Classical Reduction of Gap SVP to LWE: A Concrete Security Analysis

Palash Sarkar and Subhadip Singha
Applied Statistics Unit
Indian Statistical Institute
203, B.T.Road, Kolkata, India - 700108.
{palash, subha_r}@isical.ac.in

February 10, 2021

Abstract

Regev (2005) introduced the learning with errors (LWE) problem and showed a quantum reduction from a worst case lattice problem to LWE. Building on the work of Peikert (2009), a classical reduction from the gap shortest vector problem to LWE was obtained by Brakerski et al. (2013). A concrete security analysis of Regev's reduction by Chatterjee et al. (2016) identified a huge tightness gap. The present work performs a concrete analysis of the tightness gap in the classical reduction of Brakerski et al. It turns out that the tightness gap in the Brakerski et al. classical reduction is even larger than the tightness gap in the quantum reduction of Regev. This casts doubts on the implication of the reduction to security assurance of practical cryptosystems.

Keywords: lattices, shortest vector problem, learning with errors, classical reduction, concrete analysis.

Mathematics Subject Classification: Primary: 94A60

1 Introduction

In a landmark paper, Regev [16] introduced the learning with errors (LWE) problem. Many cryptosystems have based their security on the hardness of variants of the LWE problem. Examples of such cyptosystems are Frodo [2], Kyber [3], LAC [13], NewHope [1], Round5 [4] and Saber [8] all of which are candidates for standardisation as a post-quantum cryptosystem to be selected by the NIST of the USA. A stated reason for confidence in the hardness of the LWE problem is a reduction proved by Regev [16] from a worst-case lattice problem to LWE. The reduction obtained by Regev was quantum, i.e., the algorithm is required to make some quantum computations.

A problem left open by Regev was whether there is a classical reduction from a worst case lattice problem to LWE. The initial answer to this problem was provided by Peikert [15]. While this represented progress, Peikert's reduction was not considered to be satisfactory since either an exponential size modulus is required or, the lattice problem considered is not one of the standard problems. Later work by Brakerski et al. [6] built on Peikert's work to show a classical reduction from a standard lattice problem to LWE avoiding the exponential size modulus.

The works of Regev [16], Peikert [15] and Brakerski et al. [6] are all in the asymptotic setting where the lattice dimension is allowed to go to infinity. Practical cryptosystems, on the other hand, have a fixed value of the lattice dimension. So, it is of interest to know what kind of security assurance one obtains from the results of [16, 15, 6] for practical cryptosystems. Suppose it is believed that a lattice problem $\mathcal{P}$ is computationally hard. It is desired to translate this into a belief that a particular cryptosystem $\mathcal{C}$ is difficult to break, i.e., the difficulty of solving $\mathcal{P}$ is reduced to the difficulty of breaking $\mathcal{C}$. In other words, it is required to show that if there is an algorithm $\mathcal{A}$ to break $\mathcal{C}$, then there is an algorithm $\mathcal{B}$ (which uses $\mathcal{A}$ as an oracle) to solve $\mathcal{P}$. Suppose $\mathcal{A}$ takes time T and has success probability P_S and further, $\mathcal{B}$ takes time T' and has success probability P'_S. The tightness gap of the reduction is defined to be $(T'/P'_S)/(T/P_S)$. The reduction is said to be tight if the tightness gap is one (or, small). On the other hand, if the tightness gap is very large, then the usefulness of the reduction for obtaining security assurance of a practical cryptosystem becomes questionable.

The tightness gap of the reduction given by Regev was first investigated in [7] and in more details in [17]. The results of [7, 17] indicate that the tightness gap is very large. Based on the analysis in [7], Bernstein [5] comments that "the loss of tightness is gigantic" in [16].

In this paper, we follow up on [7, 17] and perform a concrete security analysis of the tightness gap of the reduction in [6]. The reduction of Peikert [15] is a step in the reduction performed by Brakerski et al. [6]. As a first step, we work out the tightness gap of Peikert's reduction. Then we follow the proof strategy in Brakerski et al. [6] and finally work out the end-to-end tightness gap of the classical reduction from the gap shortest vector problem to the LWE. There are two aspects to the concrete analysis. The first is a quadratic loss in the dimension of the lattice and the second is a loss of tightness. The loss of tightness in this classical reduction is more than that of the original quantum reduction by Regev [16]. The quadratic loss in the dimension was already pointed out in [6]. Due to this quadratic loss, Brakerski et al. put forward the open question of obtaining a reduction without such a loss mentioning that this would amount to a full de-quantization of Regev's reduction. The paper [6], however, does not consider the issue of the loss in tightness. Our analysis shows that due to this loss of tightness, the reduction is not very meaningful in practice, especially for determining the sizes of the parameters of a cryptosystem which would purportedly enjoy the protection offered by the hardness of a well studied worst case lattice problem.

2 Preliminaries

Fix a positive integer n. Let $\mathbf{B}$ be an $n \times n$ matrix whose columns are n linearly independent vectors in $\mathbb{R}^n$. The lattice $L = L(\mathbf{B})$ generated by $\mathbf{B}$ is the set of all vectors $\mathbf{Ba}$ where $\mathbf{a} = (a_1, \ldots, a_n)^\intercal \in \mathbb{Z}^n$. The columns of $\mathbf{B}$ (or, more generally $\mathbf{B}$ itself) is called a basis of the lattice L. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ denote the columns of $\mathbf{B}$. The Gram-Schmidt orthogonalisation (GSO) of $\mathbf{b}_1, \ldots, \mathbf{b}_n$ will be denoted as $\widetilde{\mathbf{b}}_1, \ldots, \widetilde{\mathbf{b}}_n$.

The length of a vector in L will be considered to be given by its Euclidean norm. For $i \in \{1, \ldots, n\}$, let $\lambda_i(L)$ be the least real number r such that L has i linearly independent vectors with the longest having length r. In particular, we will be interested in $\lambda_1(L)$, which is the smallest possible length of any non-zero lattice vector.

The dual of a lattice L is denoted as L^* and is defined to be the set of all vectors $\mathbf{y} \in \mathbb{R}^n$ such that $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x} \in L$. Given a basis $\mathbf{B}$ for L, the matrix $\mathbf{B}^* = (\mathbf{B}^{-1})^\intercal$ is a basis for L^* and is called the dual basis of $\mathbf{B}$.

Since $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$, the quotient group $\mathbb{R}/\mathbb{Z}$ is represented by the interval $\mathbb{T} = [0, 1)$ with addition modulo 1. The cyclic subgroup $\{0, 1/p, \ldots, (p-1)/p\}$ of $\mathbb{T}$ of order p will be denoted by $\mathbb{T}_p$. The normal distribution with mean μ and standard deviation σ will be denoted as $\mathcal{N}(\mu, \sigma)$. For $\alpha \in (0, 1)$, Ψ_α is the probability distribution over $\mathbb{T}$ obtained by sampling from $\mathcal{N}(0, \alpha/\sqrt{2\pi})$ and reducing the result modulo 1.

Fix an integer $p \geq 2$. Let $\mathbf{s}$ be chosen uniformly at random from $\mathbb{Z}_p^n$. Let χ be a probability distribution on $\mathbb{Z}_p$. The distribution $A_{p,\mathbf{s},\chi}$ on $\mathbb{Z}_p^n \times \mathbb{Z}_p$ is defined as follows: choose $\mathbf{a}$ uniformly at random from $\mathbb{Z}_p^n$; e from $\mathbb{Z}_p$ following χ and output $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$, where the addition is performed modulo p. Let ϕ be a probability density function on $\mathbb{T}$. The distribution $A_{p,\mathbf{s},\phi}$ is defined as follows: choose $\mathbf{a}$ uniformly at random from $\mathbb{Z}_p^n$; e from $\mathbb{T}$ following ϕ and output $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle / p + e)$, where the addition is performed modulo 1. When $\phi = \Psi_\alpha$, the distribution $A_{p,\mathbf{s},\Psi_\alpha}$ is written more conveniently as $A_{p,\mathbf{s},\alpha}$.

For $\mathbf{x} \in \mathbb{R}^n$ and $s > 0$, define $\rho_s(\mathbf{x}) = \exp\left(-\pi ||\mathbf{x}||^2/s^2\right)$. For a lattice L, define $\rho_s(L) = \sum_{\mathbf{x} \in L} \rho_s(\mathbf{x})$. The discrete Gaussian distribution $D_{L,s}$ on a lattice L assigns to a vector $\mathbf{v} \in L$ the probability $D_{L,s}(\mathbf{v}) = \rho_s(\mathbf{v})/\rho_s(L)$. For a lattice L and a real number $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(L)$ is the smallest s such that

$\rho_{1/s}(L^* \setminus \{0\}) \leq \epsilon$.

