ISSN 1342-2812

Research Reports on
Mathematical and
Computing Sciences

Proof of Plaintext Knowledge for the Regev Cryptosystems

Keita Xagawa, Akinori Kawachi, and Keisuke Tanaka

January 2007, C–236

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

Proof of Plaintext Knowledge for the Regev Cryptosystems

Keita Xagawa, Akinori Kawachi, and Keisuke Tanaka

Dept. of Mathematical and Computing Sciences
Tokyo Institute of Technology
W8-55, 2-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan
{xagawa5, kawachi, keisuke}@is.titech.ac.jp

January, 2007

Abstract

Goldwasser and Kharchenko (TCC 2006) showed a proof of plaintext knowledge for the Ajtai-Dwork cryptosystem and left the open problem designing a proof of plaintext knowledge for the Regev'04 cryptosystem (JACM 2004). In this paper, we show a proof of plaintext knowledge for the Regev'04 cryptosystem (JACM 2004) using their technique. Furthermore, we show that it can be applied to the Regev'05 cryptosystem (STOC 2005). The key idea is to analyze tradeoffs between the hardness of the underlying lattice problem and the variance of ciphertexts, which given by Kawachi, Tanaka, and Xagawa (SCIS 2006).

Keywords: proof of plaintext knowledge, lattice-based cryptosystem, verifiable encryption.

1 Introduction

In the last decade, the lattice-based public-key cryptosystems have been studied. In 1997, Ajtai and Dwork constructed three public-key cryptosystems based on unique shortest vector problem [2]. Recently, Regev proposed two public-key cryptosystems [14, 15], which we call R04 and R05. Ajtai also introduced a public-key cryptosystem [1].

There were many zero knowledges and proofs of knowledge for number theoretic cryptosystems. However, there were a few zero-knowledge proofs and proofs of knowledge for lattice-based cryptosystems; Goldreich and Goldwasser [6], Micciancio and Vadhan [12], and Goldwasser and Kharchenko [8]. In [8] they left the open problem to design a proof of plaintext knowledge for R04. Following Goldwasser and Kharchenko, we construct proofs of plaintext knowledge for R04, and furthermore for R05.

Proof of Plaintext Knowledge. Given an instance of a public-key cryptosystem with public key pk, a proof of plaintext knowledge (PPK) allows a prover to prove knowledge of the plaintext m of ciphertext $c \in E_{\mathsf{pk}}(m)$ to a verifier. If both the prover and the verifier are online, IND-CPA public-key cryptosystems with PPK protocol achieves interactive IND-CCA1 security [4, 5]. It was known that efficient PPKs for the number-theoretic public-key cryptosystems, such that Rabin, RSA, El-Gamal, and etc., using zero-knowledge public-coin proofs of knowledge protocols with 3 rounds (known as Σ-protocol). However, efficient PPKs for the lattice-based cryptosystems were not known except that in [8].

Summary of Our Results. We construct PPK protocols for slightly modified versions of R04 and R05 based on the protocol in [8].

We show the relation between ciphertexts of cryptosystems, R04 and R05, and instances of GapCVP_{γ}. Although the cryptosystems are less secure than the original ones, we can show that their security are based on the worst-case of certain lattice problems as in Kawachi, Tanaka, and Xagawa [9]. Unfortunately, we cannot show the relation between ciphertexts of the original cryptosystems and GapCVP$_\gamma$ with our effort.

Our connection between the ciphertexts and GapCVP$_\gamma$ implies that if we set large factor for the underlying lattice problems, for small n, the LLL algorithm [10] heuristically succeed to distinguish ciphertexts of 0 and 1. From the positive view, we can apply Micciancio and Vadhan's zero-knowledge protocol for GapCVP$_\gamma$ [12] and obtain a verifiable encryption scheme. Based on the protocol in [8] and the above connection, we construct a proof of plaintext knowledge for R04 and R05.

Organization. The rest of this paper is organized as follows: We first describe basic notions and notations and briefly review tools in Section 2. In Section 3 we briefly review R04 and describe a proof of plaintext knowledge for R04. In Section 4 we review R05 and describe a proof of plaintext knowledge for R05.

2 Preliminaries

We define a negligible amount in n as an amount that is asymptotically smaller than n^{-c} for any constant $c > 0$. More formally, $f(n)$ is a negligible function in n if $lim_{n\to\infty} n^c f(n) = 0$ for any $c > 0$. Similarly, a non-negligible amount is one which is at least n^{-c} from some $c > 0$.

The length of a vector $\mathbf{x} = {}^t(x_1, \ldots, x_n) \in \mathbb{R}^n$, denoted by $\|\mathbf{x}\|$, is $(\sum_{i=1}^n x_i^2)^{1/2}$. For any field K, the inner product of two vectors $\mathbf{x} = {}^t(x_1, \ldots, x_n) \in K^n$ and $\mathbf{y} = {}^t(y_1, \ldots, y_n) \in K^n$, denoted by $\langle \mathbf{x}, \mathbf{y} \rangle$, is $\sum_{i=1}^n x_i y_i$. For m-bit string $r \in \{0,1\}^m$, r_i denotes i-th bit of r (i.e., $r = r_1 \ldots r_m$). We define $\mathbf{I}_n$ as the n by n identity matrix. We also define $\mathbf{u}_i \in \mathbb{R}^n$ as an n-dimensional vector whose i-th coordinate is 1 and other coordinates are all 0. For any vector $\mathbf{x} \in \mathbb{R}^n$ and a set $S \subseteq \mathbb{R}^n$ we define $\mathrm{Dist}(\mathbf{x}, S) = \inf_{\mathbf{y} \in S} \|\mathbf{y} - \mathbf{x}\|$. For two real numbers x and $y > 0$ we define $x \bmod y$ as $x - \lfloor x/y \rfloor y$. For $x \in \mathbb{R}$ we define $\lfloor x \rceil$ as the integer nearest to x, more formally $\lfloor x - 1/2 \rfloor$. We also use the notation $\mathrm{frc}\,(x) := |x - \lfloor x \rceil|$, i.e., the distance of a real x to the nearest integer. Notice that for $x, y \in \mathbb{R}$, $0 \leq \mathrm{frc}\,(x) \leq 1/2$, $\mathrm{frc}\,(x) \leq |x|$, and $\mathrm{frc}\,(x+y) \leq \mathrm{frc}\,(x) + \mathrm{frc}\,(y)$. For an element $x \in \mathbb{Z}_q$ we define $|x|_q$ as the integer x if $x \in \{0, 1, \ldots, \lfloor q/2 \rfloor\}$ and as the integer $q - x$ otherwise. In other words, $|x|_q$ represents the distance of x from 0 in $\mathbb{Z}_q$.

Gaussian and other distributions. The normal distribution with mean 0 and variance σ^2 is the distribution on $\mathbb{R}$ given by the density function $(1/\sqrt{2\pi}\sigma)\exp(-(x/\sigma)^2/2)$. The sum of two independent normal variables with mean m_1 and m_2 and variance σ_1^2 and σ_2^2 is a normal variable with mean $m_1 + m_2$ and variance $\sigma_1^2 + \sigma_2^2$. For a n-dimensional vector $\mathbf{x}$ and any $s > 0$, let $\rho_s^{(n)}(\mathbf{x}) = \exp(-\pi \|\mathbf{x}/s\|^2)$ be a Gaussian function scaled by a factor of s. Also, $\nu_s^{(n)} := \rho_s^{(n)}/s^n$ is an n-dimensional probability density function. For $\alpha \in \mathbb{R}^+$ the distribution Ψ_α is the distribution on $[0, 1)$ obtained by sampling from a normal variable with mean 0 and variance $\alpha^2/(2\pi)$ and reducing the result modulo 1:

$$\Psi_\alpha(r) := \sum_{k \in \mathbb{Z}} \frac{1}{\alpha} \exp\left(-\pi \left(\frac{r-k}{\alpha} \right)^2 \right).$$

This distribution is obtained by "folding" a Gaussian distribution $N(0, \alpha^2/(2\pi))$ on $\mathbb{R}$ into the interval $[0, 1)$. Based on this distribution, the Regev'04 cryptosystem makes use of a periodic distribution $\Phi_{h,\alpha}$ defined by the density function $\Phi_{h,\alpha}(r) := \Psi_\alpha(rh \bmod 1)$. We can sample values according to this distribution by using samples from Ψ_α, as shown in [14]: (1) We sample $x \in \{0, 1, \ldots, \lceil h \rceil\}$ uniformly at random and then (2) sample y according to Ψ_α. (3) If $0 \leq (x + y)/h < 1$, we then take the value as a sample. Otherwise, we repeat.

For an arbitrary probability distribution with a density function $\phi : \mathbb{T} \to \mathbb{R}^+$ and some integer $q > 0$, we define its discretization $\bar{\phi} : \mathbb{Z}_q \to \mathbb{R}^+$ as the discrete probability distribution obtained by sampling from ϕ, multiplying by q, and rounding to the closest integer modulo q. More formally,

$$\bar{\phi}(i) := \int_{(i-1/2)q}^{(i+1/2)q} \phi(x) dx.$$

We use the following lemma in [14] to bound the tail of Gaussian distribution.

Lemma 2.1 ([14])**.** *The probability that the distance of a normal variable with variance σ^2 from its mean is more than t is at most $\sqrt{2/\pi}(\sigma/t)\exp(-(t/\sigma)^2/2)$. That is,* $\Pr_{x\sim N(m,\sigma^2)}[|x-m|>t] \leq \sqrt{2/\pi}(\sigma/t)\exp(-(t/\sigma)^2/2)$,

Given two probability density functions ϕ_1, ϕ_2 on $\mathbb{R}^n$, we define the statistical distance between them as $\Delta(\phi_1, \phi_2) := \frac{1}{2}\int_{\mathbb{R}^n} |\phi_1(\mathbf{x}) - \phi_2(\mathbf{x})| d\mathbf{x}$. A similar definition holds for discrete random variables. We sometimes abuse such notation, and use the same notation for two arbitrary functions. Note that the acceptance probability of any algorithm on inputs from X differs from its acceptance probability on inputs from Y by at most $\Delta(X, Y)$.

Lattice and Problems. An n-dimensional lattice in $\mathbb{R}^n$ is the set $L(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{\sum_{i=1}^n \alpha_i \mathbf{b}_i \mid \alpha_i \in \mathbb{Z}\}$ of all integral combinations of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. The sequence of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called a *basis* of the lattice L. For clarity of notations, we represent a basis by the matrix $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$. For n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$, we define the fundamental parallelepiped $\mathcal{P}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{\sum_{i=1}^n \alpha_i \mathbf{b}_i \mid 0 \leq \alpha_i < 1\}$. The vector $\mathbf{x} \in \mathbb{R}^n$ reduced modulo the parallelepiped $\mathcal{P}(\mathbf{B})$, denoted by $\mathbf{x} \bmod \mathcal{P}(\mathbf{B})$, is the unique vector $\mathbf{y} \in \mathcal{P}(\mathbf{B})$ such that $\mathbf{y} - \mathbf{x} \in L(\mathbf{B})$. For more details on lattices, see the textbook by Micciancio and Goldwasser [11].

The shortest vector problem (SVP) and its approximation version (SVP$_\gamma$) have been deeply studied in the computer science.

Definition 2.2 (SVP)**.** Given a basis $\mathbf{B}$ of a lattice L, find a non-zero vector $\mathbf{v} \in L$ such that for any non-zero vector $\mathbf{x} \in L$, $\|\mathbf{v}\| \leq \|\mathbf{x}\|$.

Definition 2.3 (SVP$_\gamma$)**.** Given a basis $\mathbf{B}$ of a lattice L, find a non-zero vector $\mathbf{v} \in L$ such that for any non-zero vector $\mathbf{x} \in L$, $\|\mathbf{v}\| \leq \gamma \|\mathbf{x}\|$.

The unique shortest vector problem (uSVP) is also well known as a hard lattice problem applicable to cryptographic constructions. We say the shortest vector $\mathbf{v}$ of a lattice L is f-unique if for any non-zero vector $\mathbf{x} \in L$ which is not parallel to $\mathbf{v}$, $f\|\mathbf{v}\| \leq \|\mathbf{x}\|$. The definition of uSVP is given as follows.

Definition 2.4 (f-uSVP)**.** Given a basis $\mathbf{B}$ of a lattice L whose shortest vector is f-unique, find a non-zero vector $\mathbf{v} \in L$ such that for any non-zero vector $\mathbf{x} \in L$ which is not parallel to $\mathbf{v}$, $f\|\mathbf{v}\| \leq \|\mathbf{x}\|$.

In the computational complexity theory on lattice problems, the shortest linearly independent vectors problem (SIVP) and its approximation version SIVP$_\gamma$ are also considered as a hard lattice problem.

Definition 2.5 (SIVP)**.** Given a basis $\mathbf{B}$ of a lattice L, find a sequence of n linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in L$ such that for any sequence of n linearly independent vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n \in L$, $\max_{i=1,\ldots,n} \|\mathbf{v}_i\| \leq \max_{i=1,\ldots,n} \|\mathbf{x}_i\|$.

Definition 2.6 (SIVP$_\gamma$)**.** Given a basis $\mathbf{B}$ of a lattice L, find a sequence of n linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in L$ such that for any sequence of n linearly independent vectors $\mathbf{x}_1, \ldots, \mathbf{x}_n \in L$, $\max_{i=1,\ldots,n} \|\mathbf{v}_i\| \leq \gamma \max_{i=1,\ldots,n} \|\mathbf{x}_i\|$.

