of e with respect to (n, γ, y).

There are strong evidences[13] which support the conjecture that γ^n-RP is intractable unless the factorization of n is known. This conjecture is formally stated as:

[Definition 2] (γ^n-Residually Assumption) Let Qk be polynomials, and C_{n, k}(·) a circuit with one Boolean output. Call an integer m ∈ ℤ easy with respect to C_{n, k}(·), if for a fraction 1/2 ≤ m ∈ ℤ, C_{n, k}(m, n, x, z) = 1 if x is a γ^n-residue mod n. Denote by H(n, k) the set of all the class-indexes of x with respect to C_{n, k}(·).

Then for any polynomial size circuit C_{n, k}(·), for any polynomials Qk, Q, and for all sufficiently large k,

\[ P(\frac{\text{H}(n)}{H(n)}) \leq \frac{1}{Q(k)} \]

Let I be a polynomial in k. For each k ∈ K define M_k = mk for m ∈ ℤ, l = l(k). Based on γ^n-Residually Assumption, a probabilistic cryptosystem is constructed in the following way: Let (n, y, γ) be an acceptable triple selected by Alice, where γ = O(k^n). Alice makes n, γ and y public, but keeps the factorization (p, q) of n secret. Now suppose Bob wants to securely send a message m ∈ Mk to Alice. The encryption algorithm for Bob and the decryption algorithm for Alice are as follows:

ENCRYPTION ALGORITHM E(n, γ, y, m)

From i = 1 to l, randomly choose a ∈ ℤ, and

\[ y = y^{A(k)} \]

which means that γ is bounded by a polynomial in k.

1. By γ=O(k^n), this assumption is more formal, but a little stronger, than that given in Ref. [7].
compute \( c \cdot \overline{c} \mod n \). Let \( e = \{ c_0, c_1, ..., c_{t-1} \} \) be an encryption of the message \( m = m_0, m_1, ..., m_{t-1} \).

**Decryption Algorithm** \( D(k, q, r, u, c) \)

For each \( c_i \), let \( 0 \leq i \leq t-1 \), do as follows: (1) Randomly select \( z_0, ..., z_{t-1} \) as well as \( x_0, x_1, ..., x_{t-1} \), and compute \( z_i = x_i \cdot z_i, 0 \leq i < t \). If \( \sum_{i=0}^{t-1} x_i = 0 \mod p \), then let \( m_i = \sum_{i=0}^{t-1} x_i \cdot c_i \); otherwise return to (1). Let \( m = m_0, m_1, ..., m_{t-1} \) be the message concealed in the encryption \( c = c_0, c_1, ..., c_{t-1} \).

### 3. Unapproximable Trapdoor Functions

We now generalize unapproximable trapdoor predicates defined in Ref. [4] to unapproximable trapdoor functions.

Let \( P_1, P_2 \) be two polynomials. For any \( k \in K \), let \( S_k \) denote a subset of integers which each of which is \( \alpha \) of \( P(k) \)-bit long. For any \( x \in S_k \), let \( \mathcal{L} \) be a subset of \( P(k) \)-bit sequences, i.e., \( \mathcal{L} \subseteq \{ 0, 1 \}^{bm} \).

Assume that \( J = \{ 0, 1, ..., \beta - 1 \} \), where \( \beta \neq \mathcal{R} \). For any \( x \in S_k \), define a function \( Y : \mathcal{L} \rightarrow J \). Denote the set of functions indexed by integers of length \( P(k) \) by \( \mathcal{Y} = \{ Y \mid Y \in \mathcal{L} \} \). Let \( U = \cup \mathcal{Y} \), where \( U \) is the union operation about all security parameters in \( K \).

**Definition 3.** An approximable family is a family \( A = \{ A_k(k \in K) \} \) of circuits, where each \( A_k \) is a polynomial size circuit with two inputs and one output. On input an \( n \in S_k \) and \( x \in \mathcal{L} \), \( A_k \) outputs the binary representation of an integer \( i \in U \).

**Definition 4.** Let \( A = \{ A_k(k \in K) \} \) be an approximable, let \( Y = \cup \mathcal{Y} \), and let \( k = K \) be a subset of \( J \). For any \( x \in S_k \), define a function \( Y : \mathcal{L} \rightarrow J \) for at least \( 1/\beta \) of \( k \) in \( \mathcal{L} \). Also \( A_k \in K \).

**Definition 1.** Let \( A = \{ A_k(k \in K) \} \) be an approximable, and let \( Y = \cup \mathcal{Y} \). For any \( x \in S_k \), and for any \( k \in K \), and for an\( k \in K \), define \( z = \sum_{z \in K} A_k(k \in K) \) for the set of integers \( x \in S_k \) for which \( A_k(k \in K) \) approximates the function \( Y : \mathcal{L} \rightarrow J \). \( Y \) is called unapproximable if it is a polynomial \( Q_k \) and \( Q_x \) for all sufficiently large \( k \in K \).

For any \( k \in K \), \( x \in S_k \), and \( i \in \mathcal{L} \), let \( \mathcal{L}_k(\{ x \in \mathcal{L} \}, Y \cdot x) = i \). Thus \( \mathcal{L}_k \) is the set of elements in \( \mathcal{L} \) which have the same image \( i \) under the function \( Y \).

**Definition 6.** Let \( Y = \cup \mathcal{Y} \). \( Y \) is called an unapproximable trapdoor function if:

1. \( Y \) is unapproximable.
2. \( Y \) is trapdoor in the following sense:

#### 2.1. (Encryption Condition)
Given \( \in S_k \) and \( i \in \mathcal{L} \), it is easy (i.e., can be done in probabilistic polynomial time) to select an \( x \) randomly and uniformly from \( \mathcal{L}_k \).