The origin centered parallelopiped $\mathcal{P}_{1/2}(\mathbf{B})$ of a basis $\mathbf{B}$ is defined to be $\mathcal{P}_{1/2}(\mathbf{B}) = \{\mathbf{Bc} : \mathbf{c} \in [-1/2, 1/2)^n\}$. For $\mathbf{w} \in \mathbb{R}^n$ and basis $\mathbf{B}$, the vector $\mathbf{x} = \mathbf{w} \bmod \mathbf{B}$ is the unique $\mathbf{x} \in \mathcal{P}_{1/2}(\mathbf{B})$ such that $\mathbf{w} - \mathbf{x} \in L(\mathbf{B})$; further, $\mathbf{x} = \mathbf{B}(\mathbf{B}^{-1}\mathbf{w} - \lfloor \mathbf{B}^{-1}\mathbf{w} \rceil)$.

Let X be a random variable taking values in a set D and S be a subset of D. By $f_X(S)$ we denote the probability that X takes values in S. Given two random variables X and Y over D, the statistical distance between them is denoted as $\Delta(X, Y)$ and is defined to be $\Delta(X, Y) = \max_{S \subseteq D} |f_X(S) - f_Y(S)|$.

By $\mathcal{B}_n$ we will denote the open ball in $\mathbb{R}^n$ of unit radius, i.e., $\mathcal{B}_n = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| < 1\}$. For a real number d and $\mathbf{z} \in \mathbb{R}^n$, the open ball in $\mathbb{R}^n$ centered at $\mathbf{z}$ and of radius d will be denoted as $\mathbf{z} + d \cdot \mathcal{B}_n$. The notation $\mathbf{w} \xleftarrow{\$} \mathbf{z} + d \cdot \mathcal{B}_n$ denotes the choice of a vector $\mathbf{w}$ drawn uniformly from $\mathbf{z} + d \cdot \mathcal{B}_n$.

2.1 Computational Problems

Let φ be a real valued function defined on lattices. The discrete Gaussian sampling (DGS_φ) problem is the following: An instance is a pair $(\mathbf{B}, r)$, where $\mathbf{B}$ is a basis of an n-dimensional lattice $L = L(\mathbf{B})$ and $r > \varphi(L)$ is a real number. The task is to obtain a sample from $D_{L,r}$.

A variant of the closest vector problem (CVP) was considered in [16]: An instance is a triplet $(\mathbf{B}, d, \mathbf{x})$, where $\mathbf{B}$ is the basis of an n-dimensional lattice $L = L(\mathbf{B})$, d is a positive real number with $d < \lambda_1(L)/2$, and $\mathbf{x} \in \mathbb{R}^n$ which is within distance d of L. The task is to find the closest lattice point to $\mathbf{x}$ (since $d < \lambda_1(L)/2$, there is a unique closest vector). This problem is also the bounded distance decoding problem [12].

The (worst-case) learning with errors problem $\mathrm{LWE}_{n,p,\chi}$ is the following. Let $\mathbf{s}$ be an element of $\mathbb{Z}_p^n$. Given samples from $A_{p,s,\chi}$, it is required to output $\mathbf{s}$. If the number of samples is m, then the problem is denoted as $\mathrm{LWE}_{n,m,p,\chi}$. Similarly, for a probability density function ϕ on $\mathbb{T}$, the $\mathrm{LWE}_{n,m,p,\phi}$ problem is the following. For uniform random $\mathbf{s}$ in $\mathbb{Z}_p^n$, given samples from $A_{p,s,\phi}$, it is required to output $\mathbf{s}$. If the number of samples is m, then the problem is denoted as $\mathrm{LWE}_{n,m,p,\phi}$. Both versions of the LWE problem were introduced by Regev in [16]. When $\phi = \Psi_\alpha$, the problem $\mathrm{LWE}_{n,m,p,\phi}$ is more conveniently written as $\mathrm{LWE}_{n,m,p,\alpha}$.

Let $\mathbf{s}$ be an element of $\mathbb{Z}_q^n$. The (worst-case) decision version of the LWE problem is to distinguish the uniform distribution over $\mathbb{T}_q^n \times \mathbb{T}$ from $A_{q,\mathbf{s},\alpha}$. The average-case version of the decision LWE problem, $\mathrm{decLWE}_{n,m,q,\alpha}$, is to distinguish the uniform distribution $\mathbb{T}_q^n \times \mathbb{T}$ from $A_{q,\mathbf{s},\alpha}$ for a non-negligible fraction of all possible $\mathbf{s}$, where a list of m independent samples of the relevant distribution is provided as input. Regev [16] showed a reduction of the worst-case decision LWE problem to the average-case LWE problem and the tightness gap of this reduction has been worked out in [7]. Suppose $\mathbf{s}$ is chosen uniformly at random from $\{0, 1\}^n$. The $\mathrm{binLWE}_{n,m,q,\alpha}$ problem is to distinguish the uniform distribution over $\mathbb{T}_q^n \times \mathbb{T}$ from $A_{q,\mathbf{s},\alpha}$, where a list of m independent samples of the relevant distribution is provided as input. The difference between the decLWE and the binLWE problem lies in the method to select the secret $\mathbf{s}$. Given $n, q \geq 1$ and $\alpha \in (0, 1)$, $\mathrm{binLWE}_{n,m,q,\leq\alpha}$ is the problem which requires to solve $\mathrm{binLWE}_{n,m,q,\beta}$ for any $\beta = \beta(\mathbf{s}) \leq \alpha$ [6].

Let $\gamma(n) \geq 1$ be a function from the naturals to the naturals. The problem SIVP_γ is the following: An instance is a basis $\mathbf{B}$ of an n-dimensional lattice $L = L(\mathbf{B})$ and the task is to obtain a set of n linearly independent vectors from L whose lengths are at most $\gamma(n) \cdot \lambda_n(L)$. The problem GapSVP_γ is the following: An instance is a pair $(\mathbf{B}, d)$, where $\mathbf{B}$ is a basis of an n-dimensional lattice $L = L(\mathbf{B})$ and $d > 0$ is a real number. The instance is a YES instance if $\lambda_1(L) \leq d$ and it is a NO instance if $\lambda_1(L) \geq \gamma(n) \cdot d$.

The problem ζ-to-γ-GapSVP (denoted as $\mathrm{GapSVP}_{\zeta,\gamma}$) was introduced in [15]. For functions $\zeta(n) \geq \gamma(n) \geq 1$, an instance of $\mathrm{GapSVP}_{\zeta,\gamma}$ is a pair $(\mathbf{B}, d)$, where $\mathbf{B}$ is a basis of an n-dimensional lattice $L = L(\mathbf{B})$ for which $\lambda_1(L) \leq \zeta(n)$, $\min_i \|\widetilde{\mathbf{b}}_i\| \geq 1$, and $1 \leq d \leq \zeta(n)/\gamma(n)$. The instance is a YES instance if $\lambda_1(L) \leq d$ and it is NO instance if $\lambda_1(L) > \gamma(n) \cdot d$. It has been shown in [15] that for $\zeta(n) \geq 2^{n/2}$, the $\mathrm{GapSVP}_{\zeta,\gamma}$ problem is equivalent to the standard GapSVP_γ problem.

3 Reducing DGS to LWE

Regev [16] described a quantum algorithm which given access to an LWE oracle can solve the SIVP (or, the GapSVP). In the first step, the SIVP is reduced to the DGS problem using a classical algorithm. The main part of the proof is a quantum algorithm which reduces the DGS problem to the LWE problem. The proof given by Regev [16] is in an asymptotic setting. A concrete analysis of the tightness gap in the reduction was carried out in [7] and in more details in [17]. We provide a brief overview of Regev's DGS-to-LWE reduction using some of the terminology used in [17].

Let p be a positive integer and $\alpha \in (0, 1)$. Assume that an oracle $\mathsf{solveLWE}_{n,n^c,p,\Psi_\alpha}(\mathcal{I})$ is available for some constant $c > 0$. The input $\mathcal{I}$ to the oracle consists of n^c samples from $A_{p,\mathbf{s},\Psi_\beta}$ for some $0 < \beta \leq \alpha$. The oracle is guaranteed to work correctly if $\beta = \alpha$, otherwise it might return an incorrect result. Let $\mathbf{B}$ be an $n \times n$ basis matrix of an n-dimensional lattice $L = L(\mathbf{B})$ and r is a real number satisfying $r \geq \sqrt{2n} \cdot \eta_\epsilon(L)/\alpha$. The goal is to design an algorithm $\mathsf{solveDGS}(\mathbf{B}, r)$ which returns a sample from $D_{L,r}$ using the oracle $\mathsf{solveLWE}_{n,n^c,p,\Psi_\alpha}(\mathcal{I})$ where $\alpha p > 2\sqrt{n}$.

