CCA-Secure Cryptosystem from Lattice

Chen Huiyan[1,2]

[1] Beijing Electronic Science and Technology Institute, BEIJING 100070
[2] E-mail: chenhy2003@gmail.com

Abstract. We propose a simple construction of CCA- secure public-key encryption scheme based on lattice in the standard model. Our construction regards lattice-based cryptosystem mR05 of [21], which is the multi-bit version of single-bit cryptosystems R05 [20], as building block and makes use of its indistinguishable pseudohomomorphism property which is known to be achievable without random oracles and which is the crux that we can construct a public key encryption scheme which is CCA-secure in standard model. This makes our construction approach quite different from existing ones. So far as we know, our construction is the first CCA-secure cryptosystem which is directly constructed from lattice and whose security is directly based on the standard lattice problem which is hard in the worst case for quantum algorithms.

Keywords. Lattice, CCA-security, Pseudohomomorphism

1 Introduction

The design of a secure encryption scheme is central to any system that strives to provide secure communication using an untrusted network. Following the seminal work of Goldwasser and Micali [1], increasingly strong security definitions have been formulated. The strongest notion to date is that of security against adaptive chosen-ciphertext attack (CCA-security) [2], which protects against an adversary that is given access to decryptions of ciphertexts of her choice and which has become the de facto level of security for public-key encryption schemes.

Constructions of public-key encryption schemes, which are secure against adaptive chosen ciphertext without resorting to heuristics such as the random oracle methodology, have followed several structural approaches. The first approach follows the paradigm introduced by Naor and Yung [3] to achieve non-adaptive chosen-ciphertext security, later extended to the case of adaptive chosen-ciphertext security by [4–6]. However, this approach relies on generic non-interactive zero-knowledge proofs [7, 8], and encryption schemes resulting from this approach are somewhat complicated and impractical due to the use of generic NIZK proofs. The second approach is based on the "smooth hash proof systems"of Cramer and Shoup [9], and has led to a number of practical schemes [9–12]. The third approach was suggested by Canetti, Halevi and Katz [13] (followed by [15, 16]) who constructed a CCA-secure public-key encryption scheme based on any identity-based encryption (IBE) scheme in selective-ID model [14]

with a one-time signature. Their construction is elegant, black-box, and essentially preserves the efficiency of the underlying IBE scheme. However, IBE is a rather strong cryptographic primitive, which is currently realized only based on a small number of specific number-theoretic assumptions. Recently, Peikert and Waters [22] introduced the intriguing notion of lossy trapdoor functions, and demonstrated that such functions can be used to construct a CCA-secure public-key encryption scheme in a black-box manner. In addition, Chris Peikert [22] also presented the concrete realization of lossy trapdoor functions.

In 1996, Ajtai [18] established a remarkable connection between the worst-case and average-case complexity of certain computational problems on lattices. This result opened the door to basing cryptography on a worst-case assumption. Ajtai and Dwork [24] constructed the first public-key cryptosystem whose security is based on the worst-case hardness of a lattice problem. Several cryptosystems were given in subsequent works, e.g, R04 [19], R05 [20], A05 [23], and $\mathrm{AD}_{\mathtt{GGH}}$ [25]. Compared with other lattice-based cryptosystems [27, 28] and their improvements [31, 29, 30], which have not security proofs, although the aforementioned lattice-based cryptosystems are provable security, they are unfortunately quite inefficient and are signle-bit cryptosystrems. Akinori Kawachi *et al.* [21] have tried to remedy this and extended single-bit cryptosystems R04, R05, A05, and $\mathrm{AD}_{\mathtt{GGH}}$ to their multi-bit versions mR04, mR05, mA05, $\mathrm{mAD}_{\mathtt{GGH}}$ with security proofs and without increase in the size of ciphertexts, respectively.

The Ajtai-Dwork cryptosystem [18], as well as subsequent works [25, 19, 23, 20, 21], are not secure against chosen ciphertext attacks. Indeed, it is not too difficult to see that one can extract the private key given access to the decryption oracle. In practice, there are known methods to deal with this issue. It would be interesting to find an (efficient) solution with a rigorous proof of security in the standard model. It wasn't until fairly recently that Chris Peikert *et al.* [22] designed an encryption scheme that was both relative to lattice and provably secure against chosen ciphertext attacks without the random oracle model. In Chris Peikert *et al.*'s construction of CCA-secure cryptosystem, they made use of lossy trapdoor functions, TDFs. In order to implement their construction, Chris Peikert *et al.* also presented the concrete realization of lossy TDFs based on on the "learning with errors"(LWE) problem. The LWE problem can be seen as an average-case "unique decoding"problem on a certain family of random lattices, and is believed to be hard. Moreover, Regev [20] gave a reduction showing that LWE is hard on the average if standard lattice problems are hard in the worst case for quantum algorithms.

In this work, our goal is to construct a simple CCA-secure public-key encryption scheme based on lattice in the standard model.

1.1 Our Contribution

In this work, we propose a construction of CCA-secure cryptosystem which is based on mR05. Before sketching our construction, we first recall the notion of *pseudohomomorphism* which was introduced by Akinori Kawachi *et al.* [21].

We know that the homomorphism of ciphertexts is quite useful for many cryptographic applications [33]. Lattice-based Cryptosystems mR04, mR05, mA05, $\text{mAD}_{\texttt{GGH}}$ implicitly have a similar property to the homomorphism, which is called *pseudohomomorphism*, i.e, given plaintexts m_1, $m_2 \in \{0, 1, \ldots, p-1\}$, where p is a small integer, and let $\mathcal{E}(m_1)$ and $\mathcal{E}(m_2)$ be ciphertexts of m_1, m_2, respectively. Then, we can decrypt $\mathcal{E}(m_1) + \mathcal{E}(m_2)$ to $m_1 + m_2$ by the original private key of the original cryptosystem with a small decryption error.

In our construction, the *pseudohomomorphism* property of mR05 plays an important role, we make use of it to finish the encryption of matrix $\mathbf{X} \in \mathbb{Z}_2^{h \times w}$ which is regarded as an encryption witness, this idea stemms from Chris Peikert *et al.*'s construction of CCA-secure encryption [22]. Our construction also uses a one-time signature scheme (`Gen`, `Sign`, `Ver`). We require that this scheme be secure in the sense of strong unforgeability (i.e., an adversary is unable to forge even a new signature on a previously-signed message). The use of one-time signature for CCA-security inherits from the work of D. Dolev, C. Dwork, and M. Naor [4] and is similar to the methods of [13, 22] constructing CCA-secure cryptosystems. Briefly and somewhat informally, this new encryption scheme proceeds as follows: To encrypt a message, the sender first generates a key-pair (vk, sk_σ) for a one-time strong signature scheme, then, chooses a matrix $\mathbf{X} \in \mathbb{Z}_2^{h \times w}$, encrypts it with mR05 and its *pseudohomomorphism* and gets $\mathbf{c}$, and next, encrypts the message in the secrete key which is generated with the matrix $\mathbf{X}$ and generates c_0, finally, The resulting ciphertext is $(vk, \mathbf{c}, c_0, \sigma)$, where $\sigma = \texttt{Sign}_{sk_\sigma}(\mathbf{c}, c_0, \mathbf{X})$. To decrypt a ciphertext $(vk, \mathbf{c}, c_0, \sigma)$, the receiver first gets $\mathbf{X}$ with vk and $\mathbf{c}$, and then verifies whether $Ver(vk, \mathbf{c}, c_0, \mathbf{X}, \sigma) = 1$, outputs $\perp$ if the verification fails. Otherwise, the receiver decrypts c_0.