#### 2.2. (Decryption Condition)
There is a function \( \delta : \mathcal{L} \times x \rightarrow \mathcal{R}^+ \) such that \( \delta(x) \) is of polynomial size in \( k \) for all \( n \), and such that for all \( x \in \mathcal{L} \), and for any \( x \in \mathcal{L}_k \), it is easy to compute \( Y(x) \) from \( x \) and \( \delta(x) \). \( \delta(x) \) is called the secret trapdoor of \( n \).

#### 2.3. (Constructability Condition)
For any \( k \in K \), it is easy to select randomly and uniformly an \( \mathcal{L}_k \) and hence its secret trapdoor \( \delta(x) \).

The definition of unapproximable trapdoor functions and, is two polynomials. Then there is an important fact which will be used later in the proof of Theorem 3: For all sufficiently large \( k \), for a fraction greater than \( 1 - 1/Q(k) \) of the \( n \) in \( S_k \), and for all \( x \in \mathcal{L} \), we have \( \| i \|=1/Q(k) \) if \( k \) is not the trivial circuits \( A_k \) of which each of which \( 1/\beta \) of \( Q(k) \)-approximate \( Y : \mathcal{L} \rightarrow J \) for a fraction \( 1/Q(k) \) of the \( n \) in \( S_k \). As works as follows: On input an \( x \in \mathcal{L} \), and an \( x \in \mathcal{L} \), it outputs \( i \) whenever \( i \) \( \mathcal{L}_k \) for \( Q(k) \)-approximate \( Y : \mathcal{L} \rightarrow J \) whenever \( x \in \mathcal{L} \), outputs a randomly and uniformly selected \( i \) whenever \( x \in \mathcal{L} \) whenever \( Q(k) \) for some \( x \in \mathcal{L} \) output 0 otherwise... So the fact is true.

Several functions have been proved to be unapproximable trapdoor ones (under some reasonable assumptions). One of them is based on the difficulty of breaking RSA or symmetric key systems. It is based on the well-known RSA problem in the literature. For details see Ref. [1]...

We now consider another candidate for unapproximable trapdoor functions: Let \( \beta > \gamma \) be an odd. Then \( Z = \{ 0, 1, ..., \beta - 1 \} \). Let \( H_k \) be the hard integer set. Also let \( S_k = \{ \gamma \} \times \mathcal{L}_k \), where \( \gamma \) is an acceptable triple, and let \( \mathcal{L}_k \rightarrow \mathcal{Z} \) for \( \gamma \in \mathcal{L}_k \). Finally, let \( \gamma \) be a class-index function, i.e., \( i \in \mathcal{L}_k \) if \( x \cdot x^\gamma \mod n \) for some \( x \in \mathcal{L}_k \).

Note. We have simplified the definitions for \( S_k \) and \( \mathcal{L}_k \). Rigorous definitions are troublesome, and lacking in readability: First an invertible function \( f \) mapping \( \gamma \) into a positive integer should be introduced. \( S_k \) should be defined as \( S_k = \{ 1, (f(i)) \} \}, \) and instead of \( \mathcal{L}_k \neq \mathcal{Z} \), we should have \( \mathcal{L}_k = \{ (f(i)) \} \}. \)

It is easy to see that \( f \) is trapdoor, i.e., it satisfies all the encryptions, decryptions, and constructability conditions. In Sect. 5 we will prove that \( f \) is also unapproximable under \( \gamma \)-Residuosity Assumption.

### 4. Probabilistic Cryptosystem \( C \)

Let \( L \) be a probabilistic \( \in \mathcal{L} \), and let \( Y = \cup \mathcal{Y} \) be an unapproximable trapdoor function. \( M = \{ m_i, m_i \cdot \mathcal{L}_k, m_i \in \mathcal{L} \} \) be the message space.
associated with \( k \). Along the same line as Ref. (4), we obtain from \( Y \) a probabilistic public-key cryptosystem which we call \( C_{orr} \).

On input \( k \in K \), \( C_{orr} \) outputs a randomly and uniformly selected element \( w \in \mathcal{S}_n \), its secret trapdoor \( \delta(w) \), and descriptions of encryption/decryption algorithms \( E_{orr} \) and \( D_{orr} \), specified below.

**ENCRYPTION ALGORITHM \( E_{orr}(w) \)**

For \( i = 1 \) to \( l \), select randomly and uniformly a \( c_i \) from \( \mathcal{L}_n \) such that \( Y(c_i) = m_i \). Output \( c = c_{c_1} \ldots c_{c_l} \) as encryption of \( m = m_1 \ldots m_l \). Suppose by the use of the secret trapdoor \( \delta(w) \). Output \( m = m_1 \ldots m_l \) by \( m_i \in M_i \).

When \( Z = \{0, 1\} \), i.e., when \( Y \) is an unapproximable trapdoor predicate, polynomial security of \( C_{orr} \) was proved by Goldwasser and Micali (see Ref. (4), Theorem 5.1). They considered furthermore an implementation of \( C_{orr} \) by a predicate \( B = \bigcup B_i \) (see Ref. (4) for details). Especially, they showed that under Quadratic Residuosity Assumption, \( B \) is an unapproximable trapdoor predicate, from which it follows that the concrete implementation of \( C_{orr} \) by the predicate \( B \) is indeed polynomially secure.

Our generalized probabilistic cryptosystem is a concrete implementation of \( C_{orr} \) by the set of class-index functions \( I = \bigcup I_i \) defined in Sect. 3. We now prove the polynomial security of this cryptosystem by establishing a series of theorems (Theorems 1, 2, 3 and 4).

5. Unapproximable Trapdoorness of \( I = \bigcup I_i \)

Theorems 1 and 2 to be proved below are related to the unapproximable trapdoorness of \( I = \bigcup I_i \).

