Lattice-Based Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack

Chen Huiyan[1,2], Li Zichen[1]

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

Abstract. We propose a simple and efficient construction of CCA- secure public-key encryption scheme based on lattice. Our construction needs an encryption scheme, which we call "matrix encryption", as building block, and requires the underlying matrix encryption scheme to satisfy only a relatively weak notion of security which can be achievable without random oracles. With the pseudohomomorphism property of mR04 of [3], which is the multi-bit version of single-bit cryptosystems R04 [1], we design a matrix encryption scheme which satisfies the above requirements, thus, our construction provides a new approach for constructing CCA-secure encryption schemes in the standard model. So far as we know, our construction is the first CCA-secure cryptosystem which is directly constructed from lattice and whose security is based on the unique shortest vector problem (uSVP).

In addition, the method designing the matrix encryption scheme from mR04 also adapts to mR05, mA05, $\mathrm{mAD}_{\mathtt{GGH}}$ of [3], which are the multi-bit versions of single-bit cryptosystems R05 [2], A05 [5], and $\mathrm{AD}_{\mathtt{GGH}}$ [7], respectively, since they have the same pseudohomomorphism property as mR04. This result makes our approach constructing CCA-secure cryptosystem become generic and universal.

Keywords. Lattice, CCA-security , Matrix encryption, 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. To captures the intuition that an adversary should not be able to obtain any partial information about a message given its encryption, Goldwasser and Micali [15] defined the notion of *semantic security* (also sometimes referred to as *security under chosen-plaintext attack*, i.e., CPA-security). However, this guarantee of secrecy is only valid when the adversary is completely passive, i.e., can only eavesdrop. Indeed, *semantic security* offers no guarantee of secrecy at all if an adversary can mount an active attack, for example, if an adversary can inject messages into a network, these messages may be encryptions, and the adversary may be able to extract partial information about the corresponding cleartexts through its interactions with the parties in the network. To deal with active attacks, Rackoff and Simon [16] modeled this type of attacks by simply allowing an adversary to obtain decryptions of its choice, i.e., the adversary has access to a "decryption oracle", and defined the notion of *security against adaptive chosen ciphertext attacks.* Now, *security against adaptive chosen-ciphertext attacks* (i.e., "CCA-security") has become the *de facto* level of security for public-key encryption schemes.

Nevertheless, only a relatively small number of encryption schemes have been rigorously proven secure against adaptive chosen-ciphertext attacks in the standard model, i.e., the security of schemes does not rely on the Random Oracle model, and there are the following approaches which are known for constructing these CCA-secure cryptosystems. The first follows the paradigm introduced by Naor and Yung [17] to achieve non-adaptive chosen-ciphertext security, later extended to the case of adaptive chosen-ciphertext security by [18–20], but these rely on generic non-interactive zero-knowledge proofs [21, 22] and do not currently lead to practical solutions. The second technique is based on the "smooth hash proof systems"of Cramer and Shoup [23], and has led to a number of practical schemes [23–26]. The third, and more recent, method [27] constructs a CCA-secure encryption scheme from any identity-based encryption (IBE) secure in selective-ID model [28] with a one-time signature. Boneh and Katz [29] further improve the efficiency of this scheme by using a MAC instead of a one-time signature and Boyen *et al.* [30] show that for some concrete identity-based encryption schemes (e.g., the one of Waters [31]) a more efficient and direct construction of a CCA-secure encryption scheme is possible.

In this work, we put forward a new approach for constructing CCA-secure encryption scheme which is based on lattice.

1.1 Background and Related Work

The constructions of public key encryption based on lattices have attracted considerable interest in recent years. The main reason is that, unlike many other cryptographic constructions, lattice based constructions can be based on the worst-case hardness of a problem. That is, breaking them would imply a solution to any instance of a certain lattice problem. Now, the lattice-based cryptosystems can be roughly classified into two types: (A) those who are efficient on the size of their keys and ciphertexts and the speed of encryption/decryption procedures, but have no security proofs based on the hardness of well-known lattice problems, for example, [9, 10] and their improvements [13, 11, 12]; (B) those who have security proofs based on the lattice problems but are inefficient, for example, [1, 2, 5–8]. Lattice-based cryptosystems, which belong to the type (A), are efficient multi-bit cryptosystems, however, those in the type (B) generally are single-bit cryptosystems. Therefore, it is important to improve their efficiency for secure lattice-based cryptosystems in the this type (B). Akinori Kawachi *et al.* [3] extended single-bit cryptosystems R04 [1], R05 [2], A05 [5], and $\mathrm{AD}_{\mathtt{GGH}}$ in [7] to their multi-bit versions mR04, mR05, mA05, $\mathrm{mAD}_{\mathtt{GGH}}$ with security proofs and without increase in the size of ciphertexts. Their technique requires precise evaluation of trade-offs between decryption errors and hardness of underlying lattice problems in the original lattice-based cryptosystems and simultaneously also reveals an algebraic property, named *pseudohomomorphism*, of the lattice-based cryptosystems.

Although Lattice-based cryptosystems in the type (B) and their multi-bit versions [3] have security proofs, they are *semantic security.* It wasn't until fairly recently that Chris Peikert *et al.* [4] designed an encryption scheme that was both relative to lattice and provably secure against chosen ciphertext attacks. Chris Peikert *et al.*'s construction of CCA-secure cryptosystem is based on a collection of lossy trapdoor functions (lossy TDFs) and a collection of all-but-one trapdoor functions (ABO TDFs), where lossy TDF is a new general primitive proposed by them and ABO TDF can be constructed from a collection of sufficiently lossy TDFs. In [4], Chris Peikert presented the concrete realization of lossy and all-but-one 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 [2] gave a reduction showing that LWE is hard on the average if standard lattice problems are hard in the worst case for quantum algorithms.

1.2 Our Contribution

In this work, we propose a construction of CCA-secure cryptosystem which is based on lattice and which we call CR04. Before sketching our construction, we first recall the notion of *pseudohomomorphism* which was introduced by Akinori Kawachi *et al.* [3]. We know that the homomorphism of ciphertexts is quite useful for many cryptographic applications [32]. Lattice-based Cryptosystems mR04, mR05, mA05, $\mathrm{mAD}_{\mathtt{GGH}}$ 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. The *pseudohomomorphism* property of mR04, mR05, mA05, $\mathrm{mAD}_{\mathtt{GGH}}$ plays an important role in our construction. In fact, Goldwasser and Kharchenko made use of a similar property to construct the plaintext knowledge proof system for the Ajtai-Dwork cryptosystem [33].