The closest vector problem (CVP) is also important problem.

Definition 2.7 (CVP)**.** Given a basis $\mathbf{B}$ of a lattice L and a target vector $\mathbf{y}$, find a closest vector $\mathbf{v} \in L$ such that for any vector $\mathbf{x} \in L$, $\|\mathbf{y} - \mathbf{v}\| \leq \|\mathbf{y} - \mathbf{x}\|$.

Definition 2.8 (CVP$_\gamma$)**.** Given a basis $\mathbf{B}$ of a lattice L and a target vector $\mathbf{y}$, find a closest vector $\mathbf{v} \in L$ such that for any vector $\mathbf{x} \in L$, $\|\mathbf{y} - \mathbf{v}\| \leq \gamma \|\mathbf{y} - \mathbf{x}\|$.

We often consider its decisional promise problem.

Definition 2.9 (GapCVP$_\gamma$)**.** For $\gamma > 1$, instances of the promise closest vector problem GapCVP$_\gamma$ are tuples $(\mathbf{B}, \mathbf{y}, t)$ where $\mathbf{B}$ is a basis of a lattice L in $\mathbb{R}^n$, $t > 0$, and a vector $\mathbf{y} \in \mathbb{R}^n$. $(\mathbf{B}, \mathbf{y}, t)$ is a YES instance of the GapCVP$_\gamma$ if there exists a lattice vector $\mathbf{x} \in L$ such that $\|\mathbf{x} - \mathbf{y}\| \geq t$. $(\mathbf{B}, \mathbf{y}, t)$ is a NO instance of the GapCVP$_\gamma$ if there exists no lattice vector $\mathbf{x} \in L$ such that $\|\mathbf{x} - \mathbf{y}\| > \gamma t$.

Zero Knowledge and Proof of Knowledge. We recall definitions and notations of zero knowledge and proof of knowledge.

Definition 2.10 (Auxiliary-Input Computatinal Zero Knowledge)**.** An interactive proof system (P, V) for a language L is *computational auxiliary-input zero knowledge* if for every PPT V^* and polynomial $p(\cdot)$, there exists a PPT S such that the ensembles $\{(P, V^*(z))(x)\}$ and $\{S(x, z)\}$ are computationally indistinguishable on the set $\{(x, z) : x \in L, |z| = p(|x|)\}$.

For a relation $R \subseteq \{0, 1\}^* \times \{0, 1\}^*$ and $x \in \{0, 1\}^*$, we define a set of witness of x as $R(x) := \{y \mid (x, y) \in R\}$.

Definition 2.11 (Proof of Knowlegde)**.** Let $\kappa \in (0, 1)$, an interactive protocol (P, V) with a prover P and a verifier V is a *proof of knowledge system with knowledge error κ for a relation R* is the following holds:

Completeness: For every common input x for which there exists y such that $(x, y) \in R$ the verifier V always accepts interacting with the prover P.

Validity with error η: There exists a polynomial-time interacting oracle Turing machine K and a constant $c > 0$ such that for every $x \in \{0, 1\}^*$ such that $R(x) \neq \emptyset$ and for every prover P^* the following holds: $K^{P^*}(x) \in R(x) \cup \{\perp\}$ and $\Pr[K^{P^*}(x) \in R(x)] \geq (p - \kappa)^c$, where $p > \kappa$ is a probability that V accepts while interacting with P^* on common input x.

2.1 The Ajtai-Dwork Cryptosystem and Nguyen and Stern's Embedding

The Ajtai-Dwork cryptosystem is an 1-bit lattice-based cryptosystem. Nguyen and Stern showed how to reduce distinguishing encryptions of 0 from one of 1 to GapCVP_γ for some $\gamma > 1$. We briefly review errorless version of the Ajtai-Dwork cryptosystem, which proposed by Goldreich, Goldwasser, and Halevi [7], and Nguyen and Stern's embedding techniques [13]. For more details, see [13, Section 4].

The secret key of the Ajtai-Dwork cryptosystem is $\mathbf{u} \in \mathbb{R}^n$ whose length is 1. The public key is $m + n$ vectors in n-dimensional space and an index. We denote it as $(\mathbf{w}_1, \ldots, \mathbf{w}_n, \mathbf{v}_1, \ldots, \mathbf{v}_m, i_0)$. The vectors $\mathbf{w}_i, \mathbf{v}_i$ are chosen from hyperplanes $\{\mathbf{x} \in [0, n^n]^n \mid \langle \mathbf{x}, \mathbf{u} \rangle \in \mathbb{Z}\}$ and "blurred" by adding small noises. The index i_0 is chosen from $\{1, \ldots, m\}$ such that $\langle \mathbf{u}, \mathbf{v}_i \rangle$ is near by odd integers. Encryption of $\sigma \in \{0, 1\}$ is produced as follows: (1) Choose random string $r = r_1 \ldots r_m \in \{0, 1\}^m$. (2) Compute $\mathbf{c} = (\sigma/2)\mathbf{v}_{i_0} + \sum_{i=1}^m r_i \mathbf{v}_i \bmod \mathcal{P}(\mathbf{w}_1, \ldots, \mathbf{w}_n)$. We decrypt a ciphertext $\mathbf{c} \in \mathcal{P}(\mathbf{w}_1, \ldots, \mathbf{w}_n)$ into 0 if $\mathrm{frc}(\langle \mathbf{c}, \mathbf{u} \rangle) \leq 1/4$ and into 1 if $\mathrm{frc}(\langle \mathbf{c}, \mathbf{u} \rangle) > 1/4$.

Nguyen and Stern showed the following embeddings [13]. For any public key pk of the Ajtai-Dwork cryptosystem, let $\mathbf{B}_{\mathsf{pk}} \in \mathbb{R}^{(2n+m)\times(n+m)}$ be

$$\mathbf{B}_{\mathsf{pk}} = \begin{bmatrix} K_1\mathbf{w}_1 & \ldots & K_1\mathbf{w}_n & K_1\mathbf{v}_1 & \ldots & K_1\mathbf{v}_m \\ 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & K_2 & & \\ & & & & \ddots & \\ & & & & & K_2 \end{bmatrix},$$

where K_1 and K_2 are suitably chosen and all empty spaces are set by 0. For any ciphertext $\mathbf{c} \in \mathcal{P}(\mathbf{w}_1, \ldots, \mathbf{w}_n)$, define $\mathbf{x}_\mathbf{c} = \binom{K_1\mathbf{c}}{\mathbf{0}} \in \mathbb{R}^{2n+m}$. Nguyen and Stern showed for suitably chosen K_1 and K_2, $\mathrm{Dist}(\mathbf{x}_\mathbf{c}, L(\mathbf{B}_{\mathsf{pk}}))$ is small if $\mathbf{c}$ is a legal ciphertext of 0 with pk and $\mathrm{Dist}(\mathbf{x}_\mathbf{c}, L(\mathbf{B}_{\mathsf{pk}}))$ is large if $\mathbf{c}$ decrypts into 1 with high probability.

2.2 Micciancio and Vadhan's Zero-Knowledge Protocol

In [12], Micciancio and Vadhan introduced a zero-knowledge protocol for GapCVP_{γ}. They use the following observation by Goldreich and Goldwasser [6]. Consider two n-dimensional unit hyperballs, one center locates the origin and the other center locates the point that distance is d, i.e., $B(\mathbf{0}, 1)$ and $B(\mathbf{y}, 1)$, where $\|\mathbf{y}\| = d$. If $d = \Omega(\sqrt{n/\log n})$, ratio between a volume of an intersection of two hyperballs and a volume of a hyperball is $1/\mathrm{poly}(n)$. Based on this observation, Goldreich and Goldwasser showed SZK protocol for $\mathrm{coGapCVP}_{\Omega(\sqrt{n/\log n})}$ [6]. Micciancio and Vadhan also constructed HVSZK proof system for $\mathrm{GapCVP}_{\Omega(\sqrt{n/\log n})}$ [12].

We refer Micciancio and Vadhan's protocol as the MV protocol. Let P_{MV} and V_{MV} denote the prover and the verifier, respectively. The common input is $(\mathbf{B}, \mathbf{y}, t)$. The auxiliary input to the prover is $\mathbf{w} \in \mathbb{Z}^n$ such that $\|\mathbf{B}\mathbf{w} - \mathbf{y}\| \leq t$.

Step P1 Choose k random bits $c_1, \ldots, c_k \in \{0, 1\}$ independently. Also choose error vectors $\mathbf{r}_1, \ldots, \mathbf{r}_k \in B(\mathbf{0}, \gamma t/2)$ independently and uniformly at random. Then, check if there exists an index i^* such that $\|\mathbf{r}_{i^*} + (2c_{i^*} - 1)\mathbf{u}\| \leq \gamma t/2$. If not, set $i^* = 1$ and redefine $c_{i^*} = 0$ and $\mathbf{r}_{i^*} = \mathbf{u}/2$, so that $\|\mathbf{r}_{i^*} + (2c_{i^*} - 1)\mathbf{u}\| < \gamma t/2$ is certainly satisfied. Finally, compute points $\mathbf{m}_i = c_i\mathbf{y} + \mathbf{r}_i \bmod \mathbf{B}$ for $i = 1, \ldots, k$ and send them to V_{MV}.

Step V1 Send a random challenge bit $\delta \in \{0, 1\}$ to P_{MV}.

Step P2 Receive a challenge bit $\delta \in \{0, 1\}$. If $\delta = \sum_{i=1}^{k} c_i \bmod 2$, then the prover completes the proof sending bits c_i and lattice vectors $\mathbf{B}\mathbf{v}_i = \mathbf{m}_i - (\mathbf{r}_i + c_i\mathbf{y})$ to V_{MV}. If $\delta \neq \sum_{i=1}^{k} c_i \bmod 2$, then the prover sends the same messages to V_{MV}, but with c_{i^*} and $\mathbf{B}\mathbf{v}_{i^*}$ replaced by $1 - c_{i^*}$ and $\mathbf{B}\mathbf{v}_{i^*} + (2c_{i^*} - 1)(\mathbf{y} - \mathbf{u})$.

Step V2 Receive k bits $c_1, \ldots, c_k$ and k lattice points $\mathbf{B}\mathbf{v}_1, \ldots, \mathbf{B}\mathbf{v}_k$ and check that they satisfy $\sum_{i=1}^{k} c_i = q \pmod 2$ and $\|\mathbf{m}_i - (\mathbf{B}\mathbf{v}_i + c_i\mathbf{y})\| \leq \gamma t/2$ for all $i = 1, \ldots, k$.

A completeness property is evident.

Theorem 2.12 (Zero Knowledge)**.** $(P_{\mathrm{MV}}, V_{\mathrm{MV}})$ *is a statistical zero-knowledge proof system with perfect completeness and soundness error* $1/2$*, provided one of the following conditions holds:*

- $\gamma = \Omega(\sqrt{n/\log n})$ *and* $k = \mathrm{poly}(n)$ *is a sufficiently large polynomial, or*
- $\gamma = \Omega(\sqrt{n})$ *and* $k = \omega(\log n)$ *is any superlogarithmic function of* n*, or*
- $\gamma = n^{0.5+\Omega(1)}$ *and* $k = \omega(1)$ *is any superconstant function of* n*.*

Theorem 2.13 (Proof of Knowledge)**.** *There is a probabilistic polynomial-time algorithm* K_{MV} *such that if a prover* P^* *makes* V_{MV} *accept with probability* $1/2 + \epsilon$ *on some instance* $(\mathbf{B}, \mathbf{y}, t)$*, then* $K_{\mathrm{MV}}^{P^*}(\mathbf{B}, \mathbf{y}, t)$ *outputs a vector* $\mathbf{w} \in \mathbb{Z}^n$ *satisfying* $\|\mathbf{B}\mathbf{w} - \mathbf{y}\| \leq \gamma t$ *with probability* ϵ*.*

2.3 Proof of Plaintext Knowledge for the Ajtai-Dwork Cryptosystem

Goldwasser and Kharchenko [8] showed a interactive zero-knowledge proof of plaintext knowledge (PPK) for the Ajtai-Dwork cryptosystem using the above two results.

First, we immediately obtain a statistical zero-knowledge protocol for a statement that $\mathbf{c}$ is a legal ciphertext of 0 combining the above results. They also show a statistical zero-knowledge protocol for a statement that $\mathbf{c}$ is a legal ciphertext of 1 setting parameters carefully and using the fact that $\mathbf{c}_1 = \mathbf{v}_{i_0}/2 + \mathbf{c}_0 \bmod \mathcal{P}(\mathbf{w}_1, \ldots, \mathbf{w}_n)$ for some legal ciphertexts $\mathbf{c}_1$ of 1. Thus, in other words, they showed a verifiable encryption for a statement "the ciphertext $\mathbf{c}$ decrypts into σ".

They showed PPK for the Ajtai-Dwork cryptosystem implicitly using pseudohomomorphism [9] of the cryptosystem. We state informally their protocol: Let a common input be a pair $(\mathsf{pk}, \mathbf{c})$. The auxiliary inputs to the prover are a plaintext σ and a randomness that used in the ciphertext. In the first step, the prover makes a dummy ciphertext of a random bit σ'. The verifier sends a challenge bit δ. Suppose that $\delta = 0$. The prover sends the plaintext and the randomness that used in the dummy ciphertext. The verifier checks its consistency. Next, suppose that $\delta = 1$. The prover invokes a prover of the MV protocol with a statement that the sum of input ciphertext and dummy one decrypts into $\sigma \oplus \sigma'$. The verifier invokes a verifier of the MV protocol.