Security of the new scheme against adaptive chosen-ciphertext attacks can be informally understood as follows. Consider a challenge ciphertext $c^* = (vk^*, \mathbf{c}^*, c_0^*, \sigma^*)$ given to the adversary. Any ciphertext $c = (vk, \mathbf{c}, c_0, \sigma)$ submitted by the adversary to a decryption oracle (implying $c \neq c^*$), must have $vk^* \neq vk$ by the (strong) security of the one-time signature scheme. The crux of the security proof then involves showing that the indistinguishable pseudohomomorphism property of mR05 implies that decrypting c does not give the adversary any further advantage in decrypting the challenge ciphertext. So far as we know, this new scheme is the first CCA-secure cryptosystem based on lattice and whose security is directly based on the standard lattice problem which is hard in the worst case for quantum algorithms.

1.2 Organization

The rest of this paper is organized as follows. We describe basic notions and notations in Section 2. In Section 3, we review lattice-based encryption scheme and its pseudohomomorphism property. In Section 4, we present a CCA-security cryptosystem from mR05, analysize its security and reduce its security to the LWE problem. Section 5 concludes this paper.

2 Preliminary

2.1 Notation

We denote set of real numbers by by $\mathbb{R}$, positive real numbers by $\mathbb{R}^+$, the integers by $\mathbb{Z}$, and positive integers by $\mathbb{Z}^+$. For a positive integer n, $[n]$ denotes $\{1, 2, \ldots, n\}$. For any x, $y \in \mathbb{R}$ with $y > 0$ we define x mod y to be $x - \lfloor x \rfloor y$. For $x \in \mathbb{R}$, $\lfloor x \rceil = \lfloor x + 1/2 \rfloor$ denotes the nearest integer to x (with ties broken upward). We define $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, i.e., the group of reals $[0, 1)$ with modulo 1 addition.

The n-dimensional space is denoted $\mathbb{R}^n$. We use bold lower-case letters (e.g., $\mathbf{x}$) to denote vectors in column form and bold capital letters (e.g., $\mathbf{X}$) to denote matrices. The ith component of $\mathbf{x}$ will be denoted by x_i. The norm of a vector $x \in \mathbb{R}^n$ is denoted as $\|\mathbf{x}\|$. We also use matrix notation to denote sets of vectors. For example, matrix $\mathbf{B} \in \mathbb{R}^{n \times m}$ represents the set of n-dimensional vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$, where $\mathbf{b}_1, \ldots, \mathbf{b}_m$ are the columns of $\mathbf{B}$. We denote by $\|\mathbf{B}\|$ the norm of longest vector in $\mathbf{B}$. The linear space spanned by a set of m vectors $\mathbf{B}$ is denoted span($\mathbf{B}$)=$\{\sum_i x_i \mathbf{b}_i : x_i \in \mathbb{R}, i \in [m]\}$.

The natural security parameter throughout the paper is n, and all other quantities are implicitly functions of n. We use standard O, Ω, o, and w notation to classify the growth of functions, and say that $f(n) = \widetilde{O}(g(n))$ if $f(n) = O(g(n) \cdot log^c n)$ for some fixed constant c. We let poly(n) denote an unspecified function $f(n) = O(n^c)$ for some constant c. A negligible function, denoted generically by $negl(n)$, is an $f(n)$ such that $f(n) = o(n^{-c})$ for every fixed constant c. We say that a probability (or fraction) is overwhelming if it is $1 - negl(n)$.

The statistical distance between two distributions X and Y over a countable domain D is defined to be $\Delta(X, Y) = \frac{1}{2} \sum_{v \in D} |X(v) - Y(v)|$. We say that two distributions (formally, two ensembles of distributions indexed by n) are statistically close if their statistical distance is negligible in n. Two ensembles of distributions $\{X_n\}$ and $\{Y_n\}$ are computationally indistinguishable if for every probabilistic poly-time machine $\mathcal{A}$, $|\mathtt{Pr}[\mathcal{A}(1^n, X_n) = 1] - \mathtt{Pr}[\mathcal{A}(1^n, Y_n) = 1]|$ is negligible (in n). The definition is extended to non-uniform families of poly-sized circuits in the standard way.

2.2 Cryptosystems and Security Notion

We review the definitions of public-key encryption schemes and their security against adaptive chosen-ciphertext attacks.

Definition 1. (**Public-key encryption**) *A public-key encryption scheme PKE is a triple of* PPT *algorithms* ($\mathcal{G}$, $\mathcal{E}$, $\mathcal{D}$) *such that:*

1. *The randomized key generation algorithm $\mathcal{G}$ takes as input a security parameter 1^n and outputs a public key pk and a secret key sk. We write (pk, sk)$\leftarrow \mathcal{G}(1^n)$.*

2. *The randomized encryption algorithm $\mathcal{E}$ takes as input a public key pk and a message $m \in \{0,1\}^*$, and outputs a ciphertext C. We write $C = \mathcal{E}_{pk}(m)$.*
3. *The decryption algorithm $\mathcal{D}$ takes as input a ciphertext C and a secret key sk. It returns a message $m \in \{0,1\}^*$, or the distinguished symbol $\perp$. We write $m = \mathcal{D}_{sk}(C)$.*

The standard completeness requirement is that, for all (pk, sk) output by $\mathcal{G}$, all $m \in \{0,1\}^*$, and all C output by $\mathcal{E}_{pk}(m)$, we have $\mathcal{D}_{sk}(C) = m$. We relax this notion to require that decryption is correct with overwhelming probability over all the randomness of the algorithms.

Definition 2. (**CCA Security**). *A public-key encryption scheme PKE is secure against adaptive chosen-ciphertext attacks (i.e., is "CCA-secure") if the advantage of any PPT adversary $\mathcal{A}$ in the following game is negligible in the security parameter n:*

1. *$\mathcal{G}(1^n)$ outputs (pk, sk). Adversary $\mathcal{A}$ is given 1^n and pk.*
2. *The adversary may make polynomially-many queries to a decryption oracle $\mathcal{D}_{sk}(\cdot)$.*
3. *At some point, $\mathcal{A}$ outputs two messages m_0, m_1 with $|m_0| = |m_1|$. A bit $b \in \{0,1\}$ is randomly chosen and the adversary is given a challenge ciphertext $C^* \leftarrow \mathcal{E}_{pk}(m_b)$.*
4. *$\mathcal{A}$ may continue to query its decryption oracle $\mathcal{D}_{sk}(\cdot)$ except that it may not request the decryption of C^*.*
5. *Finally, $\mathcal{A}$ outputs a guess b'.*

We say that $\mathcal{A}$ succeeds if $b' = b$, and denote the probability of this event by $\mathtt{Pr}_{\mathcal{A},PKE}[\mathtt{Succ}]$. The adversary's advantage is defined as $|\mathtt{Pr}_{\mathcal{A},PKE}[\mathtt{Succ}] - 1/2|$.