First, to establish a key probabilistic proposition in Probability Theory—the Weak Law of Large Numbers (WLLN): * \( \text{[Proposition 1]} \) Let \( \omega \) be an event which occurs with probability \( p \) in a given experiment. Let \( X_1, X_2, \ldots, X_n \) be a sequence of random variables defined as \( X_i = 1 \) if \( \omega \) occurs at the \( i \)-th trial; \( X_i = 0 \), otherwise.

Also let \( X = X_1 + X_2 + \cdots + X_n \).

Then for any \( \varepsilon > 0 \),

\[
\Pr(|X - n \cdot p| < \varepsilon) \geq 1 - \frac{4 \cdot n \cdot \varepsilon^2}{m^2} \to 1, \quad \text{as} \, n \to \infty. \tag{6}
\]

The WLLN is the basis of the extensively applied Monte Carlo experiment.

We are ready to prove Theorem 1. This theorem says that even a small amount of stochastic advantage in correctly guessing the residue of elements in \( \mathbb{Z}_m^* \) can be amplified, so that the resiliency of any element in \( \mathbb{Z}_m \) can be efficiently decided with probability arbitrarily close to 1.

Though one can view Theorem 1 as the generalization of Theorem 5.1 of Ref. (4), it seems difficult to apply the technique for proving Theorem 5.1 of Ref. (4) to the proof of Theorem 1, since here one has to handle as many as \( 2^3 \) different cases. The technique we use to prove Theorem 1 differs quite from that for proving Theorem 5.1 of Ref. (4), and in designing it we obtain some hints from the template-matching method, which is an intuitive pattern recognition technique and is well explained in Ref. (3).

**[Theorem 1]** Let \( q_1 \) and \( q_2 \) be any polynomials, and let \( H \) be the hard integer set where \( \gamma = \{0, 1\} \). There exists such a circuit \( C = \{x, y, n\} \) such that \( C(x, y, n) = \text{Irrand}(x) \) for any \( w \in \mathcal{H}(G) \), for any \( y \in \mathbb{Z}_m^* \) with \( (n, y, \gamma) \) an acceptable triple, and for a fraction greater than 1/4 \( q_1(q_2) \) of the class-index \( x \) with respect to \( (n, y, \gamma) \), for any \( w \in \mathcal{H}(G) \), any \( y \in \mathbb{Z}_m^* \) with \( (n, y, \gamma) \) an acceptable triple, and any \( y \in \mathbb{Z}_m^* \).

**Proof** The proof can be roughly divided into two stages. In the first stage, we construct two matrices \( W \) and \( \overline{W} \), where \( \overline{W} \) depends on a triple \( (n, y, \gamma) \) and \( W \) depends not only on \( (n, y, \gamma) \) but also on an element \( e \in \mathbb{Z}_m^* \) whose class-index is to be determined. In the second stage, we compare \( W \) with \( \overline{W} \). When \( W \) is obtained by shifting \( \overline{W} \) downward and cyclically for \( s \) times, and examine whether or not they are close to each other. Here the template-matching method is used. If we find that for some \( w \in \mathbb{Z}_m^* \), \( V \) and \( \overline{W} \) are quite close to each other, we decide that this is the class-index of \( x \). Error probability introduced by such a decision procedure will be proved to be negligible.

Now we describe the proof in detail. For any \( w \in \mathcal{H} \) and any acceptable triple \( (n, y, \gamma) \), define \( R = \{x \in \mathbb{Z}_m^*: y = \overline{w}(x) \mod n \} \). The WLLN is equivalent to \( \text{Irrand}(x) = 1 \). Also let \( \gamma = 1/(q_1(q_2)) \).

Assume for simplicity that \( \mathbb{Z}_m^* \) is uniformly distributed. (Discussions made below can be immediately generalized to the case when \( \mathbb{Z}_m^* \) is arbitrarily distribut ed.)

Then for any \( w \in \mathcal{H}(G) \), and any randomly and uniformly selected \( x \in \mathbb{Z}_m^* \), we have \( \Pr(C(x, y, n) = \text{Irrand}(x)) > 1 - \varepsilon \).

Now for each \( (i, j) \in \mathbb{Z}_m^* \), let \( w_{ij} = \Pr(C(x, y, \gamma) = 1 \mod R) \).

We can now define the stochastic matrix:

\[
W = \begin{bmatrix}
\frac{w_{00}}{\frac{w_{00}}{2}}, & \frac{w_{01}}{\frac{w_{01}}{2}}, & \cdots, & \frac{w_{0n}}{\frac{w_{0n}}{2}} \\
\frac{w_{10}}{\frac{w_{10}}{2}}, & \frac{w_{11}}{\frac{w_{11}}{2}}, & \cdots, & \frac{w_{1n}}{\frac{w_{1n}}{2}} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{w_{n0}}{\frac{w_{n0}}{2}}, & \frac{w_{n1}}{\frac{w_{n1}}{2}}, & \cdots, & \frac{w_{nn}}{\frac{w_{nn}}{2}}
\end{bmatrix}
\]
Three obvious properties of the matrix are:

P1: For each $i \in Z$, $\sum_{j} a_{ij} = 1$. And hence, $\sum_{i, j} a_{ij} = 1$.

P2: $\sum_{i} a_{ij} > 1 \forall i \neq y$.

P3: For any $i \in Z$, there must exist at least one $j \in Z$, with $j 
eq i$ such that $|a_{ij} - a_{ji}| > \epsilon$ (where $\epsilon < 1$). This implies that for each row $i$, there is at least one row $j$ which is very different from the row $i$.

Suppose that the property is not true. Then for any $i \in Z$,

$$\sum_{j \neq i} a_{ij} = \sum_{j} a_{ij} - a_{ii} = \sum_{j \neq i} a_{ij} - \sum_{j \neq i} \sum_{j} a_{ij} = \sum_{j \neq i} a_{ij} - \sum_{j} a_{ij} = 0$$

$$\leq \gamma - 1$$

$$\leq (\gamma - 1) - \epsilon \gamma < 1$$.