3 Proof of Plaintext Knowledge for the Regev'04 Cryptosystems

3.1 The Regev'04 Cryptosystem

Instead of the original cryptosystem, we review the modified one in Kawachi, Tanaka, and Xagawa [9]. Let $c \geq 0$ is a constant. The parameter of original one is $c = 0$.

Let n be a security parameter, $N\ 2^{8n^2}$, and $m = c_m n^2$ where c_m is a constant. Let $\gamma(n) = \omega(n^{1+c}\sqrt{\log n})$. Let $H = \{h \in [\sqrt{N}, 2\sqrt{N}) \mid \mathrm{frc}\,(h) < 1/(8n^c m)\}$.

Private Key: Choose $h \in H$ uniformly at random. Let d denote N/h. The private key is the number h (or d).

Public Key: Choose $\alpha \in [2/\gamma(n), 2\sqrt{2}/\gamma(n))$ uniformly at random. We choose m values $z_1, \ldots, z_m$ from $\Phi_{h,\alpha}$ by choosing $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$, where each x_i is chosen from $\{0, 1, \ldots, \lceil h \rceil\}$ at random and each y_i is chosen according to Ψ_α. Let i_0 be an index such that x_{i_0} is odd. For $i \in \{1, \ldots, m\}$, let a_i be $\lfloor N z_i \rfloor$. The public key is $(a_1, \ldots, a_m, i_0)$.

Encryption: A plaintext is $\sigma \in \{0, 1\}$. Choose a random string $r = r_1 \ldots r_m \in \{0, 1\}^m$. The ciphertext is $\sigma \lfloor a_{i_0}/2 \rfloor + \sum_{i=1}^{m} r_i a_i \bmod N$.

Decryption: Let $w \in \{0, \ldots, N-1\}$ be a receiving ciphertext. We decrypt 0 if $\mathrm{frc}\,(w/d) < 1/4$ and 1 otherwise.

We summary the results in [14, 9] on the decryption errors and the security of R04 as follows.

Theorem 3.1 ([14, 9]). *The security of the Regev'04 cryptosystem is based on the worst case of $O(\gamma(n)\sqrt{n})$-*uSVP*. The decryption error probability is at most $2^{-\Omega(\gamma^2(n)/n^{2c}m)}$.*

We modify parameters and key-generation algorithm as follows:

Parameters: Let $c = 3$ and $t_\alpha = n^{-3.5}$. Let also $\gamma(n) = n^4 \log n$.

Private Key: Same as the original one.

Public Key: Choose $\alpha \in [2/\gamma(n), 2\sqrt{2}/\gamma(n))$ uniformly at random. We choose m values $z_1, \ldots, z_m$ from $\Phi_{h,\alpha}$ by choosing $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$. If $|y_i|_1 > t_\alpha$ we rechoose y_i. For $i \in \{1, \ldots, m\}$, let a_i be $\lfloor N z_i \rfloor$. Let i_0 be an index such that x_{i_0} is odd and a_{i_0} is even. The public key is $(a_1, \ldots, a_m, i_0)$.

We refer this modified version as R04.

Before summarizing security and correctness of R04, we need Lemma to bound the tail of Gaussian distribution Ψ_α.

Lemma 3.2. *Let n be a security parameter. Let $\alpha > 0$ be a real number in $[2/\gamma(n), 2\sqrt{2}/\gamma(n))$. Let t_α be an integer that asymptotically larger than $2\sqrt{2}\log n/\gamma(n)$, i.e., $t_\alpha = \omega(\log n)/\gamma(n)$. Finally, let y be a random variable according to the distribution Ψ_α. Then, the probability that $\mathrm{frc}\,(y) \geq t_\alpha$ is negligible in n.*

Proof. By Lemma 2.1, we have that

$$\begin{aligned}
\Pr_{y \sim \Psi_\alpha}[\mathrm{frc}\,(y) \geq t_\alpha] &\leq \Pr_{y' \sim N(0, \alpha^2/(2\pi))}\left[\left|y'\right| \geq t_\alpha\right] \\
&\leq \sqrt{\frac{2}{\pi}} \frac{2\sqrt{2}/(\gamma(n)\sqrt{2\pi})}{t_\alpha} \exp\left(-\frac{t_\alpha^2}{2(2\sqrt{2}/(\gamma(n)\sqrt{2\pi}))^2}\right) \\
&\leq \frac{2\sqrt{2}}{\pi t_\alpha \gamma(n)} \exp\left(-\pi \frac{t_\alpha^2 \gamma(n)^2}{8}\right).
\end{aligned}$$

Since we set $t_\alpha = \omega(\sqrt{\log n})/\gamma(n)$, we obtain $\exp(-\omega(\log n))$ as the upperbound of the probability. □

Let we argue the correctness of R04.

Lemma 3.3 (Correctness)**.** *Let c_0 and c_1 be legal ciphertexts of* 0 *and* 1 *respectively. Then,*

$$\mathrm{frc}\left(\frac{c_0}{d}\right) \le \frac{1}{4n^3} + mt_\alpha \le \frac{2}{n} \text{ and } \mathrm{frc}\left(\frac{c_1}{d}\right) \ge \frac{1}{2} - \frac{1}{2n^3} + (m+1)t_\alpha \ge \frac{1}{2} - \frac{2}{n}.$$

I.e., there exist no decryption errors.

Proof. We first evaluate $\mathrm{frc}\,(c_0/d)$. Let $c_0 = \sum_{i=1}^m r_i a_i \bmod N$. Considering effects by modulo N at most m times, we have that

$$\left| c_0 - \left(\sum_{i=1}^m r_i a_i \bmod d \lfloor h \rceil \right) \right| \le m \left| N - d \lfloor h \rceil \right| = md \cdot \mathrm{frc}\,(h) < \frac{1}{8n^3} d.$$

By the triangle inequality,

$$\begin{aligned} \mathrm{frc}\left(\frac{c_0}{d}\right) &\le \frac{1}{8n^3} + \mathrm{frc}\left(\frac{\sum_{i=1}^m r_i a_i \bmod d\lfloor h \rceil}{d}\right) \\ &\le \frac{1}{8n^3} + \mathrm{frc}\left(\frac{\sum_{i=1}^m a_i}{d}\right) \\ &\le \frac{1}{8n^3} + \frac{m}{d} + \mathrm{frc}\left(\frac{N}{d}\sum_{i=1}^m z_i\right), \end{aligned}$$

where in the last inequality we use the fact $a_i = \lfloor N z_i \rfloor$. Since $z_i = (x_i + y_i)/h$ and $N = dh$,

$$\mathrm{frc}\left(\frac{N}{d}\sum_{i=1}^m z_i\right) = \mathrm{frc}\left(\sum_{i=1}^m (x_i + y_i)\right) = \mathrm{frc}\left(\sum_{i=1}^m y_i\right) \le mt_\alpha.$$

Since d is much larger than m, $\frac{1}{8n^3} + \frac{m}{d} \le \frac{1}{4n^3}$. Therefore, we obtain $\mathrm{frc}\,(c_0/d) \le \frac{1}{4n^3} + mt_\alpha$.

We next evaluate $\mathrm{frc}\,(c_1/d)$. Note that for some legal ciphertext of 0 c_0, $c_1 = \lfloor a_{i_0}/2 \rfloor + c_0 \bmod N$. From the construction of a_{i_0},

$$\mathrm{frc}\left(\frac{\lfloor a_{i_0}/2 \rfloor}{d}\right) \ge \mathrm{frc}\left(\frac{a_{i_0}/2}{d}\right) - \frac{1}{d} \ge \mathrm{frc}\left(\frac{N z_{i_0}/2}{d}\right) - \frac{2}{d} \ge \mathrm{frc}\left(\frac{x_{i_0} + y_{i_0}}{2}\right) - \frac{2}{d} \ge \frac{1}{2} - \mathrm{frc}\left(\frac{y_{i_0}}{2}\right) - \frac{2}{d} \ge \frac{1}{2} - t_\alpha,$$

where in the last inequality we use the fact d is much larger than t_α. By the triangle inequality, we obtain that

$$\begin{aligned} \mathrm{frc}\left(\frac{c_1}{d}\right) &= \mathrm{frc}\left(\frac{\lfloor a_{i_0}/2 \rfloor + c_0 \bmod N}{d}\right) \\ &\ge \frac{1}{2} - t_\alpha - \left(\frac{1}{4n^3} + mt_\alpha\right) - \frac{1}{8n^3 m} \\ &\ge \frac{1}{2} - \frac{1}{2n^3} - (m+1)t_\alpha. \end{aligned}$$

□

We define the assumption IuSVP as follows:

Assumption 3.4 (Infeasibility of uSVP)**.** There exists no polynomial-time algorithm that solves $\tilde{O}(n^{4.5})$-uSVP with non-negligible probability.

3.2 Preliminaries for PPK

Let $\mathcal{E}(\mathsf{pk}, \sigma)$ be a set of legal ciphertexts of σ with a public key pk. We define a threshold of GapCVP as $t = \sqrt{m^2 + K_2^2 m}$ and an approximation factor of GapCVP as $\gamma = \sqrt{\frac{m+2}{\log(m+2)}}$.

Definition 3.5. Let $\mathsf{pk} = (a_1, \ldots, a_m, i_0)$ be a public key of R04. Let c be an integer in $\{0, 1, \ldots, N-1\}$. Define a mapping $\mathcal{F}(\mathsf{pk}, c) = (\mathbf{B}_{\mathsf{pk}}, t, \mathbf{x}_c)$, where $\mathbf{x_c} = \binom{K_1 c}{\mathbf{0}} \in \mathbb{Z}^{m+2}$. And $\mathbf{B}_{\mathsf{pk}} \in \mathbb{Z}^{(m+2)\times(m+1)}$ is

$$\mathbf{B}_{\mathsf{pk}} = \begin{bmatrix} K_1 N & K_1 v_1 & \cdots & K_1 v_m \\ 1 & & & \\ & K_2 & & \\ & & \ddots & \\ & & & K_2 \end{bmatrix},$$

where $v_i = a_i$, $K_1 = n^4$, $K_2 = n^2$ and empty spaces are set by 0.

We remark that $K_1 > \gamma t$ and $\frac{1}{8n^3 m} + \frac{\sqrt{2}mt_\alpha}{K_2} \leq n^{-4}$.

3.3 From Ciphertexts to GapCVP (or Verifiable Encryption)

3.3.1 From Ciphertexts of 0 to Instances of GapCVP

We show that $\mathcal{F}(\cdot, \cdot)$ maps a valid ciphertext of 0 to a YES instance of GapCVP_γ and a ciphertext that decrypts to 1 to a NO instance of one. Hence, we have an interactive proof that c is a ciphertext of 0 using the MV protocol and this transformation.

Lemma 3.6.

1. *For* $(\mathsf{sk}, \mathsf{pk})$ *and* $c \in \mathcal{E}(\mathsf{pk}, 0)$, $\mathcal{F}(\mathsf{pk}, c)$ *is a YES instance of* GapCVP_γ.
2. *For any instance of* $(\mathsf{sk}, \mathsf{pk})$ *and* $c \in \{0, 1, \ldots, N-1\}$ *such that* $D(\mathsf{sk}, c) = 1$, $\mathcal{F}(\mathsf{pk}, c)$ *is a NO instance of* GapCVP_γ.

Proof. **(1)**. Since $c \in \mathcal{E}(\mathsf{pk}, 0)$, there exists a string r such that $c = \sum_{i=1}^m r_i v_i \bmod N$. Thus, there exists a vector $\mathbf{w} = {}^t(\alpha_1, \beta_1, \ldots, \beta_m)$, where $\alpha_1 \in \{-m, \ldots, 0\}$ and $\beta_i \in \{0, 1\}$, such that $c = \alpha_1 N + \sum_{i=1}^m \beta_i v_i$. It is evident that $\mathbf{B}_{\mathsf{pk}}\mathbf{w} \in L_{\mathsf{pk}}$. Hence, we obtain that

$$\begin{aligned} \mathrm{Dist}\left(\begin{pmatrix} K_1 c \\ \mathbf{0} \end{pmatrix}, L_{\mathsf{pk}}\right) &\leq \mathrm{Dist}\left(\begin{pmatrix} K_1 c \\ \mathbf{0} \end{pmatrix}, \mathbf{B}_{\mathsf{pk}}\mathbf{w}\right) \\ &= \sqrt{\alpha_1^2 + K_2^2 \sum_j^m \beta_j^2} \\ &\leq \sqrt{m^2 + K_2^2 m} = t. \end{aligned}$$

(2). Let $c \in \{0, 1, \ldots, N-1\}$ be any vector which decrypts to 1 and let $T = \gamma t$. From the remark, it follows that $T/n^4 \leq 1/4 \leq \mathrm{frc}(c/d)$. By Claim 3.7 $\mathrm{Dist}\left(\binom{K_1 c}{\mathbf{0}}, L_{\mathsf{pk}}\right) \leq T$ can not hold. Thus, $\mathcal{F}(\mathsf{pk}, c)$ is a NO instance. □

Claim 3.7. *Let* $K_1 > T > 0$, pk *be a public key of* R04, *and* $c \in \{0, 1, \ldots, N-1\}$. *For sufficiently large* n, *If* $\mathrm{Dist}\left(\binom{K_1 c}{\mathbf{0}}, L_{\mathsf{pk}}\right) \leq T$ *then* $\mathrm{frc}(c/d) \leq T(\frac{1}{8n^3 m} + \frac{\sqrt{2}mt_\alpha}{K_2}) \leq T/n^4$.