2.3 Strongly Unforgeable One-Time Signatures

We review the standard definition for signature schemes, followed by a definition of strong one-time security appropriate for it.

Definition 3. *A signature scheme consists of three PPT algorithms **Gen**, **Sign**, and **Ver** such that:*

1. ***Gen** takes as input the security parameter 1^n and outputs a verification key vk and a signing key sk_σ. We assume for simplicity that the length of vk is fixed for any given value of n.*
2. ***Sign** takes as input a signing key sk_σ and a message M (in some implicit message space), and outputs a signature σ.*
3. ***Ver** takes as input a verification key vk, a message M, and a signature σ, and outputs a bit $b \in \{0,1\}$ (where $b = 1$ signifies acceptance and $b = 0$ signifies rejection). We write this as $b := \mathtt{Ver}(vk, M, \sigma)$.*

Here, we give a definition of security tailored to the requirements of our construction, i.e., we require only "one-time" security for our message signature.

Definition 4. *A signature scheme* $\mathtt{Sig}$ *is a strong one-time signature scheme if the success probability of any* $\mathtt{ppt}$ *adversary* $\mathcal{A}$ *in the following game is negligible in the security parameter* n*:*

1. $\mathtt{Gen}(1^n)$ *outputs* (vk, sk_σ) *and the adversary is given* 1^n *and* vk
2. $\mathcal{A}$ *may do one of the following:*
   (a) $\mathcal{A}$ *may output a pair* (M^*, σ^*) *and halt. In this case* (M, σ) *are undefined.*
   (b) $\mathcal{A}$ *may output a message* M*, and is then given in return* $\sigma \leftarrow \mathtt{Sign}_{sk_\sigma}(M)$*. Following this,* $\mathcal{A}$ *outputs* (M^*, σ^*)*.*

We say the adversary succeeds if $\mathtt{Ver}(vk, M^*, \sigma^*) = 1$ *but* $(M^*, \sigma^*) \neq (M, \sigma)$*.*

Strongly unforgeable one-time signatures can be constructed from any one-way function [34] and and from collision-resistant hash functions [35].

2.4 Universal One-way Hash Function

The notion of universal one-way hash function UOWHF was introduced by Naor and Yung [37] and is defined as follow.

Definition 5. *A family of* UOWHF*s is a collection of keyed hash functions* $\{H_k\}_{k\in K}$ *with the following property: if an adversary chooses a message* x*, and then a key* k *is chosen at random and given to the adversary, it is hard for he adversary to find a different message* $y \neq x$ *such that* $H_k(x) = H_k(y)$*.*

As a cryptographic primitive, a UOWHF is an attractive alternative to the more traditional notion of a collision-resistant hash function (CRHF) (which is characterized by the following property: given a random key k, it is hard to find two different messages x and y such that $H_k(x) = H_k(y)$.) because (1) in the complexity theoretic view, Simon [36] that shows that there exists an oracle relative to which UOWHFs exist but CRHFs do not, i.e, CRHFs cannot be constructed based on an arbitrary one-way permutation, whereas Naor and Yung [37] show that a UOWHF can be so constructed, and (2) in many applications, most importantly for building digital signature schemes, a UOWHF is sufficient.

2.5 Lattice

Let $\mathbf{B}=\{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$ consist of n linearly independent vectors. The n-dimensional lattice Λ generated by the basis $\mathbf{B}$ is

$$\Lambda = \mathcal{L}(\mathbf{B}) = \{\mathbf{Bz} : \mathbf{z} \in \mathbb{Z}^n\}$$

A lattice is a discrete additive subgroup of $\mathbb{R}^n$. The minimum distance $\lambda_1(\Lambda)$ of a lattice Λ is the length of its shortest nonzero vector: $\lambda_1(\Lambda)=\mathtt{min}_{0\neq\mathbf{x}\in\Lambda} \|\mathbf{x}\|$. More generally, the i-th successive minimum $\lambda_i(\Lambda)$ is the smallest radius r such that Λ contains i linearly independent vectors of norm at most r.

We recall two standard worst-case approximation problems on lattices, i.e., the shortest vector problem (SVP_γ), whose decision version (GapSVP_γ) is common to be considered, and the shortest independent vectors problem which is given in its search version, where $\gamma = \gamma(n)$ is the approximation factor as a function of the dimension n.

Definition 6. (**GapSVP**$_\gamma$). *An input to* GapSVP$_\gamma$ *is a pair* $(\mathbf{B}, d)$ *where* $\mathbf{B}$ *is a basis for a full-rank* n*-dimensional lattice and* $d \in \mathbb{R}$*. It is a YES instance if* $\lambda_1(\mathcal{L}(\mathbf{B})) \leq d$*, and is a NO instance if* $\lambda_1(\mathcal{L}(\mathbf{B})) > \gamma(n)d$

Definition 7. (**SIVP**$_\gamma$). *An input to* SIVP$_\gamma$ *is a full-rank basis* $\mathbf{B}$ *of an* n*-dimensional lattice. The goal is to output a set of* n *linearly independent lattice vectors* $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ *such that* $\|\mathbf{S}\| \leq \gamma(n)\lambda_n(\mathcal{L}(\mathbf{B}))$*.*

Probability distributions The normal (Gaussian) distribution with mean 0 and variance σ^2 (or standard deviation σ) is the distribution on $\mathbb{R}$ having density function $\frac{1}{\sigma\sqrt{2\pi}} \exp(-x^2/2\sigma^2)$. The sum of two independent normal variables with mean 0 and variances σ_1^2 and σ_2^2 (respectively) is a normal variable with mean 0 and variance $\sigma_1^2 + \sigma_2^2$. We will also need a standard tail inequality: a normal variable with variance σ^2 is within distance $t\sigma$ (i.e., t standard deviations) of its mean, except with probability at most $\frac{1}{t} \exp(-t^2/2)$.

For $\alpha \in \mathbb{R}^+$, Ψ_α is defined to be the distribution on $\mathbb{T}$ of a normal variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$, reduced modulo 1. For any probability distribution ϕ over $\mathbb{T}$ and an integer $q \in \mathbb{Z}^+$ (often implicit) its discretization $\overline{\phi}$ is the discrete distribution over $\mathbb{Z}_q$ of the random variable qX_ϕ mod q, where X_ϕ has distribution ϕ.