On the other hand, from the properties P1 and P2, $\sum_{i} a_{ij} = 1,$ $\forall i \neq y$, and $i = 1,$ $2,$ $\ldots,$ $\gamma - 1.$ Increment $\text{Counter}_{ij}$ by 1 if $C_{ij}(x, y, \alpha) = i.$

2. For each $i \in Z$, let $\tilde{a}_{ii} = \text{Counter}_{ii}.$

Denote by $\tilde{W}$ the matrix $(\tilde{a}_{ij}, i \in Z, j \in Z).$ From the WLLN, we know that

$$\lim_{n \to \infty} \mathbb{E}[\tilde{a}_{ij} - a_{ij}] = 0$$

Consequently, $\tilde{a}_{ij}$, and hence $\tilde{W}$ are very favorable estimates of $a_{ij}$, and $W$, respectively.

Now suppose we are given an element $a \in Z$ whose class-index $L$ should be determined, where $a \in \mathbb{R}(C_{ij}).$

From this element $a$, we construct a matrix $V = (a_{ij}, i \in Z, j \in Z)$ as follows:

1. Replace $x_{i} = y_{j}$ $\mod n$ in the step 1 of ESTIMATING-1 with $x_{i} = y_{j}$ $\mod n$ and, $\tilde{a}_{ij}$ in the step 2 of ESTIMATING-1 with $a_{ij}$. Then do the newly designed Monte Carlo experiment.

Clearly, the class-index of $x_{i} = y_{j}$ $\mod n$ is $i + j$ mod $n$. For each $(i, j) \in Z, \tilde{a}_{ij}$ is a satisfac-

tory estimate of $a_{ij}(\tilde{a}_{ij})$. Since by the WLLN, we have

$$\mathbb{P} \left( |\tilde{a}_{ij} - a_{ij}(\tilde{a}_{ij})| < \epsilon \right) \to 1 - \epsilon$$

Denote by $V^{W}(\tilde{W}^{W})$, respectively the matrix obtained by shifting $W,W^{W}$, downward and cyclically, for $\epsilon$ times, and by $\tilde{a}_{ij}(\tilde{a}_{ij})$ respectively the element of $V^{W}(\tilde{W}^{W})$, respectively at the position $(i, j)$.

Now we know that both $V$ and $\tilde{W}$ are good estimates of $W^{*}$. So the two matrices $V$ and $\tilde{W}$ must be quite similar to each other. In fact, for each $(i, j) \in Z$, $\tilde{a}_{ij}$, $\tilde{a}_{ii}$, $\tilde{a}_{ji}$, and center $\tilde{a}_{ij}$. Then the distance between points $\tilde{a}_{ij}$ and $\tilde{a}_{ij}$ is less than $\epsilon^{2}$, if both of the two points are in the circle. Thus

$$\mathbb{P} \left( |\tilde{a}_{ij} - a_{ij}| < \epsilon \right) \to 1 - \epsilon$$

$$\mathbb{P} \left( |\tilde{a}_{ij} - a_{ij}| < \epsilon \right) \to 1 - \epsilon$$

$$\mathbb{P} \left( |\tilde{a}_{ij} - a_{ij}| < \epsilon \right) \to 1 - \epsilon$$

$$\mathbb{P} \left( |\tilde{a}_{ij} - a_{ij}| < \epsilon \right) \to 1 - \epsilon$$

$$\mathbb{P} \left( |\tilde{a}_{ij} - a_{ij}| < \epsilon \right) \to 1 - \epsilon$$

This suggests to us that we can decide $L$, by matching $V$, in turn, with $\tilde{W}$ for $s = \epsilon$, and examining whether or not the distance between $W^{W}$ and $\tilde{W}$, measured with a predetermined distance-measure $d$, is negligibly small. (Note: A distance-measure for a set $X$ is a feasible function $d : X \times X \to [0, +\infty)$ such that $d(x, y) = d(y, x)$ whenever $x = y$, $d(x, y)$ is called the distance between $x$ and $y$ measured by $d$.)

To estimate how correct the above matching procedure is, it is necessary that the distance-measure $d$ satisfies the following:

**CONDITION:** The distance between $W^{W}$ and $\tilde{W}$ measured by $d$ is smaller than some constant when $s = \epsilon$, and not smaller than the constant when $s > \epsilon$, both with probability greater than $1 - \epsilon$.

Notice that $\gamma = O(\delta)$. So if there exists actually such a distance-measure, it can be quickly certified. The following three lemmas assure us there exists definitely at least one distance-measure such that CONDITION is satisfied.

**Lemma 1:** There exists at least one distance-measure $\delta$ such that for some positive real number $\gamma > 0$, and for some $(i, k) \in Z$, $\tilde{a}_{ij}$, the distance between $W^{W}$ and $\tilde{W}$, measured by $d$, is denoted by $d((i, k))$ for convenience, is greater than $\gamma$.

**Proof:** Assume for contradiction that there is no distance-measure $\delta$ such that for any $(i, k) \in Z$, $\tilde{a}_{ij}$, for $\gamma > 0$, the distance $d((i, k))$ between $W^{W}$ and $\tilde{W}$ is greater than $\gamma$. 

Then every $W_s$ is identical to $W$. Hence by the property P2 we have
\[ \varepsilon_i \in \left[ \frac{w_i}{u_i} - 1 + \gamma, \frac{w_i}{u_i}\right] \text{ for every } s \in Z, \] and
\[ \forall i,j, \varepsilon_i, \varepsilon_j \in \left[ \frac{w_i}{u_i} - 1 + \gamma, \frac{w_i}{u_i}\right] \text{ implies } \varepsilon_i \leq \varepsilon_j \] \[ \implies \gamma \sum_{i} w_i u_i \gamma \leq \varepsilon_i \]
This contradicts the property P1.