Proof. From the assumption, there exists $\mathbf{w} = {}^t(\alpha_1,\beta_1,\ldots,\beta_m)$ such that $\left\|\binom{K_1 c}{\mathbf{0}} - \mathbf{B}_{\mathsf{pk}}\mathbf{w}\right\| \leq T$. We define $e = K_1 c - K_1(\alpha_1 N + \sum_{i=1}^m \beta_i \mathbf{v}_i)$. From the construction of $\mathbf{B}_{\mathsf{pk}}$, we obtain that

$$\alpha_1^2 + K_2^2 \sum_{i=1}^m \beta_i^2 + e^2 \leq T^2.$$

From the fact $K_1 > T$ and $e \in K_1\mathbb{Z}$, e must be 0. Recall that $c = \alpha_1 N + \sum_{i=1}^m \beta_i \mathbf{v}_i + e/K_1$. Therefore,

$$\begin{aligned}\mathrm{frc}\,(c/d) &\leq |\alpha_1|\,\mathrm{frc}\,(N/d) + \sum_{i=1}^m |\beta_i|\,\mathrm{frc}\,(v_i/d)\\ &\leq T\,\mathrm{frc}\,(h) + \sum_{i=1}^m |\beta_i|\,(1/d + \mathrm{frc}\,(y_i))\end{aligned}$$

By the Cauchy-Schwartz inequality and the upper bound of $\sum \beta_i^2$, we have $\sum_{i=1}^m \beta_i(1/d + \mathrm{frc}\,(y_i)) \leq \sqrt{\sum_{i=1}^m \beta_i^2}\sqrt{\sum_{i=1}^m (1/d + \mathrm{frc}\,(y_i))^2} \leq \sqrt{\sum_{i=1}^m 2\mathrm{frc}\,(y_i)^2 T/K_2}$. Moreover, from the key generation algorithm, we have $\sqrt{\sum_{i=1}^m 2\mathrm{frc}\,(y_i)^2} \leq \sqrt{2mt_\alpha}$. Hence, we obtain $\mathrm{frc}\,(c/d) \leq T(\frac{1}{8n^3 m} + \frac{\sqrt{2mt_\alpha}}{K_2})$ and conclude the proof. □

Protocol$_0$: proving that a ciphertext decrypts to 0: Let P_0 and V_0 denote the prover and the verifier, respectively. Let the common input be a pair (pk, c), where pk is a public key of R04 and c is an element in $\{0, 1, \ldots, N-1\}$. The auxiliary input to the prover is $\beta_1,\ldots,\beta_m \in \{0,1\}$ such that $c = \sum_{i=1}^m \beta_i v_i \bmod N$.

Prover P_0: Computes an integer α_1 such that $c = \alpha_1 N + \sum_{i=1}^m \beta_i v_i$. Invokes the prover P_{MV} to prove that input $\mathcal{F}(\mathsf{pk}, c)$ is a YES instance of GapCVP_γ with an auxiliary input $\mathbf{B}_{\mathsf{pk}}\mathbf{w}$, where $\mathbf{w} = {}^t(\alpha_1,\beta_1,\ldots,\beta_m)$.

Verifier V_0: Invoke the verifier V_{MV} to verify that input $\mathcal{F}(\mathsf{pk}, c)$ is a YES instance of GapCVP_γ.

Hence we use the MV protocol, we obtain the lemma as follows.

Lemma 3.8. *Protocol (P_0, V_0) is a statistical zero-knowledge protocol.*

3.3.2 From Ciphertexts of1 to Instances of GapCVP

If c is a valid ciphertext of 1 then $y := c - \lfloor v_{i_0}/2 \rfloor \bmod N$ is a valid ciphertext of 0. On the other hand, even if c be a ciphertext that decrypts to 0, there are the case that y is *not* a ciphertext that decrypts to 1 because $\mathrm{frc}\,(v_{i_0})$ is not 0 and there are effects by modulo N. However, we ensure $\mathcal{F}(\mathsf{pk}, y)$ is a NO instance of GapCVP_γ as follows.

Lemma 3.9. *Let $y = c - \lfloor v_{i_0}/2 \rfloor \bmod N$.*

1. *For $(\mathsf{sk}, \mathsf{pk})$ and $c \in \mathcal{E}(\mathsf{pk}, 1)$, $\mathcal{F}(\mathsf{pk}, y)$ is a YES instance of GapCVP_γ.*
2. *For any instance of $(\mathsf{sk}, \mathsf{pk})$ and $c \in \{0, 1, \ldots, N-1\}$ such that $D(\mathsf{sk}, c) = 0$, $\mathcal{F}(\mathsf{pk}, y)$ is a NO instance of GapCVP_γ.*

Proof. **(1).** Since c is a legal ciphertext of 1, we have y is a legal ciphertext of 0. Therefore, by Lemma 3.6, $\mathcal{F}(\mathsf{pk}, y)$ is a YES instance of GapCVP_γ.
(2) Let $c \in \{0, 1, \ldots, N-1\}$ be a ciphertext that decrypts into 0. By the triangle inequality,

$$\mathrm{frc}\left(\frac{c - \lfloor v_{i_0}/2 \rfloor \bmod N}{d}\right) \geq \mathrm{frc}\left(\frac{\lfloor v_{i_0}/2 \rfloor}{d}\right) - \mathrm{frc}\left(\frac{c}{d}\right) - \mathrm{frc}\,(h)\,.$$

From the decryption algorithm, $\mathrm{frc}\,(c/d) \leq 1/4$. Therefore, we obtain

$$\mathrm{frc}\left(\frac{c - \lfloor v_{i_0}/2 \rfloor \bmod N}{d}\right) \geq \frac{1}{2} - t_\alpha - 1/4 - \frac{1}{8n^3m} \geq \frac{1}{4} - \left(t_\alpha + \frac{1}{8n^3m}\right).$$

Note that $\frac{\gamma t}{n^4} < \frac{1}{4} - \left(t_\alpha + \frac{1}{8n^3m}\right)$. Thus, by Claim 3.7, $\mathrm{Dist}\left(\binom{K_1c}{\mathbf{0}}, L_{\mathsf{pk}}\right) \leq \gamma t$ can not hold, and $\mathcal{F}(\mathsf{pk}, y)$ is a NO instance of GapCVP_γ. □

Protocol$_1$: proving that a ciphertext decrypts to 1: Let P_1 and V_1 denote the prover and the verifier, respectively. The common input is a pair (pk, c), where pk is a public key of R04 and c is an integer in $\{0, 1, \ldots, N-1\}$. The auxiliary input to the prover is $\beta_1, \ldots, \beta_m \in \{0, 1\}$ such that $c = \lfloor v_{i_0}/2 \rfloor + \sum_{i=1}^m \beta_i v_i \bmod N$.

Prover P_1: Let $y = c - \lfloor v_{i_0}/2 \rfloor \bmod N$. Computes an integer α_1 such that $c = \alpha_1 N + \sum_{i=1}^m \beta_i v_i$. Invokes the prover P_{MV} to prove that input $\mathcal{F}(\mathsf{pk}, y)$ is a YES instance of GapCVP_γ with an auxiliary input $\mathbf{B}_{\mathsf{pk}}\mathbf{w}$, where $\mathbf{w} = {}^t(\alpha_1, \beta_1, \ldots, \beta_m)$.

Verifier V_1: Invoke the verifier V_{MV} to verify that input $\mathcal{F}(\mathsf{pk}, y)$ is a YES instance of GapCVP_γ.

Similar to the case of ciphertexts of 0, we obtain the following lemma.

Lemma 3.10. *Protocol (P_1, V_1) is a statistical zero-knowledge protocol.*

3.4 Lemmas

In this section, we consider the sum of ciphertexts and its pseudohomomorphism [9]. In the following section, we define $t' = 4t$.

Definition 3.11. Let $\mathsf{pk} = (a_1, \ldots, a_m, i_0)$ be a public key of R04, c and c' elements from $\{0, 1, \ldots, N-1\}$, σ' and $\sigma'' \in \{0, 1\}$, $r' \in \{0, 1\}^m$, and $\mathbf{p}$ be a point from L_{pk}. We say that input (pk, c) and witness $(c', \sigma', r', \sigma'', \mathbf{p})$ are in R_{R04} if:

- $c' = E_{\mathsf{pk}}(\sigma'; r')$
- $\mathrm{Dist}\left(\binom{K_1(c+c'-\sigma''\lfloor v_{i_0}/2 \rfloor \bmod N)}{\mathbf{0}}, \mathbf{p}\right) \leq \gamma t'$ (i.e., $c + c' \bmod N$ decrypts to σ''.)

Theorem 3.12. *Let $(\mathsf{pk}, \mathsf{sk})$ be an instance of* R04*. If $((\mathsf{pk}, c), w) \in R_{\mathrm{R04}}$ for $w = (c', \sigma', r', \sigma'', \mathbf{p})$, then $\sigma' \oplus \sigma'' = D(\mathsf{sk}, c)$.*

Proof. We first consider the case $\sigma'' = 0$. In this case, we have that an inequality

$$\mathrm{Dist}\left(\begin{pmatrix} K_1(c + c' \bmod N) \\ \mathbf{0} \end{pmatrix}, \mathbf{p}\right) \leq \gamma t'.$$

Applying Claim 3.7, we obtain that $\mathrm{frc}\,((c + c' \bmod N)/d) \leq \gamma t'/n^4$. Suppose that $\sigma' = 0$. Since c' is a legal ciphertext, $\mathrm{frc}\,(c'/d) \leq 2/n$. It implies that $\mathrm{frc}\,(c/d) \leq \gamma t'/n^4 + 2/n + 1/8n^3m \leq 1/4$ and $D(\mathsf{sk}, c) = 0$. We also suppose that $\sigma' = 1$. Since c' is a legal ciphertexts, $\mathrm{frc}\,(c'/d) \geq 1/2 - 2/n$. Therefore, by triangle inequality $\mathrm{frc}\,(c/d) \geq 1/2 - 2/n - \gamma t'/n^4 - 1/8n^3m \geq 1/4$ and $D(\mathsf{sk}, c) = 1$.

Next, we consider the case $\sigma'' = 1$, i.e.,

$$\mathrm{Dist}\left(\begin{pmatrix} K_1(c + c' - \lfloor v_{i_0}/2 \rfloor \bmod N) \\ \mathbf{0} \end{pmatrix}, \mathbf{p}\right) \leq \gamma t'.$$

Applying Claim 3.7, we obtain that $\mathrm{frc}\,((c + c' - \lfloor v_{i_0}/2 \rfloor \bmod N)/d) \leq \gamma t'/n^4$. It implies that $\mathrm{frc}\,((c + c' \bmod N)/d) \geq 1/2 - (\mathrm{frc}\,(h) + 2t_\alpha) - \gamma t'/n^4 \geq 1/2 - 2/n$. Suppose that $\sigma' = 0$. Since $\mathbf{c}'$ is a legal ciphertext, $\mathrm{frc}\,(c'/d) \leq 2/n$. It implies that $\mathrm{frc}\,(c/d) \geq 1/2 - 2/n - 2/n - 1/8n^3m \geq 1/4$ and $D(\mathsf{sk}, \mathbf{c}) = 1$. Next, we suppose that $\sigma' = 1$. Since c' is a legal ciphertext, we have that $\mathrm{frc}\,(c'/d) \geq 1/2 - (2\mathrm{frc}\,(h) + 2mt_\alpha) \geq 1/2 - 2/n$. It implies that $\mathrm{frc}\,(c/d) \leq 2/n + 2/n + 1/8n^3m \leq 1/4$ and $D(\mathsf{sk}, \mathbf{c}) = 0$. We conclude the proof. □

3.5 Main Protocol

Let P and V denote a prover and a verifier, respectively. A common input is (pk, c). An auxiliary input to the prover is (σ, r) such that $c = E_{\mathsf{pk}}(\sigma; r)$.

Define a mapping $\mathcal{G}(\mathsf{pk}, c) = (\mathbf{B}_{\mathsf{pk}}, \mathbf{x}_c, t')$ where $t' = 2t$ and $\mathbf{B}_{\mathsf{pk}}$ and $\mathbf{x}_c$ are similar to $\mathcal{F}(\mathsf{pk}, c)$. Let $\text{Protocol}'_0$ (or $\text{Protocol}'_1$) be Protocol_0 (or Protocol_1) where $\mathcal{F}(\cdot,\cdot)$ is replaced by $\mathcal{G}(\cdot,\cdot)$ respectively.

Protocol PPK:

Step P1 P selects $\sigma' \in \{0, 1\}$ and $r' \in \{0, 1\}^m$ randomly. Computes $c' = E_{\mathsf{pk}}(\sigma'; r')$ and sends c' to V.
Step V1 V sends a random challenge bit $\delta \in \{0, 1\}$ to P.
Step P2 If $\delta = 0$, P sends pair (σ', r'). If $\delta = 1$, P computes $\sigma'' = \sigma + \sigma' \bmod 2$ and sends σ'' to V. Let $\overline{c} = (c + c') \bmod N$ and runs $\text{Protocol}'_{\sigma''}$ on input $(\mathsf{pk}, \overline{c})$ as prover.
Step V2 If $\delta = 0$. V accepts if $c' = E_{\mathsf{pk}}(\sigma'; r')$, else rejects. If $\delta = 1$. Run the $\text{Protocol}'_{\sigma''}$ on input $(\mathsf{pk}, \overline{c})$ as verifier.