For an integer $q \geq 2$ and some probability distribution χ over $\mathbb{Z}_q$, an integer dimension $n \in \mathbb{Z}^+$ and a vector $\mathbf{s} \in \mathbb{Z}_q^n$, define $A_{s,\chi}$ as the distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ of the variable $(\mathbf{a}, \mathbf{a}^T\mathbf{s} + x)$ where $a \in \mathbb{Z}_q^n$ is uniform and $x \leftarrow \chi$ are independent, and all operations are performed in $\mathbb{Z}_q$.

Learning with errors (LWE) . For an integer $q = q(n)$ and a distribution χ on $\mathbb{Z}_q$, the goal of the (average-case) learning with errors problem LWE$_{q,\chi}$ is to distinguish (with non-negligible probability) between the distribution $A_{s,\chi}$ for some uniform (secret) $\mathbf{s} \leftarrow \mathbb{Z}_n^q$ and the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ (via oracle access to the given distribution). In other words, if LWE is hard, then the collection of distributions $A_{s,\chi}$ is pseudorandom.

Regev demonstrated that for certain moduli q and Gaussian error distributions χ, LWE$_{q,\chi}$ is as hard as solving several standard worst-case lattice problems using a quantum algorithm.

Proposition 1. ([20]). *Let* $\alpha = \alpha(n) \in (0, 1)$ *and let* $q = q(n)$ *be a prime such that* $\alpha q > 2\sqrt{n}$*. If there exists an efficient (possibly quantum) algorithm that solves* LWE$_{q,\overline{\Psi}_\alpha}$*, then there exists an efficient quantum algorithm for approximating* SIVP *and* GapSVP *in the* ℓ_2 *norm, in the worst case, to within* $\widetilde{O}(n/\alpha)$ *factors.*

This result was subsequently extended to hold for SIVP and GapSVP in any ℓ_p norm, $2 \leq p \leq \infty$, for essentially the sames $\widetilde{O}(n/\alpha)$ approximation factors [32].

3 mR05 and its pseudohomomorphism

In this section, we review the mR05 and its pseudohomomorphism, which are used in our construction.

The cryptosystem mR05 proposed in [21] can be parameterized by three integers m, q, p , a probability distribution χ on $\mathbb{Z}_q$, and a real $r \in (0, 1)$ which controls the trade-off between the size of plaintext space and the hardness of underlying lattice problems. A setting of these parameters that guarantees both security and correctness is the following. Choose q to be some prime number between n^2 and $2n^2$, let $m = 5(n + 1)(2 \log n + 1)$. Let also p be an integer such that $p \leq n^r = o(n)$, which is the size of the plaintext space in mR05. The probability distribution χ is taken to be $\overline{\Psi}_\beta$ where the parameter $\beta = \beta(n) = \alpha/n^r = o(1/(n^{0.5+r} \log n))$ is used to control the distribution instead of α in R05 [20] and satisfies $\beta(n)q(n) > 2\sqrt{n}$. mR05 proceeds as follows.

- **Common Parameter**: Given security parameter n, parameters m, q, p, r, β are taken according the above description.
- **Key Generation**: The private key $\mathbf{s}$ is chosen uniformly at random from $\mathbb{Z}_q^n$. m vectors $\mathbf{a}_1, \ldots, \mathbf{a}_m$ chosen from $\mathbb{Z}_q^n$ uniformly at random and e_i $(i \in [m])$is also chosen according to the distribution $\overline{\Psi}_\beta$. Let $b_i =< \mathbf{a}_i, \mathbf{s} > +e_i$. The public key is $\{\mathbf{a}_i, b_i\}_{i=1}^m$.
- **Encryption**: Choose a uniformly random subset S of $\{1, \ldots, m\}$. For a plaintext $m \in \{0, 1, \ldots, p-1\}$ the ciphertext is $(\sum_{i \in S} \mathbf{a}_i,\ q\frac{m}{p} + \sum_{i \in S} b_i\ )$.
- **Decryption**: Decrypt a received ciphertext $(\mathbf{a}, b)$ to $\lfloor (b - < \mathbf{a}, \mathbf{s} >)p/q \rceil) \mathrm{mod} p$.

Here, we only introduce the results about the pseudohomomorphism of mR05.

Theorem 1. (**Pseudohomomorphism**) *Let β=$\beta(n)$=α/n^r=$o(1/(n^{0.5+r} \log n))$. Also let $p(n)$ be an integer and κ be an integer such that $\kappa p \leq n^r$ for any constant $0 < r < 1$. For any κ plaintexts σ_1, . . . ,σ_κ $(0 \leq \sigma_i \leq p-1)$, we can decrypt the sum of κ ciphertexts $\sum_{i=1}^{\kappa} \mathcal{E}^{mR05}(\sigma_i)$ into $\sum_{i=1}^{\kappa}(\sigma_i) mod\ p$ with decryption error probability at most $2^{-\Omega(1/m\beta^2(n)n^{2r})}$, where the addition is defined over $\mathbb{Z}_q^n \times \mathbb{Z}_q$.*

Theorem 2. (**Indistinguishable Pseudohomomorphism**) *If there exist two sequences of plaintext σ_1, . . . ,σ_κ and σ'_1, . . . ,σ'_κ $(0 \leq \sigma_i, \sigma'_i \leq p-1)$ and a polynomial time algorithm $\mathcal{D}_1$ that distinguishes between $(\sum_{i=1}^{\kappa} \mathcal{E}^{mR05}(\sigma_i), pk)$ and $(\sum_{i=1}^{\kappa} \mathcal{E}^{mR05}(\sigma'_i), pk)$, then there exists a polynomial-time quantum algorithm for the worst case of $\mathrm{SVP}_{\widetilde{O}(n/\beta(n))}$ and $\mathrm{SIVP}_{\widetilde{O}(n/\beta(n))}$ in the case of mR05.*

4 CCA-security Cryptosystem

In this section, we presents a CCA-secure encryption scheme based on mR05.

4.1 Our Construction

Before giving our construction, we introduce a operator which will be needed. Given two matrices $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_w) \in \mathbb{Z}_p^{h \times w}$, $\mathbf{X} = (\mathbf{x}_1, \ldots, \mathbf{x}_w) \in \mathbb{Z}_2^{h \times w}$, we define:

$$\mathbf{B} * \mathbf{X} := (< \mathbf{x}_1, \mathbf{b}_1 >, \ldots, < \mathbf{x}_w, \mathbf{b}_w >)$$

We now describe our CCA-secure cryptosystem.