Let $r_i = r \cdot (\alpha p/\sqrt{n})^i$ for $i = 1, \ldots, 3n$. A list $\mathcal{L}$ containing samples from $D_{L,r_{3n}}$ can be created without using the LWE oracle. The algorithm $\mathsf{solveDGS}(\mathbf{B}, r)$ starts with such a list and iterates a procedure over $3n$ steps with i going down from $3n$ to 1. The i-th step updates the list $\mathcal{L}$ consisting of n^c samples from D_{L,r_i} with n^c samples from $D_{L,r_{i-1}}$. At the end of the procedure, a sample from the final list $\mathcal{L}$ is returned. Each iteration updates the list $\mathcal{L}$ using a quantum sampling procedure n^c times. Each application of the quantum sampling procedure uses a classical algorithm $\mathsf{solveCVP}(L^*, \mathcal{L}, \mathbf{z})$, where L^* is the dual lattice of L, $\mathcal{L}$ contains n^c samples from D_{L,r_i} for some $i \in \{1, \ldots, 3n\}$, and $\mathbf{z}$ is within distance $\lambda_1(L^*)/2$ of L^*. The algorithm $\mathsf{solveCVP}$ solves the CVP problem for L^* mentioned in Section 2.1. It is the algorithm $\mathsf{solveCVP}$ which invokes the oracle $\mathsf{solveLWE}_{n,n^c,p,\Psi_\alpha}(\mathcal{I})$. So, the main part of the DGS-to-LWE reduction is the design of the algorithm $\mathsf{solveCVP}$.

In Regev's reduction, $\mathsf{solveCVP}(L^*, \mathcal{L}, \mathbf{z})$ solves the unique closest vector problem on L^* using a list $\mathcal{L}$ of samples from $D_{L,\mathfrak{r}}$ with $\mathfrak{r} \geq \sqrt{2}p \cdot \eta_\epsilon(L)$, and $\mathbf{z}$ is within distance $\alpha q/(\sqrt{2}\mathfrak{r}) < \lambda_1(L^*)/2$ of L^*. As used in [15], by interchanging the roles of L and L^*, it is possible to invoke $\mathsf{solveCVP}(L, \mathcal{L}, \mathbf{z})$ to solve the unique closest vector problem on L using a list $\mathcal{L}$ of samples from $D_{L^*,\mathfrak{r}}$ with $\mathfrak{r} \geq \sqrt{2}p \cdot \eta_\epsilon(L^*)$, and $\mathbf{z}$ is within distance $\alpha q/(\sqrt{2}\mathfrak{r}) < \lambda_1(L)/2$ of L. We record this as follows.

Proposition 1. *[16, 15] Let $\mathbf{B}$ be an $n \times n$ basis matrix for an n-dimensional lattice $L = L(\mathbf{B})$, p be a positive integer, $\mathfrak{r}$ be a real number satisfying $\mathfrak{r} \geq \sqrt{2}p \cdot \eta_\epsilon(L^*)$ and $\alpha \in (0, 1)$ be such that $\alpha p > 2\sqrt{n}$. Let $c > 0$ be a constant. Given a list $\mathcal{L}$ consisting of n^c samples from $D_{L^*,\mathfrak{r}}$ and an oracle $\mathsf{solveLWE}_{n,n^c,p,\Psi_\alpha}(\mathcal{I})$, where $\mathcal{I}$ consists of n^c samples from $A_{p,\mathbf{s},\Psi_\beta}$ for some $0 < \beta \leq \alpha$, there is an algorithm $\mathsf{solveCVP}(L, \mathcal{L}, \mathbf{z})$, where $\mathbf{z}$ is within distance $\alpha q/(\sqrt{2}\mathfrak{r}) < \lambda_1(L)/2$ of L, which finds the unique vector in L which is closest to $\mathbf{z}$.*

Following [17], we have the following facts.

1. Algorithm $\mathsf{solveCVP}$ calls the oracle $\mathsf{solveLWE}$ a total of n^{2c+2} times.

2. The success probability of algorithm $\mathsf{solveCVP}$ is at least

$$\left(1 - \max(\exp\left(-m(\mu_0 - t)^2/2\right), \exp\left(-mt^2/2\right))\right)^{n^{2c+2}} \tag{1}$$

   where $\mu_0 = \exp(-\pi\alpha^2)$, and $t \in (0, \mu_0)$ and $m \leq n^c$ are chosen so as to maximise (1). Setting $m = n^c$ and $t = \mu_0/2$, the expression in (1) becomes

$$\left(1 - \exp\left(-n^c \exp\left(-2\pi\alpha^2\right)/8\right)\right)^{n^{2c+2}} \tag{2}$$

Using this lower bound for the success probability, it has been shown in [17] that an upper bound on the tightness gap of the DGS to LWE reduction is the following.

$$3n^{3c+3} \cdot \left(1 - \exp\left(-n^c \exp(-2\pi\alpha^2)/8\right)\right)^{-3n^{3c+3}}. \tag{3}$$

For most practical cryptosystems[1], α is at most $1/\sqrt{n}$. Considering $\alpha = 1/\sqrt{n}$, the tightness gap given by (3) is essentially $3n^{3c+3}$ [17]. The tightness gap of the reduction from DGS to LWE has been extended to obtain the tightness gap of the reduction from SIVP to average-case decision LWE in [7] and updated in [17] and is given by the following expression.

$$6pn^{3c+d_1+2d_2+9}. \tag{4}$$

Here d_1 and d_2 are non-negative integers such that average-case decision LWE can be solved for a fraction n^{-d_1} of all the secrets with advantage at least n^{-d_2}.

4 Reducing GapSVP$_{\zeta,\gamma}$ to LWE

Peikert [15] showed a classical reduction of GapSVP$_{\zeta,\gamma}$ to LWE$_{n,n^c,q,\Psi_\alpha}$, where $\gamma = \gamma(n) \geq n/(\alpha\sqrt{\log n})$, $q = q(n) \geq \zeta(n) \cdot \omega(\sqrt{\log n/n})$ and $c > 0$ is a constant. The reduction makes use of Proposition 1, i.e., it uses an LWE oracle to solve CVP.

Let $\mathbf{B}$ be an $n \times n$ basis matrix of an n-dimensional lattice $L = L(\mathbf{B})$ and $r \geq \max_i \|\widetilde{b_i}\| \cdot \omega(\sqrt{\log n})$. By $\mathsf{sample}(\mathbf{B}, r)$ we denote the sampling algorithm which on input $\mathbf{B}$ and r returns a sample which is within negligible statistical distance from $D_{L,r}$. Such an algorithm is described in [9].

The algorithm for reducing GapSVP$_{\zeta,\gamma}$ to LWE given by Peikert [15] is shown in Algorithm 1. The algorithm solveCVP in turn calls the LWE oracle solveLWE. So, overall solveGapSVP$_{\zeta,\gamma}$ solves GapSVP$_{\zeta,\gamma}$ by calling the LWE oracle solveLWE. Algorithm solveGapSVP$_{\zeta,\gamma}$ calls solveCVP a total of N times.

Algorithm 1 Reducing GapSVP$_{\zeta,\gamma}$ to LWE$_{q,\Psi_\alpha}$, where $\gamma = \gamma(n) \geq n/(\alpha\sqrt{\log n})$ and $q = q(n) \geq \zeta(n) \cdot \omega(\sqrt{\log n/n})$.

function solveGapSVP$_{\zeta,\gamma}(\mathbf{B}, d)$
    Let $\mathbf{D}$ be the reverse dual basis of $\mathbf{B}$;
    $d' = d \cdot \sqrt{n/(4\ln n)}$; $r = q\sqrt{2n}/(\gamma d)$;
    for $i \leftarrow 1$ to N **do**
        $\mathbf{w} \xleftarrow{\$} d' \cdot \mathcal{B}_n$; $\mathbf{x} = \mathbf{w} \bmod \mathbf{B}$;
        $\mathcal{L} \leftarrow \{\}$;
        for $j \leftarrow 1$ to n^c **do**
            $\mathcal{L} \leftarrow \mathcal{L} \cup \mathsf{sample}(D, r)$;
        end for
        $\mathbf{v} \leftarrow \mathsf{solveCVP}(\mathbf{B}, \mathcal{L}, \mathbf{x})$
        if $\mathbf{v} \neq \mathbf{x} - \mathbf{w}$ **then**
            return accept;
        end if
    end for
    return reject;
end function

It has been noted in Section 3 that solveCVP calls solveLWE a total of n^{2c+2} times. So, solveGapSVP$_{\zeta,\gamma}$ calls solveLWE a total of $N \cdot n^{2c+2}$ times.

We now consider the success probability of solveGapSVP$_{\zeta,\gamma}$. As in Section 3, assume that $m = n^c$, $\alpha = 1/\sqrt{n}$ and $t = \mu_0/2$. The probability that a single call to solveCVP is successful is at least ε, where using (2),

[1] This was mentioned by Chris Peikert in an email.

$\varepsilon = \left(1 - \exp\left(-n^c \exp(-2\pi\alpha^2)/8\right)\right)^{n^{2c+2}}$. The N calls to $\mathsf{solveCVP}$ in Algorithm $\mathsf{solveGapSVP}_{\zeta,\gamma}$ are independent. Let E be the event that all these calls are successful and so $\Pr[E] \geq \varepsilon^N$.

For $i = 1, \ldots, N$, let S_i be the event that the event $\mathbf{v} \neq \mathbf{x} - \mathbf{w}$ holds in the i-th iteration. The events $S_1, \ldots, S_N$ are independent (even when conditioned on E).