[Lemma 2] There exists at least one distance-measure $e^\ast$ such that for some positive real number $\gamma_0 > 0$, and for any $(i, j) \in Z \times Z$, we have $e^\ast(s, n) \leq e^\ast(s, n_0)$.

(Proof) By Lemma 1, there exists a distance-measure $e^\ast$ such that $e^\ast(s, i) > x$ for some $(i, h) \in Z \times Z$, and for some positive real number $x$.

Assume without loss of generality that $e^\ast(i, j) \leq x$ for any $(i, j) \in Z \times Z$, with $(i, j) \neq (i, h)$. Let $g = x^\gamma > 1$ and call $g$ an amplification factor.

From the distance-measure $e^\ast$, we can obtain a new distance-measure $e^\ast$. With this new distance-measure, we measure the distance between two matrices $W_s$ and $W^\alpha$ (both $i$ and $j$ are not necessarily known) as follows:

We first measure the distance between $W_s$ and $W^\alpha$ with the distance-measure $e^\ast$. If $e^\ast(i, j) > x$, then we know that $(i, j) \neq (i, h)$, and let $e^\ast(i, j) = g - e^\ast(i, j)$. Otherwise, from $s = 0$ to $\gamma - 1$ and $t = 0$ to $\gamma - 1$, we shift, down and up, cyclically, the matrix $W_s$ for $s$ times, and the matrix $W^\alpha$ for $t$ times. Every time the matrices are shifted, we measure the distance between the two newly gotten matrices $W_{s+i}\oplus W_{t+j}$ and $W_{s+i}\oplus W_{t+j}$. There exists certainly a pair $(s, i) \in Z \times Z$ such that the distance between $W_{s+i}\oplus W_{t+j}$ and $W_{s+i}\oplus W_{t+j}$ is greater than $x$.

Now let $e^\ast(i, j) = |s - i| + |t - j|\gamma - x$.

From the foregoing description of measuring procedure with $e^\ast$, we know that $e^\ast(0, 0) = 0$ for all $(i, j) \in Z \times Z$, and $e^\ast(i, j) > x$ for all $(i, j) \in Z \times Z$, with $(i, j) = (i, h)$.

Let $e^\ast$ be the above constructed distance-measure $e^\ast$, which concludes the proof.

[Lemma 3] There exists at least one distance-measure $e^\ast$ such that for $x \geq 1 - 1/\theta(k)$, and for any $s \in Z$, we have $e^\ast(s, n) \geq x$. (Proof) From the property P3, we know that for at least one $(i, j) \in Z \times Z$, and for at least one position $(i, j) \in Z \times Z$, the $\varepsilon_i$ is less than or equal to $\varepsilon_j$. Thus by Lemma 1, we can find a distance-measure $e^\ast$ such that $e^\ast(s, 0) > e^\ast(s, 1)$. And by Lemma 1, we can furthermore construct a distance-measure $e^\ast$ such that $e^\ast(s, 0) > e^\ast(s, 1) > e^\ast(s, 1) > e^\ast(s, 1)$. By ($\ast$), we know that with probability greater than $1 - \delta$, $e^\ast(s, 0)$ is a satisfactory estimate of $e^\ast(s, 0)$ for any $s \in Z$, and any $(i, j) \in Z \times Z$. Also we know that $e^\ast$ is of polynomial size. So from the above Lemma 3, we can find in polynomial time a distance-measure for $\left(\sum_{i} e^\ast(s, n)\right)\forall s$ such that it both satisfies CONDITION and corresponds, with probability greater than $1 - \delta$, to one of the distance-measures $e^\ast$ for $\left(\sum_{i} e^\ast(s, n)\right)\forall s$ observed in the Lemma 3. We say that such a distance-measure for $\left(\sum_{i} e^\ast(s, n)\right)\forall s$ is truthfully with probability greater than $1 - \delta^\gamma$. Now we outline our algorithm $A_w$.

(THE OUTLINE OF THE ALGORITHM $A_w$) $A_w(s, n) = 1$:

1. Determine $\left(\sum_{i} e^\ast(s, n)\right)\forall s$ as follows:
   1.1. Query the circuit $C_s$ with random elements in $Z$ whose class-indices are known to us. Get an estimate $W$ for the stochastic matrix $W$ from the outputs of $C_s$.
   1.2. For each $s \in Z$, obtain $W^\alpha$ by shifting $W$ and query the circuit $C_s$ with these elements. Get a matrix $V$ from the outputs of $C_s$.
   3. Find some distance-measure $e^\ast$ for $\left(\sum_{i} e^\ast(s, n)\right)\forall s$ such that $e^\ast$ satisfies CONDITION.
   4. Match $V$ with $W^\alpha$ for $s = 0 \rightarrow s = \gamma - 1$. If the distance between $W^\alpha$ and $V$ measured by $e^\ast$ is less than some constant (say, $\delta^\gamma$, then judge that the class-index of $e^\ast$ is equal to $s$.

Obviously $A_w$ runs in probabilistic polynomial time. The probability with which $A_w$ outputs correctly the class-index $i$ of $x$ is:

$\Pr(A_w(0)) \geq \Pr(A_w(0))$ (true)

$\Pr(\text{true}) \geq \sum_{i} e^\ast(i) > x^\gamma - x^\gamma$. This completes the proof of Theorem 1.

(2) Under $\gamma$-Residuosity Assumption (Definition 3 in Sect. 3, is an unapproximable trapezoid function.)

(Proof) The trapfondness of $T$ discussed in Section 3. Now we prove that $I$ is unapproximable, by the use of Theorem 1. Assume there is an approximatation $A = (A_{s, n}^{(k)})$ such that for any polynomials $Q_n$ and $Q_{n_0}$, for infinitely many $k \in K$.

(3) Denote by $F^a$ the infinite set of above $k$'s, and by $S_{A_s, (Q_{n_0}^{(k)}))} = (Q_{n_0}^{(k)}))$ the set of $F_{k}^{(k)}$, for which $A_{s, n_0}^{(k)}$ can $F_{k}^{(k)}$-approximates the function $F_{s, n}^{(k)} : Z \times Z \rightarrow Z$.