- **Common Parameter**: Given security parameter n, let $r \in (0, 1)$ be any constant, $\beta = o(1/(n^{0.5+r} \log n))$, p be an integer such that $\lfloor \lg p \rfloor p \leq n^r = o(n)$, $h = \lfloor \lg p \rfloor$, q be a prime such that $q\beta > 2\sqrt{n}$. Let $H_1 : \{0,1\}^\ell \to \mathbb{Z}_d$ is a hash function which is chosen from the family of universal one-way hash functions $\mathcal{H}_1$, where $d \geq q$ is an integer. Let $H_2 : \{0,1\}^{h \times w} \to \{0,1\}^k$ is a hash function which is chosen from the family of universal one-way hash functions $\mathcal{H}_2$. Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_w)$ and $\mathbf{b}_i = (b_{1i}, \ldots, b_{hi})^T = (1, 2, \ldots, 2^{h-1})^T$, $i \in [w]$. Let $(\mathtt{Gen}, \mathtt{Sign}, \mathtt{Ver})$ be a strongly unforgeable one-time signature where the public verification keys are in $\{0,1\}^\ell$. Let $a \in \mathbb{Z}_q$ chosen uniformly at random. Define $f : \mathbb{Z}_d \times \mathbb{Z}_d \to \{0,1\}$ as follows:

$$f(x, y) = \begin{cases} 0 & \text{if } x = y, \\ 1 & \text{if } x \neq y. \end{cases}$$

- **Key Generation**:
  1 Private key generation: For $i = 1, \ldots, w$, choose w vectors $\mathbf{s}_1, \ldots, \mathbf{s}_w \in \mathbb{Z}_q^n$ and w vectors $\mathbf{s}'_1, \ldots, \mathbf{s}'_w \in \mathbb{Z}_q^n$ uniformly at random. The private key generation is $\mathbf{S} = (\mathbf{s}_1, \ldots, \mathbf{s}_w)$ and $\mathbf{S}' = (\mathbf{s}'_1, \ldots, \mathbf{s}'_w)$.
  2 Public key generation:
    (1) For $i = 1, \ldots, m$, choose m vectors $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$ uniformly at random, and let $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_m)$.
    (2) Choose e_{ij}, e'_{ij} ($i \in [m]$ and $j \in [w]$) according to the distribution $\overline{\Psi}_\beta$. Let $y_{ij} =< \mathbf{a}_i, \mathbf{s}_j > + e_{ij}$ and $y'_{ij} =< \mathbf{a}_i, \mathbf{s}'_j > + e'_{ij}$ ($i \in [m]$ and $j \in [w]$).
    (3) Let $\mathbf{y}_j = (y_{1j}, \ldots, y_{mj})^T$, $\mathbf{e}_j = (e_{1j}, \ldots, e_{mj})^T$, $\mathbf{g}_j = (< \mathbf{a}_1, \mathbf{s}_j >, \ldots, < \mathbf{a}_m, \mathbf{s}_j >)^T$ and $\mathbf{y}'_j = (y'_{1j}, \ldots, y'_{mj})^T$, $j \in [w]$.
    (4) Let $\mathbf{Y} = (\mathbf{y}_1 + \mathbf{e}_1 - \mathbf{y}'_1, \ldots, \mathbf{y}_w + \mathbf{e}_w - \mathbf{y}'_w)$ and $\mathbf{Y}' = (\mathbf{y}'_1 + \mathbf{g}_1, \ldots, \mathbf{y}'_w + \mathbf{g}_w)$. The public key is $< \mathbf{A}, \mathbf{Y}, \mathbf{Y}' >$.
- **Encryption**: $\mathcal{E}$ takes as input (pk, M) where $pk =< \mathbf{A}, \mathbf{Y}, \mathbf{Y}' >$ is the public key and $M \in \{0,1\}^k$ is the message.
  1. Firstly generate a keypair for one-time signature $(vk, sk_\sigma) \leftarrow \mathtt{Gen}$.
  2. Compute $r = H_1(vk)$ and $t = f(r, a)$.
  3. Generate the matrix $\mathbf{V} = (\mathbf{v}_1, \ldots, \mathbf{v}_h) \in \mathbb{Z}_2^{m \times h}$, where each $\mathbf{v}_i = (v_{1i}, \ldots, v_{mi})^T$, $i \in [h]$, is chosen independently and uniformly from $\mathbb{Z}_2^m$ at random.
  4. Compute $\mathbf{PK}_{mR05} = (\mathbf{Y}' + t\mathbf{Y})/2^t = (\mathbf{pk}_1, \ldots, \mathbf{pk}_w)$.

5. Compute $\mathbf{C} = (\mathbf{AV}, \mathbf{C}') = (c_{ij})$, where $c_{ij} = (\mathbf{A}\mathbf{v}_i, < \mathbf{v}_i, \mathbf{pk}_j > + \lfloor q\frac{b_{ij}}{p} \rceil) = \mathcal{E}^{mR05}_{\mathbf{pk}_j}(b_{ij})$
6. Choose $\mathbf{X} = (x_{ij}) = (\mathbf{x}_1, \ldots, \mathbf{x}_w) \in \mathbb{Z}_2^{h \times w}$ at random and compute

$$\begin{aligned}\mathbf{c}^1 &= (\mathbf{AVX}, \mathbf{C}' * \mathbf{X}) = (\sum_{i=1}^{h} x_{i1}c_{i1}, \ldots, \sum_{i=1}^{h} x_{iw}c_{iw}) = (c_1, \ldots, c_w) \\ &= (\mathcal{E}^{mR05}_{\mathbf{pk}_1}(\sum_{i=1}^{h} x_{i1}b_{i1}), \ldots, \mathcal{E}^{mR05}_{\mathbf{pk}_w}(\sum_{i=1}^{h} x_{iw}b_{iw})) \\ c^2 &= H_2(\mathbf{X}) \bigoplus M.\end{aligned}$$

6. Sign the tuple $(\mathbf{c}^1, c^2, \mathbf{X})$ as $\sigma \leftarrow \mathtt{Sign}_{sk_\sigma}(\mathbf{c}^1, c^2, \mathbf{X})$
7. The ciphertext c is output as $c = (vk, \mathbf{c}^1, c^2, \sigma)$.

- **Decryption**: $\mathcal{D}$ takes as input (sk, c) where $sk =< \mathbf{S}, \mathbf{S}' >$ is private key and $c = (vk, \mathbf{c}^1, c^2, \sigma)$.
1. Compute $H_1(vk) = a'$, and $\mathbf{SK}_{mR04} = \mathbf{S} + (1 - f(a', a))\mathbf{S}' = (\mathbf{sk}_1, \ldots, \mathbf{sk}_w)$
2. Compute

$$\begin{aligned}\mathbf{B} * \mathbf{X} &= (\mathcal{D}^{mR05}_{\mathbf{sk}_1}(c_1), \ldots, \mathcal{D}^{mR05}_{\mathbf{sk}_w}(c_w)) = (< \mathbf{x}_1, \mathbf{b}_1 >, \ldots, < \mathbf{x}_w, \mathbf{b}_w >) \\ &= (\sum_{j=1}^{h} x_{j1} D^{mR05}_{\mathbf{sk}_1}(c_{j1}), \ldots, \sum_{j=1}^{h} x_{jw} \mathcal{D}^{mR05}_{\mathbf{sk}_w}(c_{jw})).\end{aligned}$$

3. Compute $\mathbf{X}$ from $\mathbf{B} * \mathbf{X}$
4. Check that $\mathtt{Ver}(vk, \mathbf{c}^1, c^2, \mathbf{X}, \sigma) = 1$; if not, it output $\perp$
5. Output $c^2 \oplus H_1(\mathbf{X})$.