First consider the instance $(\mathbf{B}, r)$ to be NO instance of $\mathrm{GapSVP}_{\zeta,\gamma}$. Let succNO be the event that algorithm $\mathsf{solveGapSVP}_{\zeta,\gamma}$ is successful on a NO instance. Then $\Pr[\mathsf{succNO}] = \Pr[\overline{S}_1 \wedge \cdots \wedge \overline{S}_N] \geq \Pr[\overline{S}_1 \wedge \cdots \wedge \overline{S}_N | E] \Pr[E] = \Pr[E] \cdot \left(\prod_{i=1}^N \Pr[\overline{S}_i | E]\right) \geq \varepsilon^N \cdot \left(\prod_{i=1}^N \Pr[\overline{S}_i | E]\right)$. It has been shown in [15] that $\Pr[\overline{S}_i | E] \approx 1$, $i = 1, \ldots, N$, and so we may assume that $\Pr[\mathsf{succNO}]$ is lower bounded by ε^N.

Next consider the instance $(\mathbf{B}, r)$ to be a YES instance of $\mathrm{GapSVP}_{\zeta,\gamma}$. Let $\mathsf{succYES}$ be the event that algorithm $\mathsf{solveGapSVP}_{\zeta,\gamma}$ is successful on a YES instance. So, $\mathsf{succYES}$ is the event $S_1 \vee (\overline{S}_1 \wedge S_2) \vee \cdots \vee (\overline{S}_1 \wedge \cdots \wedge \overline{S}_{N-1} \wedge S_N)$. For $i = 1, \ldots, N$, let δ be the common value of $\Pr[\overline{S}_i | E]$. It follows (using a probability calculation) that

$$\Pr[\mathsf{succYES}] \quad \geq \quad \Pr[\mathsf{succYES} | E] \Pr[E] = (1 - \delta^N) \Pr[E] \geq (1 - \delta^N) \varepsilon^N.$$

It has been shown in [15], that for a YES instance, $\delta = \Pr[\overline{S}_i | E] \leq 1 - 1/\mathsf{poly}(n)$. The $1 - 1/\mathsf{poly}(n)$ term arises from the asymptotic form of a result which states that for any constants $c_1, d > 0$ and any $\mathbf{z} \in \mathbb{R}^n$ with $\|\mathbf{z}\| \leq d$ and $d' = d \cdot \sqrt{n/(c_1 \log n)}$ the statistical distance between the uniform distribution on $d' \cdot \mathcal{B}_n$ and the uniform distribution on $\mathbf{z} + d' \cdot \mathcal{B}_n$ is at most $1 - 1/\mathsf{poly}(n)$. This result is proved in [10] and the proof shows that the term $1 - 1/\mathsf{poly}(n)$ can be taken to be $1 - 3/n^2$. Using this we have $\delta \leq 1 - 3/n^2$. So, $\Pr[\mathsf{succYES}] \geq (1 - (1 - 3/n^2)^N) \varepsilon^N$.

Between the NO and YES instances, the lower bound on the success probability is less for YES instances. As a result, the upper bound on the tightness gap for YES instances is higher and this upper bound is taken to be the upper bound on the overall tightness gap of the reduction. So, an upper bound on the tightness gap of the $\mathrm{GapSVP}_{\zeta,\gamma}$ to LWE reduction is

$$\left(N \cdot n^{2c+2}\right) / \left((1 - (1 - 3/n^2)^N) \varepsilon^N\right). \tag{5}$$

Following [10], for $N = n^2$, $(1 - (1 - 3/n^2)^N) \approx 1$ and so the tightness gap in (5) becomes

$$N \cdot n^{2c+2} \cdot \varepsilon^{-N} = n^{2c+4} \left(1 - \exp\left(-n^c \exp(-2\pi\alpha^2)/8\right)\right)^{-n^{2c+4}}. \tag{6}$$

We note that for $c = 1$, the expression in (6) is almost the same as the expression in (3). It has been shown in [17], that for $\alpha \leq 1/\sqrt{n}$, $\varepsilon \approx 1$ and so the tightness gap of $\mathrm{GapSVP}_{\zeta,\gamma}$ to $\mathrm{LWE}_{q,\Psi_\alpha}$ becomes

$$n^{2c+4}. \tag{7}$$

Remark: It is known [15] that for $\zeta(n) \geq 2^{n/2}$, the problem $\mathrm{GapSVP}_{\zeta,\gamma}$ is equivalent to the standard GapSVP_γ problem. The reduction from $\mathrm{GapSVP}_{\zeta,\gamma}$ to $\mathrm{LWE}_{q,\Psi_\alpha}$ given in [15] holds under the condition $q = q(n) \geq \zeta(n) \cdot \omega(\sqrt{\log n/n})$. So, for $q(n) \geq 2^{n/2} \cdot \omega(\sqrt{\log n/n})$, there is a classical reduction from GapSVP_γ to $\mathrm{LWE}_{q,\Psi_\alpha}$, where $\gamma = \gamma(n) \geq n/(\alpha\sqrt{\log n})$.

5 Reducing GapSVP_γ to Decision LWE

The remark at the end of Section 4 shows that there is a classical reduction of GapSVP_γ to $\mathrm{LWE}_{q,\Psi_\alpha}$ for $q(n) \geq 2^{n/2} \cdot \omega(\sqrt{\log n/n})$. So, if the modulus of the LWE problem is exponential in the dimension of the lattice, then the result from [15] provides a classical reduction of GapSVP_γ to LWE. A later work by Brakerski et al. [6] showed a reduction of GapSVP_γ to a decision version of LWE with polynomial sized modulus. The reduction is quite intricate and is built by composing reductions between several pairs of problems. The goal of the present section is to perform a concrete security analysis of the reduction provided in [6].

The LWE problem considered in Section 2.1 is a search problem. For the classical reduction of GapSVP_γ to LWE, the $\text{binLWE}_{n,m,q,\alpha}$ problem has been considered.

Let $\mathcal{D}_0$ be the distribution $A_{q,\mathbf{s},\alpha}$ and $\mathcal{D}_1$ be the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{T}$. For $i = 0, 1$, let $\mathcal{I} \stackrel{m}{\leftarrow} \mathcal{D}_i$ denote the selection of a list $\mathcal{I}$ of m independent samples from $\mathcal{D}_i$. Let $\mathcal{A}$ be a distinguisher for $\text{decLWE}_{n,m,q,\alpha}$. Let $\mathcal{A}(\mathcal{I}) \Rightarrow 1$ denote the event that $\mathcal{A}$ produces 1 as output. The advantage of $\mathcal{A}$ is the following.

$$\mathsf{Adv}(\mathcal{A}) \quad = \quad |\Pr[\mathcal{A}(\mathcal{I}) \Rightarrow 1 : I \stackrel{m}{\leftarrow} \mathcal{D}_0] - \Pr[\mathcal{A}(\mathcal{I}) \Rightarrow 1 : I \stackrel{m}{\leftarrow} \mathcal{D}_1]|. \tag{8}$$

Similarly, one defines the advantage of a distinguisher for $\text{binLWE}_{n,m,q,\alpha}$.

The classical reduction in [6] reduces GapSVP to binLWE. This reduction is done in several steps. The first step is Peikert's reduction of GapSVP to LWE with exponential size modulus. The goal of the following steps is to reduce the LWE problem with exponential size modulus to binLWE problem with polynomial size modulus. A trade-off is an increase in the dimension. The various steps of the overall reduction are as follows.

Reducing GapSVP_γ to $\text{LWE}_{k,m_1,q_1,\alpha_1}$: This follows from Peikert's result [15]. Here $\alpha_1 \in (0,1)$, $q_1 \geq 2^{k/2} \cdot \omega(\sqrt{\log k/k})$, $\gamma \geq k/(\alpha_1\sqrt{\log k})$ and $m_1 = k^c$ for some constant $c \geq 1$. For simplicity, in the following, we will assume $q_1 = 2^{k/2}$.

Suppose W_0 is an algorithm to solve $\text{LWE}_{k,m_1,q_1,\alpha_1}$. Then following the analysis in Section 4, there is an algorithm W to solve GapSVP_γ where the number of times W calls W_0 is k^{2c+4} (which is obtained from (7) by replacing n with k).

Reducing $\text{LWE}_{k,m_1,q_1,\alpha_1}$ to $\text{decLWE}_{k,m_1,q_1,\alpha_2}$: This follows as a special case of Theorem 3.1 in [14]. Here $1/q_1 < \alpha_1 < 1/\omega(\sqrt{\log n})$ and $\alpha_2 = \alpha_1 \cdot \omega(\log k)$.

To determine the tightness gap of the reduction, we follow the proof of Theorem 3.1 in the case where $q_1 = 2^{k/2}$. Let W_1 be an algorithm to solve $\text{decLWE}_{k,m_1,q_1,\alpha_2}$. The proof of Theorem 3.1 in [14] uses W_1 to first construct an algorithm W_1' following the construction used in Lemma 4.1 of [16]. Specifically, Lemma 4.1 of [16] shows how to boost the advantage of a distinguisher for the distributions $A_{q_1,\mathbf{s},\chi}$ and $U(\mathbb{Z}_{q_1}^n \times \mathbb{Z}_{q_1})$. The same method can be used to boost the advantage of a distinguisher for the distributions $A_{q_1,\mathbf{s},\alpha_2}$ and the uniform distribution on $\mathbb{Z}_{q_1}^n \times \mathbb{T}$. This is the situation considered in Theorem 3.1 of [14].

