A Converse to the Ajtai-Dwork Security Proof and its Cryptographic Implications

(Extended abstract)

Phong Nguyen
Phong.Nguyen@ens.fr

Jacques Stern
Jacques.Stern@ens.fr

École Normale Supérieure
Laboratoire d'Informatique
45, rue d'Ulm
F – 75230 Paris Cedex 05

Abstract. Recently, Ajtai [3] discovered a fascinating connection between the worst-case complexity and the average-case complexity of some well-known lattice problems. Later, Ajtai and Dwork [4] proposed a cryptosystem inspired by Ajtai's work, provably secure if a particular lattice problem is difficult. We show that there is a converse to the Ajtai-Dwork security result, by reducing the question of distinguishing encryptions of one from encryptions of zero to approximating some lattice problems. This is especially interesting in view of a result of Goldreich and Goldwasser [13], which seems to rule out any form of NP-hardness for such approximation problems.

1 Introduction

Lattices are discrete subgroups of some n-dimensional space and have been the subject of intense research, going back to Gauss, Dirichlet, Hermite and Minkowski, among others. More recently, lattices have been investigated from an algorithmic point of view and two basic problems have emerged: the shortest vector problem (SVP) and the closest vector problem (CVP). SVP refers to the question of computing the lattice vector with minimum non-zero euclidean length while CVP addresses the non-homogeneous analog of finding a lattice element minimizing the distance to a given vector. It has been known for some time that CVP is NP-complete [11] and Ajtai has recently proved that SVP is NP-hard for polynomial random reductions [2].

The celebrated LLL algorithm [17] provides a partial answer to SVP since it runs in polynomial time and approximates the shortest vector within a factor of $2^{n/2}$ where n denotes the dimension of the lattice. This has been improved to the bound $(1+\varepsilon)^n$ by Schnorr [18]. Babai [6] gave an algorithm that approximates the closest vector by a factor of $(3/\sqrt{2})^n$. The existence of polynomial bounds is completely open: CVP is presumably hard to approximate within a factor $2^{(\log n)^{0.99}}$ as shown in [5] but a result of Goldreich and Goldwasser [13] suggests that it is hopeless to try to extend this inapproximability result to $\sqrt{n/\log n}$.

Recently, in a beautiful paper, Ajtai [3] found the first connection between the worst-case and the average-case complexity of SVP. He established a reduction from the problem of finding the shortest non zero element u of a lattice provided that it is "unique" (*i.e.* that it is polynomially shorter than any other element of the lattice which is not linearly related) to the

ISSN 1433-8092

problem of approximating SVP for randomly chosen instances of a specific class of lattices. This reduction was improved in [8]. Later, Ajtai and Dwork [4] proposed a cryptosystem inspired by Ajtai's work. Actually, they introduced three such systems which we will describe as AD1, AD2 and AD3 and showed that the third was provably secure under the assumption that the "unique" shortest vector problem considered above is difficult.

Again, from a theoretical point of view, the achievement in the Ajtai-Dwork paper is a masterpiece. However, its practical significance is unclear. This is partly due to the fact, exemplified by RSA, that the success of a cryptosystem is not only dependent on the computational hardness of the problem on which it is based, but also on the performances that it displays in terms of speed, key size, expansion rate, *etc.* It is also related to the fact that, so far, use of lattices in cryptography has been directed at successfully breaking schemes [1, 19, 7, 16, 10, 20, 15, 9]: experiments have shown that lattice reduction algorithms behave surprisingly well and can provide much better approximations to SVP or CVP than expected. At the "rump" session of CRYPTO'97, Victor Shoup and the authors reported on initial experiments on the cryptosystem AD1: their conclusion was that, in order to be secure, practical implementations of AD1 would require lattices of very high dimension.

At this point, it was natural to ask whether or not the security level offered by the Ajtai-Dwork cryptosystem (AD3) is exactly measured by the hardness of approximating lattice problems. In other terms, is there a converse to the Ajtai-Dwork security result? The present paper shows that this is actually the case by reducing the question of distinguishing encryptions of one from encryptions of zero to approximating CVP or SVP (recall that AD encrypts bits). More precisely, we prove that if one can approximate CVP within a factor $cn^{1.33}$, then one can distinguish encryptions with a constant advantage d, where c and d are related constants. This is especially interesting in view of the result of Goldreich and Goldwasser quoted above since it seems to rule out any form of NP-hardness for AD. We prove a similar result for SVP, with a more restrictive factor. This shows that AD is essentially equivalent to approximating the shortest vector within a polynomial ratio and allows to reverse the basic paradigm of AD: for dimensions where lattice reduction algorithms behave well in practice, AD is insecure. This opens the way to a practical assessment of the security of AD for real-size parameters.

2 The Ajtai-Dwork Cryptosystem

In this section we recall the construction of Ajtai and Dwork [4]. We adopt the notations and the presentation of [14]. For any ε between 0 and $\frac{1}{2}$, we denote by $\mathbf{Z}\pm\varepsilon$ the set of real numbers for which the distance to the nearest integer is at most ε. We denote the inner product of two vectors in the Euclidean space $\mathbf{R}^n$ by $< x, y >$. Given a set of n linearly independent vectors $w_1, \ldots, w_n$, the *parallelepiped spanned by the* w_i's is the set $P(w_1, \ldots, w_n)$ of all linear combinations of the w_i's with coefficients in $[0, 1[$. Its *width* is the minimum over i of the Euclidean distance between w_i and the hyperplane spanned by the other w_j's. Reducing a vector v modulo a parallelepiped $P(w_1, \ldots, w_n)$ means obtaining a vector $v' \in P$ such that $v' - v$ belongs to the lattice spanned by the w_i's, which we denote by $v' = v \pmod P$. To simplify the exposition we present the scheme in terms of real numbers, but we always mean numbers with some fixed finite precision. Given security parameter n (which is also the precision of the binary expansion for real numbers), we let $m = n^3$ and $\rho_n = 2^{n \log n}$. We denote by B_n the big n-dimensional cube of side-length ρ_n. We also denote by S_n the small n-dimensional ball of radius n^{-8}.

Given n, the private key is a uniformly chosen vector u in the n-dimensional unit sphere. For such a private key, we denote by $\mathcal{H}_u$ the distribution on points in B_n induced by the following construction:

1. Pick a point a uniformly at random from $\{x \in B_n \ : < x, u > \in \mathbf{Z}\}$.
2. Select $\delta_1, \ldots, \delta_n$ uniformly at random from S_n.
3. Output the point $v = a + \sum_i \delta_i$.

The public key corresponding to u is obtained by picking the points $w_1, \ldots, w_n$, $v_1, \ldots, v_m$ independently at random from the distribution $\mathcal{H}_u$, subject to the constraint that the width of the parallelepiped $w = P(w_1, \ldots, w_n)$ is at least $n^{-2}\rho_n$ (which is likely to be satisfied, see [4]).