4.2 Proof of Security

Given a ciphertext $c = (vk, \mathbf{c}^1, c^2, \sigma) = (vk, (\mathbf{AVX}, \mathbf{C}' * \mathbf{X}), H_2(\mathbf{X}) \bigoplus M, \mathtt{Sign}_{sk_\sigma}$ ($\mathbf{c}^1$, c^2, $\mathbf{X}$)). If $\mathbf{X}'$ which we get by c with mR05 is not equal to $\mathbf{X}$, $\mathtt{Ver}(vk$, $\mathbf{c}^1$, c^0, $\mathbf{X}'$, $\sigma) \neq 1$. Thus, the above cryptosystem has not the error of decryption. Since $\mathbf{B} * \mathbf{X} = (\mathcal{D}^{mR05}_{\mathbf{sk}_1}(c_1), \ldots, \mathcal{D}^{mR05}_{\mathbf{sk}_w}(c_w))$ and $\mathbf{c} = \mathbf{C} * \mathbf{X} = (c_1, \ldots, c_w)$, we know that the decryption error probability of $\mathcal{D}^{mR05}_{\mathbf{sk}_i}(c_i)$, $i \in [w]$, is at most $2^{-\Omega(1/m\beta^2(n)n^{2r})}$ with Theorem 1. In other words, our construction possibly refuse a correct ciphertext and the rejective probability of a correct ciphertext is at most $(1 - (1 - 2^{-\Omega(1/m\beta^2(n)n^{2r})})^w)$.

In the section, we will mainly prove the following theorem

Theorem 3. *If* (`Gen`, `Sign`, `Ver`) *is a strong one-time signature scheme and the hash functions H_1 and H_2 are the universal one-way hash function, if there exist a PPT adversary $\mathcal{A}$that breaks the above cryptosystem in adaptive chosen ciphertext attacks. then there exists a polynomial-time quantum algorithm for the worst case of* $\mathrm{SVP}_{\widetilde{O}(n/\beta(n))}$ *and* $\mathrm{SIVP}_{\widetilde{O}(n/\beta(n))}$ *in the case of the above cryptosystem.*

Proof. To prove the theorem, we will assume that there is an adversary, $\mathcal{A}$, that can break the cryptosystem and show how to use this adversary, $\mathcal{A}$, to construct a statistical test for the decisional LWE problem, i.e, distinguish (with non-negligible probability) the distribution $A_{s,\overline{\Psi}_\beta}$ for some uniform (secret) $\mathbf{s} \leftarrow \mathbb{Z}_n^q$ from the uniform distribution U on $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

For the statistical test, we are given a distribution R that is either U or $A_{s,\overline{\Psi}_\beta}$. At a high level, our construction works as follows. We build a simulator, $\mathcal{S}$, that simulates the joint distribution consisting of adversary's view in its attack on the cryptosystem, and the hidden bit b generated uniformly at random by the the simulator, $\mathcal{S}$ (which is not a part of the adversary's view). We will show that if the input comes from $A_{s,\overline{\Psi}_\beta}$, the simulation is nearly perfect, and so the adversary will have a non-negligible advantage in guessing the hidden bit b. We will also show that if the input comes from U, then the adversary's view is essentially independent of b, and therefore the adversary's advantage is negligible. This immediately implies a statistical test distinguishing the distribution $A_{s,\overline{\Psi}_\beta}$ for some uniform (secret) $\mathbf{s} \leftarrow \mathbb{Z}_n^q$ from the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

We now give the details of the simulator, $\mathcal{S}$. The input to the simulator is the a distribution R that is either U or $A_{\mathbf{s},\overline{\Psi}_\beta}$ on $\mathbb{Z}_q^n \times \mathbb{Z}_q$. The simulator constructs the cryptosystem parameters and runs the key generation algorithm, using the given distribution R. More specifically,

1. Given a distribution R that is either U or $A_{s,\overline{\Psi}_\beta}$ for some uniform (secret) $\mathbf{s} \leftarrow \mathbb{Z}_n^q$, $\mathcal{S}$ generates public parameters $\{m, q, p, r, \beta\, H_1, H_2, h, f, \mathbf{B}\}$, takes a one-time signature scheme ($\mathtt{Gen}$, $\mathtt{Sign}$, $\mathtt{Ver}$), takes m samples $(\mathbf{a}_i, y_i)_{i=1}^m$ from R, and choose $\mathbf{s}_j \leftarrow \mathbb{Z}_n^q$ uniformly at random, compute $y_{ij} =< \mathbf{a}_i, \mathbf{s}_j > +e_{ij}$, where e_{ij} is taken according to $\overline{\Psi_\beta}$ ($i \in [m]$ and $j \in [w]$). Let $\mathbf{y} = (y_1, \ldots, y_m)^T$, $\mathbf{y}_j = (y_{1j}, \ldots, y_{mj})^T$, $\mathbf{e}_j = (e_{1j}, \ldots, e_{mj})^T$, and $\mathbf{g}_j = (< \mathbf{a}_1, \mathbf{s}_j >, \ldots, < \mathbf{a}_m, \mathbf{s}_j >)^T$, $j \in [w]$. Let $\mathbf{Y} = (\mathbf{y}_1 + \mathbf{e}_1 - \mathbf{y}, \ldots, \mathbf{y}_w + \mathbf{e}_w - \mathbf{y})$ and $\mathbf{Y}' = (\mathbf{y} + \mathbf{g}_1, \ldots, \mathbf{y} + \mathbf{g}_w)$.
2. The public key is $< \mathbf{Y}, \mathbf{Y}' >$, and that $< \mathbf{s}, \mathbf{s}_1, \ldots, \mathbf{s}_w >$ is the corresponding and possible private key.
3. Generate a keypair for one-time signature $(vk^*, sk_\sigma^*) \leftarrow \mathtt{Gen}$ and Compute $a = H_1(vk^*)$.
4. Let the set of public parameters $\mathtt{param}$=$\{m, q, p, r, \beta\, H_1, H_2, a, h, f, \mathbf{B}$, ($\mathtt{Gen}$, $\mathtt{Sign}$, $\mathtt{Ver}$)$\}$.