In the construction of CR04, we make use of the *pseudohomomorphism* of mR04 and propose a matrix encryption scheme which is used as building block of CR04. In order to make CR4 be CCA-secure, we only require that this matrix encryption scheme satisfies restricted CPA-security which is a weak notion of security and is defined in Section 3.2. Briefly and somewhat informally, CR04 proceeds as follows: CR04's public and private key pair is generated with key generation algorithm. To encrypt a message, the sender first generates a string *str* which generates the public and private key pair of the matric encryption scheme with CR04's public and private key pair, then encrypts a matrix $\mathbf{X}$ and generates $\mathbf{c}$ with the matric encryption scheme, and next, encrypts the message in the secrete key which is generated with the matrix $\mathbf{X}$ and generate

c_0, finally, The resulting ciphertext is $(str, \mathbf{c}, c_0, \texttt{tag})$, where $\texttt{tag}$ is now a message authentication code computed on $(str, \mathbf{c}, c_0)$ using key $\mathbf{X}$. To decrypt a ciphertext $(str, \mathbf{c}, c_0, \texttt{tag})$, the receiver first gets $\mathbf{X}$ with str and $\mathbf{c}$, and then verifies the correctness of $\texttt{tag}$, outputs $\perp$ if the verification fails. Otherwise, the receiver decrypts c_0.

Security of CR04 against adaptive chosen-ciphertext attacks can be simply and informally understood as follows: we first reduce the indistinguishable pseudohomomorphism property of mR04, which is based on the unique shortest vector problem (uSVP), to the restricted CPA-security of the matrix encryption scheme, then reduce the restricted CPA-security of the matrix encryption scheme to CCA-security of CR04. So far as we know, CR04 is the first CCA-secure cryptosystem which is directly constructed from lattice and whose security is based on uSVP. Since lattice-based Cryptosystems mR05, mA05, $\text{mAD}_{\texttt{GGH}}$ like mR04 have the *pseudohomomorphism* property, the method, with which we construct CCA-secure CR04, adapts to mR05, mA05, $\text{mAD}_{\texttt{GGH}}$, i.e., we can construct CCA-secure cryptosystems from mR05, mA05, $\text{mAD}_{\texttt{GGH}}$, respectively.

1.3 Organization

The rest of this paper is organized as follows. We describe basic notions and notations in Section 2. In Section 3, we first definite matrix encryption and a weaker notion of security on matrix encryption scheme, then we review the pseudohomomorphism property of ciphertexts, and presents a generic approach constructing matrix encryption scheme from mR04, which adapts to constructing matrix encryption scheme from mR05, mA05, $\text{mAD}_{\texttt{GGH}}$. In Section 4, we present a CCA-security cryptosystem (CR04) from meR04. 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 $x \bmod y$ 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, and let $\text{frc}(x)$ be the distance from x to the closest integer.

The n-dimensional Euclidean 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 Euclidean norm of a vector $x \in \mathbb{R}^n$ is $\|\mathbf{x}\| = \sqrt{\sum_{i=1}^{n} x_i^2}$. 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 maximum length of a vector in $\mathbf{B}$. The linear space spanned by a set of m vectors $\mathbf{B}$ is denoted $\text{span}(\mathbf{B}) = \{\sum_i x_i \mathbf{b}_i : x_i \in \mathbb{R}, i \in [m]\}$.

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 $f(n) = \tilde{\mathrm{O}}(g(n))$ 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:*

- *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)* $\leftarrow \mathcal{G}(1^n)$.
- *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* $C = \mathcal{E}_{pk}(m)$.
- *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*:*

- $\mathcal{G}(1^n)$ *outputs (pk, sk). Adversary* $\mathcal{A}$ *is given* 1^n *and pk.*
- *The adversary may make polynomially-many queries to a decryption oracle* $\mathcal{D}_{sk}(\cdot)$.

– *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 $C^* \leftarrow \mathcal{E}_{pk}(m_b)$.*
–*$\mathcal{A}$ may continue to query its decryption oracle $\mathcal{D}_{sk}(\cdot)$ except that it may not request the decryption of C^*.*
–*Finally, $\mathcal{A}$ outputs a guess b'.*

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

In the above game, we limit adversary, i.e., it cannot issue decryption queries while attacking the challenge public key, thus, a public key system is said to be semantically secure if no polynomial time adversary can win the game with a non-negligible advantage. As shorthand we say that a semantically secure public key system is CPA-security.

2.3 Message Authentication

We view a message authentication code as a pair of ppt algorithms (Mac, Vrfy). The authentication algorithm Mac takes as input a key *sk* and a message *M*, and outputs a string tag. The verification algorithm Vrfy takes as input a key *sk*, a message *M*, and a string tag; it outputs either 0 ("reject") or 1 ("accept"). We require that for all *sk* and *M* we have $\mathtt{Vrfy}_{sk}(M; \mathtt{Mac}_{sk}(M))$=1. For simplicity, we assume that Mac and Vrfy are deterministic. We give a definition of security tailored to the requirements of our construction; in particular, we require only "one-time" security for our message authentication code.

Definition 3. (**Message authentication**) *A message authentication code (Mac, Vrfy) is secure against a one-time chosen-message attack if the success probability of any ppt adversary $\mathcal{A}$ in the following game is negligible in the security parameter n:*

1. *A random key $sk \in \{0,1\}^n$ is chosen.*
2. *$\mathcal{A}(1^n)$ outputs a message M and is given in return tag=$\mathit{Mac}_{sk}(M)$.*
3. *$\mathcal{A}$ outputs a pair (M', tag'). We say that $\mathcal{A}$ succeeds if $(M, \mathit{tag}) \neq (M', \mathit{tag}')$ and $\mathit{Vrfy}_{sk}(M', \mathit{tag}') = 1$.*

In the above, the adversary succeeds even if $M = M'$ but $\mathtt{tag} \neq \mathtt{tag}'$. Thus, the definition corresponds to what has been termed "strong" security in the context of signature schemes.

2.4 Universal One-way Hash Function

The notion of universal one-way hash function UOWHF was introduced by Naor and Yung [35] and is defined as follow.

Definition 4. *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 [34] 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 [35] 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 and Relative Problems

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

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

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

A central problem in the computational study of lattices is the *Shortest Vector Problem* (SVP): given a lattice basis $\mathbf{B}$, find a nonzero lattice vector $\mathbf{Bx} \neq 0$ achieving the minimum distance $\|\mathbf{Bx}\|=\lambda_1(\mathcal{L}(\mathbf{B}))$. A γ-approximate solution to the shortest vector problem (SVP$_\gamma$) is defined as follows, where $\gamma = \gamma(n)$ is the approximation factor as a function of the dimension.

Definition 5. **(SVP$_\gamma$)**. *Given a lattice basis* $\mathbf{B}$*, find a nonzero lattice vector* $\boldsymbol{v}$ *such that* $\|\boldsymbol{v}\|\leq \gamma\lambda_1(\mathcal{L}(\mathbf{B}))$.