For any $k \in F^a$ and any $Q_n$, for infinitely many $k \in F^a$, we can, by Theorem 1, construct a probabilistic polynomial time algorithm $A_k$ which finds the class-index of $x \in Z$ with probability greater than $1 - 1/\theta(k)$. From the algorithm $A_k$, we can get a circuit $C_g$ of polynomial size which for a function $F_{s, n}^{(k)}$ of integers $s \in Z$, solves $\gamma^\gamma$-RP with probability greater than $1 - 1/\theta(k)$. This contradicts $\gamma^\gamma$-Residuosity Assumption.
6. Polynomial Security of $C_{prw}$

In this section we prove that the cryptosystem $C_{prw}$ is polynomially secure when $\beta$ is of polynomial size.

(Thm 3) Let $Y = Y_1, Y_2$ be an unapproximable trapdoor function, where $Y_1 : \{0, 1\}^n \rightarrow \Sigma$, $Y_2 : \Sigma \rightarrow \{0, 1\}^k$ and $\beta = \beta(Y)$. The cryptosystem $C_{prw}$ constructed from $Y$ is polynomially secure.

(Proof) We first sketch the proof as follows: Suppose that some $F_{m}$ can find two messages $m_{1}, m_{2} \in M_{K}$ such that $T_{m}$ behaves quite differently about the two messages. From $m_{1}$ and $m_{2}$ we can find other two messages $m_{3} = b_{m_{1}} \cdot m_{1}$ and $m_{4} = b_{m_{2}} \cdot m_{2}$ such that $T_{m_{3}}$ behaves differently about the two messages $T_{m_{3}}$ and $T_{m_{4}}$. Then, given any element $e \in \mathbb{Q}_{\Sigma}$, we can judge which $\delta$ the element $x$ belongs to by the use of the records of the behaviors of $T_{m}$.

Let $Q_{1}$ and $Q_{2}$ be any two polynomials, and let $\epsilon = 1/\mu(\delta)$ and $\mu = 1/\mu(q(k))$. Suppose there is a message finder $F_{m}$ such that for infinitely many $\epsilon$, for any line $T_{m} \in \{1, \ldots, n\}$, for a fraction $\mu_{1}$ of $\delta_{e} \in \mathbb{Q}_{\delta}$, for some constant $\mu_{2}$, and for all $\epsilon$, there is a $\mu_{3}$ such that $\mu_{2} > \mu_{3} > \mu_{1}$. Denote $\delta$ by the set of the above infinitely many $\delta_{e}$, and let $S_{\mu}(F_{m}, 1)$ the set of elements $\delta_{e} \in \mathbb{Q}_{\delta}$ for which $\epsilon_{m}$ finds two messages $m_{1}, m_{2} \in M_{K}$ such that $\mu_{2} < \mu_{3} > \mu_{1}$.

We now introduce two other polynomials $Q_{1}$ and $Q_{2}$. It is assumed that $Q_{1}(k) = Q_{2}(k)$ and that for some constant $\mu_{2}$, and for all $\epsilon$, there is a $\mu_{3}$ such that $\mu_{2} > \mu_{3} > \mu_{1}$. From the discussion made in Sect. 3, we know that for all sufficiently large $\epsilon_{m} \in K$, for a fraction greater than $\mu_{2} - \mu_{3}$, and for all $\epsilon_{m} \in K$, there is a $\mu_{4}$ such that $\mu_{2} > \mu_{4} > \mu_{3}$.

Thus, for all sufficiently large $\epsilon_{m} \in K$, for some line lapper $T_{m}$, for a fraction greater than $\mu_{2} - \mu_{3}$, and for all $\epsilon_{m}$, we have the following two things:

(1) $1/\mu_{4}(k) < \epsilon_{m} < 1/\mu_{2}(k)$ for all $\in \Sigma$, and

(2) $F_{m}$ finds two messages $m_{1}, m_{2} \in M_{K}$ such that $\mu_{2} < \mu_{3} > \mu_{1}$, and it indicates the lower-bound on the fraction of $\delta_{e} \in \mathbb{Q}_{\delta}$, such that the two things hold. Denote by $\delta_{e}$ the set of the above infinitely many $\delta_{e}$, and let $S_{\mu}(F_{m}, 1)$ the set of elements $\delta_{e} \in \mathbb{Q}_{\delta}$ for which $\epsilon_{m}$ finds two messages $m_{1}, m_{2} \in M_{K}$ such that $\mu_{2} > \mu_{3} > \mu_{1}$.

Now we show that for any $\epsilon_{m} \in k$, a probabilistic polynomial time algorithm $A_{prw}$ can be constructed from $F_{m}$ and $T_{m}$ such that $A_{prw}$ can $1/2\beta$-approximate $Y_{2}$ for a fraction greater than $\theta_{\epsilon}$ of the of $e \in \Sigma$. Consider a $k \times k$ and an $e \in \mathbb{Q}_{\Sigma}$. Let $x = x_{\Sigma} - x_{\Sigma} - 1$ and $y = y_{\Sigma}$ be two sequences over $\Sigma = \{0, 1, \ldots, \beta - 1\}$. The (Hamming) distance between $x$ and $y$ is the number of positions where $x$ and $y$ are different. We say $x$ and $y$ are adjacent if the distance between $x$ and $y$ is 1.

Recall that $m_{1}, m_{2} \in M_{K}$ are two messages generated by $F_{m}$ such that for $T_{m}, \mu_{2} - \mu_{3} > \mu_{1}$, and $\mu_{2} > \mu_{3}$. Suppose the distance between them is $\mu_{2} - \mu_{3}$.