Then, the simulator, $\mathcal{S}$, interacts with adversary $\mathcal{A}$ as follows:

1. Send system parameters $\mathtt{param}$ and the public key $< \mathbf{A}, \mathbf{Y}, \mathbf{Y}' >$ to $\mathcal{A}$.
2. When $\mathcal{A}$ makes decryption oracle query $\mathcal{D}(c)$, where $c = (vk, \mathbf{c}^1, c^2, \sigma)$, the simulator, $\mathcal{S}$, proceeds as follows:
   (1) Compute $a' = H_1(vk)$, if $a' = a$, the simulator, $\mathcal{S}$, halts and outputs $\perp$.
   (2) Let $\mathbf{SK}_{mR05} = (\mathbf{s}_1 + (1 - f(a', a))\mathbf{s}, \ldots, \mathbf{s}_w + (1 - f(a', a))\mathbf{s}) = (\mathbf{sk}_1, \ldots, \mathbf{sk}_w)$
   (3) Then compute $\mathbf{B} * \mathbf{X} = (\mathcal{D}_{\mathbf{sk}_1}^{mR05}(c_1), \ldots, \mathcal{D}_{\mathbf{sk}_w}^{mR05}(c_w)) = (< \mathbf{x}_1, \mathbf{b}_1 > , \ldots, < \mathbf{x}_w, \mathbf{b}_w >)$
   (4) Compute $\mathbf{X}$ from $\mathbf{B} * \mathbf{X}$

(5) Check that $\texttt{Ver}(vk, \mathbf{c}^1, c^2, \mathbf{X}, \sigma) = 1$; if not, it output $\perp$
(6) Output $c^2 \oplus H_1(\mathbf{X})$.

3. At some point, $\mathcal{A}$ outputs two equal-length messages M_0 and $M_1 \in \{0,1\}^k$ on which it wishes to be challenged. The simulator, $\mathcal{S}$, responds as follows:
(1) Choose $\mathbf{X}^* \in \mathbb{Z}_2^{h\times w}$ at random and $\mathbf{V}^* = (\mathbf{v}_1^*, \ldots, \mathbf{v}_h^*) \in \mathbb{Z}_2^{m\times h}$, where each $\mathbf{v}_i^* = (v_{1i}^*, \ldots, v_{mi}^*)^T$, $i \in [h]$, and compute

$$\mathbf{c}^{1*} = (((\mathbf{AV}^*)\mathbf{X}^*), \mathbf{C}'^* * \mathbf{X}^*), c^{2*} = H_2(\mathbf{X}^*) \bigoplus M_b.$$

where $\mathbf{C}'^* = (c_{ij}^*) = (< \mathbf{v}_i^*, \mathbf{y} + \mathbf{g}_j > + \lfloor q\frac{b_{ij}}{p} \rceil)$.
(2) Sign the tuple $(\mathbf{c}^{1*}, c^{2*}, \mathbf{X}^*)$ as $\sigma^* \leftarrow \texttt{Sign}_{sk_\sigma^*}(\mathbf{c}^{1*}, c^{2*}, \mathbf{X}^*)$
(3) Return ciphertext $c^* = (vk^*, \mathbf{c}^{1*}, c^{2*}, \sigma^*)$ to $\mathcal{A}$.
Hence, if the simulator's input comes from $A_{\mathbf{s},\overline{\Psi}_\beta}$ on $\mathbb{Z}_q$, then c^* is a valid encryption of M_b under public key $(\mathbf{Y}' + f(H_1(vk^*), a)\ \mathbf{Y})/2^{f(H_1(vk^*),a)} = (\mathbf{y}+\mathbf{g}_1, \ldots, \mathbf{y}+\mathbf{g}_w)$. However, corresponding to the public key $(\mathbf{y}+\mathbf{g}_1, \ldots, \mathbf{y}+\mathbf{g}_w)$, the private key is $< \mathbf{s}_1 + \mathbf{s}, \ldots, \mathbf{s}_w + \mathbf{s} >$. On the other hand, when the simulator's input comes from uniform distribution U on $\mathbb{Z}_q$, then c^* is independent of b in the adversary's view, since $\mathbf{s}_j$, $i \in [w]$, is chosen uniformly at random from $\mathbb{Z}_n^q$, and H_1 is the universal one-way hash.

4. $\mathcal{A}$ may continue to make decryption oracle queries, and these are answered as before, except that $\mathcal{A}$ makes decryption oracle query $\mathcal{D}(vk, \mathbf{c}^1, c^2, \sigma)$ with $H_1(vk) = H_1(vk^*)$. Under the case of $H_1(vk) = H_1(vk^*)$, the simulator, $\mathcal{S}$, halts and outputs $\perp$.

5. Finally, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. If $b = b'$ then $\mathcal{S}$ outputs 1 meaning that R is the distribution $A_{\mathbf{s},\overline{\Psi}_\beta}$ on $\mathbb{Z}_q^n \times \mathbb{Z}_q$, Otherwise, it outputs 0 meaning that R is uniform distribution U on $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

That completes the description of the simulator. If the distribution R is the uniform distribution U on $\mathbb{Z}_q^n \times \mathbb{Z}_q$, we showed that b is independent of the adversary's view, then $\texttt{Pr}[b = b'] = 1/2$. When the distribution R is the distribution $A_{\mathbf{s},\overline{\Psi}_\beta}$ on $\mathbb{Z}_q^n \times \mathbb{Z}_q$, we analyze the advantage that the simulator, $\mathcal{S}$, outputs 1. If $\mathcal{S}$ outputs 1 successfully, $\mathcal{A}$ does not issue a decryption query for $c = (vk, \mathbf{c}^1, c^2, \sigma)$ with $H_1(vk) = a$, and $\mathcal{A}$'s view is identical to its view in a real attack game under the above case. Let $\texttt{Success}$ denote the event that $\mathcal{A}$ attacks successfully our construction, $\texttt{NoFailure}$ denote the event that $\mathcal{S}$ is not failed. Therefore $|\texttt{Pr}[b = b'] - 1/2| = \texttt{Pr}[\texttt{Success} \wedge \texttt{NoFailure}] = \texttt{Pr}[\texttt{Success} \mid \texttt{NoFailure}] \times \texttt{Pr}[\texttt{NoFailure}]$. By the description of the simulator, $\mathcal{S}$, the case, which leads to the failure of simulator $\mathcal{S}$, is that $\mathcal{A}$ issues a decryption query for $c = (vk, \mathbf{c}^1, c^2, \sigma)$ with $H_1(vk) = a$, however, the probability the the above case happens is negligible, since H_1 is a universal one-way hash function. Assuming $\mathcal{A}$ breaks our construction with probability at least ε, then $|\texttt{Pr}[b = b'] - 1/2| > \varepsilon \times \texttt{Pr}[\texttt{NoFailure}] > \varepsilon/2$. Thus, the advantage that $\mathcal{S}$ distinguishs the distribution $A_{s,\overline{\Psi}_\beta}$ from the uniform distribution U on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is $|\texttt{Pr}[\mathcal{S}(1^n, A_{s,\overline{\Psi}_\beta}) = 1] - \texttt{Pr}[\mathcal{S}(1^n, U) = 1]| \geq |1/2 \pm \varepsilon/2 - 1/2| = \varepsilon/2$. According to Proposition 1, we can construct a polynomial-time quantum algorithm $\mathcal{C}$, which uses $\mathcal{S}$, for the worst case of $\text{SVP}_{\widetilde{O}(n/\beta(n))}$ and $\text{SIVP}_{\widetilde{O}(n/\beta(n))}$ in the case of the above cryptosystem.