The problem underlying public key cryptosystems, e.g, R04, A05, and AD$_{\mathtt{GGH}}$ can be described as a restriction of SVP$_\gamma$ to a special class of lattices, namely lattices such that $\lambda_2(\mathcal{L}(\mathbf{B})) > \gamma\lambda_1(\mathcal{L}(\mathbf{B}))$, The restriction of SVP$_\gamma$ to such lattices is usually referred to as the unique shortest vector problem (uSVP$_\gamma$).

Definition 6. **(uSVP$_\gamma$)**. *Given a lattice basis* $\mathbf{B}$ *such that* $\lambda_2(\mathcal{L}(\mathbf{B})) > \gamma\lambda_1(\mathcal{L}(\mathbf{B}))$*, find a nonzero lattice vector* $\boldsymbol{v} \in \mathcal{L}(\mathbf{B})$ *of length* $\lambda_1(\mathcal{L}(\mathbf{B}))$.

The name of this problem is motivated by the fact that in such lattices the shortest nonzero vector $\boldsymbol{v}$ is unique, in the sense that any vector of length less than $\gamma\lambda_1(\mathcal{L}(\mathbf{B}))$ is parallel to $\boldsymbol{v}$. It is also easy to see that for such lattices, finding a γ-approximate solution to SVP$_\gamma$ is equivalent to finding the shortest nonzero lattice vector exactly.

2.6 Probability Distributions

Here, we give several useful distributions on the segment [0, 1). For $\alpha \in \mathbb{R}^+$, the distribution $\mathcal{Q}_\alpha$ is a normal distribution with mean 0 and variance $\frac{\alpha^2}{2\pi}$ reduced modulo 1 (i.e., a periodization of the normal distribution):

$$\mathcal{Q}_\alpha(r) = \sum_{k=-\infty}^{\infty} \frac{1}{\alpha} e^{-\pi(\frac{r-k}{\alpha})^2}$$

Apparently, one can efficiently sample from $\mathcal{Q}_\alpha$ by sampling a normal variable and reducing the result modulo 1. Another distribution is $\Phi_{\mu,\alpha}$, where $\mu \in \mathbb{N}$ and $\alpha \in \mathbb{R}^+$. Its density function is defined as:

$$\Phi_{\mu,\alpha}(r) = \mathcal{Q}_\alpha(r\mu \bmod 1) = \sum_{k=-\infty}^{\infty} \frac{1}{\alpha} e^{-\pi(\frac{r\mu-k}{\alpha})^2}$$

By adding a normalization factor we can extend the definition of $\Phi_{\mu,\alpha}$ to non-integer μ. So in general,

$$\Phi_{\mu,\alpha}(r) = \frac{1}{\int_0^1 \mathcal{Q}_\alpha(r\mu \bmod 1)dx} \mathcal{Q}_\alpha(r\mu \bmod 1)$$

Here, we recall a sampling procedure which was proposed in [1] and which is used later, i.e., for a real μ, we can sample values according to $\Phi_{\mu,\alpha}$ by using samples from $\mathcal{Q}_\alpha$: (1) We sample $x \in \{0, \ldots, \lceil \mu \rceil\}$ uniformly at random; (2) Then, sample y according to $\mathcal{Q}_\alpha$; (3) If $0 \leq (x + y)/\mu < 1$, we then take the value as a sample. Otherwise, we repeat (1) and (2).

3 Matrix Encryption

This section defines the notion of matrix encryption (ME) and presents a construction of MB scheme based on lattice.

3.1 Notion of Matrix Encryption

Matrix encryption plays an important role in constructing a CCA-security cryptosystem later. Here, we give a formal definition to it as follows:

Definition 7. *A matrix encryption scheme (ME) is a triple of* PPT *algorithms* $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ *such that:*

- *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)* $\leftarrow \mathcal{G}(1^n)$.
- *The randomized encryption algorithm* $\mathcal{E}$ *takes as input a public key pk and a message* $\mathbf{X} \in \mathbb{Z}_2^{h\times w}$, *and outputs a ciphertext* $\boldsymbol{c}$. *We write* $\boldsymbol{c} = \mathcal{E}_{pk}(\mathbf{X})$.
- *The decryption algorithm* $\mathcal{D}$ *takes as input a ciphertext* $\mathbf{c}$ *and a secret key sk. It returns a message* $\mathbf{X} \in \mathbb{Z}_2^{h\times w}$, *or the distinguished symbol* $\perp$. *We write* $\mathbf{X} = \mathcal{D}_{sk}(\boldsymbol{c})$.

Generally, the standard completeness requirement is that, for all (pk, sk) output by $\mathcal{G}$, all $\mathbf{X} \in \mathbb{Z}_2^{h \times w}$, and all $\boldsymbol{c}$ output by $\mathcal{E}_{pk}(\mathbf{X})$, we have $\mathcal{D}_{sk}(\boldsymbol{c}) = \mathbf{X}$. We relax this notion to require that decryption is correct with overwhelming probability over all the randomness of the algorithms.

For a secure ME scheme, we present the following the definition. While this definition is a weaker notion of security, it suffices for our applications.

Definition 8. (*Restricted CPA Security*). *A matrix encryption scheme as Definition 7 is secure against restricted chosen plaintext attacks (i.e., is "RCPA-secure") if the advantage of any* `PPT` *adversary $\mathcal{A}$ in the following game is negligible in the security parameter n:*

- *$\mathcal{G}(1^n)$ outputs (pk, sk). Adversary $\mathcal{A}$ is given 1^n and pk.*
- *$\mathcal{A}$ outputs two different messages $\mathbf{X}_0 = (\boldsymbol{x}_{10}, \dots, \boldsymbol{x}_{w0})$, $\mathbf{X}_1 = (\boldsymbol{x}_{11}, \dots, \boldsymbol{x}_{w1}) \in \mathbb{Z}_2^{h \times w}$ with $\|\boldsymbol{x}_{i0}\| = \|\boldsymbol{x}_{i1}\|$, $i \in [w]$. A bit $b \in \{0, 1\}$ is randomly chosen and the adversary is given a challenge ciphertext $\boldsymbol{c}^* \leftarrow \mathcal{E}_{pk}(\mathbf{X}_b)$.*
- *Finally, $\mathcal{A}$ outputs a guess b'.*

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

3.2 Pseudohomomorphism

In [3], Akinori Kawachi *et al.* proposed multi-bit lattice-based cryptosystems mR04, mR05, mA05, mAD$_{\mathtt{GGH}}$ based on R04 [1], R05 [2], A05 [5], and AD$_{\mathtt{GGH}}$ [7], respectively. These four multi-bit lattice-based cryptosystems have a common property, i.e., *pseudohomomorphism*. This *pseudohomomorphism* of ciphertexts is just crucial to the construction of matrix encryption scheme based on mR04, mR05, mA05, mAD$_{\mathtt{GGH}}$. We will show this property with mR04.