Let ζ_1 be the advantage of W_1 and c_1 and c_2 be such that W_1 is successful on a fraction k^{-c_1} of all possible secrets and

$$\zeta_1 \quad = \quad k^{-c_2}. \tag{9}$$

Following the method of Lemma 4.1 in [16] it is possible to construct W_1' which accepts with probability exponentially close to one on inputs from $A_{q_1,\mathbf{s},\alpha_2}$ and rejects with probability exponentially close to one on inputs from the uniform distribution over $\mathbb{Z}_{q_1}^n \times \mathbb{T}$. From the proof of Lemma 4.1 in [16] we have that the algorithm W_1' calls the algorithm W_1 a total of $k^{c_1+2c_2+2}$ times.

The proof of Theorem 3.1 in [14] uses W_1' to construct an algorithm W_0 which solves $\text{LWE}_{k,m_1,q_1,\alpha_1}$. The secret $\mathbf{s} = (s_1, \ldots, s_k)$. The components $s_1, \ldots, s_k$ are determined one by one. Consider the determination of s_1. This is determined iteratively as $s_1 \bmod 2$, followed by $s_1 \bmod 2^2$, followed by $s_1 \bmod 2^3$, up to at most $s_1 \bmod 2^{k/2}$. Given the value of $s_1 \bmod 2^i$, there are only two possible values for $s_1 \bmod 2^{i+1}$. A single call to W_1' can be used to determine the correct value. So, to find s_1, at most $k/2$ calls to W_1' are required, and to find the entire vector $\mathbf{s}$, at most $k^2/2$ calls to W_1' are required. Each call to W_1' requires $k^{c_1+2c_2+2}$ calls to W_1. So, the number of times W_0 calls W_1 is

$$k^{c_1+2c_2+4}. \tag{10}$$

Reducing $\text{decLWE}_{k,m_1,q_1,\alpha_2}$ to $\text{binLWE}_{n,m_1,q_1,\leq\sqrt{10n}\alpha_2}$: This reduction follows from Theorem 4.1 of [6]. Here $n \geq (k+1)\log_2 q_1 + 2\log_2(1/\delta)$, $\alpha_2 \geq \sqrt{\ln(2n(1+1/\varepsilon_1))/\pi}/q_1$, where $\delta > 0$ and $\varepsilon_1 \in (0, 1/2)$. Suppose there is an algorithm W_2 for $\text{binLWE}_{n,m_1,q_1,\leq\sqrt{10n}\alpha_2}$ which has advantage ζ_2. Theorem 4.1 of [6] shows an algorithm W_1 for $\text{decLWE}_{k,m_1,q_1,\alpha_2}$ with advantage ζ_1 where

$$\zeta_1 \quad \geq \quad \frac{\zeta_2 - \delta}{3m_1} - \frac{41\varepsilon_1}{2} - 2^{-k-1}. \tag{11}$$

From the proof of Theorem 4.1 of [6] one obtains that W_1 calls W_2 once.

Remark: We note a peculiarity in (11). The number of samples m_1 appears in the denominator of the right hand side. If ζ_2 is fixed, then as m_1 increases, the right hand side decreases. In other words, for a fixed value of ζ_2, as the number of samples increases, the lower bound on the advantage ζ_1 decreases. Intuitively, one may expect that as the number of samples increases, more information is obtained, and so the advantage should be non-decreasing. This does not seem to hold for ζ_1. A possible explanation has been provided by the reviewer. It is likely that m_1 and ζ_2 are positively correlated in which case, if m_1 increases, ζ_2 will also increase leaving the lower bound unchanged. Since the nature of dependence of ζ_2 on m_1 is unknown, the issue cannot be definitively settled.

Reducing $\text{binLWE}_{n,m_1,q_1,\leq\sqrt{10n}\alpha_2}$ to $\text{binLWE}_{n,m_1,q_2,\leq\alpha_3}$: This reduction follows from Corollary 3.2[2] of [6]. Here $q_1 \geq q_2 \geq \sqrt{2\ln(2n(1+1/\varepsilon_2))}\cdot(\sqrt{n}/\alpha_2)$ and $\alpha_3^2 \geq 10n\alpha_2^2 + (4n/(\pi q_2^2))\ln(2n(1+1/\varepsilon_2))$ where $\varepsilon_2 \in (0, 1/2)$. Suppose there is an algorithm W_3 for $\text{binLWE}_{n,m_1,q_2,\leq\alpha_3}$ having advantage ζ_3. Corollary 3.2 of [6] shows an algorithm W_2 for $\text{binLWE}_{n,m_1,q_1,\leq\sqrt{10n}\alpha_2}$ with advantage ζ_2 where

$$\zeta_2 \quad \geq \quad \zeta_3 - 14\varepsilon_2 m_1. \tag{12}$$

Further, W_2 calls W_3 once.

Reducing $\text{binLWE}_{n,m_1,q_2,\leq\alpha_3}$ to $\text{binLWE}_{n,m_2,q_2,\alpha_3}$: This reduction follows from Lemma 2.15 of [6]. Suppose there is an algorithm W_4 for $\text{binLWE}_{n,m_2,q_2,\alpha_3}$ having advantage ζ_4. Lemma 2.15 of [6] states that the algorithm W_3 for $\text{binLWE}_{n,m_1,q_2,\leq\alpha_3}$ has advantage ζ_3 where $\zeta_3 \geq 1/3$. Further, in [6] it is stated that both m_1 and the number of times W_3 calls W_4 are $\text{poly}(m_2, 1/\zeta_4, n, \log q_2)$. In Lemma 2 (given in the appendix) we show that $m_1 = \mathfrak{k} m_2$ and the number of times W_3 calls W_4 is $\mathfrak{k}(1 + 36m_2/\zeta_4)$ where $\mathfrak{k} \geq \max(32\ln 12, 8\ln(432m_2/\zeta_4))/\zeta_4^2$. For simplicity, we take $\mathfrak{k} = 1/\zeta_4^2$. We assume that there are constants $d_1, d_2 > 0$, such that $m_2 = n^{d_1}$ and $\zeta_4 = n^{-d_2}$.

Putting together the various reductions, yields a reduction from GapSVP_γ on a lattice of dimension k to $\text{binLWE}_{n,m_2,q_2,\alpha_3}$. The number of times C the algorithm W_4 (for solving $\text{binLWE}_{n,m_2,q_2,\alpha_3}$) is called by the algorithm W (for solving GapSVP_γ) is obtained from the above analysis to be the following.

$$C \quad = \quad k^{2c+4} \cdot k^{c_1+2c_2+4} \cdot \frac{1}{\zeta_4^2}\left(1 + \frac{36m_2}{\zeta_4}\right) \approx k^{2c+4} \cdot k^{c_1+2c_2+4} \cdot \frac{m_2}{\zeta_4^3} = k^{2c+4} \cdot k^{c_1+2c_2+4} \cdot n^{d_1+3d_2}. \tag{13}$$

Let the runtime of W_4 be T and the runtime of W be T'. Then $T'/T \approx C$. The advantage of W_4 is ζ_4 while the success probability of W is almost 1. The tightness gap of the reduction is $T'/(T/\zeta_4) = C\zeta_4$ which is equal to

$$G \quad = \quad k^{2c+4} \cdot k^{c_1+2c_2+4} \cdot n^{d_1+2d_2}. \tag{14}$$

The relations among the various parameters are as follows.

[2]A distribution $\mathcal{D}$ over $\mathbb{Z}^n$ is (B, δ)-bounded, for $B, \delta \in \mathbb{R}$, if the probability that $\mathbf{x} \leftarrow \mathcal{D}$ has norm greater than B is at most δ. Corollary 3.2 of [6] is stated in terms of (B, δ) distribution $\mathcal{D}$. In the present context, $\mathcal{D}$ is the uniform distribution over $\{0, 1\}$ which is $(\sqrt{n}, 0)$-bounded.

1. $\gamma \geq k/(\alpha_1\sqrt{\log k})$;
2. $q_1 = 2^{k/2}$;
3. $m_1 = k^c$ for some constant $c \geq 1$;
4. $1/q_1 < \alpha_1 < 1/\omega(\sqrt{\log n})$ and $\alpha_2 = \alpha_1 \cdot \omega(\log k)$;
5. The constants c_1 and c_2 are such that W_1 is successful on a fraction k^{-c_1} of all possible secrets and $\zeta_1 = k^{-c_2}$;
6. $n \geq (k+1)\log_2 q_1 + 2\log_2(1/\delta)$;
7. $\alpha_2 \geq \sqrt{\ln(2n(1+1/\varepsilon_1))/\pi}/q_1$, and $\zeta_1 \geq \frac{\zeta_2-\delta}{3m_1} - \frac{41\varepsilon_1}{2} - 2^{-k-1}$, where $\delta > 0$ and $\varepsilon_1 \in (0, 1/2)$;
8. $q_1 \geq q_2 \geq \sqrt{2\ln(2n(1+1/\varepsilon_2))} \cdot (\sqrt{n}/\alpha_2)$, $\alpha_3^2 \geq 10n\alpha_2^2 + (4n/(\pi q_2^2))\ln(2n(1+1/\varepsilon_2))$, and $\zeta_2 \geq \zeta_3 - 14\varepsilon_2 m_1$, where $\varepsilon_2 \in (0, 1/2)$;
9. $\zeta_3 \geq 1/3$;
10. $m_1 = m_2/\zeta_4^2$;
11. $m_2 = n^{d_1}$ and $\zeta_4 = n^{-d_2}$ for constants $d_1, d_2 > 0$.