Encryption is bit-by-bit. To encrypt a '0', uniformly select $b_1, \ldots, b_m$ in $\{0, 1\}$, and reduce the vector $\sum_{i=1}^m b_i v_i$ modulo the parallelepiped w. The vector obtained is the ciphertext. The ciphertext of '1' is just a randomly chosen vector in the parallelepiped w. To decrypt a ciphertext x with the private key u, compute $\tau =< x, u >$. If $\tau \in \mathbf{Z} \pm \frac{1}{n}$, then x is decrypted as '0', and otherwise as '1'. Thus, an encryption of '0' will always be decrypted as '0', and an encryption of '1' has a probability of $\frac{2}{n}$ to be decrypted as '0'. These decryption errors can be removed (see [14]). The main result of [4] states that a probabilistic algorithm distinguishing encryptions of a '0' from encryptions of a '1' with some polynomial advantage can be used to find the shortest nonzero vector in any n-dimensional lattice where the shortest vector v is unique, in the sense that any other vector whose length is at most $n^8 ||v||$ is parallel to v.

In this article, we are interested in a converse to the Ajtai-Dwork theorem. We first describe a reduction that works for any choice of the keys. Next, we improve the bound, based on a probabilistic analysis. Finally, we show how to use a SVP-oracle instead of a CVP-oracle.

3 Deciphering with a CVP-oracle

We define an (n, k)-CVP-oracle to be any algorithm which, given a point $x \in \mathbf{R}^n$ and a n-dimensional lattice L, outputs a lattice point $\alpha \in L$ such that for every $\beta \in L$: $\text{dist}(x, \alpha) \leq k\text{dist}(x, \beta)$, where *dist* denotes the Euclidean distance. Each oracle call made by a Turing machine contributes by a single unit to the overall complexity of the machine.

Using such an oracle, we will see how one can distinguish in probabilistic polynomial time ciphertexts of '0' from ciphertexts of '1'. To any choice of the keys, we will associate a particular lattice. Given a ciphertext, one can build a vector such that: if this vector is close enough to the lattice, then the ciphertext is a ciphertext of '0' with high probability. To check whether this vector is close enough, one calls an oracle.

Let $(u, w_1, \ldots, w_n, v_1, \ldots, v_m)$ be a set of keys. We first need a basic result:

Lemma 1. *Let x be a ciphertext of '0': $x - \sum_{i=1}^m b_i v_i = \sum_{j=1}^n \alpha_j w_j$ with $b_i \in \{0, 1\}$ and $\alpha_j \in \mathbf{Z}$, where we keep notations introduced in the previous section. Then the α_j's satisfy: $|\alpha_j| \leq n^5 \sqrt{n}$.*

Proof. We have $\alpha_j = \lfloor \theta_j \rceil$ where the θ_j's are defined by: $\sum_{i=1}^m b_i v_i = \sum_{j=1}^n \theta_j w_j$. If we project this equality on the orthogonal complement of each hyperplane spanned by $(w_k)_{k \neq j}$, we find that $|\theta_j| \leq n^5 \sqrt{n}$, since the width of the parallelepiped $P(w_1, \ldots, w_n)$ is at least $n^{-2}\rho_n$. □

For any real β, let L_β be the $n+m$-dimensional lattice (in $\mathbf{R}^{2n+m}$) spanned by the columns of the following matrix:

$$\begin{pmatrix} \beta w_1 & \ldots & \beta w_n & \beta v_1 & \ldots & \beta v_m \\ 1 & 0 & & \ldots & & 0 \\ 0 & \ddots & & & & \\ & & 1 & \ddots & & \vdots \\ \vdots & & \ddots & n^4\sqrt{n} & & \\ & & & & \ddots & 0 \\ 0 & & \ldots & & 0 & n^4\sqrt{n} \end{pmatrix}$$

From the previous lemma, we infer the following:

Proposition 2. *If x is a ciphertext of '0', then, for any choice of β,*

$$dist\left(\begin{pmatrix} \beta x \\ 0 \end{pmatrix}, L_\beta\right) \leq \sqrt{2}n^6.$$

In other words, a ciphertext of '0' is, in some sense, close to the lattice L_β. But there is more:

Proposition 3. *Let $\varepsilon > 0$ and y be a point in the parallelepiped $w = P(w_1, \ldots, w_n)$. If*

$$dist\left(\begin{pmatrix} \beta y \\ 0 \end{pmatrix}, L_\beta\right) \leq \varepsilon n^{6.5}, \qquad then \qquad < u, y > \in \mathbf{Z} \pm \varepsilon\left(1 + \frac{1}{n^{3.5}} + \frac{n^{6.5}}{\beta}\right).$$

Proof. We have $\beta y = \beta\left(\sum_{i=1}^m b_i v_i + \sum_{j=1}^n \alpha_j w_j\right) + e$, where $||e||^2$ and $\sum_{i=1}^m b_i^2 n^9 + \sum_{i=1}^n \alpha_j^2$ are both less than $\varepsilon^2 n^{13}$. Thus, $\mathrm{dist}(\mathbf{Z}, < u, y >)$ is less than

$$\sum_{i=1}^m |b_i| \mathrm{dist}(\mathbf{Z}, < u, v_i >) + \sum_{j=1}^n |\alpha_j| \mathrm{dist}(\mathbf{Z}, < u, w_j >) + \varepsilon \frac{n^{6.5}}{\beta}.$$

Since $< v_i, u >$ belongs to $\mathbf{Z} \pm \frac{1}{n^7}$, the Cauchy-Schwarz inequality implies that the first term is less than:

$$\left(\sum_{i=1}^m b_i^2\right)^{1/2} \times \left(m\frac{1}{n^{14}}\right)^{1/2} \leq \varepsilon n^2 n^{-5.5} = \varepsilon n^{-3.5}.$$

Also, since $< w_j, u >$ belongs to $\mathbf{Z} \pm \frac{1}{n^7}$, the second term is less than:

$$\left(\sum_{j=1}^n \alpha_j^2\right)^{1/2} \times \left(n\frac{1}{n^{14}}\right)^{1/2} \leq \varepsilon n^{6.5} n^{-6.5} = \varepsilon.$$

The result follows. □

If we collect these propositions, we obtain a probabilistic reduction:

Theorem 4. *For any $\varepsilon > 0$, there exists a polynomial time Turing machine, taking a ciphertext x as an input and making a single call to a $\left(n+m, \varepsilon\sqrt{n/2}\right)$-CVP-oracle, which outputs a yes/no answer such that:*

- *If the answer is no, then x is a ciphertext of '1'.*
- *If the answer is yes, then x is a ciphertext of '0' with probability at least $1 - 3\varepsilon$.*

Proof. We let $\beta = 4n^{6.5}$. Calling once a $(n+m, \varepsilon\sqrt{n/2})$-CVP-oracle, we obtain a lattice point $\alpha \in L_\beta$ such that, for all $\gamma \in L_\beta$:

$$\text{dist}\left(\alpha, \begin{pmatrix} \beta x \\ 0 \end{pmatrix}\right) \leq \varepsilon\sqrt{n/2}\text{dist}\left(\gamma, \begin{pmatrix} \beta x \\ 0 \end{pmatrix}\right)$$

We output 'yes' if and only if

$$\text{dist}\left(\alpha, \begin{pmatrix} \beta x \\ 0 \end{pmatrix}\right) \leq \varepsilon n^{6.5}.$$

If x is a ciphertext of '0', proposition 2 ensures that this inequality is satisfied. Hence, if the answer is no, then x is a ciphertext of '1', or else, by proposition 3, one can infer that $< u, x >$ belongs to $\mathbf{Z} \pm \varepsilon(1 + \frac{1}{4} + \frac{1}{4})$, and the result follows. □

4 Improving the bound

In this section, we show how to improve the reduction by increasing the $\varepsilon\sqrt{n/2}$ factor, using probabilistic arguments.