Theorem 3.13 (Regev 04 PPK)**.** *Interactive protocol (P, V) is a proof of knowledge system with knowledge error $3/4$ for R_{R04}. Moreover, the protocol (P, V) is a computational zero knowledge under the assumption IuSVP.*

The proofs of following Lemma 3.14 and Lemma 3.15 are in Appendix A. We need the lemmas for larger protocol PPK.

Lemma 3.14. *For sufficiently large n,*

1. *If $(\mathsf{sk}, \mathsf{pk})$ is an instance of* R04*, $c = c_1 + c_2 \bmod N$ such that $D(\mathsf{sk}, c) = 0$ and $c_1, c_2 \in \mathcal{E}(\mathsf{pk}, \cdot)$, $\mathcal{G}(\mathsf{pk}, c)$ is a YES instance of* GapCVP_γ.
2. *Let $(\mathsf{sk}, \mathsf{pk})$ be an instance of* R04 *and $c \in \{0, 1, \ldots, N-1\}$. If $\operatorname{frc}(c/d) > 1/8$, then $\mathcal{G}(\mathsf{pk}, c)$ is a NO instance of* GapCVP_γ.

Lemma 3.15. *For sufficiently large n,*

1. *If $(\mathsf{sk}, \mathsf{pk})$ is an instance of* R04*, $c = c_1 + c_2 \bmod N$ such that $D(\mathsf{sk}, c) = 1$ and $c_1, c_2 \in \mathcal{E}(\mathsf{pk}, \cdot)$, $\mathcal{G}(\mathsf{pk}, y)$ is a YES instance of* GapCVP_γ*, where $y = c - \lfloor v_{i_0}/2 \rfloor \bmod N$.*
2. *Let $(\mathsf{sk}, \mathsf{pk})$ be an instance of* R04 *and $c \in \{0, 1, \ldots, N-1\}$. If $\operatorname{frc}(c/d) < 3/8$, then $\mathcal{G}(\mathsf{pk}, y)$ is a NO instance of* GapCVP_γ*, where $y = c - \lfloor v_{i_0}/2 \rfloor \bmod N$.*

Proof of Completeness. Since it is evident, we omit the proof. □

Proof of Validity with error $3/4$. Let $\mathsf{pk} = (a_1, \ldots, a_m, i_0)$ be a public key of R04. and $c \in \{0, 1, \ldots, N-1\}$. Let P^* be an arbitrary prover that make V accept with probability $\epsilon + 3/4$ for $\epsilon > 0$ on common input (pk, c).

We construct a knowledge extractor K as follows. K's input is (pk, c). First, K choose a random tape of P^*. Let δ_1 denotes a challenge bit in $\text{Protocol}'_{\sigma''}$. K runs P^* three times, where the challenge bit are 0, $(1, 0)$ and $(1, 1)$. K obtains three views T_0, T_1, and T_2. Views are in forms that $T_0 = (c', 0, \sigma', r')$, $T_1 = (c', 1, \sigma'', T'_1)$, and $T_2 = (c', 1, \sigma'', T'_2)$, where T'_1 and T'_2 are transcripts of $\text{Protocol}'_{\sigma''}$ that δ_1 are 0 and 1 respectively. If any one of three views is rejected, K outputs $\perp$ and halts. Otherwise, i.e., three views are accepted, K obtains a vector $\mathbf{p}$ that is witness of GapCVP_γ using the extractor in $\text{Protocol}'_0$ or $\text{Protocol}'_1$. Outputs $(c', \sigma', r', \sigma'', \mathbf{p})$ and halts.

Note that the probability K does not output $\perp$ is at least ϵ. Therefore, K is indeed the knowledge extractor. □

Proof of Zero-knowledge of PPK. We construct a simulator S as follows: Let S_σ is a simulator for $\text{Protocol}'_\sigma$.

Step P1 Chooses $\Delta \in \{0, 1\}$ randomly (Predictor of a challenge bit). If $\Delta = 0$, chooses σ', r' randomly and computes $c' = E_{\mathsf{pk}}(\sigma'; r')$. If $\Delta = 1$, chooses σ'', r'' randomly, computes $\overline{c} = E_{\mathsf{pk}}(\sigma''; r'')$, and sets $c' = \overline{c} - c \bmod N$. Sends c' to V^*.

Step V1 Receives a challenge bit δ from V^*.

Step P2, V2 If $\Delta \neq \delta$, outputs $\perp$ and halts. If $\Delta = \delta = 0$ outputs $(c', \delta, \sigma', r')$. If $\Delta = \delta = 1$, invoke $S_{\sigma''}$ with input $(\mathsf{pk}, \overline{c})$. Let $T = S_{\sigma''}(\mathsf{pk}, \overline{c})$. Outputs $(c', \delta, \sigma'', T)$ and halts.

We assume that ISVP holds, hence according to the security property of R04 if $\Delta = 0$ then c' is computationally indistinguishable from the uniform distribution on $\{0, 1, \ldots, N - 1\}$; if $\Delta = 0$ then $c' = \overline{c} - c \bmod N$ is also indistinguishable from the uniform distribution. Therefore, the generated transcripts is computationally indistinguishable from a real transcript. □

4 Proof of Plaintext Knowledge on the Regev'05 Cryptosystem

4.1 The Regev'05 Cryptosystem

We briefly review the Regev'05 cryptosystem [15].

Let n be a security parameter (or a dimension of underlying lattice problems). Let q be a prime and $\alpha \in (0, 1)$ a real such that $\alpha q > 2\sqrt{n}$. Let m be an integer larger than $5(n + 1)\log q$.

Private Key: Choose $\mathbf{s} \in \mathbb{Z}_q^n$ uniformly at random. A private key is $\mathbf{s}$.

Public Key: Choose m vectors $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$ independently at random. Choose $e_1, \ldots, e_m \in \mathbb{Z}_q$ independently according to $\overline{\Psi}_\alpha$. Compute $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \bmod q$. A public key is $\{(\mathbf{a}_i, b_i)\}_{i=1,\ldots,m}$.

Encryption: Choose a random string $r \in \{0, 1\}^m$. Let $\sigma \in \{0, 1\}$ be a plaintext. A ciphertext is $(\sum_{i=1}^m r_i \mathbf{a}_i \bmod q, \sigma \lfloor q/2 \rfloor + \sum_{i=1}^m r_i b_i \bmod q)$.

Decryption: Let $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ be a received ciphertext. If $|b - \langle \mathbf{a}, \mathbf{s} \rangle|_q \leq q/4$ then decrypt into 0, otherwise into 1.

Regev recommended $q \in (n^2, 2n^2)$ and $\alpha = o(1/\sqrt{n}\log n)$ to tighten the approximation factor of underlying lattice problems.

Theorem 4.1 ([15])**.** *The security of the Regev'05 cryptosystem is based on the worst case of* $\mathrm{SVP}_{\tilde{O}(n/\alpha(n))}$ *and* $\mathrm{SIVP}_{\tilde{O}(n/\alpha(n))}$ *for polynomial-time quantum algorithms. The decryption error probability is at most* $2^{-\Omega(1/(m\alpha^2(n)))} + 2^{-\Omega(n)}$.

We modify the key generation algorithm and parameters as follows:

Parameter: Let $q = \Theta(n^4)$ be a prime and $m = 5(n + 1)(\log q + 1)$. We also define $\alpha = 1/m^2$. Note that $q\alpha = \Theta(n^2/\log^2 n) > 2\sqrt{n}$ for sufficiently large n. Let $t_\alpha = n^2 \log n$. Note that $t_\alpha = \omega(q\alpha\sqrt{\log n})$.

Private Key: Same as the original one.

Public Key: Choose m vectors $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$ independently at random. Choose m elements $e_1, \ldots, e_m \in \mathbb{Z}_q$ independently according to $\overline{\Psi}_\alpha$. If $|e_i|_q \leq t_\alpha$ for all i then compute $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \bmod q$, else re-choose $e_1, \ldots, e_m$. A public key is $\{(\mathbf{a}_i, b_i)\}_{i=1,\ldots,m}$.

We refer this modified version as R05. Note that the probability that there exists i such that $|e_i|_q > t_\alpha$ is negligible in n from the following Lemma 4.2. We also note that there exist no decryption errors in R05.

Lemma 4.2. *Let n be a security parameter. Let q be a prime and $\alpha > 0$ a real number such that $q\alpha > 2\sqrt{n}$. Let t_α be an integer that asymptotically larger than $q\alpha\sqrt{\log n}$, i.e., $t_\alpha = \omega(q\alpha\sqrt{\log n})$. Finally, let e be a random variable according to the distribution $\overline{\Psi}_\alpha$. Then, the probability that $|e|_q \geq t_\alpha$ is negligible in n.*

Proof. By Lemma 2.1, we have that

$$\begin{aligned}\Pr_{e \sim \Psi_\alpha}[|e|_q \geq t_\alpha] &\leq \Pr_{e' \sim \Psi_\alpha}[|e'| \geq (t_\alpha - 1)/q] \\ &\leq \sqrt{\frac{2}{\pi}} \frac{\alpha/\sqrt{2\pi}}{(t_\alpha - 1)/q} \exp\left(-\frac{(t_\alpha - 1)^2/q^2}{2(\alpha/\sqrt{2\pi})^2}\right) \\ &\leq \frac{q\alpha}{\pi(t_\alpha - 1)} \exp\left(-\pi\frac{(t_\alpha - 1)^2}{q^2\alpha^2}\right).\end{aligned}$$

Since we set $t_\alpha = \omega(q\alpha\sqrt{\log n})$, we obtain $\exp(-\omega(\log n))$ as the upperbound of the probability. □

The security follows from Theorem 4.1. We summarize the property of R05 as follows.

Theorem 4.3. *The security of* R05 *is based on the worst case of* $\mathrm{SVP}_{\tilde{O}(n^3)}$ *and* $\mathrm{SIVP}_{\tilde{O}(n^3)}$ *for polynomial-time quantum algorithms. There exist no decryption errors.*

We define the assumption ISVP as follows:

Assumption 4.4 (Infeasibility of SVP)**.** There exists no quantum polynomial-time algorithm that solves $\mathrm{SVP}_{\tilde{O}(n^3)}$ and $\mathrm{SIVP}_{\tilde{O}(n^3)}$ with non-negligible probability.

4.2 Preliminaries for PPK

Let $\mathcal{E}(\mathsf{pk}, \sigma)$ be a set of legal ciphertexts of σ with a public key pk. We define a threshold of GapCVP as $t = \sqrt{(n+1)m^2 + K_2^2 m}$ and an approximation factor of GapCVP as $\gamma = \sqrt{\frac{2n+m+3}{\log(2n+m+3)}}$.

Definition 4.5. Let $\mathsf{pk} = \{(\mathbf{a}_i, b_i)\}_{i=1,\ldots,m}$ be a public key of R05. Let $\mathbf{c}$ be a vector in $\mathbb{Z}_q^{n+1}$. Define a mapping $\mathcal{F}(\mathsf{pk}, \mathbf{c}) = (\mathbf{B}_{\mathsf{pk}}, t, \mathbf{x}_{\mathbf{c}})$, where $\mathbf{x}_{\mathbf{c}} = \binom{K_1\mathbf{c}}{\mathbf{0}} \in \mathbb{Z}^{2n+m+3}$. $\mathbf{B}_{\mathsf{pk}} \in \mathbb{Z}^{(2n+m+3)\times(n+m+2)}$ is

$$\mathbf{B}_{\mathsf{pk}} = \begin{bmatrix} K_1 q\mathbf{I}_{n+1} & K_1(q-1)\mathbf{u}_{n+1} & K_1\mathbf{v}_1 & \ldots & K_1\mathbf{v}_m \\ \mathbf{I}_{n+1} & & & & \\ & 1 & & & \\ & & K_2 & & \\ & & & \ddots & \\ & & & & K_2 \end{bmatrix},$$

where $\mathbf{v}_i = \binom{\mathbf{a}_i}{b_i} \in \mathbb{Z}_q^{n+1}$, $K_1 = n^4$, and $K_2 = n^2$.

From the definitions of t and γ, we have that $\gamma t = O(n^2 m)$. We remark that, for sufficiently large n, $4\gamma t = O(n^2 m) < K_1$ and $4\gamma t(1 + \sqrt{m}t_\alpha/K_2) = O(n^2 m)O(1 + \sqrt{m}\log n) < O(n^4) = q/8$ from the definitions of K_1, K_2, q, and t_α.

4.3 From Ciphertexts of 0 to Instances of GapCVP (or Verifiable Encryption)

We show that $\mathcal{F}(\cdot,\cdot)$ maps a valid ciphertext of 0 to a YES instance of GapCVP_γ and a ciphertext that decrypts into 1 to a NO instance of one. Hence, we have an interactive proof that $\mathbf{c}$ is a ciphertext of 0 using the MV protocol and the transformation $\mathcal{F}(\cdot,\cdot)$.

Lemma 4.6.

1. *For* $(\mathsf{sk}, \mathsf{pk})$ *and* $\mathbf{c} \in \mathcal{E}(\mathsf{pk}, 0)$, $\mathcal{F}(\mathsf{pk}, \mathbf{c})$ *is a YES instance of* GapCVP_γ.
2. *For any instance of* $(\mathsf{sk}, \mathsf{pk})$ *and* $\mathbf{c} \in \mathbb{Z}_q^{n+1}$ *such that* $D(\mathsf{sk}, \mathbf{c}) = 1$, $\mathcal{F}(\mathsf{pk}, \mathbf{c})$ *is a NO instance of* GapCVP_γ.