The cryptosystem mR04 can be parameterized by three integers m, N, p, a density function $\Phi_{\mu,\alpha}$, 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 p to be some prime number between 2 and n^r, let $N = 2^{8n^2}$, $m = c_0 n^2$ where c_0 is a sufficiently large constant, and $\delta(n) = \omega(n^{1+r}\sqrt{\log n})$. mR04 proceeds as follows.

- **Common Parameter**: Given security parameter n, parameters m, N, p, r, $\delta(n)$, and the density function $\Phi_{\mu,\alpha}$ are taken according the description of Section 2.6.
- **Key Generation**: Let $\mathrm{U}_r = \{\mu \in [\sqrt{N}, 2\sqrt{N}) : \mathrm{frc}(\mu) < 1/(8n^r m)\}$. We choose $\mu \in \mathrm{U}_r$ uniformly at random and set $d = N/\mu$. Choosing $\alpha \in [2/\delta(n)$,$(2\sqrt{2})/\delta(n))$, we sample m values $z_1, \dots, z_m$ from the distribution $\Phi_{\mu,\alpha}$ by choosing $x_1, \dots, x_m$ and $y_1, \dots, y_m$ as described in Section 2.6. Let $a_i = \lceil N z_i \rceil$, $i \in [m]$. Additionally, we choose an index i_0 uniformly at random from $\{i : x_i \neq \theta p, \theta \in \mathbb{Z}\}$. Then, we compute $k \equiv x_{i_0} \mathrm{mod} p$. The private key is (d, k) and the public key is $(a_1, \dots, a_m, i_0)$.

- **Encryption**: Choose a uniformly random subset S of $\{1,\ldots,m\}$. For a plaintext $M \in \{0,1,\ldots,p-1\}$ the ciphertext is $c = \lceil \frac{Ma_{i_0}}{p} \rfloor + \sum_{i\in S} \mathbf{a}_i$.
- **Decryption**: For a received ciphertext c, compute $\tau = c/d \text{mod} 1$, decrypt the ciphertext c to $\lceil p\tau \rfloor k^{-1} \text{mod} p$, where k^{-1} is the inverse of k in $\mathbb{Z}_p$.

Thus, the following two theorems show the pseudohomomorphism property of mR04. On the pseudohomomorphism property of other three multi-bit encryption schemes, please refer for [3].

Theorem 1. *Let $\delta(n) = \omega(n^{1+r}\sqrt{\log n})$. Also let $p(n)$ be a prime 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 $\sum_{i=1}^{\kappa} \mathcal{E}^{mR04}(\sigma_i)$ into $\sum_{i=1}^{\kappa}(\sigma_i) mod\, p$ with decryption error probability at most $2^{-\Omega(\delta(n)^2/n^{2r}m)}$.*

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 $(\sum_{i=1}^{\kappa} \mathcal{E}^{mR04}(\sigma_i), pk)$ and $(\sum_{i=1}^{\kappa} \mathcal{E}^{mR04}(\sigma'_i), pk)$, then there exists a probabilistic polynomial-time algorithm $\mathcal{A}$ that solves the worst case of $\text{uSVP}_{\widetilde{O}(\delta(n)\sqrt{n})}$ in the case of mR04.*

3.3 Construction of ME

In this subsection, we give an matrix encryption (meR04) from mR04.

Before giving this matrix encryption, we introduce two operators which will be needed. Given matrices $\mathbf{B} = (\mathbf{b}_1,\ldots,\mathbf{b}_w) \in \mathbb{Z}_p^{h\times w}$, $\mathbf{X} = (\mathbf{x}_1,\ldots,\mathbf{x}_w) \in \mathbb{Z}_2^{h\times w}$, $\mathbf{V} = (\mathbf{v}_1,\ldots,\mathbf{v}_{h\times w}) \in \mathbb{Z}_2^{m\times(h\times w)}$ and $\mathbf{a} \in \mathbb{Z}_N^m$, we define:

$$\begin{aligned} \mathbf{B} * \mathbf{X} &:= (<\mathbf{x}_1, \mathbf{b}_1>, \ldots, <\mathbf{x}_w, \mathbf{b}_w>) \\ \mathbf{a} \otimes \mathbf{V} &:= (w_{ij}) \in \mathbb{Z}_N^{h\times w}, \text{where } w_{ij} =< \mathbf{v}_{(i-1)w+j}, \mathbf{a} > \end{aligned}$$

The matrix encryption scheme meR04 proceeds as follows.

- **Common Parameter**: Given security parameter n, parameters m, N, r, $\delta(n)$, and the density function $\Phi_{\mu,\alpha}$ are taken as mR04, except that p be a prime such that $\lfloor \lg p \rfloor p \leq n^r = o(n)$, $h = \lfloor \lg p \rfloor$. In addition, let $\mathbf{B} = (\mathbf{b}_1,\ldots,\mathbf{b}_w)$ and $\mathbf{b}_i = (b_{1i},\ldots,b_{hi})^T = (1,2,\ldots,2^{h-1})^T$, $i \in [w]$.
- **Key Generation**: Let $\text{U}_r = \{\mu \in [\sqrt{N}, 2\sqrt{N}) : \text{frc}(\mu) < 1/(8n^r m)\}$. We choose $\mu \in \text{U}_r$ uniformly at random and set $d = N/\mu$. Choosing $\alpha \in [2/\delta(n),(2\sqrt{2})/\delta(n))$, we sample m values z_1, ..., z_m from the distribution $\Phi_{\mu,\alpha}$ by choosing x_1, ..., x_m and y_1, ..., y_m as described in Section 2.6. Let $a_i = \lceil Nz_i \rceil$, $i \in [m]$. Additionally, we choose an index i_0 uniformly at random from $\{i : x_i \neq \theta p, \theta \in \mathbb{Z}\}$. Then, we compute $k \equiv x_{i_0} \text{mod} p$, and let $\mathbf{a} = (a_1,\ldots,a_m)$. The private key sk is (d,k) and the public key pk is $(\mathbf{a}, i_0)$.
- **Encryption**: To encrypt $\mathbf{X} = (x_{ij}) = (\mathbf{x}_1,\ldots,\mathbf{x}_w) \in \mathbb{Z}_2^{h\times w}$, do the following:
  1. Generate the matrix $\mathbf{V} = (\mathbf{v}_1,\ldots,\mathbf{v}_{h\times w}) \in \mathbb{Z}_2^{m\times(h\times w)}$, where each $\mathbf{v}_i$ $(i \in [h\times w])$ is chosen independently and uniformly from $\mathbb{Z}_2^m$ at random.