Lemma 5. *Let t be a vector in the n-dimensional unit sphere. Let s be a randomly chosen point (with uniform distribution) from the hypercube B_n. Then $E[< s, t >] = 0$ and Var$[< s, t >] = \frac{\rho_n^2}{3}$.*

Proof (Sketch). Decompose s and t with respect to the canonical basis to express the dot product $< s, t >$. The result follows from a short computation, using the fact that the coordinates of s are independent random variables uniformly distributed over $] - \rho_n, +\rho_n[$. □

We now notice that the upper bound of lemma 1 is quite pessimistic:

Lemma 6. *Let x be a ciphertext of '0': $x - \sum_{i=1}^m b_i v_i = \sum_{j=1}^n \alpha_j w_j$. Assume that $v_1, v_2, \ldots, v_m$ are independent random variables uniformly distributed over the hypercube B_n. Then:*

$$E[\alpha_j^2] \leq \frac{1}{3}n^7$$

Proof. We have $\alpha_j = \lfloor \theta_j \rceil$ where the θ_j's are defined by: $\sum_{i=1}^m b_i v_i = \sum_{j=1}^n \theta_j w_j$. Denote by $w_j^\perp$ a unit vector orthogonal to the hyperplane spanned by $(w_k)_{k \neq j}$. Since the width of the parallelepiped $P(w_1, \ldots, w_n)$ is at least $n^{-2}\rho_n$, we have for all j:

$$\theta_j^2 \leq \frac{n^4}{\rho_n^2} < \sum_{i=1}^m b_i v_i, w_j^\perp >^2 .$$

From the previous lemma and by independence of the v_i's, we know that:

$$E\left[< \sum_{i=1}^m b_i v_i, w_j^\perp >^2\right] = \sum_{i=1}^m b_i^2 E\left[< v_i, w_j^\perp >^2\right] \leq m\frac{\rho_n^2}{3} = n^3\frac{\rho_n^2}{3}.$$

We conclude since $E[\alpha_j^2] \leq E[\theta_j^2]$. □

This leads us to replace the $n^4\sqrt{n}$ coefficients by $n^2\sqrt{n}$ in the definition of our previous lattice L_β. We obtain a refinement of proposition 2:

Proposition 7. *Let $\eta > 0$. Then for sufficiently large n, the following holds: let x be a ciphertext of '0'; let the public key vectors $v_1, v_2, \ldots, v_m$ be independently chosen at random from $\mathcal{H}_u$; for any $\varepsilon_1 > 0$, we have with probability at least $1 - \varepsilon_1$, for any choice of β,*

$$dist\left(\begin{pmatrix} \beta x \\ 0 \end{pmatrix}, L_\beta\right) \leq n^4\sqrt{1 + \frac{1+\eta}{3\varepsilon_1}}.$$

Proof. We first assume that $v_1, \ldots, v_m$ are uniformly distributed over the hypercube B_n. Lemma 6 implies that $E\left[\sum_{j=1}^n \alpha_j^2\right] \leq \frac{1}{3}n^8$, where the α_j's are defined as in lemma 6. Therefore, by Markov's inequality, we have with probability at least $1 - \varepsilon_1$,

$$\sum_{j=1}^n \alpha_j^2 \leq \frac{1}{3\varepsilon_1}n^8.$$

Hence:

$$\text{dist}\left(\begin{pmatrix} \beta x \\ 0 \end{pmatrix}, L_\beta\right) \leq \sqrt{\frac{1}{3\varepsilon_1}n^8 + n^3 n^5} \leq n^4\sqrt{1 + \frac{1}{3\varepsilon_1}}.$$

We now show how to modify the proof in order to take care of the actual distribution of the vectors v_i. Let a denote a point chosen at random from $\{x \in B_n \ : < x, u > \in \mathbf{Z}\}$. Let λ be randomly chosen in $[0, 1[$. Then, the sum $a + \lambda u$ is uniformly distributed over an n-dimensional volume C_n, which differs from B_n by points y such that the segment $[y, y+u]$ crosses the border of B_n. Such points are within distance 1 of this border. It follows that one can bound the volume of the difference of B_n and C_n by $2n\rho_n^{n-1}$. Replacing the uniformly distributed variable v_i by $a_i + \lambda_i u$ chosen according to the above distribution, one sees that the expected value of $E\left[\sum_{j=1}^n \alpha_j^2\right]$ is modified by at most $\frac{2n}{\rho_n}n^{12}$, since α_j^2 is always less than n^{11}. Applying Markov's inequality as above, one gets, with probability at least $1 - \varepsilon_1$,

$$\sum_{j=1}^n \alpha_j^2 \leq \frac{1}{\varepsilon_1}\left(\frac{1}{3}n^8 + \frac{2n^{13}}{\rho_n}\right).$$

Noting that the actual v_i is obtained from some instance of a_i by adding a small perturbation vector δ_i, and that $\frac{2n^{13}}{\rho_n} = o(1)$ as n grows, the result follows. □

To obtain a similar improvement to proposition 3, we need another technical lemma:

Lemma 8. *Let u be a vector in the n-dimensional unit sphere. Let δ be a randomly chosen point from S_n. Then $E[< u, \delta >] = 0$ and $Var[< u, \delta >] = \frac{4W_n^2}{(n+2)n^{16}}$, where W_n denotes the n-th Wallis integral:*

$$W_n = \int_0^{\pi/2} \sin^n \theta d\theta.$$

Proof (Sketch). The expectation $E[< u, \delta >]$ is clearly zero. To compute the variance, we can assume that $u = (1, 0, 0, \ldots, 0)$ since S_n is invariant by rotation. We obtain:

$$\mathrm{Var}[< u, \delta >] = \int_{-n^{-8}}^{n^{-8}} x^2 \frac{V_{n-1}(\sqrt{n^{-16} - x^2})}{V_n(n^{-8})} dx,$$

where $V_n(r)$ denotes the volume of the n-dimensional ball of radius r. The result follows after a few simplifications using Wallis integrals. □

Proposition 9. *Let u be a vector in the n-dimensional unit sphere. Let v be a randomly chosen point from the distribution $\mathcal{H}_u$. Then:*

$$E\left[dist(\mathbf{Z}, < u, v >)^2\right] \leq \frac{2\pi}{(n+2)n^{16}}.$$

Proof (Sketch). Write $v = a + \sum_i \delta_i$ where the δ_i's are independently chosen with uniform distribution over S_n. Apply the previous lemma with u and δ_i. Conclude as $W_n^2 \leq \frac{2\pi}{n}$. □