Proof. **(1)**. Since $\mathbf{c} \in \mathcal{E}(\mathsf{pk}, 0)$, there exists a string $r \in \{0,1\}^m$ such that $\mathbf{c} = \sum_{i=1}^m r_i \mathbf{v}_i \bmod q$. Thus, there exists a vector $\mathbf{w} = {}^t(\alpha_1, \ldots, \alpha_{n+1}, 0, \beta_1, \ldots, \beta_m)$, where $\alpha_i \in \{-m, \ldots, 0\}$ and $\beta_i \in \{0,1\}$, such that $\mathbf{c} = \sum_{i=1}^{n+1} \alpha_i q \mathbf{u}_i + \sum_{j=1}^m \beta_j \mathbf{v}_j$. It is evident that $\mathbf{B}_{\mathsf{pk}}\mathbf{w} \in L(\mathbf{B}_{\mathsf{pk}})$. Hence, we obtain that

$$\begin{aligned}\mathrm{Dist}\left(\begin{pmatrix} K_1\mathbf{c} \\ \mathbf{0}\end{pmatrix}, L(\mathbf{B}_{\mathsf{pk}})\right) &\le \mathrm{Dist}\left(\begin{pmatrix} K_1\mathbf{c} \\ \mathbf{0}\end{pmatrix}, \mathbf{B}_{\mathsf{pk}}\mathbf{w}\right) \\ &= \sqrt{\sum_i^{n+1} \alpha_i^2 + K_2^2 \sum_j^m \beta_j^2} \\ &\le \sqrt{(n+1)m^2 + K_2^2 m} = t.\end{aligned}$$

(2). Let $\mathbf{c} = \binom{\mathbf{a}}{b} \in \mathbb{Z}_q^{n+1}$ be any vector which decrypts into 1. Let $T = \gamma t$. From the remark, it follows that $T(1 + \sqrt{m} t_\alpha / K_2) \le q/4 \le |b - \langle \mathbf{a}, \mathbf{s}\rangle|_q$. By Claim 4.7 $\mathrm{Dist}\left(\binom{K_1\mathbf{c}}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le T$ can not hold. Thus, $\mathcal{F}(\mathsf{pk}, \mathbf{c})$ is a NO instance. □

Claim 4.7. *Let* $K_1 > T > 0$. *Let* pk *be a public key of* R05 *and* $\mathbf{c} \in \mathbb{Z}_q^{n+1}$. *For sufficiently large* n, *if* $\mathrm{Dist}\left(\binom{K_1\mathbf{c}}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le T$ *then* $|b - \langle \mathbf{a}, \mathbf{s}\rangle|_q \le T(1 + \sqrt{m} t_\alpha / K_2)$.

Proof. From the assumption, there exists $\mathbf{w} = {}^t(\alpha_1, \ldots, \alpha_{n+2}, \beta_1, \ldots, \beta_m)$ such that $\left\|\binom{K_1\mathbf{c}}{\mathbf{0}} - \mathbf{B}_{\mathsf{pk}}\mathbf{w}\right\| \le T$. We define $\mathbf{e} = K_1\mathbf{c} - K_1(q\sum_i^{n+1} \alpha_i \mathbf{u}_i + (q-1)\alpha_{n+2}\mathbf{u}_{n+1} + \sum_{j=1}^m \beta_i \mathbf{v}_i)$. From the construction of $\mathbf{B}_{\mathsf{pk}}$, we obtain that

$$\sum_{i=1}^{n+2} \alpha_i^2 + K_2^2 \sum_{j=1}^m \beta_i^2 + \|\mathbf{e}\|^2 \le T^2.$$

From the fact $K_1 > T$ and $\mathbf{e} \in K_1\mathbb{Z}^{n+1}$, $\mathbf{e}$ must be $\mathbf{0}$. We note that $\alpha_{n+2}^2 \le T^2$. Now, recall that $\mathbf{c} = \sum_{i=1}^{n+1} \alpha_i q \mathbf{u}_i + (q-1)\alpha_{n+2}\mathbf{u}_{n+1} + \sum_{j=1}^m \beta_i \mathbf{v}_i + \mathbf{e}/K_1$. Therefore,

$$b - \langle \mathbf{a}, \mathbf{s}\rangle \equiv (q-1)\alpha_{n+2} + \sum_{i=1}^m \beta_i b_i - \sum_{i=1}^m \beta_i \langle \mathbf{a}_i, \mathbf{s}\rangle \equiv -\alpha_{n+2} + \sum_{i=1}^m \beta_i e_i \pmod{q}.$$

By the Cauchy-Schwartz inequality and the upper bound of $\sum \beta_i^2$, we have $|\sum_{i=1}^m \beta_i e_i|_q \le \sqrt{\sum_{i=1}^m \beta_i^2}\sqrt{\sum_{i=1}^m |e_i|_q^2} \le \sqrt{\sum_{i=1}^m |e_i|_q^2} T/K_2$. Moreover, from the key generation algorithm, we have $\sqrt{\sum_{i=1}^m |e_i|_q^2} \le \sqrt{m} t_\alpha$. Hence, by triangle inequality, we obtain $|b - \langle \mathbf{a}, \mathbf{s}\rangle|_q \le T(1 + \sqrt{m} t_\alpha / K_2)$ and complete the proof. □

Protocol$_0$: proving that a ciphertext decrypts into 0: P_0 and V_0 denote the prover and the verifier, respectively. The common input is a pair $(\mathsf{pk}, \mathbf{c})$, where pk is a public key of R05 and $\mathbf{c}$ is a vector in $\mathbb{Z}_q^{n+1}$. The prover's auxiliary input is $\beta_1, \ldots, \beta_m \in \{0,1\}$ such that $\mathbf{c} = \sum_{i=1}^m \beta_i \mathbf{v}_i \bmod q$.

Prover P_0**:** Compute integers $\alpha_1, \ldots, \alpha_{n+1}$ such that $\mathbf{c} = \sum_{i=1}^m \beta_i \mathbf{v}_i + \sum_{j=1}^{n+1} q\alpha_i \mathbf{u}_i$. Invoke the prover P_{MV} to prove that the input $\mathcal{F}(\mathsf{pk}, \mathbf{c})$ is a YES instance of GapCVP$_\gamma$ with an auxiliary input $\mathbf{B}_{\mathsf{pk}}\mathbf{w}$, where $\mathbf{w} = {}^t(\alpha_1, \ldots, \alpha_{n+1}, 0, \beta_1, \ldots, \beta_m)$.

Verifier V_0**:** Invoke the verifier V_{MV} to verify that the input $\mathcal{F}(\mathsf{pk}, \mathbf{c})$ is a YES instance of GapCVP$_\gamma$.

Hence we use the MV protocol, we obtain the lemma as follows.

Lemma 4.8. *The protocol* (P_0, V_0) *is a statistical zero-knowledge protocol.*

4.4 From Ciphertexts of 1 to Instances of GapCVP (or Verifiable Encryption)

Lemma 4.9. *Let* $\mathbf{y} = \mathbf{c} - \lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q$*.*

1. *For* $(\mathsf{sk}, \mathsf{pk})$ *and* $\mathbf{c} \in \mathcal{E}(\mathsf{pk}, 1)$*,* $\mathcal{F}(\mathsf{pk}, \mathbf{y})$ *is a YES instance of* GapCVP_γ*.*
2. *For any instance of* $(\mathsf{sk}, \mathsf{pk})$ *and* $\mathbf{c} \in \mathbb{Z}_q^{n+1}$ *such that* $D(\mathsf{sk}, \mathbf{c}) = 0$*,* $\mathcal{F}(\mathsf{pk}, \mathbf{y})$ *is a NO instance of* GapCVP_γ*.*

Proof. **(1)**. Since $\mathbf{c}$ is a legal ciphertext of 1, $\mathbf{y}$ is a legal ciphertext of 0. The proof is similar to that of Lemma 4.6.
(2). We consider $\mathbf{y} = \mathbf{c} - \lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q$. In this case, $D(\mathsf{sk}, \mathbf{y}) = 1$. Therefore, we prove in a similar way to the proof of Lemma 4.6. □

Protocol$_1$: proving that a ciphertext decrypts into 1: P_1 and V_1 denote the prover and the verifier, respectively. The common input is a pair $(\mathsf{pk}, \mathbf{c})$, where pk is a public key of R05 and $\mathbf{c}$ is a vector from $\mathbb{Z}_q^{n+1}$. The prover's auxiliary input is $\beta_1, \ldots, \beta_m \in \{0, 1\}$ such that $\mathbf{c} = \sum_{i=1}^m \beta_i \mathbf{v}_i \bmod q$.

Prover P_1**:** Let $\mathbf{y} = \mathbf{c} - \lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q$. Compute integers $\alpha_1, \ldots, \alpha_{n+1}$ such that $\mathbf{c} = \lfloor q/2 \rfloor \mathbf{u}_{n+1} + \sum_{i=1}^m \beta_i \mathbf{v}_i + \sum_{j=1}^{n+1} q\alpha_i \mathbf{u}_i$. Invoke the prover P_{MV} to prove that input $\mathcal{F}(\mathsf{pk}, \mathbf{y})$ is a YES instance of GapCVP_γ with an auxiliary input $\mathbf{B}_{\mathsf{pk}}\mathbf{w}$, where $\mathbf{w} = {}^t(\alpha_1, \ldots, \alpha_{n+1}, 0, \beta_1, \ldots, \beta_m)$.
Verifier V_1**:** Invoke the verifier V_{MV} to verify that input $\mathcal{F}(\mathsf{pk}, \mathbf{y})$ is a YES instance of GapCVP_γ.

We obtain the following lemma in a similar way to the case of ciphertexts of 0.

Lemma 4.10. *The protocol* (P_1, V_1) *is a statistical zero-knowledge protocol.*

4.5 Definition of Relation

We define $t' = 4t$.

Definition 4.11. Let $\mathsf{pk} = \{(\mathbf{a}_i, b_i)\}_{i=1,\ldots,m}$ be a public key of R05. Let $\mathbf{c}$ and $\mathbf{c}'$ be vectors from $\mathbb{Z}_q^{n+1}$. Let σ' and σ'' be bits, r' an m-bit string, and $\mathbf{p}$ a vector in $L(\mathbf{B}_{\mathsf{pk}})$. We say that input $(\mathsf{pk}, \mathbf{c})$ and witness $(\mathbf{c}', \sigma', r', \sigma'', \mathbf{p})$ are in R_{R05} if:

- $\mathbf{c}' = E_{\mathsf{pk}}(\sigma'; r')$ and
- $\mathrm{Dist}\left(\begin{pmatrix} K_1(\mathbf{c}+\mathbf{c}'-\sigma''\lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q) \\ \mathbf{0} \end{pmatrix}, \mathbf{p}\right) \le \gamma t'$ (i.e., $\mathbf{c} + \mathbf{c}' \bmod q$ decrypts into σ''.)

Theorem 4.12. *Let* $(\mathsf{pk}, \mathsf{sk})$ *be an instance of* R05*. If* $((\mathsf{pk}, \mathbf{c}), w) \in R_{\mathrm{R05}}$ *for* $w = (\mathbf{c}', \sigma', r', \sigma'', \mathbf{p})$*, then* $\sigma' \oplus \sigma'' = D(\mathsf{sk}, \mathbf{c})$*.*

Proof. Let $\mathsf{pk} = \{(\mathbf{a}_i, b_i)\}_{i=1,\ldots,m}$ be a public key of R05.

We first consider the case $\sigma'' = 0$. In this case, we have that an inequality

$$\mathrm{Dist}\left(\begin{pmatrix} K_1(\mathbf{c} + \mathbf{c}' \bmod q) \\ \mathbf{0} \end{pmatrix}, \mathbf{p}\right) \le \gamma t'.$$

Applying Claim 4.7, we obtain that $|b + b' - \langle \mathbf{a} + \mathbf{a}', \mathbf{s} \rangle|_q \le \gamma t'(1 + \sqrt{m} t_\alpha / K_2)$. Suppose that $\sigma' = 0$. Since $\mathbf{c}'$ is a legal ciphertext, $|b' - \langle \mathbf{a}, \mathbf{s} \rangle|_q \le m t_\alpha$. It implies that $|b - \langle \mathbf{a}, \mathbf{s} \rangle|_q \le m t_\alpha + \gamma t'(1 + \sqrt{m} t_\alpha / K_2) \le q/4$ and $D(\mathsf{sk}, \mathbf{c}) = 0$. We also suppose that $\sigma' = 1$. Since $\mathbf{c}'$ is a legal ciphertext, $|b' - \langle \mathbf{a}, \mathbf{s} \rangle|_q \ge q/2 - m t_\alpha$. It implies that $|b - \langle \mathbf{a}, \mathbf{s} \rangle|_q \ge q/2 - m t_\alpha - \gamma t'(1 + \sqrt{m} t_\alpha / K_2) \ge q/4$ and $D(\mathsf{sk}, \mathbf{c}) = 1$.