2. Compute $\mathbf{U} = (u_{ij})$, where $u_{ij} = \lceil \frac{2^i a_{i0}}{p} \rfloor$, $i \in [h], j \in [w]$.
3. Compute $\mathbf{C} = (c_{ij}) = \mathbf{a} \otimes \mathbf{V} + \mathbf{U}$, where $c_{ij} = \mathcal{E}_{pk}^{mR04}(2^i) = (< \mathbf{v}_{(i-1)w+j}, \mathbf{a} > + u_{ij})$.
4. Compute
$$\mathbf{c} = \mathbf{C} * \mathbf{X} = (c_1, \ldots, c_w) = (\sum_{i=1}^{h} x_{i1} \mathcal{E}_{pk}^{mR04}(2^i), \ldots, \sum_{i=1}^{h} x_{iw} \mathcal{E}_{pk}^{mR04}(2^i)).$$

- **Decryption**: For a received ciphertext $\mathbf{c}$, do the following:
  1. Compute $\mathbf{B} * \mathbf{X} = (\mathcal{D}_{sk}^{mR04}(c_1), \ldots, \mathcal{D}_{sk}^{mR04}(c_w))$,
  2. compute $\mathbf{X}$ from $\mathbf{B} * \mathbf{X}$.

Theorem 3. *Let $\delta(n) = \omega(n^{1+r}\sqrt{\log n})$. Also let $p(n)$ be a prime such that $\lfloor \lg p \rfloor p \leq n^r = o(n)$ for any constant $0 < r < 1$. If there exists an adversary $\mathcal{A}$ that breaks meR04 under restrictedly chosen plaintext attack, then there exists a probabilistic polynomial-time algorithm $\mathcal{C}$ that solves the worst case of* uSVP$_{\widetilde{O}(\delta(n)\sqrt{n})}$ *in the case of meR04.*

Proof. See Appendix A.

By the above description of meR04, it is evident that we mainly make use of the pseudohomomorphism property of mR04 whether in the construction of meR04 or in the security proof of meR04. Likwise, the above method of constructing meR04 adapts to mR05, mA05, mAD$_{\texttt{GGH}}$, i.e., we can simply construct matrix encryption scheme from mR05, mA05, mAD$_{\texttt{GGH}}$, rescpectively, since these three multi-bit lattice-based cryptosystems also have the pseudohomomorphism property. Because of the limited length of paper, we do not discuss the ME construction from them, respectively.

4 Construction of CCA-Security Cryptosystem

In this section, we present a CCA-security cryptosystem (CR04) from meR04. Likewise, we can also construct a CCA-security cryptosystem from the matrix encryption which is designed from any of mR04, mR05, mA05, mAD$_{\texttt{GGH}}$ and which is secure against restricted chosen plaintext attack (RCPA-security).

4.1 Description of CR04

We now describe our construction of CCA-security cryptosystem

- **Common Parameter**: Given security parameter n, parameters m, N, r, $\delta(n)$, and the density function $\Phi_{\mu,\alpha}$ are taken as mR04, except that p be a prime such that $\lfloor \lg p \rfloor p \leq n^r = o(n)$, $h = \lfloor \lg p \rfloor$. 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 $H_1 : \{0,1\}^{\ell} \to \mathbb{Z}_q$ is a hash function which is chosen from the family of universal one-way hash functions $\mathcal{H}_1$. 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 (`Mac`, `Vrfy`) be a message authentication code. Let $a \in \mathbb{Z}_q$ chosen uniformly at random. Define $f : \mathbb{Z}_q \times \mathbb{Z}_q \to \{0,1\}$ as follows:

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

- **Key Generation**: Let $\mathrm{U}_r=\{\mu\in[\sqrt{N},2\sqrt{N}):\mathrm{frc}(\mu)<1/(8n^r m)\}$. We choose $\mu_0,\mu_1\in\mathrm{U}_r$ uniformly at random and set $d_0=N/\mu_0, d_1=N/\mu_1$. Choosing $\alpha_0,\alpha_1\in[2/\delta(n),(2\sqrt{2})/\delta(n))$, we sample m values $z_1^0,\ldots,z_m^0$ from the distribution Φ_{μ_0,α_0} and m values $z_1^1,\ldots,z_m^1$ from the distribution Φ_{μ_1,α_1} as meR04, respectively. Let $a_i^0=\lceil Nz_i^0\rceil$, $a_i^1=\lceil Nz_i^1\rceil$, $i\in[m]$. Additionally, we choose two indices i_0,i_1 uniformly at random from $\{i:x_i^0\neq\theta p,\theta\in\mathbb{Z}\}$ and $\{i:x_i^1\neq\theta p,\theta\in\mathbb{Z}\}$, respectively. Then, we compute $k_0\equiv x_{i_0}\mathrm{mod}p$ and $k_1\equiv x_{i_1}\mathrm{mod}p$, and let $\mathbf{a}_0=(a_1^0,\ldots,a_m^0)$ and $\mathbf{a}_1=(a_1^1,\ldots,a_m^1)$. The private key sk is $(d_{00},k_{00};d_{11},k_{11})=(d_0-d_1,k_0-k_1;d_1,k_1)$ and the public key pk is $(\mathbf{a}_{00},i_{00};\mathbf{a}_{11},i_{11})=(\mathbf{a}_0-\mathbf{a}_1,i_0-i_1;\mathbf{a}_1,i_1)$.
- **Encryption**: $\mathcal{E}$ takes as input (pk,M) where $pk=(\mathbf{a}_{00},i_{00};\mathbf{a}_{11},i_{11})$ is the public key and $M\in\{0,1\}^k$ is the message.
  1. Choose a $\mathtt{str}\in\{0,1\}^\ell$ uniformly at random and compute $t=H_1(\mathtt{str})$.
  2. Compute $pk_{meR04}=(\mathbf{a}_{11}+f(t,a)\mathbf{a}_{00},i_{11}+f(t,a)i_{00})$
  3. Choose $\mathbf{X}=(x_{ij})=(\mathbf{x}_1,\ldots,\mathbf{x}_w)\in\mathbb{Z}_2^{h\times w}$ at random and compute
  $$\mathbf{c}=\mathcal{E}^{meR04}_{pk_{meR04}}(\mathbf{X}),\qquad c_0=H_2(\mathbf{X})\bigoplus M.$$
  4. Using $\mathbf{X}$ as a key for a message authentication code; i.e., computes $\mathtt{tag}=\mathtt{Mac}_{\mathbf{X}}(\mathtt{str},\mathbf{c},c_0)$.
  5. The ciphertext c is output as $c=(\mathtt{str},\mathbf{c},c_0,\mathtt{tag})$.
- **Decryption**: $\mathcal{D}$ takes as input (sk,c) where $sk=(d_{00},k_{00};d_{11},k_{11})$ is private key and $c=(\mathtt{str},\mathbf{c},c_0,\mathtt{tag})$.
  1. Compute $H_1(\mathtt{str})=t$, and $sk_{meR04}=(d_{11}+f(t,a)d_{00},k_{11}+f(t,a)k_{00})$
  2. Compute $\mathbf{X}=\mathcal{D}^{meR04}_{sk_{meR04}}(\mathbf{c})$.
  3. Check that $\mathtt{Vrfy}_{\mathbf{X}}(\mathtt{str},\mathbf{c},c_0,\mathtt{tag})=1$; if not, it output $\perp$
  4. Output $c_0\oplus H_1(\mathbf{X})$.