This leads to the following refinement of proposition 3:

Proposition 10. *Let y be a point in the parallelepiped $w = P(w_1, \ldots, w_n)$. Let $\varepsilon, \varepsilon_2 > 0$. If*

$$dist\left(\left(\begin{array}{c} \beta y \\ 0 \end{array}\right), L_\beta\right) \leq \varepsilon \sqrt{\frac{\varepsilon_2}{2\pi}} n^8,$$

then, the following holds with probability at least $1 - \varepsilon_2$ (with respect to the choice of $w_1, \ldots, w_n$):

$$< u, y > \in \mathbf{Z} \pm \varepsilon \left(1 + \sqrt{\frac{\varepsilon_2}{2\pi}} \left(1 + \frac{n^8}{\beta}\right)\right).$$

Proof. As in the proof of proposition 3, we find that $\sum_{i=1}^m b_i^2 n^5 + \sum_{i=1}^n \alpha_j^2 \leq \varepsilon^2 \frac{\varepsilon_2}{2\pi} n^{16}$ and

$$\mathrm{dist}(\mathbf{Z}, < u, y >) \leq \sum_{i=1}^m |b_i| \mathrm{dist}(\mathbf{Z}, < u, v_i >) + \sum_{j=1}^n |\alpha_j| \mathrm{dist}(\mathbf{Z}, < u, w_j >) + \frac{\varepsilon}{\beta} \sqrt{\frac{\varepsilon_2}{2\pi}} n^8.$$

By the Cauchy-Schwarz inequality, the first term is bounded by $\sqrt{\varepsilon^2 \frac{\varepsilon_2}{2\pi} n^{11}} \times \sqrt{m \frac{1}{n^{14}}} = \varepsilon \sqrt{\frac{\varepsilon_2}{2\pi}}$. Also, the second term is less than:

$$\sqrt{\sum_{j=1}^n \alpha_j^2} \times \sqrt{\sum_{j=1}^n \mathrm{dist}(\mathbf{Z}, < u, w_j >)^2}.$$

We know that the first term of this product is bounded by $\varepsilon\sqrt{\frac{\varepsilon_2}{2\pi}}n^8$. Furthermore, if we denote by X the random variable $\sum_{j=1}^n \mathrm{dist}(\mathbf{Z}, < u, w_j >)^2$, we have from proposition 10:

$$E[X] = \sum_{j=1}^{n} E\left[\mathrm{dist}(\mathbf{Z}, < u, w_j >)^2\right] \leq n\frac{2\pi}{(n+2)n^{16}} \leq \frac{2\pi}{n^{16}}.$$

By Markov's inequality, it follows that with probability at least $1-\varepsilon_2$, $\sqrt{X} \leq n^{-8}\sqrt{\frac{2\pi}{\varepsilon_2}}$. We conclude from all the inequalities obtained. □

From all these propositions, we derive an improved probabilistic reduction:

Theorem 11. *For any $\varepsilon, \varepsilon_1, \varepsilon_2$ in $]0,1]$, there exists a polynomial time Turing machine, taking a ciphertext x as an input and making a single call to a $\left(n+m, \varepsilon\sqrt{\frac{\varepsilon_1\varepsilon_2}{\pi(1+2\varepsilon_1)}}n^4\right)$-CVP-oracle, which outputs a yes/no answer such that, for sufficiently large n:*

- *If the answer is no, then x is a ciphertext of '1' with probability at least $1-\varepsilon_1$, with respect to the choice of $v_1, \ldots, v_m$.*
- *If the answer is yes, then x is a ciphertext of '0' with probability at least $(1-3\varepsilon)(1-\varepsilon_2)$ with respect to x, $w_1, \ldots, w_n$.*

Proof. We let $\beta = 4n^8\sqrt{\frac{\varepsilon_2}{2\pi}}$. Calling once a $\left(n+m, \varepsilon\sqrt{\frac{\varepsilon_1\varepsilon_2}{\pi(1+2\varepsilon_1)}}n^4\right)$-CVP-oracle, we obtain a lattice point $\alpha \in L_\beta$ such that, for all $\gamma \in L_\beta$:

$$\mathrm{dist}\left(\alpha, \begin{pmatrix} \beta x \\ 0 \end{pmatrix}\right) \leq \varepsilon\sqrt{\frac{\varepsilon_1\varepsilon_2}{\pi(1+2\varepsilon_1)}}n^4 \mathrm{dist}\left(\gamma, \begin{pmatrix} \beta x \\ 0 \end{pmatrix}\right)$$

We output 'yes' if and only if $\mathrm{dist}\left(\alpha, \begin{pmatrix} \beta x \\ 0 \end{pmatrix}\right) \leq \varepsilon\sqrt{\frac{\varepsilon_2}{2\pi}}n^8$. If x is a ciphertext of '0', proposition 7 with $\eta = 1/2$ ensures that this inequality is satisfied with probability at least $1-\varepsilon_1$. Hence, if the answer is no, then x is a ciphertext of '1' with probability at least $1-\varepsilon_1$, with respect to the choice of $v_1, \ldots, v_m$. Otherwise, proposition 10 implies that $< u, x >$ belongs to $\mathbf{Z} \pm \varepsilon(1 + \frac{1}{4} + \frac{1}{4})$, with probability at least $1-\varepsilon_2$, with respect to the choice of $w_1, \ldots, w_n$. □

5 Deciphering with a SVP-oracle

We now try to use SVP-oracles. Given a n-dimensional lattice L, an (n,k)-SVP-oracle outputs a point $\alpha \in L$ such that for every $\beta \in L$: $\|\alpha\| \leq k\|\beta\|$.

Theorem 12. *Let $\theta, \gamma > 0$ such that $\frac{5\gamma}{2} + 2\theta < 2$. There exists a polynomial time oracle Turing machine calling a $(n^{2+\gamma}, n^\theta)$-SVP-oracle which distinguishes, for sufficiently large n, encryptions of '0' from encryptions of '1' with a polynomial advantage.*

Note: recall that the advantage ε of a distinguishing algorithm $\mathcal{A}$ is such that

$$P[\mathcal{A} \text{ answers correctly}] \geq \frac{1}{2} + \varepsilon.$$

We will need a technical improvement over the computations of section 4 which reads as the following two lemmas, whose proofs can be found in the appendix. The key to the improvement is to replace Markov's inequality by moments inequalities, using the multinomial formula.

Lemma 13. *Let k be a positive integer. There exists a constant $M_1(k)$ depending only on k, such that the following holds for all sufficiently large n: let y be a ciphertext of '0', and $\varepsilon_1 > 0$, then with probability at least $1 - \varepsilon_1$, y comes from a sequence $b_1, \ldots, b_m$ such that writing $y - \sum_{i=1}^m b_i v_i = \sum_{j=1}^n \alpha_j w_j$, one gets*

$$\sum_{j=1}^{n} \alpha_j^2 \leq M_1(k) n^8 \varepsilon_1^{-1/k}.$$

Given ε_1, we say that y is a *good ciphertext* if it satisfies the inequality of the previous lemma. Note that it is possible to produce good ciphertexts, given the public key, by a polynomial time algorithm.