$\mu_{2} > \mu_{3}$. Suppose that $\delta_{e}$ is an $e \in \mu_{2}$-length sequence of length $\mu_{3}$, and $\mu_{2} = \mu_{3}$. Suppose $m_{3}$ is adjacent to $m_{2}$ for all $\mu_{2} < \mu_{3}$. Corresponding to these $\mu_{2}$ sequences, there are $\mu_{2} - \mu_{3}$, $\mu_{2} = \mu_{3}$, $\mu_{2} < \mu_{3}$.

There must exist at least one $\mu_{2} < \mu_{3} - 1$ such that $\mu_{2} \in \mu_{3}$, and such that an $e$ can be easily found. This can be explained by elementary mathematics. We know that

$\mu_{2} - \mu_{3} > \mu_{1}, e \in \mu_{2}$

$\mu_{2} = \mu_{3}, e \in \mu_{3}$

$\mu_{2} < \mu_{3}, e \in \mu_{3}$

Thus if there did not exist any $\mu_{2} < \mu_{3} - 1$ such that $\mu_{2} \in \mu_{3}$, we would have $\mu_{2} - \mu_{3} > \mu_{1}, e \in \mu_{2}$

$\mu_{2} = \mu_{3}, e \in \mu_{3}$

$\mu_{2} < \mu_{3}, e \in \mu_{3}$

This is not true. Suppose we have found such an $e$, and suppose $\mu_{2} = \mu_{3}, e \in \mu_{3}$, $\mu_{2} < \mu_{3}, e \in \mu_{3}$.

$\mu_{2} > \mu_{3}, e \in \mu_{3}$

where $\delta_{e}, \delta_{e} \in \Sigma$, and $\epsilon_{m} = \delta_{e}$. For notational simplicity, let $\Sigma = \delta_{e}, \delta_{e} \in \Sigma$, and let $\delta_{e}$ be the sequence obtained by replacing the letter $\delta_{e}$ in the sequence $\delta_{e}$ with the letter $\delta_{e}$. Also let $p_{e} = p_{e}(k))$, and assume without loss of generality that $p_{e} > p_{e}$.

$\mu_{3} - \mu_{2} > \mu_{2} - \mu_{3}$

$\mu_{2} - \mu_{3} > \mu_{2} - \mu_{3}$

$\mu_{2} - \mu_{3} > \mu_{2} - \mu_{3}$

$\mu_{2} - \mu_{3} > \mu_{2} - \mu_{3}$

$\mu_{2} - \mu_{3} > \mu_{2} - \mu_{3}$

The reason is as follows:

Suppose $\mu_{e} > \mu_{e}$, $\mu_{e} > \mu_{e}$, $\mu_{e} > \mu_{e}$, $\mu_{e} = \mu_{e}$, $\mu_{e} > \mu_{e}$, $\mu_{e} > \mu_{e}$.

Then we have $\mu_{e} > \mu_{e}$, $\mu_{e} > \mu_{e}$, $\mu_{e} > \mu_{e}$, $\mu_{e} > \mu_{e}$, $\mu_{e} > \mu_{e}$, $\mu_{e} > \mu_{e}$.

Assume, for simplicity once again, that $\Sigma$ and $\Sigma$ are uniformly distributed for all $\epsilon_{m} \in K$ and $\epsilon_{m} = \epsilon_{m}$. Let $\epsilon_{m} = \epsilon_{m} + \epsilon_{m} + \epsilon_{m} + \epsilon_{m} + \epsilon_{m} + \epsilon_{m}$. Now we estimate $\mu_{e}$ for all $\epsilon_{m} \in \Sigma$ by the following Monte Carlo experiment.
ENTIMATING 2: For any $r \in \mathbb{X}$, do the following three steps.
(0) Set $C_{r}= \emptyset$, $r=0$.

(1) Repeat for $t$ times: By means of $E_{r+1}$, form a random and uniform encryption of $E_{r+1}(H(k))$ of the sequence $H(k)$, and input the pair $(i, \text{code}(E_{r+1}(H(k))))$ to the circuit $T_r$. Increment $C_{r}$ by 1 iff the output of $T_r$ is 1.

(2) Let $p_{r}=|C_{r}|$ as an estimate of $p_r$. By the WLLN, we have
\[ P_r\left|p_{r} \geq \frac{1}{\sqrt{n}}\right| \geq 1 - \frac{1}{4} \left(\frac{1}{\sqrt{2n}}\right)^2 \geq 1 - \frac{1}{4} \frac{1}{n}. \]

Next we show that $p_r \geq \epsilon/4 + \epsilon_0/\epsilon' \beta^H$ with high probability. Let $c_r$ and $c_i$ be two circles with radii $\epsilon/4 + \epsilon_0/\epsilon' \beta^H$ and centers $p_r$ and $p_i$, respectively. Recall that the distance between $p_r$ and $p_i$ is greater than $\epsilon_0/\epsilon'$. So the distance between $p_r$ and $p_i$ is greater than $\epsilon_0/\epsilon$ if $p_r$ is in the circle $c_i$ and $p_r$ is in the circle $c_r$. Consequently,
\[ P_r\{p_r \geq \frac{\epsilon_0}{\epsilon'} + \frac{\epsilon_0}{\epsilon' \beta^H}\} \geq P_r\{p_r \geq \frac{\epsilon_0}{\epsilon'} \}
\geq 1 - \frac{\epsilon_0}{\epsilon'^2}. \]

Let $P_r^*=\{0, p_1, \ldots, p_r\}$. Notice that neither the summation of $p_0, p_1, \ldots, p_{r-1}$ nor that of $p_0, p_r, \ldots, p_{r-1}$ is necessarily equal to 1. Since $p_r-p_o = \epsilon/4 + \epsilon_0/\epsilon' \beta^H$ with probability $1 - \epsilon_0/\epsilon'$, and $P_r^*$ is finite ($\beta$), we can find, with the same probability $1 - \epsilon_0/\epsilon'$, a threshold $r'$ with $p_r = p_{r'} < r' < \frac{\epsilon_0}{\epsilon'} + \frac{\epsilon_0}{\epsilon' \beta^H}$ such that the set $\Sigma$ can be divided into two non-empty sets $\Sigma' = \{0, p_1, \ldots, p_{r'}\}$ and $\Sigma'' = \{p_{r'+1}, \ldots, p_r\}$.