4.2 Analysis of RC04

Given a ciphertext $c=(\mathtt{str},\mathbf{c},c_0,\mathtt{tag})$=($\mathtt{str}$, $\mathcal{E}^{meR04}_{pk_{meR04}}(\mathbf{X})$, $H_2(\mathbf{X})\bigoplus M$, $\mathtt{Mac}_{\mathbf{X}}$ ($\mathtt{str}$, $\mathbf{c},c_0$)), if $\mathcal{D}^{meR04}_{sk_{meR04}}(\mathbf{c})\neq\mathbf{X}$, the message authentication code $\mathtt{tag}$ can not be passed, i.e., $\mathtt{Vrfy}_{\mathbf{X}}(\mathtt{str},\mathbf{c},c_0,\mathtt{tag})\neq 1$. Thus, RC04 has not the error of decryption. Since $\mathbf{B}*\mathbf{X}=(\mathcal{D}^{mR04}_{sk_{meR04}}(c_1),\ldots,\mathcal{D}^{mR04}_{sk_{meR04}}(c_w))$ and $\mathbf{c}=\mathbf{C}*\mathbf{X}=(c_1,\ldots,c_w)$, we know that the decryption error probability of $\mathcal{D}^{mR04}_{sk_{meR04}}(c_i)$, $i\in[w]$, is at most $2^{-\Omega(\delta(n)^2/n^{2r}m)}$ with Theorem 1. In other words, RC04 possibly refuse a correct ciphertext and the rejective probability of a correct ciphertext is at most $(1-(1-2^{-\Omega(\delta(n)^2/n^{2r}m)})^w)$.

On the security of RC04, we have the following result.

Theorem 4. *If ($\mathtt{Mac}$, $\mathtt{Vrfy}$) is a strong one-time message authentication code, and hash functions H_1 and H_2 are universal one-way hash function, the above cryptosystem is secure against adaptive chosen ciphertext attack assuming that meR04 is secure against restrictedly chosen plaintext attack (i.e., RCPA-security).*

Proof. See Appendix B.

5 Conclusion

In this work, we present a CCA-secure cryptosystem CR04 and definite matrix encryption and a weaker notion of security, i.e., RCAP-security. Security of CR04 against adaptive chosen-ciphertext attacks is based on the restricted CPA-security of the matrix encryption scheme, then we reduce the indistinguishable pseudohomomorphism property of mR04 , which is based on the unique shortest vector problem (uSVP), to the restricted CPA-security of the matrix encryption scheme. So far as we know, CR04 is the first CCA-secure cryptosystem which is directly constructed from lattice and whose security is based on uSVP. Since lattice-based Cryptosystems mR05, mA05, $\text{mAD}_{\texttt{GGH}}$ like mR04 have the *pseudohomomorphism* property, the method, with which we construct CCA-secure CR04, adapts to mR05, mA05, $\text{mAD}_{\texttt{GGH}}$, i.e., we can construct CCA-secure cryptosystems from mR05, mA05, $\text{mAD}_{\texttt{GGH}}$, respectively. This results make our method constructing CR04 become generic and universal.

References

1. Oded Regev. New lattice-based cryptographic constructions. J. ACM, 51(6):899-942, 2004.
2. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In STOC, pages 84-93, 2005.
3. Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Multi-bit cryptosystems based on lattice problems. In PKC, pages 315-329, 2007.
4. Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In STOC, pages 187-196, 2008.
5. M. Ajtai. Representing hard lattices with $O(n \log n)$ bits. In STOC 2005, pages 94-103, 2005.
6. 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
7. 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.
8. Jin-Yi Cai and Thomas W. Cusick. A lattice-based public-key cryptosystem. Information and Computation, 151(1-2):17-31, 1999.
9. Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In CRYPTO'97, pages 112-131, 1997
10. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In ANTS-III, pages 267-288, 1998
11. 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.
12. Phong Q. Nguyen and David Pointcheval. Analysis and improvements of NTRU encryption paddings. In CRYPTO 2002, pages 210-225, 2002.

13. 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
14. 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.
15. S. Goldwasser and S. Micali. Probabilistic encryption. Journal of Computer and System Sciences, 28:270-299, 1984.
16. 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.
17. 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.
18. D. Dolev, C. Dwork, and M. Naor. Non-Malleable Cryptography. SIAM J. Computing 30(2): 391-437, 2000.
19. 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
20. 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.
21. U. Feige, D. Lapidot, and A. Shamir. Multiple Non-Interactive Zero-Knowledge Proofs Under General Assumptions. SIAM J. Computing 29(1): 1-28, 1999.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Advances in Cryptology-EUROCRYPT 2003. Springer-Verlag, 2003.
29. 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.
30. 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.

31. Brent Waters. Efficient identity based encryption without random oracles. In Advances in Cryptology-EUROCRYPT 2005, Lecture Notes in Computer Science. Springer Verlag, 2005
32. Dörte Rappe. Homomorphic cryptosystems and their applications. Ph.D. Thesis, University of Dortmund, 2004. Also available at http://eprint.iacr.org/2006/001.
33. Shafi Goldwasser and Dmitriy Kharchenko. Proof of plaintext knowledge for the Ajtai-Dwork cryptosystem. In TCC 2005, pages 529-555, 2005.
34. 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.
35. M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In 21st Annual ACM Symposium on Theory of Computing, 1989.

A The Proof of Theorem 3

Proof. Given any adversary $\mathcal{A}$ that breaks meR04 in restricted chosen plaintext attacks, we show how to construct an adversary $\mathcal{B}$ that successfully attacks the indistinguishable pseudohomomorphism property of mR04. The game between the challenger and the adversary $\mathcal{B}$ starts with the challenger first generating the public parameters of mR04 $\texttt{param} = (N, m, r, \mathbf{B}, \delta(n), \varPhi_{\mu,\alpha})$ and the public and corresponding private key pairs $(pk,\ sk)$. The challenger gives $\texttt{param}$ and pk to the adversary $\mathcal{B}$. The adversary $\mathcal{B}$ interacts with the adversary $\mathcal{A}$ as follows:

1. The adversary $\mathcal{B}$ relays $\texttt{param}$ and pk to the adversary $\mathcal{A}$.
2. The adversary $\mathcal{A}$ outputs two different messages $\mathbf{X}^0 = (\mathbf{x}_1^0, \ldots, \mathbf{x}_w^0)$, $\mathbf{X}^1$=($\mathbf{x}_1^1$, ..., $\mathbf{x}_w^1) \in \mathbb{Z}_2^{h\times w}$ with $||\mathbf{x}_i^0|| = ||\mathbf{x}_i^1||$, where $\mathbf{x}_i^0 = (x_{1i}^0, \ldots, x_{hi}^0)^T$, and $\mathbf{x}_i^1 = (x_{1i}^1, \ldots, x_{hi}^1)^T \in \mathbb{Z}_2^h$, $i \in [w]$. Without loss of generality, we assume that $\mathbf{x}_1^0 \neq \mathbf{x}_1^1$. The adversary $\mathcal{A}$ gives $\mathbf{X}^0$ and $\mathbf{X}^1$ to the adversary $\mathcal{B}$.
3. The adversary $\mathcal{B}$ relays $\mathbf{x}_1^0$ and $\mathbf{x}_1^1$ to the challenger.
4. The challenger generates ciphertexts $c^0 = \mathcal{E}_{pk}^{meR04}(\mathbf{x}_1^0) = \sum_{i=1}^h x_{i1}^0 \mathcal{E}_{pk}^{mR04}(2^{i-1})$ and $c^1 = \mathcal{E}_{pk}^{meR04}(\mathbf{x}_1^1) = \sum_{i=1}^h x_{i1}^1 \mathcal{E}_{pk}^{mR04}(2^{i-1})$, and gives them to the adversary $\mathcal{B}$.
5. The adversary $\mathcal{B}$ chooses a c^g from $\{c^0, c^1\}$ and a bit $b \in \{0, 1\}$ uniformly at random, respectively, and generates the following ciphertext
$$\mathbf{c}^b = (c^g, \sum_{i=1}^{h} x_{i2}^b \mathcal{E}_{pk}^{mR04}(2^{i-1}), \ldots, \sum_{i=1}^{h} x_{iw}^b \mathcal{E}_{pk}^{mR04}(2^{i-1}))$$
and gives it to $\mathcal{A}$.
6. Finally, $\mathcal{A}$ output a bit b'. $\mathcal{B}$ concludes its own game by outputting a guess as follows. If $b = b'$, then $\mathcal{B}$ outputs 1 meaning $c^g = c^b = \sum_{i=1}^h x_{i1}^b \mathcal{E}_{pk}^{mR04}(2^{i-1})$, otherwise, it outputs 0 meaning $c^g \neq c^b$.

In the above game, let $\texttt{Succ}$ denote the event that $\mathcal{B}$ outputs 1, $\texttt{Event}$ denote the event that $c^g = c^b$. If $c^g = c^b$, $\mathcal{B}$ provides a perfect simulation for $\mathcal{A}$ and succeeds with whenever $\mathcal{A}$ succeeds, i.e., the view of the adversary $\mathcal{A}$ is identical to its view in the real attack game. Therefore, in the case, $\mathcal{A}$ must satisfies $|\texttt{Pr}[b = b'] - 1/2| > \epsilon$ (Assuming that the adversary $\mathcal{A}$ breaks the our construction with at least advantage ϵ in restricted chosen plaintext attacks). On the other hand, if $c^g \neq c^b$, ciphertext $\mathbf{c}^b$ is independent of b in the view of adversary $\mathcal{A}$, then $\mathtt{Pr}[b = b'] = 1/2$. Then we have

$$\begin{aligned} |\mathtt{Pr}[\mathcal{B}(\mathtt{param}, pk, c^0) = 1] - \mathtt{Pr}[\mathcal{B}(\mathtt{param}, pk, c^1) = 1| \\ &= |\mathtt{Pr}[\ \mathtt{Succ}|\mathtt{Event}\ ] - \mathtt{Pr}[\ \mathtt{Succ}|\ \overline{\mathtt{Event}}\ ]| \\ &\geq |1/2 \pm \epsilon - 1/2| = \epsilon \end{aligned}$$

Thus, $\mathcal{B}$ can distinguish $c^0 = \sum_{i=1}^{h} x_{i1}^0 \mathcal{E}_{pk}^{mR04}(2^{i-1})$ and $c^1 = \sum_{i=1}^{h} x_{i1}^1 \mathcal{E}_{pk}^{mR04}(2^{i-1})$ with non-negligible advantage. According to Theorem 2 (i.e., the indistinguishable pseudohomomorphism property of mR04), we can construct an algorithm $\mathcal{C}$ that uses the adversary $\mathcal{B}$ to solve the worst case of uSVP$_{\tilde{O}(\delta(n)\sqrt{n})}$.

B The Proof of Theorem 4

Proof. Given any adversary $\mathcal{A}$ that breaks our construction in adaptive chosen ciphertext attacks, we show how to construct an adversary $\mathcal{B}$ that successfully breaks meR04 in restricted chosen plaintext attacks.

The game between the challenger and $\mathcal{B}$ starts with the challenger first generating the public parameters of meR04 $\mathtt{param} =< N, m, r, p$, $\mathbf{B}$, $\delta(n)$, $\Phi_{\mu,\alpha} >$, and the public key $pk = (\mathbf{a}_0, i_0)$ and the corresponding private key $sk = (d_0, k_0)$. The challenger interacts with the adversary $\mathcal{B}$ as follows:

1. The challenger gives $\mathtt{param}$ and pk to $\mathcal{B}$.
2. $\mathcal{B}$ outputs two different messages $\mathbf{X}_0 = (\mathbf{x}_1^0, \ldots, \mathbf{x}_w^0)$, $\mathbf{X}_1 = (\mathbf{x}_1^1, \ldots, \mathbf{x}_w^1) \in \mathbb{Z}_2^{h\times w}$ with $||\mathbf{x}_i^0|| = ||\mathbf{x}_i^1||$, where $\mathbf{x}_i^0 = (x_{1i}^0, \ldots, x_{hi}^0)^T$, and $\mathbf{x}_i^1 = (x_{1i}^1, \ldots, x_{hi}^1)^T \in \mathbb{Z}_2^h$, $i \in [w]$, and gives $\mathbf{X}_0$ and $\mathbf{X}_1$ to the challenger.
3. The challenger randomly chooses a bit $b \in \{0, 1\}$ and generates ciphertext $\mathbf{c}_b^* = \mathcal{E}_{pk}^{meR04}(\mathbf{X}_b)$ and gives it to $\mathcal{B}$.

Next, $\mathcal{B}$ uses $\mathtt{param}$ and (pk, sk) which are given by the challenger and generates the parameters $\mathtt{param}^*$ and the public and corresponding private key pair(pk^*, sk^*) of our construction as follows.