Lemma 14. *Let k be a positive integer. There exists a real $M_2(k)$ such that the following holds for all sufficiently large n: let $\varepsilon_2 > 0$, then with probability at least $1-\varepsilon_2$ over the choice of the public key only, one gets, for good ciphertexts y of '0',*

$$dist(\mathbf{Z}, < u, y >) \leq M_2(k) \frac{1}{n^4 (\varepsilon_1 \varepsilon_2)^{1/2k}}.$$

We now fix some constants. Since $2\theta + \frac{5\gamma}{2} < 2$, there exist strictly positive $\gamma_1, \gamma_2, \eta_1, \eta_2, k, \lambda$ such that

$$2\theta + \frac{3\gamma}{2} + \gamma_2 + \lambda + \frac{1}{2k}(4 + \gamma + \gamma_1 + \gamma_2 + \eta_1 + \eta_2) < 2,$$

with $\gamma_2 > \gamma_1 > \gamma$, $\gamma_1 < \gamma + \lambda$. We let $\varepsilon_1 = \dfrac{1}{n^{2+\gamma+\gamma_1+\eta_1}}$ and $\varepsilon_2 = \dfrac{1}{n^{2+\gamma+\gamma_2+\eta_2}}$. We will use our oracle as follows: let $\nu = n^{2+\gamma}$ and consider a sequence $(y_1, \ldots, y_\nu)$ of elements of $P(w_1, \ldots, w_n)$. Choose a random permutation σ of $\{1, \ldots, \nu\}$ and apply the $(n^{2+\gamma}, n^\theta)$-SVP-oracle to the lattice spanned by the columns of the following matrix, with $\beta = n^6 n^{1+\frac{\gamma}{2}}$:

$$\begin{pmatrix} \beta y_{\sigma(1)} & \beta y_{\sigma(2)} & \cdots & \beta y_{\sigma(\nu)} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

The output is a vector $(z, \lambda_1, \ldots, \lambda_\nu)$. Say that y_i is *hit* if $0 < |\lambda_{\sigma^{-1}(i)}| \leq n^{\frac{\gamma}{2}+\theta+\lambda}$. The following two propositions show that ciphertexts of '0' and '1' behave differently.

Proposition 15. *If $y_1, \ldots, y_\nu$ are ciphertexts of '1', then y_1 is hit with probability $\Omega\left(\frac{1}{n^{\gamma_1}}\right)$.*

Proposition 16. *If y_1 is a ciphertext of '1' and $y_2, \ldots, y_\nu$ are good ciphertexts of '0', then y_1 is hit with probability $\mathcal{O}\left(\frac{1}{n^{\gamma_2}}\right)$.*

These propositions are proved in the appendix. We now show how to conclude. The distributions $S_\nu = (y_1, \ldots, y_\nu : y_i$ is a ciphertext of '1') and $T_\nu = (y_1, \ldots, y_\nu : y_1$ is a ciphertext of '1' and the others are good ciphertexts of '0') are distinguished by the test "y_1 is hit" with advantage $\Omega(\frac{1}{n^{\gamma_1}})$. Using the "hybrid method" (see [12]), we introduce the distributions $S_i = (y_1, \ldots, y_\nu : y_1, \ldots, y_i$ are ciphertexts of '1' and $y_{i+1}, \ldots, y_\nu$ are good ciphertexts of '0'). There exists i such that S_{i-1} and S_i are distinguished by the test with advantage $\Omega(\frac{1}{n^{\gamma_1} n^{2+\gamma}})$. One can check whether a given y is a ciphertext of '0' or '1' by querying the answer of the test for $(y_1, \ldots, y_{i-1}, y, y_{i+1}, \ldots, y_\nu)$ where $y_1, \ldots, y_{i-1}$ are random ciphertexts of '1' and $y_{i+1}, \ldots, y_\nu$ are random good ciphertexts of '0'. Since the bad lattices that contradict lemma 14 form a set of probability less than $\varepsilon_2 \leq n^{-2-\gamma-\gamma_1-\eta_2}$ and the bad ciphertexts of '0' form a set of probability less than $\varepsilon_1 = n^{-2-\gamma-\gamma_1-\eta_1}$, these do not harm the advantage of the distinguisher.

Note: the above construction is non-uniform. Eliminating the non-uniformity requires "sampling" the test for the various distributions S_i (see [12]).

6 Conclusion

We have shown how to reduce the question of distinguishing encryptions of one from encryptions of zero in the Ajtai-Dwork cryptosystem to approximating CVP or SVP. For simplicity, our results were proved with the choice of constants from [14]. Of course, the method extends to a more general setting as well, with the same proofs. More precisely, if we let $m = n^c$ (instead of n^3) and denote by S_n the n-dimensional ball of radius n^{-d} (instead of n^{-8}), theorem 11 remains valid with a $\left(n + m, \varepsilon\sqrt{\frac{\varepsilon_1 \varepsilon_2}{\pi(1+2\varepsilon_1)}} n^{d-(c+5)/2}\right)$-CVP-oracle. Theorem 12 also remains valid if θ and γ are such that $\frac{5\gamma}{2} + 2\theta < d - (9+c)/2$ and we use a $(n^{2+\gamma}, n^\theta)$-SVP-oracle.

References

[1] L. M. Adleman. On breaking generalized knapsack public key cryptosystems. In *Proc. 15th ACM Symposium on Theory of Computing*, pages 402–412, 1983.

[2] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions. Preprint. Revision of ECCC Report TR97-047, Nov 11, 1997. Can be found at `http://www.eccc.uni-trier.de/eccc/`.

[3] M. Ajtai. Generating hard instances of lattice problems. In *Proc. 28th ACM Symposium on Theory of Computing*, pages 99–108, 1996.

[4] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proc. 29th ACM Symposium on Theory of Computing*, pages 284–293, 1997.

[5] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *Journal of Computer and System Sciences*, 54(2):317–331, 1997.

[6] L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.

[7] E. Brickell. Breaking iterated knapsacks. In *Proc. CRYPTO'84*, volume 196 of *LNCS*, pages 342–358, 1985.

[8] J.-Y. Cai and A. P. Nerurkar. An improved worst-case to average-case connection for lattice problems. In *Proc. 38th IEEE Conference on Foundations of Computer Science*, pages 468–477, 1997.

[9] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. of Cryptology*, 10(4):233–260, 1997.

[10] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.-P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2:111–128, 1992.

[11] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical report, Mathematische Instituut, University of Amsterdam, 1981. Report 81-04.

[12] O. Goldreich. *Foundations of Cryptography (Fragments of a Book)*. Weizmann Institute of Science, 1995.

[13] O. Goldreich and S. Goldwasser. On the limits of non-approximability of lattice problems. Preprint. Revision of ECCC Report TR97-031, Oct 16, 1997. Can be found at `http://www.eccc.uni-trier.de/eccc/`.