Note that

$$\begin{aligned} \zeta_1 &\geq \frac{\zeta_2-\delta}{3m_1} - \frac{41\varepsilon_1}{2} - 2^{-k-1} \geq \frac{\zeta_3}{3m_1} - \frac{14\varepsilon_2}{3} - \frac{\delta}{3m_1} - \frac{41\varepsilon_1}{2} \geq \frac{1}{9m_1} - \frac{14\varepsilon_2}{3} - \frac{\delta}{3m_1} - \frac{41\varepsilon_1}{2}, \\ \alpha_3^2 &\geq 10n\alpha_2^2 + \frac{4n}{\pi q_2^2}\ln(2n(1+1/\varepsilon_2)) \geq 10n\alpha_1^2\omega(\log^2 k) + \frac{4n}{\pi q_2^2}\ln(2n(1+1/\varepsilon_2)). \end{aligned}$$

Performing a meaningful concrete security analysis with the exact form of the above relations is almost impossible. To simplify the analysis, we ignore logarithmic factors. Also, we will assume that the parameters ε_1, ε_2 and δ can be chosen in a manner (say, $1/\text{poly}(n)$) such that they do not have much effect on the concrete security analysis. Using these and other reasonable simplifications, we have the following relations.

$$\begin{array}{l} q_1 = 2^{k/2}; \quad n = k^2; \\ \alpha_1 = \alpha_2 = \alpha_3/\sqrt{n} = \alpha_3/k; \\ \gamma = k/\alpha_1 = k^2/\alpha_3; \\ k^{-c_2} = \zeta_1 = 1/m_1 = k^{-c}, \\ q_2 = \sqrt{n}/\alpha_2 = n/\alpha_3; \\ k^c = m_1 = n^{d_1+2d_2}. \end{array} \tag{15}$$

From (15), we have $c_2 = c = 2d_1 + 4d_2$. As mentioned earlier, following Theorem 4.1 of [6], algorithm W_1 for $\text{decLWE}_{k,m_1,q_1,\alpha_2}$ is constructed from the algorithm W_2 for $\text{binLWE}_{n,m_1,q_1,\leq\sqrt{10n}\alpha_2}$. The reduction shows that W_1 is successful for almost all secrets and so we take $c_1 = 0$. Using $c_2 = c = 2d_1 + 4d_2$ and $c_1 = 0$ in (14), the overall tightness gap is obtained to be

$$n^{4+5d_1+10d_2}. \tag{16}$$

The tightness gap given by (16) is to be compared to the tightness gap of Regev's reduction given by (4). While the numerical values of the tightness gaps for the two reductions can be compared, it should be kept in mind that the problems being connected by the two reductions are different.

Summary: We have the following concrete form of the reduction of GapSVP to binLWE.

> If there is an algorithm which solves $\text{binLWE}_{n,m_2,q_2,\alpha_3}$ with advantage n^{-d_2}, where $q_2 = n/\alpha_3$ and $m_2 = n^{d_1}$, then there is an algorithm to solve $\text{GapSVP}_{k^2/\alpha_3}$ on a lattice of dimension $k = \sqrt{n}$. The tightness gap of the reduction is given by $n^{4+5d_1+10d_2}$.

Regev [16] had described a cryptosystem where the public key is a collection of $n^{1+\epsilon}$ LWE samples and the secret key is $\mathbf{s} \in \mathbb{Z}_q^n$. A successful adversary against the scheme is able to distinguish between encryptions of 0 and 1 with advantage at least n^{-d} for some $d > 0$. It was shown in [16] that a successful adversary against the cryptosystem can be used to obtain an algorithm for the average case decision LWE problem such that the algorithm is successful for a fraction $1/(4n^d)$ of all secrets with advantage at least $1/(8n^d)$.

The problem $\text{binLWE}_{n,m_2,q_2,\alpha_3}$ would be used as a basis for proving security of cryptosystems. We consider $\alpha_3 = 1/\sqrt{n} = 1/k$. The security of any such cryptosystem would be given by a reduction of the type given by Regev for his cryptosystem. Suppose $\mathfrak{C}$ is such a cryptosystem and that an adversary is successful in breaking $\mathfrak{C}$ if it can distinguish between encryptions of 0 and 1 with advantage at least $1/n^d$ for some $d > 0$. Following the reduction of Regev for his cryptosystem, we assume that successful adversary for $\mathfrak{C}$ can be used to build algorithm W_4 for $\text{binLWE}_{n,m_2,q_2,\alpha_3}$ such that W_4 is successful on a fraction $\approx n^{-d}$ of the secrets with advantage at least n^{-d}. This suggests $d_2 \approx d$. (A similar approximation was made in [7].) We further assume that $d_1 \approx d$. As a numerical example, consider $n = 2^{10}$. Aiming at 128-bit security, ζ_4 would be 2^{-128} and so for $n = 2^{10}$, $d = 12.8$. In this case, the tightness gap in (16) is 2^{1960}. In other words, the quantitative effect of the reduction is the following. If T is the time required to solve $\text{binLWE}_{n,m_2,q_2,\alpha_3}$ on a lattice of dimension 2^{10}, then there is an algorithm to solve GapSVP_γ for a lattice of dimension $k = \sqrt{n} = 2^5$ and $\gamma = k^3 = 2^{15}$ which takes time $2^{1960}T$. So, the tightness gap is 2^{1960}. In comparison, for $n = 2^{10}$ and 128-bit security, the tightness gap in [7, 17] has been obtained to be 2^{524}.

Note that the dimension of the lattice for which GapSVP is to be solved is $\sqrt{n}$ where n is the dimension of the lattice for which binLWE is to be solved. Brakerski et al. [6] mention this point. Due to the drawback of the quadratic loss in the dimension, they mention as an open problem the task of obtaining a reduction where such a quadratic loss does not occur. In their words, this would constitute a "full dequantization" of Regev's reduction.

The issue of tightness gap has not been considered in [6]. For the GapSVP to binLWE reduction to be meaningfully used to derive parameters for practical cryptosystems, the tightness gap needs to be taken into consideration. So, for a full dequantization of Regev's reduction which can also be used in practice, one needs a *tight* reduction which does not suffer the quadratic loss in the dimension.

6 Conclusion

We have performed a concrete security analysis of the tightness gap in the classical reduction of the shortest vector problem to the LWE problem given by Brakerski et al. [6]. Previous works [7, 17] had already pointed out that the tightness gap in the quantum reduction of Regev [16] is huge. Our analysis shows that the tightness gap of the classical reduction by Brakerski et al. is more than that of Regev's original quantum reduction. This leaves open the question of obtaining a tight reduction of a worst case lattice problem to LWE, or, showing that there is no such reduction.

Acknowledgement

We are grateful to the reviewer for providing comments and suggestions to improve the paper.

References

[1] Erdem Alkim, Roberto Avanzi, Joppe Bos, Leo Ducas, Antonio de la Piedra, Thomas Poppelmann, Peter Schwabe, Douglas Stebila, Martin R. Albrecht, Emmanuela Orsini, Valery Osheter, Kenneth G. Paterson, Guy Peer, and Nigel P. Smart. NewHope: algorithm specifications and supporting documentation. https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions, 2019.

[2] Erdem Alkim, Joppe Bos, Leo Ducas, Patrick Longa, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, and Douglas Stebila. FrodoKEM: Learning With Errors key encapsulation. https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions, 2019.

[3] Roberto Avanzi, Joppe Bos, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber: algorithm specifications and supporting documentation. https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions, 2009.

[4] Hayo Baan, Sauvik Bhattacharya, Scott Fluhrer, Oscar Garcia-Morchon, Thijs Laarhoven, Rachel Player, Ronald Rietman, Markku-Juhani O. Saarinen, Ludo Tolhuizen, Jose-Luis Torre-Arce, and Zhenfei Zhang. Round5: KEM and PKE based on (Ring) Learning With Rounding. https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions, 2019.

[5] Daniel J. Bernstein. Comparing proofs of security for lattice-based encryption. Cryptology ePrint Archive, Report 2019/691, 2019. https://eprint.iacr.org/2019/691.

[6] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 575–584. ACM, 2013.

[7] Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, and Palash Sarkar. Another look at tightness II: practical issues in cryptography. In Raphael C.-W. Phan and Moti Yung, editors, *Paradigms in Cryptology - Mycrypt 2016. Malicious and Exploratory Cryptology - Second International Conference, Mycrypt 2016, Kuala Lumpur, Malaysia, December 1-2, 2016, Revised Selected Papers*, volume 10311 of *Lecture Notes in Computer Science*, pages 21–55. Springer, 2016.