Let's estimate the probability with which the pair $(\Sigma', \Sigma'')$ is equal to one of the above-mentioned pairs $(\Sigma_1, \Sigma_2)$. First, we notice that if $(\Sigma', \Sigma'')$ does not coincide with any of $(\Sigma_1, \Sigma_2)$, then $|p_r - p_0| > \epsilon_0/\epsilon' \beta^H$ for at least one $i \in \Sigma'$. Therefore,
\[ P_r(|p_r - p_0| > \frac{\epsilon_0}{\epsilon'} \beta^H) \geq \frac{\epsilon_0}{\epsilon'} \beta^H \geq \frac{\epsilon_0}{\beta^H}, \]
and hence
\[ P_r(\Sigma', \Sigma'' \text{any of } (\Sigma_1, \Sigma_2)) = \frac{1}{2} P_r(\Sigma', \Sigma'') + \frac{1}{2} P_r(|p_r - p_0| > \frac{\epsilon_0}{\beta^H}) \geq 1 - \frac{\epsilon_0}{\beta^H}. \]

Now we approximate $Y_d(x)$ for any $x \in \Sigma_1$, where $n \in \Sigma_1 \cup \Sigma_2$ using the following algorithm APPRX:

ALGORITHM APPRX $(n, z)$

0. Let $C_{r}= \emptyset$, $r=0$.

1. Repeat for $t$ times: For every $i \in \{1, 2, \ldots, n\}$, set randomly and uniformly an $x_i \in \Sigma_1$ as an encryption of $b_i$. Then input the pair $(i, \text{code}(E_{i}(x_i)))$ to the circuit $T_i$, where $x_i = a_{i-1} b_{i-1} \cdots a_0 b_0$, $i \in \Sigma_1$. Increment $C_{r}$ by 1 iff the output of $T_r$ is 1.

2. Let $y = \text{Count}(\Sigma')$.

3. Select, randomly and uniformly, an $i \in \Sigma_1$ and a $j \in \Sigma''$; then approximate $Y_d(x)$ as follows:
\[ Y_d(x) = \begin{cases} i, & \text{if } y > r' + \frac{\epsilon_0}{\beta^H}; \\ j, & \text{otherwise}. \end{cases} \]

We have completed the description of the algorithm $A_{TR}$. Finally, we estimate the probability with which $A_{TR}$ outputs $Y_d(x)$ correctly.

Notice that
\[ P_r(\text{APPRX}(n, z) = Y_d(x) | Y_d(x) \in \Sigma_1) = \frac{1}{\sqrt{p_r}}, \]
and
\[ P_r(\text{APPRX}(n, z) = Y_d(x) | Y_d(x) \in \Sigma_2) = \frac{1}{\sqrt{p_r}}, \]
respectively. Thus we get
\[ P_r(\text{APPRX}(n, z) = Y_d(x)) = P_r(\text{APPRX}(n, z) = Y_d(x) | Y_d(x) \in \Sigma_1) \cdot P_r(Y_d(x) \in \Sigma_1) + P_r(\text{APPRX}(n, z) = Y_d(x) | Y_d(x) \in \Sigma_2) \cdot P_r(Y_d(x) \in \Sigma_2). \]

Let's estimate the probability with which the pair $(\Sigma', \Sigma'')$ is equal to one of the above-mentioned pairs $(\Sigma_1, \Sigma_2)$. First, we notice that if $(\Sigma', \Sigma'')$ does not coincide with any of $(\Sigma_1, \Sigma_2)$, then $|p_r - p_0| > \epsilon_0/\epsilon' \beta^H$ for at least one $i \in \Sigma'$.

Therefore,
\[ P_r(\Sigma', \Sigma'' \text{any of } (\Sigma_1, \Sigma_2)) \leq \frac{\epsilon_0}{\epsilon'} \beta^H \cdot P_r(|p_r - p_0| > \frac{\epsilon_0}{\beta^H}) \leq \frac{\epsilon_0}{\beta^H}, \]
and hence
\[ P_r(\Sigma', \Sigma'' \text{any of } (\Sigma_1, \Sigma_2)) \geq 1 - \frac{\epsilon_0}{\beta^H}. \]
For all \( k \in \mathbb{K} \), we can construct from \( A_{\mathcal{T}} \) a polynomial size circuit \( C_{\mathcal{T}} \) (see for example Ref. (6)) such that this circuit can \( 1/5\)-approximates \( Y_k \) for all \( x \in \mathcal{S}_k \), i.e., for a fraction greater than \( \theta - \gamma_k \) of \( x \) in \( S_n \), where \( \theta \) is an arbitrary but fixed real number within the range (0, 1). This contradicts the unapproximability of \( Y \) and the proof for Theorem 3 is completed.

[Theorem 4] (Under \( \gamma^n \)-Residuosity Assumption) The probabilistic cryptosystem based on \( \gamma^n \)-RP is polynomially secure.

(Proof) It follows from Theorems 2 and 3.

7. Concluding Remarks

In proving Theorem 1, we benefited a lot from fully-developed pattern matching techniques. Partitioning \( \Sigma \) into two non-empty sets \( \Sigma' \) and \( \Sigma'' \) is the key point of the proof for Theorem 3. This proof technique, however, seems not directly generalizable to the case when \( \beta \) is not of polynomial size. It would be nice to show that the cryptosystem \( C_{\mathcal{T}} \) is also polynomially secure even when \( \beta \) is exponentially large.

References