[14] O. Goldreich, S. Goldwasser, and S. Halevi. Eliminating decryption errors in the Ajtai-Dwork cryptosystem. In *Proceedings of Crypto'97*, volume 1294 of *LNCS*, pages 105–111. Springer-Verlag, 1997.

[15] A. Joux and J. Stern. Lattice reduction: a toolbox for the cryptanalyst. (to appear in J. of Cryptology).

[16] J.C. Lagarias and A.M. Odlyzko. Solving low-density subset sum problems. In *Proc. 24th IEEE Symposium on Foundations of Computer Science*, pages 1–10. IEEE, 1983.

[17] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[18] C.-P. Schnorr. A hierarchy of polynomial lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.

[19] A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. In *Proc. 23rd IEEE Symposium on Foundations of Computer Science*, pages 145–152, 1982.

[20] J. Stern. Secret linear congruential generators are not cryptographically secure. In *Proc. 28th IEEE Conference on Foundations of Computer Science*, pages 421–426, 1987.

A Appendix

In this appendix, we provide the missing proofs of section 5.

A.1 Proof of Lemma 13

We first generalize lemma 5. Let $t = (t_1, \ldots, t_n)$ be a vector in the n-dimensional unit sphere. Let $s = (s_1, \ldots, s_n)$ be a randomly chosen point with uniform distribution from B_n. We have:

$$E[< s, t >^{2k}] = E\left[\left(\sum_{j=1}^{n} s_j t_j\right)^{2k}\right]$$

If we expand this product, we obtain m^{2k} terms. All the terms for which some s_j has an odd exponent disappear. We obtain by the multinomial formula:

$$E[< s, t >^{2k}] = \sum_{i_1+\cdots+i_n=k} \frac{(2k)!}{(2i_1)!\cdots(2i_n)!} E\left[(s_1t_1)^{2i_1}\cdots(s_nt_n)^{2i_n}\right].$$

And since the s_j's are independent:

$$E\left[(s_1t_1)^{2i_1}\cdots(s_nt_n)^{2i_n}\right] = t_1^{2i_1}\cdots t_n^{2i_n}\rho_n^{2i_1+\cdots+2i_n}\frac{1}{2i_1+1}\cdots\frac{1}{2i_n+1}.$$

Therefore:

$$E[< s, t >^{2k}] = \rho_n^{2k} \sum_{i_1+\cdots+i_n=k} \frac{(2k)!}{(2i_1+1)!\cdots(2i_n+1)!} t_1^{2i_1}\cdots t_n^{2i_n}.$$

And this sum is less than:

$$\frac{(2k)!}{k!} \sum_{i_1+\cdots+i_n=k} \frac{k!}{i_1!\cdots i_n!} t_1^{2i_1}\cdots t_n^{2i_n} = \frac{(2k)!}{k!}(t_1^2+\cdots+t_n^2)^k = \frac{(2k)!}{k!}.$$

Thus:

$$E[< s, t >^{2k}] \leq \frac{(2k)!}{k!}\rho_n^{2k}.$$

Note that if there was an odd power instead of $2k$, the expectation would be equal to zero. Now, as in the proof of proposition 7, we can first assume that the v_i's are distributed uniformly over B_n. The proof of lemma 6 becomes, by the same argument about the disappearance of "odd" terms:

$$E\left[< \sum_{i=1}^{m} b_i v_i, w_j^{\perp} >^{2k}\right] \leq \sum_{i_1+\cdots+i_m=k} \frac{(2k)!}{(2i_1)!\cdots(2i_m)!} \prod_{\ell=1}^{m} E\left[< v_\ell, w_j^{\perp} >^{2i_\ell}\right].$$

We know that each product is less than $\prod_{\ell=1}^{m} \frac{(2i_\ell)!}{i_\ell!}\rho_n^{2i_\ell} \leq \rho_n^{2k}(2k)!^k$. And

$$\sum_{i_1+\cdots+i_m=k} \frac{(2k)!}{(2i_1)!\cdots(2i_m)!} \leq \frac{(2k)!}{k!} \sum_{i_1+\cdots+i_m=k} \frac{k!}{i_1!\cdots i_m!} = \frac{(2k)!}{k!}m^k.$$

It follows that $E\left[< \sum_{i=1}^{m} b_i v_i, w_j^\perp >^{2k}\right] \leq \rho_n^{2k}((2k)!)^k \frac{(2k)!}{k!}m^k$, and therefore,

$$E\left[\alpha_j^{2k}\right] \leq n^{4k}(2k)!^{k+1}m^k = n^{7k}(2k)!^{k+1}.$$

As previously, note that if there was an odd power instead of $2k$, the expectation would be equal to zero. Apply one last time the multinomial formula:

$$\begin{aligned} E\left[(\alpha_1^2+\cdots+\alpha_n^2)^k\right] &\leq \sum_{i_1+\cdots+i_n=k} \frac{k!}{i_1!\cdots i_n!} \prod_{j=1}^{n} E\left[\alpha_j^{2i_j}\right] \\ &\leq \sum_{i_1+\cdots+i_n=k} \frac{k!}{i_1!\cdots i_n!} n^{7k}\left((2k)!^{k+1}\right)^k \\ &= n^{7k}(2k)!^{k(k+1)}n^k. \end{aligned}$$

Hence:

$$E\left[(\alpha_1^2+\cdots+\alpha_n^2)^k\right] \leq n^{8k}(2k)!^{k(k+1)}.$$

Now, if the v_i's are chosen from their actual distribution $\mathcal{H}_u$, as in the proof of proposition 7, one can show that the expected value is modified by at most $n^k n^{11k}\frac{2n}{\rho_n}$, since α_j^2 is always less than n^{11}. Therefore, for sufficiently large n (depending only on k), due to the $\frac{1}{\rho_n}$ factor:

$$E\left[(\alpha_1^2+\cdots+\alpha_n^2)^k\right] \leq n^{8k}(2k+1)!^{k(k+1)}.$$

Finally, we apply a moment inequality to obtain, with probability at least $1-\varepsilon_1$:

$$\sum_{j=1}^{n} \alpha_j^2 \leq \frac{1}{\varepsilon_1^{1/k}} n^8 (2k+1)!^{k+1}.$$

The result follows with $M_1(k) = (2k+1)!^{k+1}$.