[8] Jan-Pieter DAnvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. SABER: Mod-LWR based KEM (round 2 submission). https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions, 2019.

[9] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Cynthia Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 197–206. ACM, 2008.

[10] Oded Goldreich and Shafi Goldwasser. On the limits of nonapproximability of lattice problems. *J. Comput. Syst. Sci.*, 60(3):540–563, 2000.

[11] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[12] Yi-Kai Liu, Vadim Lyubashevsky, and Daniele Micciancio. On bounded distance decoding for general lattices. In Josep Díaz, Klaus Jansen, José D. P. Rolim, and Uri Zwick, editors, *Approximation, Randomization,*

and Combinatorial Optimization. Algorithms and Techniques, 9th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2006 and 10th International Workshop on Randomization and Computation, RANDOM 2006, Barcelona, Spain, August 28-30 2006, Proceedings, volume 4110 of *Lecture Notes in Computer Science*, pages 450–461. Springer, 2006.

[13] Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, Zhenfei Zhang, Zhe Liu, Hao Yang, Bao Li, and Kunpeng Wang. LAC: Lattice-based Cryptosystems. https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions, 2019.

[14] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. Cryptology ePrint Archive, Report 2011/501, https://eprint.iacr.org/2011/501, 2011. An abridged version of this paper appeared in the proceedings of Eurocrypt 2012.

[15] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 333–342. ACM, 2009.

[16] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.

[17] Palash Sarkar and Subhadip Singha. Verifying solutions to LWE with implications for concrete security. *Advances in Mathematics of Communications*, 2020. https://www.aimsciences.org/article/doi/10.3934/amc.2020057.

A Reducing $\text{binLWE}_{n,m_1,q,\leq\alpha}$ to $\text{binLWE}_{n,m_2,q,\alpha}$

Suppose there is an algorithm $\mathcal{A}$ which has advantage θ in solving $\text{binLWE}_{n,m_2,q,\alpha}$. Lemma 2.15 of [6] states that using $\mathcal{A}$, it is possible to construct an algorithm $\mathcal{B}$ which solves $\text{binLWE}_{n,m_1,q,\leq\alpha}$ with advantage at least 1/3 where both m_1 and the runtime of $\mathcal{B}$ are $\text{poly}(m_2, 1/\theta, n, \log q)$. In [6], it was mentioned that the proof is standard and is based on Lemma 3.7 of [16]. The following brief idea of the proof was provided.

> "The idea is to use Chernoff bound to estimate $\mathcal{A}$'s success probability on the uniform distribution, and then add noise in small increments to our given distribution and estimate $\mathcal{A}$'s behavior on the resulting distributions. If there is a gap between any of these and the uniform behavior, the input distribution is deemed non-uniform."

Below we provide the details of the proof based on the above idea and also work out the dependence of m_1 on m_2 and θ.

Lemma 2. *Let $\mathcal{A}$ be an algorithm which has advantage at least θ in solving $\text{binLWE}_{n,m_2,q,\alpha}$. Using $\mathcal{A}$, it is possible to construct an algorithm $\mathcal{B}$ which has advantage 1/3 in solving $\text{binLWE}_{n,m_1,q,\leq\alpha}$, where $m_1 = \mathfrak{k}m_2$ with $\mathfrak{k}$ satisfying $\mathfrak{k} \geq \max(32\ln 12, 8\ln(432m_2/\theta))/\theta^2$. Further, $\mathcal{B}$ invokes $\mathcal{A}$ a total of $\mathfrak{k}(1 + 36m_2/\theta)$ times.*

Proof. An input to $\mathcal{A}$ is a collection of samples $\mathcal{I}$ of size m_2. By "$\mathcal{I}$ is real" we will mean that the samples are drawn independently from $A_{q,s,\alpha}$, while by "$\mathcal{I}$ is random" we will mean that the samples are drawn independently and uniformly from $\mathbb{Z}_q^n \times \mathbb{T}$. The output of $\mathcal{A}$ is a bit. The advantage of $\mathcal{A}$ is

$$\text{Adv}_{\mathcal{A}} \quad = \quad |\Pr[\mathcal{A}(\mathcal{I}) \Rightarrow 1 : \mathcal{I} \text{ is real}] - \Pr[\mathcal{A}(\mathcal{I}) \Rightarrow 1 : \mathcal{I} \text{ is random}]|. \tag{17}$$

Let $p_\star = \Pr[\mathcal{A}(\mathcal{I}) = 1 : \mathcal{I} \text{ is real}]$ and $p_\$ = \Pr[\mathcal{A}(\mathcal{I}) = 1 : \mathcal{I} \text{ is random}]$. For the sake of convenience of the analysis, we will assume that $p_\star > p_\$$, the other case being similar. Since it is given that $\mathrm{Adv}_\mathcal{A}$ is at least θ, we have

$$\theta \leq p_\star - p_\$. \tag{18}$$

The construction of $\mathcal{B}$ using $\mathcal{A}$ is shown in Algorithm 2. The input to $\mathcal{B}$ is a collection of samples $\mathcal{J}$ of size m_1 where $m_1 = km_2$. By "$\mathcal{J}$ is real" we will mean that the samples are drawn independently from $A_{q,\mathbf{s},\beta}$ for some unknown $\beta \leq \alpha$, while by "$\mathcal{J}$ is random" we will mean that the samples are drawn independently and uniformly from $\mathbb{Z}_q^n \times \mathbb{T}$.

Steps 2 to 4 of Algorithm 2 compute an estimate $\hat{p}_\$$ of $p_\$$. From the additive form of the Chernoff-Hoeffding bound [11], we have

$$\Pr[p_\$ - \theta/4 \leq \hat{p}_\$ \leq p_\$ + \theta/4] \geq 1 - 2\exp(-2\mathfrak{k}(\theta/4)^2). \tag{19}$$

Consider the set Z defined in Step 6 and let $t = \#Z$. Note that $t = m_3^2$. The loop from Step 7 to 18 runs for t steps. For $i = 1, \ldots, t$, let p_i^{real} (resp. p_i^{rnd}) be the value of p computed at Step 14 in the i-th iteration of the loop when the input $\mathcal{J}$ is real (resp. random).

The loop in Steps 9 to 12 adds a certain amount of noise to the samples in $\mathcal{J}$ to obtain $\mathcal{J}'$. If $\mathcal{J}$ is random, then $\mathcal{J}'$ is also random and the inputs $\mathcal{J}_1, \ldots, \mathcal{J}_k$ on which $\mathcal{A}$ is invoked are also random. By the additive form of the Chernoff-Hoeffding bound, we have

$$\Pr[p_\$ - \theta/4 \leq p_i^{\text{rnd}} \leq p_\$ + \theta/4] \geq 1 - 2\exp(-2\mathfrak{k}(\theta/4)^2). \tag{20}$$

For the case when $\mathcal{J}$ is real, we follow an argument from the proof of Lemma 3.7 of [16]. In this case, the samples in $\mathcal{J}$ are from $A_{q,\mathbf{s},\beta}$, for some unknown $\beta \leq \alpha$. In other words, each element of $\mathcal{J}$ is a pair of the form $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s}\rangle/q + e)$, where e is drawn from Ψ_β. Step 11 converts such a pair to $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s}\rangle/q + e + \varepsilon)$, where ε is drawn from Ψ_γ. This creates a pair $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s}\rangle/q + e')$, where $e' = e + \varepsilon$ and so, e' follows $\Psi_{\sqrt{\beta^2+\gamma}}$. Consider the smallest γ such that $\gamma \geq \alpha^2 - \beta^2$ and so $\gamma \leq \alpha^2 - \beta^2 + m_3^{-2}\alpha^2$. Suppose this γ is considered in the ℓ-th iteration of the loop in Steps 7 to 18. Let $\alpha' = \sqrt{\beta^2 + \gamma}$ so that $\alpha \leq \alpha' \leq \sqrt{\alpha^2 + m_3^{-2}\alpha^2} \leq (1 + m_3^{-2})\alpha$. By Claim 2.2 of [16], the statistical distance between Ψ_α and $\Psi_{\alpha'}$ is at most $9m_3^{-2}$. Consequently, the statistical distance between m_2 samples from Ψ_α and $\Psi_{\alpha'}$ is at most $9m_2m_3^{-2}$. So, in the ℓ-th iteration of the loop in Steps 7 to 18, for $j = 1, \ldots, \mathfrak{k}$, the statistical distance between $\mathcal{J}_j$ and m_2 samples from $A_{q,\mathbf{s},\alpha}$ is at most $9m_2m_3^{-2}$.