5 Conclusion

We propose a simple construction of CCA- secure public-key encryption scheme based on lattice. Our construction approach is similar to the one in [22] and also uses a one-time signature scheme (`Gen`, `Sign`, `Ver`). We require that this scheme be secure in the sense of strong unforgeability. Our construction regards lattice-based cryptosystem mR05 of [21] as building block and makes use of its indistinguishable pseudohomomorphism property which is known to be achievable without random oracles and which is the crux that we construct CCA-secure public key encryption scheme. This makes our construction approach quite different from existing ones. So far as we know, our construction is the first CCA-secure cryptosystem which is directly constructed from lattice and whose security is directly based on the standard lattice problems $\mathrm{SVP}_{\widetilde{O}(n/\beta(n))}$ and $\mathrm{SIVP}_{\widetilde{O}(n/\beta(n))}$ which are hard in the worst-case for quantum algorithms.

References

1. S. Goldwasser and S. Micali. Probabilistic encryption. Journal of Computer and System Sciences, 28:270-299, 1984.
2. C. Rackoff and D. Simon. Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack. In Advances in Cryptology Crypto '91, pages 433-444, 1991.
3. M. Naor and M. Yung. Public-Key Cryptosystems Provably-Secure against Chosen-Ciphertext Attacks. 22nd ACM Symposium on Theory of Computing, ACM, pp. 427-437, 1990.
4. D. Dolev, C. Dwork, and M. Naor. Non-Malleable Cryptography. SIAM J. Computing 30(2): 391-437, 2000.
5. Y. Lindell. A Simpler Construction of CCA-Secure Public-Key Encryption Under General Assumptions. Adv. in Cryptology–Eurocrypt 2003, LNCS vol. 2656, Springer-Verlag, pp. 241-254, 2003
6. A. Sahai. Non-Malleable Non-Interactive Zero Knowledge and Adaptive Chosen-Ciphertext Security. 40th IEEE Symposium on Foundations of Computer Science (FOCS), IEEE, pp. 543-553, 1999.
7. U. Feige, D. Lapidot, and A. Shamir. Multiple Non-Interactive Zero-Knowledge Proofs Under General Assumptions. SIAM J. Computing 29(1): 1-28, 1999.
8. M. Blum, P. Feldman, and S. Micali. Non-Interactive Zero-Knowledge and its Applications. 20th ACM Symposium on Theory of Computing (STOC), ACM, pp. 103-112, 1988.
9. R. Cramer and V. Shoup. A Practical Public Key Cryptosystem Provably Secure Against Chosen Ciphertext Attack. Adv. in Cryptology-Crypto 1998, LNCS vol. 1462, Springer- Verlag, pp. 13-25, 1998.
10. R. Cramer and V. Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. Adv. in Cryptology-Eurocrypt 2002, LNCS vol. 2332, Springer-Verlag, pp. 45-64, 2002.
11. J. Camenisch and V. Shoup. Practical Verifiable Encryption and Decryption of Discrete Logarithms. Adv. in Cryptology-Crypto 2003, LNCS vol. 2729, Springer-Verlag, pp. 126-144, 2003.

12. K. Kurosawa and Y. Desmedt. A New Paradigm of Hybrid Encryption Scheme. Adv. in Cryptology-Crypto 2004, LNCS vol. 3152, Springer-Verlag, pp. 426-442, 2004.
13. R. Canetti, S. Halevi, and J. Katz. Chosen-Ciphertext Security from Identity-Based Encryption. Adv. in Cryptology-Eurocrypt 2004, LNCS vol. 3027, Springer-Verlag, pp. 207-222, 2004.
14. Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Advances in Cryptology-EUROCRYPT 2003. Springer-Verlag, 2003.
15. Dan Boneh and Jonathan Katz. Improved efficiency for CCA-secure cryptosystems built using identity based encryption. In Proceedings of RSA-CT 2005. Springer-Verlag, 2005.
16. X. Boyen, Q. Mei, and B. Waters. Direct Chosen Ciphertext Security from Identity-Based Techniques. 12th ACM Conference on Computer and Communications Security, ACM, pp. 320-329, 2005.
17. Brent Waters. Efficient identity based encryption without random oracles. In Advances in Cryptology-EUROCRYPT 2005, Lecture Notes in Computer Science. Springer Verlag, 2005
18. M. Ajtai. Generating hard instances of lattice problems (extended abstract). In STOC, pages 99-108, 1996.
19. Oded Regev. New lattice-based cryptographic constructions. J. ACM, 51(6):899-942, 2004.
20. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In STOC, pages 84-93, 2005.
21. Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Multi-bit cryptosystems based on lattice problems. In PKC, pages 315-329, 2007.
22. Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In STOC, pages 187-196, 2008.
23. M. Ajtai. Representing hard lattices with $O(n \log n)$ bits. In STOC 2005, pages 94-103, 2005.
24. M. Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In STOC'97, pages 284-293, 1997. Also available at ECCC TR96-065
25. Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Eliminating decryption errors in the Ajtai-Dwork cryptosystem. In CRYPTO'97, pages 105-111, 1997. Also available at ECCC TR97-018.
26. Jin-Yi Cai and Thomas W. Cusick. A lattice-based public-key cryptosystem. Information and Computation, 151(1-2):17-31, 1999.
27. Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In CRYPTO'97, pages 112-131, 1997
28. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In ANTS-III, pages 267-288, 1998
29. Nick Howgrave-Graham, Phong Q. Nguyen, David Pointcheval, John Proos, Joseph H. Silverman, Ari Singer, andWilliam Whyte. The impact of decryption failures on the security of NTRU encryption. In CRYPTO 2003, pages 226-246, 2003.
30. Phong Q. Nguyen and David Pointcheval. Analysis and improvements of NTRU encryption paddings. In CRYPTO 2002, pages 210-225, 2002.
31. Seong-Hun Paeng, Bae Eun Jung, and Kil-Chan Ha. A lattice based public key cryptosystem using polynomial representations. In PKC 2003, pages 292-308, 2003

32. Chris Peikert. Limits on the hardness of lattice problems in ℓ_p norms. In IEEE Conference on Computational Complexity, pages 333-346, 2007. Full version in ECCC Report TR06-148.
33. Dörte Rappe. Homomorphic cryptosystems and their applications. Ph.D. Thesis, University of Dortmund, 2004. Also available at http://eprint.iacr.org/2006/001.
34. Oded Goldreich. Foundations of Cryptography, volume II. Cambridge University Press, 2004
35. Qiong Huang, Duncan S. Wong, and Yiming Zhao. Generic transformation to strongly unforgeable signatures. In ACNS, pages 1-17, 2007.
36. D. Simon. Finding collisions on a one-way street: can secure hash functions be based on general assumptions ? In Advances in Cryptology-Eurocrypt '98, pages 334-345, 1998.
37. M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In 21st Annual ACM Symposium on Theory of Computing, 1989.