A.2 Proof of lemma 14

The method is similar to the one used in the proof of lemma 13. This time, we need to generalize lemma 8 and proposition 9. Let u be a vector in the n-dimensional unit sphere. Let δ be a randomly chosen point from S_n. The proof of lemma 8 becomes:

$$E[< u, \delta >^{2k}] = 4\frac{W_n}{n^{16}} \int_0^1 (1-y^2)^{(n-1)/2} y^{2k} dy.$$

This integral is equal to $I(n,k) = \int_0^{\pi/2} \sin^n\theta\cos^{2k}\theta d\theta$. We have $I(n,0) = W_n$ and an integration by parts shows that:

$$I(n,k) = \int_0^{\pi/2} \frac{1}{n+1}\sin^{n+1}\theta \times (2k-1)\sin\theta\cos^{2k-2}\theta d\theta = \frac{2k-1}{n+1} I(n+2,k-1).$$

It follows that:

$$I(n,k) = \frac{(2k-1)(2k-3)\cdots 1}{(n+1)(n+3)\cdots(n+2k-1)} W_n \leq \frac{(2k)!}{n^k} W_n.$$

Hence:

$$E[< u, \delta >^{2k}] \leq \frac{4}{n^{16}} \frac{(2k)!}{n^k} W_n^2 \leq \frac{2\pi(2k)!}{n^{17+k}}.$$

The expectation would be equal to zero if there was an odd power instead of $2k$. Now, let $v = a + \sum_i \delta_i$ be a randomly chosen point from the distribution $\mathcal{H}_u$. Since "odd" terms disappear, we write the multinomial formula as:

$$\begin{aligned}
E\left[\text{dist}(\mathbf{Z}, < u, v >)^{2k}\right] &\leq E\left[\left(\sum_{i=1}^{n} < u, \delta_i >\right)^{2k}\right] \\
&= \sum_{i_1+\cdots+i_n=k} \frac{(2k)!}{(2i_1)!\cdots(2i_n)!} \prod_{j=1}^{n} E[< u, \delta_j >^{2i_j}] \\
&\leq \sum_{i_1+\cdots+i_n=k} \frac{(2k)!}{(2i_1)!\cdots(2i_n)!} \frac{1}{n^{17+k}} \left(2\pi(2k)!\right)^{2k} \\
&\leq \frac{1}{n^{17+k}} \left(2\pi(2k)!\right)^{2k} \frac{(2k)!}{k!} n^k \\
&\leq \frac{1}{n^{17}} 4^k \pi^{2k} (2k)!^{2k+1}.
\end{aligned}$$

Again, with an odd power, the expectation would be equal to zero. Therefore:

$$\begin{aligned}
E\left[\left(\sum_{j=1}^{n} \text{dist}(\mathbf{Z}, < u, w_j >)^2\right)^k\right] &\leq \sum_{j_1+\cdots+j_n=k} \frac{k!}{j_1!\cdots j_n!} \prod_{\ell=1}^{n} E\left[\text{dist}(\mathbf{Z}, < u, w_j >)^{2j_\ell}\right] \\
&\leq \sum_{j_1+\cdots+j_n=k} \frac{k!}{j_1!\cdots j_n!} \frac{1}{n^{17k}} \left(4^k \pi^{2k} (2k)!^{2k+1}\right)^k \\
&\leq \frac{1}{n^{16k}} \left(4^k \pi^{2k} (2k)!^{2k+1}\right)^k
\end{aligned}$$

Thus, by the moment inequality, we have with probability at least $1 - \varepsilon_2$ (with respect to the choice of $w_1, \ldots, w_n$):

$$\sum_{j=1}^{n} \text{dist}(\mathbf{Z}, < u, w_j >)^2 \leq \frac{1}{\varepsilon_2^{1/k}} \frac{1}{n^{16}} 4^k \pi^{2k} (2k)!^{2k+1}.$$

And the result follows from the Cauchy-Schwarz inequality and the definition of good ciphertexts, as in the proof of proposition 10 with:

$$M_2(k) = 2\sqrt{M_1(k)4^k\pi^{2k}(2k)!^{2k+1}}.$$

A.3 Proof of proposition 15

We first need a combinatorial lemma:

Lemma 17. *There exists N such that for all $n \geq N$, the following holds: let $y_1, \ldots, y_\nu$ be elements of the parallelepiped $P(w_1, \ldots, w_n)$, then there exist coefficients λ_i (not all zero) in $\{-1, 0, +1\}$ such that*

$$\left\|\sum_{i=1}^{\nu} \lambda_i y_i\right\| \leq \frac{1}{n^6}.$$

Proof. Let $z_i = \lfloor n^{10} y_i \rfloor$. Each z_i has integral entries in $\{-n^{10}\rho_n, \ldots, n^{10}\rho_n\}$. Consider all combinations $\sum \lambda_i z_i$ with $\lambda_i \in \{0, 1\}$. There are 2^ν such combinations, but there are at most $(2\nu n^{10}\rho_n + 1)^n$ distinct combinations. By the pigeon-hole principle, it follows that if $2^\nu > (2\nu n^{10}\rho_n + 1)^n$, which is satisfied for sufficiently large n, then there exist two distinct sequeunces $(\lambda_1, \ldots, \lambda_\nu)$ and $(\mu_1, \ldots, \mu_\nu)$ in $\{0, 1\}^\nu$ such that: $\sum_{i=1}^{\nu} \lambda_i z_i = \sum_{i=1}^{\nu} \mu_i z_i$. Letting $\kappa_i = \lambda_i - \mu_i$, we obtain:

$$\sum_{i=1}^{\nu} \kappa_i z_i = \frac{\sum_{i=1}^{\nu} \kappa_i \left(n^{10} z_i - \lfloor n^{10} z_i \rfloor\right)}{n^{10}},$$

whose norm is less than $\frac{\sum_{k=1}^{\nu} \sqrt{n}}{n^{10}} \leq \frac{1}{n^6}$. □

Lemma 18. *Let $\lambda_1, \ldots, \lambda_\nu$ be integers not all zero. If $y_1, \ldots, y_\nu$ are chosen at random in the parallelepiped $P(w_1, \ldots, w_n)$ then*

$$Pr\left[\left\|\sum_{i=1}^{\nu} \lambda_i y_i\right\| \leq \frac{1}{2n^2}\right] \leq \frac{1}{\rho_n^n}.$$

Proof. Assume that the inequality on the norm is satisfied. Write $\sum_{i=1}^{\nu} \lambda_i y_i$ as $\sum_{j=1}^{n} \alpha_j w_j$. We have:

$$|\alpha_j| \leq \left\|\sum_{i=1}^{\nu} \lambda_i y_i\right\| \frac{n^2}{\rho_n} \leq \frac{1}{2\rho_n}.$$

The probability is therefore bounded by the probability that each α_j is between $-\frac{1}{2\rho_n}$ and $\frac{1}{2\rho_n}$.

Each y_i is of form $\sum_{\ell=1}^{n} \mu_{i,\ell} w_\ell$ where the $\mu_{i,\ell}$'s are independently chosen in $[0, 1[$ with uniform distribution. It follows that:

$$\alpha_j = \sum_{i=1}^{\nu} \lambda_i \mu_{i,j}.$$

If λ_i is non-zero, then $\lambda_i \mu_{i,j}$ modulo 1 is uniformly distributed over $[0, 1[$. Since the λ_i's are not all zero, α_j modulo 1 is therefore uniformly distributed over $[0, 1[$. Furthermore, the α_j's are independent, and the result follows. □

This probabilistic lemma is the core of the following result:

Lemma 19. *Let $\tau = \gamma_1 - \gamma$. If $y_1, \ldots, y_\nu$ are chosen at random in $P(w_1, \ldots, w_n)$ then the probability that there exist $\lambda_1, \ldots, \lambda_\nu$ not all zero such that*

$$\begin{aligned} \left\| \sum_{i=1}^{\nu} \lambda_i y_i \right\| &\leq \sqrt{2}\frac{1}{n^{6-\theta}} && (1) \\ \|(\lambda_1, \ldots, \lambda_\nu)\| &\leq \sqrt{2} n^{1+\gamma/2+\theta} && (2) \\ |\{i : \lambda_i \neq 0\}| &\leq n^{2-\tau} && (3) \end{aligned}$$

is exponentially small (with respect to n).