Next, we consider the case $\sigma'' = 1$, i.e.,

$$\mathrm{Dist}\left(\begin{pmatrix} K_1(\mathbf{c} + \mathbf{c}' - \lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q) \\ \mathbf{0} \end{pmatrix}, \mathbf{p}\right) \le \gamma t'.$$

Applying Claim 4.7, we obtain that $|b + b' - \lfloor q/2 \rfloor - \langle \mathbf{a} + \mathbf{a}', \mathbf{s} \rangle|_q \leq \gamma t'(1 + \sqrt{m} t_\alpha / K_2)$. Hence we have $|b + b' - \langle \mathbf{a} + \mathbf{a}', \mathbf{s} \rangle|_q \geq q/2 - \gamma t'(1 + \sqrt{m} t_\alpha / K_2)$. Suppose that $\sigma' = 0$. Since $\mathbf{c}'$ is a legal ciphertext, $|b' - \langle \mathbf{a}, \mathbf{s} \rangle|_q \leq m t_\alpha$. It implies that $|b - \langle \mathbf{a}, \mathbf{s} \rangle|_q \geq q/2 - m t_\alpha - \gamma t'(1 + \sqrt{m} t_\alpha / K_2) \geq q/4$ and $D(\mathsf{sk}, \mathbf{c}) = 1$. Next, we suppose that $\sigma' = 1$. Since $\mathbf{c}'$ is a legal ciphertext, we have that $|b' - \langle \mathbf{a}', \mathbf{s} \rangle|_q \geq q/2 - m t_\alpha$. It implies that $|b - \langle \mathbf{a}, \mathbf{s} \rangle|_q \leq \gamma t'(1 + \sqrt{m} t_\alpha / K_2) + m t_\alpha \leq q/4$ and $D(\mathsf{sk}, \mathbf{c}) = 0$. We complete the proof. □

4.6 Main Protocol

Let P and V denote the prover and the verifier, respectively. The common input is a pair $(\mathsf{pk}, \mathbf{c})$. The auxiliary input is a pair (σ, r) such that $\mathbf{c} = E_{\mathsf{pk}}(\sigma; r)$.

Define a mapping $\mathcal{G}(\mathsf{pk}, \mathbf{c}) = (\mathbf{B}_{\mathsf{pk}}, \mathbf{x}_{\mathbf{c}}, t')$ where $t' = 4t$ and both $\mathbf{B}_{\mathsf{pk}}$ and $\mathbf{x}_{\mathbf{c}}$ are similar to $\mathcal{F}(\mathsf{pk}, \mathbf{c})$. Let Protocol$'_0$ (or Protocol$'_1$) be Protocol$_0$ (or Protocol$_1$) where $\mathcal{F}(\cdot, \cdot)$ is replaced by $\mathcal{G}(\cdot, \cdot)$ respectively.

Protocol PPK:

Step P1 P selects $\sigma' \in \{0, 1\}$ and $r' \in \{0, 1\}^m$ randomly. P computes $\mathbf{c}' = E_{\mathsf{pk}}(\sigma'; r')$ and sends $\mathbf{c}'$ to V.
Step V1 V sends a random challenge bit $\delta \in \{0, 1\}$ to P.
Step P2 If $\delta = 0$, P sends the pair (σ', r'). If $\delta = 1$, P computes $\sigma'' = \sigma + \sigma' \bmod 2$ and sends σ'' to V. Let $\bar{\mathbf{c}} = (\mathbf{c} + \mathbf{c}') \bmod q$ and runs Protocol$'_{\sigma''}$ on the input $(\mathsf{pk}, \bar{c})$ as the prover.
Step V2 If $\delta = 0$, V accepts if $\mathbf{c}' = E_{\mathsf{pk}}(\sigma'; r')$, else rejects. If $\delta = 1$, V runs the Protocol$'_{\sigma''}$ on the input $(\mathsf{pk}, \bar{\mathbf{c}})$ as the verifier.

Theorem 4.13 (PPK for R05)**.** *The interactive protocol (P, V) is a proof of knowledge system with knowledge error $3/4$ for R_{R05}. Moreover, the protocol (P, V) is a computational zero knowledge under the assumption ISVP.*

Our proof is based on the proof of Goldwasser and Kharchenko [8]. Before describing the proof, we need lemmas that give the properties of the protocols.

Lemma 4.14. *For sufficiently large n,*

1. *If $(\mathsf{sk}, \mathsf{pk})$ be an instance of* R05 *and $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2 \bmod q$ such that $D(\mathsf{sk}, \mathbf{c}) = 0$ and $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{E}(\mathsf{pk}, \cdot)$, $\mathcal{G}(\mathsf{pk}, \mathbf{c})$ is a YES instance of* GapCVP$_\gamma$.
2. *Let $(\mathsf{sk}, \mathsf{pk})$ be an instance of* R05 *and $\mathbf{c} = \binom{\mathbf{a}}{b} \in \mathbb{Z}_q^{n+1}$. If $|b - \langle \mathbf{a}, \mathbf{s} \rangle|_q > q/8$, then $\mathcal{G}(\mathsf{pk}, \mathbf{c})$ is a NO instance of* GapCVP$_\gamma$.

Lemma 4.15. *For sufficiently large n,*

1. *If $(\mathsf{sk}, \mathsf{pk})$ be an instance of* R05 *and $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2 \bmod q$ such that $D(\mathsf{sk}, \mathbf{c}) = 1$ and $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{E}(\mathsf{pk}, \cdot)$, $\mathcal{G}(\mathsf{pk}, \mathbf{y})$ is a YES instance of* GapCVP$_\gamma$*, where $\mathbf{y} = \mathbf{c} - \lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q$.*
2. *Let $(\mathsf{sk}, \mathsf{pk})$ be an instance of* R05 *and $\mathbf{c} = \binom{\mathbf{a}}{b} \in \mathbb{Z}_q^{n+1}$. If $|b - \langle \mathbf{a}, \mathbf{s} \rangle|_q > 3q/8$, then $\mathcal{G}(\mathsf{pk}, \mathbf{y})$ is a NO instance of* GapCVP$_\gamma$*, where $\mathbf{y} = \mathbf{c} - \lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q$.*

The proofs of Lemma 4.14 and Lemma 4.15 are in Appendix B. Let us prove Theorem 4.13.

Proof of completeness. Since it is evident, we omit the proof. □

Proof of validity with error $3/4$. Let $\mathsf{pk} = \{(\mathbf{a}_i, b_i)\}_{i=1,\dots,m}$ be a public key of R05 and $\mathbf{c} = (\mathbf{a}, b) \in \mathbb{Z}_q^{n+1}$. Let P^* be an arbitrary prover that make V accept with probability $\epsilon + 3/4$ for $\epsilon > 0$ on the common input $(\mathsf{pk}, \mathbf{c})$.

We construct a knowledge extractor K as follows. K's input is $(\mathsf{pk}, \mathbf{c})$. First, K chooses a random tape of P^*. Let δ_1 denote a challenge bit in Protocol$'_{\sigma''}$. K runs P^* three times, where the challenge bits are 0, $(1, 0)$ and $(1, 1)$. K obtains three views T_0, T_1, and T_2. Views are in forms that $T_0 = (\mathbf{c}', 0, \sigma', r')$, $T_1 = (\mathbf{c}', 1, \sigma'', T'_1)$, and $T_2 = (\mathbf{c}', 1, \sigma'', T'_2)$, where T'_1 and T'_2 are transcripts of Protocol$'_{\sigma''}$ that δ_1 are 0 and 1 respectively. If any one of three views is rejected, K outputs $\perp$ and halts. Otherwise, i.e., three views are accepted, K obtains a vector $\mathbf{p}$ that is witness of GapCVP_γ using the extractor of $\mathrm{Protocol}'_0$ or $\mathrm{Protocol}'_1$. K outputs $(\mathbf{c}', \sigma', r', \sigma'', \mathbf{p})$ and halts.

Note that the probability K does not output $\perp$ is at least $\Theta(\epsilon)$. Therefore, K is indeed the knowledge extractor. □

Proof of zero-knowledge of PPK. Let $S_{\sigma''}$ be a simulator for $\mathrm{Protocol}'_{\sigma''}$. We construct a simulator S as follows:

Step P1 Chooses $\Delta \in \{0, 1\}$ randomly (a predictor of a challenge bit). If $\Delta = 0$, chooses σ', r' randomly and computes $\mathbf{c}' = E_{\mathsf{pk}}(\sigma'; r')$. If $\Delta = 1$, chooses σ'', r'' randomly, computes $\overline{\mathbf{c}} = E_{\mathsf{pk}}(\sigma''; r'')$, and sets $\mathbf{c}' = \overline{\mathbf{c}} - \mathbf{c} \bmod q$. Sends $\mathbf{c}'$ to V^*.

Step V1 Receives a challenge bit δ from V^*.

Step P2, V2 If $\Delta \neq \delta$, outputs $\perp$ and halts. If $\Delta = \delta = 0$ outputs $(\mathbf{c}', \delta, \sigma', r')$. If $\Delta = \delta = 1$, invoke $S_{\sigma''}$ with input $(\mathsf{pk}, \overline{\mathbf{c}})$. Let $T = S_{\sigma''}(\mathsf{pk}, \overline{\mathbf{c}})$. Outputs $(\mathbf{c}', \delta, \sigma'', T)$ and halts.

We assume that ISVP holds, hence according to the security property of R05 if $\Delta = 0$ then $\mathbf{c}'$ is computationally indistinguishable from the uniform distribution on $\mathbb{Z}_q^{n+1}$; if $\Delta = 0$ then $\mathbf{c}' = \overline{\mathbf{c}} - \mathbf{c} \bmod q$ is also indistinguishable from the uniform distribution. Therefore, the generated transcripts is computationally indistinguishable from a real transcript. □

5 Concluding Remarks

In this paper we constructed PPKs for R04 and R05.

We list up a few open problems: Verifiable decryption for the lattice-based cryptosystems and non-malleable proofs for plaintext knowledge for the lattice-based cryptosystems. The former has many applications. The latter are sources of interactive CCA2-secure cryptosystems.

References

[1] Ajtai, M. Representing hard lattices with $O(n \log n)$ bits. In Gabow and Fagin [3], pp. 94–103.

[2] Ajtai, M., and Dwork, C. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings on 29th Annual ACM Symposium on Theory of Computing (STOC '97)* (El Paso, Texas, USA, May 1997), ACM, pp. 284–293. See also ECCC TR96-065.

[3] Gabow, H. N., and Fagin, R., Eds. *Proceedings on the 37th Annual ACM Symposium on Theory of Computing (STOC 2005)* (Baltimore, MD, USA, May 2005), ACM.

[4] Galil, Z., Haber, S., and Yung, M. Symmetric public-key encryption. In *Advances in Cryptology – CRYPTO '85* (Santa Barbara, California, USA, August 1985), H. C. Williams, Ed., vol. 218 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 128–137.

[5] Goldreich, O. *Foundations of Cryptography: Basic Tools*. Cambridge University Press, 2001.

[6] Goldreich, O., and Goldwasser, S. On the limits of nonapproximability of lattice problems. *Journal of Computer and System Sciences 60*, 3 (2000), 540–563.

[7] Goldreich, O., Goldwasser, S., and Halevi, S. Eliminating decryption errors in the Ajtai-Dwork cryptosystem. In *Advances in Cryptology – CRYPTO '97* (Santa Barbara, California, USA, August 1997), B. S. Kaliski, Jr., Ed., vol. 1294 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 105–111. See also ECCC TR97-018.

[8] Goldwasser, S., and Kharchenko, D. Proof of plaintext knowledge for the Ajtai-Dwork cryptosystem. In *Theory of Cryptography, 2nd Theory of Cryptography Conference, TCC 2005* (Cambridge, MA, USA, February 2005), J. Kilian, Ed., vol. 3378 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 529–555.

[9] Kawachi, A., Tanaka, K., and Xagawa, K. Multi-bit cryptosystems based on lattice problems, 2006. Manuscript.

[10] Lenstra, A. K., Lenstra, H. W., and Lovász, L. Factoring polynomials with rational coefficients. *Mathematische Annalen 261*, 4 (1982), 513–534.

[11] Micciancio, D., and Goldwasser, S. *Complexity of Lattice Problems: a cryptographic perspective*, vol. 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, March 2002.

[12] Micciancio, D., and Vadhan, S. Statistical zero-knowledge proofs with efficient provers: Lattice problems and more. In *Advances in Cryptology – CRYPTO 2003* (Santa Barbara, California, USA, August 2003), D. Boneh, Ed., vol. 2729 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 282–298.

[13] Nguyen, P. Q., and Stern, J. Cryptanalysis of the Ajtai-Dwork cryptosystem. In *Advances in Cryptology – CRYPTO '98* (Santa Barbara, California, USA, August 1998), H. Krawczyk, Ed., vol. 1462 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 223–242.

[14] Regev, O. New lattice-based cryptographic constructions. *Journal of the ACM 51*, 6 (2004), 899–942. Preliminary version in *STOC 2003*, 2003.

[15] Regev, O. On lattices, learning with errors, random linear codes, and cryptography. In Gabow and Fagin [3], pp. 84–93.

A Proof of Lemmas

Proof of Lemma 3.14. **(1)** There are two cases that c can decrypts into 0: when both c_1 and c_2 are ciphertexts of 0 and when both are ciphertexts of 1.