Let $\hat{p}_\star$ be the probability that $\mathcal{A}$ outputs 1 when the input consists of m_2 samples from a distribution whose statistical distance from $A_{q,\mathbf{s},\alpha}$ is at most $9m_2m_3^{-2}$. So, $|\hat{p}_\star - p_\star| \leq 9m_2m_3^{-2}/2$. In the ℓ-th iteration, for $j = 1, \ldots, \mathfrak{k}$, the probability that $\mathcal{A}$ outputs 1 on input $\mathcal{J}_j$ is $\hat{p}_\star$. Let $\epsilon_1 = \theta/4 - 9m_2m_3^{-2}/2$. By the additive form of the Chernoff-Hoeffding bound we have

$$\Pr[\hat{p}_\star - \epsilon_1 \leq p_\ell^{\text{real}} \leq \hat{p}_\star + \epsilon_1] \geq 1 - 2\exp(-2\mathfrak{k}\epsilon_1^2). \tag{21}$$

Combining (21) with $|\hat{p}_\star - p_\star| \leq 9m_2m_3^{-2}/2$, we have

$$\Pr[p_\star - \epsilon_1 - 9m_2m_3^{-2}/2 \leq p_\ell^{\text{real}} \leq p_\star + \epsilon_1 + 9m_2m_3^{-2}/2] \geq 1 - 2\exp(-2\mathfrak{k}\epsilon_1^2). \tag{22}$$

So,

$$\Pr[p_\star - \theta/4 \leq p_\ell^{\text{real}} \leq p_\star + \theta/4] \geq 1 - 2\exp(-2\mathfrak{k}(\theta/4 - 9m_2m_3^{-2}/2)^2). \tag{23}$$

We define two sets of events. Suppose the input $\mathcal{J}$ to $\mathcal{B}$ is random. For $i = 1, \ldots, t$, let E_i be the event that the $|p_i^{\text{rnd}} - \hat{p}_\$| > \theta/2$, i.e., the if-condition at Step 15 is satisfied in the i-th iteration on random input. Next suppose that the input $\mathcal{J}$ to $\mathcal{B}$ is real. For $i = 1, \ldots, t$, let F_i be the event that the $|p_i^{\text{real}} - \hat{p}_\$| > \theta/2$, i.e., the if-condition at Step 15 is satisfied in the i-th iteration on real input.

We consider the probability of $\overline{E}_i$. Let G_1 be the event $|\hat{p}_\$ - p_\$| \leq \theta/4$ and H_i be the event $|p_i^{\text{rnd}} - p_\$| \leq \theta/4$. Note that G_1 and H_i are independent. Further, $G_1 \wedge H_i$ implies $\overline{E}_i$ and so using (19) and (20), we obtain

$$\Pr[\overline{E}_i] \geq \Pr[G_1 \wedge H_i] \geq (1 - 2\exp(-2\mathfrak{k}(\theta/4)^2))^2 \geq 1 - 4\exp(-2\mathfrak{k}(\theta/4)^2) = 1 - \delta_1 \tag{24}$$

where $\delta_1 = 4\exp(-2\mathfrak{k}(\theta/4)^2)$. Using $\mathfrak{k} \geq 8\ln(432m_2/\theta)/\theta^2$ and $m_3^2 = 36m_2/\theta$, we have

$$t\delta_1 = 4m_3^2\exp(-2\mathfrak{k}(\theta/4)^2) = \frac{144m_2}{\theta}\exp(-2\mathfrak{k}(\theta/4)^2) \leq 1/3. \tag{25}$$

Next we consider the probability of F_ℓ. Let G_2 be the event $|p_\ell^{\text{real}} - p_\star| < \theta/4$. Note that G_1 and G_2 are independent events. We have G_2 to be the event $p_\star - \theta/4 \leq p_\ell^{\text{real}} \leq p_\star + \theta/4$; and G_1 to be the event $p_\$ - \theta/4 \leq \hat{p}_\$ \leq p_\$ + \theta/4$ which is equivalent to $-p_\$ + \theta/4 \geq -\hat{p}_\$ \geq -p_\$ - \theta/4$. So, if G_1 and G_2 both hold, we have $p_\star - p_\$ - \theta/2 \leq p_\ell^{\text{real}} - \hat{p}_\$$. Using $p_\star - p_\$ \geq \theta$, the last condition shows that $\theta/2 \leq p_\ell^{\text{real}} - \hat{p}_\$$ and so F_ℓ holds. This shows that $G_1 \wedge G_2$ implies F_ℓ and using (19) and (23), we obtain

$$\begin{aligned}\Pr[F_\ell] \geq \Pr[G_1 \wedge G_2] &\geq (1 - 2\exp(-2\mathfrak{k}(\theta/4)^2)) \times (1 - 2\exp(-2\mathfrak{k}(\theta/4 - 9m_2{m_3}^{-2}/2)^2)) \\ &\geq 1 - 2\exp(-2\mathfrak{k}(\theta/4)^2) - 2\exp(-2\mathfrak{k}(\theta/4 - 9m_2{m_3}^{-2}/2)^2) = 1 - \delta_2\end{aligned} \tag{26}$$

where $\delta_2 = 2\exp(-2\mathfrak{k}(\theta/4)^2) + 2\exp(-2\mathfrak{k}(\theta/4 - 9m_2m_3^{-2}/2)^2)$. Using $m_3 = 6(m_2/\theta)^{1/2}$, we have $\theta/4 - 9m_2m_3^{-2}/2 = \theta/8$ so, $\delta_2 = 2\exp(-2\mathfrak{k}(\theta/4)^2) + 2\exp(-2\mathfrak{k}(\theta/8)^2) \leq 4\exp(-2\mathfrak{k}(\theta/8)^2)$. Using $\mathfrak{k} \geq 32\ln 12/\theta^2$, we have

$$\delta_2 = 2\exp(-2\mathfrak{k}(\theta/4)^2) + 2\exp(-2\mathfrak{k}(\theta/4 - 9m_2m_3^{-2}/2)^2) \leq 4\exp(-2\mathfrak{k}(\theta/8)^2) \leq 1/3. \tag{27}$$

We now compute the advantage of $\mathcal{B}$.

$$\begin{aligned}\text{Adv}_{\mathcal{B}} &= |\Pr[\mathcal{B}(\mathcal{J}) \Rightarrow 1 : \mathcal{J} \text{ is real}] - \Pr[\mathcal{B}(\mathcal{J}) \Rightarrow 1 : \mathcal{J} \text{ is random}]| \\ &= |\Pr[F_1 \vee \cdots \vee F_t] - \Pr[E_1 \vee \cdots \vee E_t]| \\ &\geq |\Pr[F_\ell] - \Pr[E_1 \vee \cdots \vee E_t]| \\ &\geq |\Pr[F_\ell] - \sum_{i=1}^{t}\Pr[E_i]| \\ &\geq |1 - \delta_2 - t\delta_1| \quad \text{(from (24) and (26))} \\ &\geq \frac{1}{3} \quad \text{(from (25) and (27)).}\end{aligned} \tag{28}$$

In Algorithm 2, $\mathcal{A}$ is called $\mathfrak{k}$ times in Step 4 and in each iteration of the loop in Steps 7 to 18, $\mathcal{A}$ is invoked $\mathfrak{k}$ times in Step 14. The loop in Steps 7 to 18 runs for $t = m_3^2$ iterations and so the total number of times $\mathcal{B}$ invokes $\mathcal{A}$ is $\mathfrak{k}(m_3^2 + 1) = \mathfrak{k}(1 + 36m_2/\theta)$. □

Algorithm 2 Construction of a distinguisher $\mathcal{B}$ for $\mathrm{binLWE}_{n,m_1,q,\leq\alpha}$ using a distinguisher $\mathcal{A}$ for $\mathrm{binLWE}_{n,m_2,q,\alpha}$. In the algorithm, θ is a known lower bound on the advantage of $\mathcal{A}$.

function $\mathcal{B}(\mathcal{J})$
  let $\mathcal{S}$ be a collection of m_1 samples drawn independently and uniformly from $\mathbb{Z}_p^n \times \mathbb{T}$;
  partition $\mathcal{S}$ as $\mathcal{S} = \cup_{i=1}^{\mathfrak{k}} \mathcal{S}_i$, such that $\#\mathcal{S}_i = m_2$, $i = 1, \ldots, \mathfrak{k}$;
  let $\hat{p}_{\$} = (\mathcal{A}(\mathcal{S}_1) + \cdots + \mathcal{A}(\mathcal{S}_{\mathfrak{k}}))/\mathfrak{k}$;
  $m_3 \leftarrow 6(m_2/\theta)^{1/2}$;
  let Z be the set of all integer multiples of $m_3^{-2}\alpha^2$ in the range $(0, \alpha^2]$;
  for γ in Z **do**
    $\mathcal{J}' \leftarrow \emptyset$;
    for $(\mathbf{a}, e) \in \mathcal{J}$ **do**
      sample ε from $\Psi_{\sqrt{\gamma}}$;
      $\mathcal{J}' \leftarrow \mathcal{J}' \cup \{(\mathbf{a}, e + \varepsilon)\}$;
    end for
    partition $\mathcal{J}'$ as $\mathcal{J}' = \cup_{i=1}^{k} \mathcal{J}_i$, such that $\#\mathcal{J}_i = m_2$, $i = 1, \ldots, k$;
    let $p = (\mathcal{A}(\mathcal{J}_1) + \cdots + \mathcal{A}(\mathcal{J}_{\mathfrak{k}}))/\mathfrak{k}$;
    if $|p - \hat{p}_{\$}| > \theta/2$ **then**
      return **1;**
    end if
  end for
  return **0;**
end function.