Proof. The number of non-zero $(\lambda_1, \ldots, \lambda_\nu)$ satisfying (2) and (3) is at most

$$\begin{pmatrix} n^{2+\gamma} \\ n^{2-\tau} \end{pmatrix} (2n^{1+\gamma/2+\theta})^{n^{2-\tau}},$$

which is bounded by $(n^{2+\gamma})^{n^{2-\tau}} (2n^{1+\gamma/2+\gamma})^{n^{2-\tau}}$. Since $\theta < 3$, by lemma 18, each vector has probability less than $\frac{1}{\rho_n^n}$ to satisfy (1), this yields an overall probability less than

$$(n^{2+\gamma})^{n^{2-\tau}} (2n^{1+\gamma/2+\theta})^{n^{2-\tau}} \frac{1}{\rho_n^n}$$

Taking logarithms we get $n^{2-\tau}\left[(2+\gamma)\log n + (1+\gamma/2+\theta)\log n + 1\right] - n^2 \log n$. Since $2-\tau < 2$, the leading term is $-n^2 \log n$ and the result follows. □

Now, consider the output $(z, \lambda_1, \ldots, \lambda_\nu)$ of the oracle. By lemma 17 and by definition of the oracle, $\|z\|^2$ and $\sum_{i=1}^{\nu} \lambda_i^2$ are both less than:

$$n^{2\theta}\left(\beta^2 \frac{1}{n^{12}} + \nu\right) \leq n^{2\theta}\left(n^{2+\gamma} + n^{2+\gamma}\right) = 2n^{2+\gamma+2\theta}.$$

Therefore, $\|\lambda_1 v_{\sigma(1)} + \cdots + \lambda_\nu v_{\sigma(\nu)}\| \leq \sqrt{2} n^{6-\theta}$, and $\|(\lambda_1, \ldots, \lambda_\nu)\| \leq \sqrt{2} n^{1+\gamma/2+\theta}$. This means that (1) and (2) are satisfied if we use the $y_{\sigma(i)}$'s instead of the y_i's. Since the λ_i's are not all zero and $y_1, \ldots, y_\nu$ are ciphertexts of '1', lemma 19 implies that with overwhelming probability, (3) is not satisfied: at least $n^{2-\tau}$ coefficients are non zero. By symmetry, the probability that y_i is hit does not depend on i. Furthermore, (2) implies that the number x of $(\lambda_1, \ldots, \lambda_\nu)$'s such that $|\lambda_i| \geq n^{\gamma/2+\theta+\lambda}$ is such that

$$x n^{\gamma+2\theta+2\lambda} \leq \|(\lambda_1, \ldots, \lambda_\nu)\|^2 \leq 2n^{2+\gamma+2\theta},$$

hence $x \leq 2n^{2-2\lambda}$. If $\lambda > \tau$, this number is negligible with respect to $n^{2-\tau}$. Now, the probability that λ_i is hit is:

$$\Omega\left(\frac{n^{2-\tau}}{n^{2+\gamma}}\right) = \Omega\left(\frac{1}{n^{\gamma+\tau}}\right) = \Omega\left(\frac{1}{n^{\gamma_1}}\right).$$

This concludes the proof.

A.4 Proof of proposition 16

As in the proof of proposition 15, consider the output $(z, \lambda_1, \ldots, \lambda_\nu)$ of the oracle. $\|z\|$ and $\|(\lambda_1, \ldots, \lambda_\nu)\|$ are still less than $\sqrt{2}n^{1+\theta+\gamma/2}$. And:

$$\lambda_{\sigma^{-1}(1)} y_1 = \frac{1}{\beta} z - \sum_{i=2}^{\nu} \lambda_{\sigma^{-1}(i)} y_i.$$

Since $y_2, \ldots, y_\nu$ are good ciphertexts of '0', lemma 14 implies that we have, with probability at least $1 - \varepsilon_2$ (with respect to the choice of $w_1, \ldots, w_n$), for $i \geq 2$:

$$\mathrm{dist}(\mathbf{Z}, < u, y_i >) \leq M_2(k) \frac{1}{n^4 (\varepsilon_1 \varepsilon_2)^{1/2k}}.$$

And therefore, by the Cauchy-Schwarz inequality:

$$\begin{aligned}
\mathrm{dist}\left(\mathbf{Z}, < \sum_{i=2}^{\nu} \lambda_{\sigma^{-1}(i)} y_i, u >\right) &\leq \sqrt{\sum_{i=1}^{\nu} \lambda^2_{\sigma^{-1}(i)}} \times \sqrt{\nu M_2(k)^2 \frac{1}{n^8 (\varepsilon_1 \varepsilon_2)^{1/k}}} \\
&\leq \sqrt{2} n^{1+\theta+\gamma/2} M_2(k) n^{1+\gamma/2-4} \frac{1}{(\varepsilon_1 \varepsilon_2)^{1/2k}} \\
&\leq M_2(k) \frac{\sqrt{2}}{(\varepsilon_1 \varepsilon_2)^{1/2k}} n^{\theta+\gamma-2}.
\end{aligned}$$

Furthermore, $\mathrm{dist}(\mathbf{Z}, < \frac{z}{\beta}, u >) \leq \sqrt{2} \frac{1}{n^{6-\theta}}$. Therefore, for sufficiently large n:

$$\mathrm{dist}(\mathbf{Z}, < \lambda_{\sigma^{-1}(1)} y_1, u >) \leq M_2(k) \frac{\sqrt{3}}{(\varepsilon_1 \varepsilon_2)^{1/2k}} n^{\theta+\gamma-2}.$$

If $\lambda_{\sigma^{-1}(1)}$ is a fixed integer, since y_1 is a random vector in the parallelepiped, the latter inequality is satisfied with probability at most:

$$2M_2(k) \frac{\sqrt{3}}{(\varepsilon_1 \varepsilon_2)^{1/2k}} n^{\theta+\gamma-2}.$$

But if y_1 is hit, then $|\lambda_{\sigma^{-1}(1)}| \in \left\{1, 2, \ldots, n^{\frac{\gamma}{2}+\theta+\lambda}\right\}$. Hence, y_1 is hit with probability at most $2M_2(k) \frac{2\sqrt{3}}{(\varepsilon_1 \varepsilon_2)^{1/2k}} n^{\theta+\gamma-2} 2n^{\gamma/2+\theta+\lambda}$. As n grows, this is:

$$\mathcal{O}\left(n^{2\theta+3\gamma/2+\lambda-2+\frac{1}{2k}(4+\gamma+\gamma_1+\gamma_2+\eta_1+\eta_2)}\right) = \mathcal{O}\left(\frac{1}{n^{\gamma_2}}\right).$$

This concludes the proof.