Suppose that $c_1, c_2 \in \mathcal{E}(\mathsf{pk}, 0)$. From Lemma 3.6, $\mathrm{Dist}\left(\binom{K_1 c_i}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le t$ for $i = 1, 2$. By Lemma A.1 below, Thus, for $c = c_1 + c_2 \bmod N$, we have that

$$\mathrm{Dist}\left(\begin{pmatrix} K_1 c \\ \mathbf{0} \end{pmatrix}, L(\mathbf{B}_{\mathsf{pk}})\right) \le 2t + 1 \le 4t = t'.$$

Next, suppose that $c_1, c_2 \in \mathcal{E}(\mathsf{pk}, 1)$. Thus, for $i = 1, 2$, $\overline{c_i} = c_i - v_{i_0}/2 \bmod N \in \mathcal{E}(\mathsf{pk}, 0)$. By Lemma A.1 below, we have that for $\overline{c} = \overline{c_1} + \overline{c_2} \bmod N$, $\mathrm{Dist}\left(\binom{K_1 \overline{c}}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le 2t + 1$. Consider the vector $c = \overline{c} + v_{i_0} \bmod N$. By Lemma A.2, we have that

$$\mathrm{Dist}\left(\begin{pmatrix} K_1 c \\ \mathbf{0} \end{pmatrix}, L(\mathbf{B}_{\mathsf{pk}})\right) \le 2t + 1 + \sqrt{K_2^2 + 1} \le 4t = t'.$$

(2) Let $c \in \{0, 1, \ldots, N - 1\}$ be any ciphertext such that $\mathrm{frc}\,(c/d) > 1/8$. Let $T = \gamma t'$. Note that $T/n^4 \le 1/8 < \mathrm{frc}\,(c/d)$. Hence, by Claim 3.7 $\mathrm{Dist}\left(\binom{K_1 c}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le T$ can not hold. Thus, $\mathcal{G}(\mathsf{pk}, c)$ is a NO instance of the GapCVP_γ. □

Proof of Lemma 3.15. **(1)** Without a loss of generality, we suppose that $c_1 \in \mathcal{E}(\mathsf{pk}, 0)$ and $c_2 \in \mathcal{E}(\mathsf{pk}, 1)$. Since c_1 is a legal ciphertext of 0, from Lemma 3.6, for some $\mathbf{p}_1 \in L(\mathbf{B}_{\mathsf{pk}})$, $\mathrm{Dist}\left(\binom{K_1 c_1}{\mathbf{0}}, \mathbf{p}_1\right) \le t$. Since c_1

is a legal ciphertext of 1, from Lemma 3.9, for some $\mathbf{p}_2 \in L(\mathbf{B}_{\mathsf{pk}})$, $\mathrm{Dist}\left(\binom{K_1(c_2-v_{i_0}/2 \bmod N)}{\mathbf{0}}, \mathbf{p}_2\right) \le t$. Hence, from $y = c_1 + c_2 - v_{i_0}/2 \bmod N$, we obtain

$$\mathrm{Dist}\left(\binom{K_1 y}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le 2t + 1 \le 4t = t'$$

by Lemma A.1.

(2) Let $c \in \{0, 1, \dots, N-1\}$ be any ciphertext such that $\mathrm{frc}\,(c/d) < 3/8$. In this case, we obtain that $\mathrm{frc}\,(y/d) > 1/4$ in a similar way to the proof of Lemma 3.9. Let $T = \gamma t'$. Note that $T/n^4 \le 1/4 < \mathrm{frc}\,(y/d)$. Hence, by Claim 3.7 $\mathrm{Dist}\left(\binom{K_1 y}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le T$ can not hold. Thus, $\mathcal{G}(\mathsf{pk}, y)$ is a NO instance of the GapCVP$_\gamma$. □

Lemma A.1. *Let* pk *be a public key of* R04, $\mathbf{p}_1$ *and* $\mathbf{p}_2$ *points from* $L(\mathbf{B}_{\mathsf{pk}})$. *If for* $c_1, c_2 \in \{0, 1, \dots, N-1\}$, $\mathrm{Dist}\left(\binom{K_1 c_1}{\mathbf{0}}, \mathbf{p}_1\right) \le d_1$ *and* $\mathrm{Dist}\left(\binom{K_1 c_2}{\mathbf{0}}, \mathbf{p}_2\right) \le d_2$, *then* $\mathrm{Dist}\left(\binom{K_1(c_1+c_2 \bmod N)}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le d_1 + d_2 + 1$.

Proof. Represent $K_1(c_1 + c_2 \bmod N) = K_1(c_1 + c_2 + \alpha_1 N)$. Since both vectors c_1 and c_2 belong to $\{0, 1, \dots, N-1\}$, we can bound $|\alpha_1| \le 1$. Consider a vector $\mathbf{p} = \mathbf{B}_{\mathsf{pk}}{}^t(\alpha_1, 0, \dots, 0)$. Thus, we obtain that

$$\mathrm{Dist}\left(\binom{K_1 \alpha N}{\mathbf{0}}, \mathbf{p}\right) \le 1.$$

By the triangle inequality, the lemma follows. □

Lemma A.2. *Let* pk *be a public key of* R04 *and* $\mathbf{p}$ *a point from* $L(\mathbf{B}_{\mathsf{pk}})$. *If for* $c \in \{0, 1, \dots, N-1\}$, $\mathrm{Dist}\left(\binom{K_1 c}{\mathbf{0}}, \mathbf{p}\right) = d$ *then* $\mathrm{Dist}\left(\binom{K_1(c+v_{i_0} \bmod N)}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le d + \sqrt{K_2^2 + 1}$.

Proof. Represent $K_1(c + v_{i_0} \bmod N) = K_1(c + v_{i_0} + \alpha_1 N)$ for some $\alpha_1 \in \{-1, 0\}$. Consider a vector $\mathbf{p}'$ in $L(\mathbf{B}_{\mathsf{pk}})$ such that $\mathbf{p}' = L(\mathbf{B}_{\mathsf{pk}})^t(0, \dots, 0, 1, 0, \dots, 0)$ (with 1 at the $(i_0 + 1)$-th position). By the construction of $\mathbf{B}_{\mathsf{pk}}$, we have that $\mathrm{Dist}\left(\binom{K_1(v_{i_0}+\alpha_1 N)}{\mathbf{0}}, \mathbf{p}'\right) \le \sqrt{K_2^2 + 1}$. By the triangle inequality, the lemma follows. □

B Proof of Lemmas

Proof of Lemma 4.14.

(1) There are two cases that $\mathbf{c}$ can decrypts into 0: when both $\mathbf{c}_1$ and $\mathbf{c}_2$ are ciphertexts of 0 and when both are ciphertexts of 1.

Suppose that $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{E}(\mathsf{pk}, 0)$. From Lemma 4.6, $\mathrm{Dist}\left(\binom{K_1 \mathbf{c}_i}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le t$ for $i = 1, 2$. By Lemma B.1 below, Thus, for $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2 \bmod q$, we have that

$$\mathrm{Dist}\left(\binom{K_1 \mathbf{c}}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le 2t + \sqrt{n+1} \le 4t = t'.$$

Next, suppose that $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{E}(\mathsf{pk}, 1)$. Thus, for $i = 1, 2$, $\bar{\mathbf{c}}_i = \mathbf{c}_i - \lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q \in \mathcal{E}(\mathsf{pk}, 0)$. By Lemma B.1 below, we have that for $\bar{\mathbf{c}} = \bar{\mathbf{c}}_1 + \bar{\mathbf{c}}_2 \bmod q$, $\mathrm{Dist}\left(\binom{K_1 \bar{\mathbf{c}}}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le 2t + \sqrt{n+1}$. Consider the vector $\mathbf{c} = \bar{\mathbf{c}}_1 + \bar{\mathbf{c}}_2 + 2\lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q$. Since q is a prime, we have $2\lfloor q/2 \rfloor = q - 1$. By Lemma B.2 below, we have that $\mathrm{Dist}\left(\binom{K_1 \mathbf{c}}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le 2t + \sqrt{n+1} + 1 \le 4t = t'$.

(2) Let $\mathbf{c} = \binom{\mathbf{a}}{b} \in \mathbb{Z}_q^{n+1}$ be any ciphertext such that $|b - \langle \mathbf{a}, \mathbf{s} \rangle|_q > q/8$. Let $T = \gamma t'$. Recall that $T(1 + \sqrt{m} t_\alpha / K_2) \le q/8 < |b - \langle \mathbf{a}, \mathbf{s} \rangle|_q$. Hence, by Claim 4.7 $\mathrm{Dist}\left(\binom{K_1 \mathbf{c}}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le T$ can not hold. Thus, $\mathcal{G}(\mathsf{pk}, \mathbf{c})$ is a NO instance of the GapCVP$_\gamma$. □

Proof of Lemma 4.15. **(1)** Without loss of generality, we suppose that $\mathbf{c}_1 \in \mathcal{E}(\mathsf{pk}, 0)$ and $\mathbf{c}_2 \in \mathcal{E}(\mathsf{pk}, 1)$. From Lemma 4.6 and Lemma 4.9, for some $\mathbf{p}_1, \mathbf{p}_2 \in L(\mathbf{B}_{\mathsf{pk}})$ $\mathrm{Dist}\left(\binom{K_1 \mathbf{c}_1}{\mathbf{0}}, \mathbf{p}_1\right) \le t$ and $\mathrm{Dist}\left(\binom{K_1(\mathbf{c}_2 - \lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q)}{\mathbf{0}}, \mathbf{p}_2\right) \le t$. Hence, from $\mathbf{y} = \mathbf{c}_1 + \mathbf{c}_2 - \lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q$, we obtain

$$\mathrm{Dist}\left(\binom{K_1 \mathbf{y}}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \le 2t + 1 \le 4t = t'$$

by Lemma B.1.

(2) Let $\mathbf{c} = \binom{\mathbf{a}}{b} \in \mathbb{Z}_q^{n+1}$ be any ciphertext such that $|b - \langle \mathbf{a}, \mathbf{s} \rangle|_q \leq 3q/8$. Let $\mathbf{y} = \binom{\mathbf{a}'}{b'}$. In this case, we obtain that $|b' - \langle \mathbf{a}', \mathbf{s} \rangle|_q \geq q/8$. Let $T = \gamma t'$. Note that $T(1 + \sqrt{m} t_\alpha / K_2) \leq q/8 < |b' - \langle \mathbf{a}', \mathbf{s} \rangle|_q$. Hence, by Claim 4.7 $\mathrm{Dist}\left(\binom{K_1 \mathbf{y}}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \leq T$ can not hold. Thus, $\mathcal{G}(\mathsf{pk}, \mathbf{y})$ is a NO instance of GapCVP_γ. □

Lemma B.1. *Let* pk *be a public key of* R05, $\mathbf{p}_1$ *and* $\mathbf{p}_2$ *points from* $L(\mathbf{B}_{\mathsf{pk}})$. *If for* $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{Z}_q^{n+1}$, $\mathrm{Dist}\left(\binom{K_1 \mathbf{c}_1}{\mathbf{0}}, \mathbf{p}_1\right) = d_1$ *and* $\mathrm{Dist}\left(\binom{K_1 \mathbf{c}_2}{\mathbf{0}}, \mathbf{p}_2\right) = d_2$, *then* $\mathrm{Dist}\left(\binom{K_1(\mathbf{c}_1 + \mathbf{c}_2 \bmod q)}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \leq d_1 + d_2 + \sqrt{n+1}$.

Proof. Represent $K_1(\mathbf{c}_1 + \mathbf{c}_2 \bmod q) = K_1(\mathbf{c}_1 + \mathbf{c}_2 + \sum_{i=1}^{n+1} \alpha_i q \mathbf{u}_i)$. Since both vectors $\mathbf{c}_1$ and $\mathbf{c}_2$ belong to $\{0, 1, \ldots, q-1\}^{n+1}$, we can bound $|\alpha_i| \leq 1$ for all i. Consider a vector $\mathbf{p}_3 = {\mathbf{B}_{\mathsf{pk}}}^t(\alpha_1, \ldots, \alpha_{n+1}, 0, \ldots, 0)$. Thus, we obtain that

$$\mathrm{Dist}\left(\begin{pmatrix} K_1 \sum_{i=1}^{n+1} \alpha_i q \mathbf{u}_i \\ \mathbf{0} \end{pmatrix}, \mathbf{p}_3\right) \leq \sqrt{\sum_{i=1}^{n+1} \alpha_i^2} \leq \sqrt{n+1}.$$

By the triangle inequality, the lemma follows. □

Lemma B.2. *Let* pk *be a public key of* R05 *and* $\mathbf{p}$ *a point from* $L(\mathbf{B}_{\mathsf{pk}})$. *If for* $\mathbf{c} \in \mathbb{Z}_q^{n+1}$, $\mathrm{Dist}\left(\binom{K_1 \mathbf{c}}{\mathbf{0}}, \mathbf{p}\right) = d$ *then* $\mathrm{Dist}\left(\binom{K_1(\mathbf{c} + 2\lfloor q/2 \rfloor \mathbf{u}_{n+1} \bmod q)}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \leq d + 1$.

Proof. Since q is an odd prime, we have that $2\lfloor q/2 \rfloor = q - 1$. Represent $K_1(\mathbf{c} + (q-1)\mathbf{u}_{n+1} \bmod q) = K_1(\mathbf{c} + (q-1)\mathbf{u}_{n+1} + \alpha_{n+2}(q-1)\mathbf{u}_{n+1})$ for some $\alpha \in \{-1, 0\}$. Consider a vector $\mathbf{p}'$ in $L(\mathbf{B}_{\mathsf{pk}})$ such that $\mathbf{p}' = L(\mathbf{B}_{\mathsf{pk}})^t(0, \ldots, 0, \alpha_{n+2}, 0, \ldots, 0)$ (with 1 at the $(n+2)$-th position). By the construction of $\mathbf{B}_{\mathsf{pk}}$, we have that $\mathrm{Dist}\left(\binom{K_1((q-1)\mathbf{u}_{n+1} + \alpha_{n+2}(q-1)\mathbf{u}_{n+1})}{\mathbf{0}}, L(\mathbf{B}_{\mathsf{pk}})\right) \leq 1$. By the triangle inequality, the lemma follows. □