1. Let $\mathrm{U}_r = \{\mu \in [\sqrt{N}, 2\sqrt{N}) : \mathrm{frc}(\mu) < 1/(8n^r m)\}$, choose $\mu_1 \in H_r$ uniformly at random and set $d_1 = N/\mu_1$.
2. Choose $\alpha_1 \in [2/\delta(n)$,$(2\sqrt{2})/\delta(n))$, and sample m values $z_1^1, \ldots, z_m^1$ from the distribution Φ_{μ_1,α_1} by choosing $x_1^1, \ldots, x_m^1$ and $y_1^1, \ldots, y_m^1$ as described in Section 2.6.
3. Let $a_i^1 = \lceil N z_i^1 \rceil$, $i \in [m]$, choose an index i_1 uniformly at random from $\{i : x_i^1 \neq \theta p, \theta \in \mathbb{Z}\}$, compute $k_1 \equiv x_{i_1} \mathrm{mod} p$, and let $\mathbf{a}_1 = (a_1^1, \ldots, a_m^1)$.
4. The private key sk^* is $(d_{00}, k_{00}; d_{11}, k_{11}) = (d_1 - d_0, k_1 - k_0; d_0, k_0)$, where $\mathcal{B}$ does not know d_0 and k_0, and the public key pk^* is $(\mathbf{a}_{00}, i_{00}; \mathbf{a}_{11}, i_{11}) = (\mathbf{a}_1 - \mathbf{a}_0, i_1 - i_0; \mathbf{a}_0, i_0)$.
5. Choose two hash functions $H_1 : \{0, 1\}^\ell \to \mathbb{Z}_q$ and $H_2 : \{0, 1\}^{h\times w} \to \{0, 1\}^k$ from the family of universal one-way hash functions $\mathcal{H}_1$ and from the family of universal one-way hash functions $\mathcal{H}_2$, respectively, and define the function $f : \mathbb{Z}_q \times \mathbb{Z}_q \to \{0, 1\}$ as follows:

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

.

6. Choose a $\texttt{str}^* \in \{0,1\}^\ell$, compute $a = H_1(\texttt{str}^*)$, let ($\texttt{Mac}$, $\texttt{Vrfy}$) be a message authentication scheme, and set the parameters of our construction $\texttt{param}^* =< \texttt{param}, H_1, H_2, a, f, (\texttt{Mac}, \texttt{Vrfy}) >$.

Then, $\mathcal{B}$ interacts with $\mathcal{A}$ as follows.

1. Give the $\texttt{param}^*$ and pk^* to $\mathcal{A}$
2. When $\mathcal{A}$ makes decryption oracle query $\mathcal{D}(c)$, where $c = (\texttt{str}, \mathbf{c}, c_0, \texttt{tag})$, the adversary $\mathcal{B}$ proceeds as follows:
   1. Compute $H_1(\texttt{str}) = a'$. If $a' = a$, aborts and output $\perp$.
   2. Compute $sk_{meR04} = (d_{11} + f(a', a)d_{00}, k_{11} + f(a', a)k_{00})$
   2. Compute $\mathbf{X} = \mathcal{D}^{meR04}_{sk_{meR04}}(\mathbf{c})$.
   4. Check that $\texttt{Vrfy}_{\mathbf{X}}(\texttt{str}, \mathbf{c}, c_0, \texttt{tag}) = 1$; if not, it output $\perp$
   5. Output $c_0 \oplus H_1(\mathbf{X})$.
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 adversary $\mathcal{B}$ responds as follows:
   (1) Randomly choose $g, g_0 \in \{0,1\}$, and compute $c_0^* = H_2(\mathbf{X}_g) \oplus m_{g_0}$
   (2) Using $\mathbf{X}_g$ as a key for a message authentication code; i.e., computes $\texttt{tag}^* = \texttt{Mac}_{\mathbf{X}_g}(\texttt{str}^*, \mathbf{c}_b^*, c_0^*)$.
   (3) Return ciphertext $c^* = (\texttt{str}^*, \mathbf{c}_b^*, c_0^*, \texttt{tag}^*)$ to $\mathcal{A}$.
4. Finally, $\mathcal{A}$ outputs a bit g_0'. If g_0=g_0', $\mathcal{B}$ outputs a guessing bit b'=g; otherwise, outputs a guessing bit b'=$1 - g$.

In $\mathcal{B}$'s interaction with $\mathcal{A}$, let $\texttt{Succ}$ denote the event that $b = b'$, $\texttt{Succ}_0$ denote the event that $b = g$, $\texttt{Fail}$ denote the event that $\mathcal{A}$ issues a decryption query for $c = (\texttt{str}, \mathbf{c}, c_0, \texttt{tag})$ with $H_1(\texttt{str}) = a$. Apparently, if the event $\texttt{Succ}_0$ occurs, $\mathcal{B}$ provides a perfect simulation for $\mathcal{A}$, thus $\mathcal{B}$ succeeds with whenever $\mathcal{A}$ succeeds unless that the event $\texttt{Fail}$ occurs, however, the probability that the above case happens is negligible, since H_1 is a universal one-way hash function, in which case $|\texttt{Pr}[g_0 = g_0'] - 1/2| > \epsilon$ (Assuming that $\mathcal{A}$ breaks the our construction with at least advantage ϵ in adaptive chosen cipherext attacks). If the event $\overline{\texttt{Succ}_0}$ occurs, that g_0 is independent of the adversary's view, since the ciphertext c^* is invalid with overwhelming probability, and H_2 is the universal one-way hash, in which case $\texttt{Pr}[g_0 \neq g_0'] = 1/2$. Thus, we have the following result:

$$\begin{aligned}
|\texttt{Pr(Succ)} - \frac{1}{2}| &= |\texttt{Pr(Succ} \wedge \texttt{Succ}_0) + \texttt{Pr(Succ} \wedge \overline{\texttt{Succ}_0}) - \frac{1}{2}| \\
&= |\texttt{Pr(Succ}|\texttt{Succ}_0)\texttt{Pr(Succ}_0) + \texttt{Pr(Succ}|\overline{\texttt{Succ}_0})\texttt{Pr(}\overline{\texttt{Succ}_0}) - \frac{1}{2}| \\
&= |\frac{1}{2}\texttt{Pr(Succ}|\texttt{Succ}_0) + \frac{1}{2}\texttt{Pr(Succ}|\overline{\texttt{Succ}_0}) - \frac{1}{2}| \\
&\geq |\frac{1}{2}[\texttt{Pr}(g_0 = g_0'|\texttt{Succ}_0) - \texttt{Pr(Fail}|\texttt{Succ}_0) + \texttt{Pr}(g_0 \neq g_0'|\overline{\texttt{Succ}_0})] - \frac{1}{2}| \\
&\geq |\frac{1}{2}[\frac{1}{2} \pm \epsilon - \texttt{Pr(Fail}|\texttt{Succ}_0) - \frac{1}{2}] - \frac{1}{2}| \\
&\geq |\frac{1}{2}[\epsilon - \texttt{Pr(Fail}|\texttt{Succ}_0)]|
\end{aligned}$$

Since $\texttt{Pr(Fail}|\texttt{Succ}_0)$ is negligible, $|\texttt{Pr(Succ)} - \frac{1}{2}| > \frac{1}{4}\epsilon$.