Polynomial Time Reduction from Approximate Shortest Vector Problem to Principle Ideal Problem for Lattices in Cyclotomic Rings

Hao Chen *

June 28, 2015

Abstract

Many cryptographic schemes have been established based on the hardness of lattice problems. For the asymptotic efficiency, ideal lattices in the ring of cyclotomic integers are suggested to be used in most such schemes. On the other hand in computational algebraic number theory one of the main problem is called principle ideal problem (PIP). Its goal is to find a generators of any principle ideal in the ring of algebraic integers in any number field. In this paper we establish a polynomial time reduction from approximate shortest lattice vector problem for principle ideal lattices to their PIP's in many cyclotomic integer rings. Combining with the polynomial time quantum algorithm for PIP of arbitrary number fields, this implies that some approximate SVP problem for principle ideal lattices within a polynomial factor in some cyclotomic integer rings can be solved by polynomial time quantum algorithm.

1 Introduction

A lattice $\mathbf{L}$ is a discrete subgroup in $\mathbf{R}^n$ generated by several linear independent vectors $\mathbf{b}_1, ..., \mathbf{b}_m$ where $m \leq n$. $\mathbf{L} := \{a_1\mathbf{b}_1 + \cdots + a_m\mathbf{b}_m : a_1 \in \mathbf{Z}, ..., a_m \in \mathbf{Z}\}$. The volume $vol(\mathbf{L})$ of this lattice is $\sqrt{det(\mathbf{B} \cdot \mathbf{B}^\tau)}$, where $\mathbf{B} := (b_{ij})$ is the $m \times n$ generator matrix of this lattice, where

*Hao Chen is with the Department of Mathematics, School of Sciences, Hangzhou Dianzi University, Hangzhou, Zhejiang Province, 310018, China. This research is supported by NSFC Grant 11371138.

$\mathbf{b}_i = (b_{i1}, ..., b_{in}) \in \mathbf{R}^n$ are the base of this lattice. The length of the shortest non-zero lattice vector is denoted by $\lambda_1(\mathbf{L})$. The famous shortest vector problem (SVP) is: given a $\mathbf{Z}$ basis of an arbitrary lattice $\mathbf{L}$ to find a lattice vector with length $\lambda_1(\mathbf{L})$. The approximate SVP is to find some lattice vectors of length within $f(n)\lambda_1(\mathbf{L})$ where $f(n)$ is some approximate factor ([17]). A breakthrough result of M. Ajtai [1] showed that SVP is NP-hard under the randomized reduction. Another breakthrough by Micciancio proved that approximate SVP within some constant factor is NP-hard under the randomized reduction ([17]). For the latest development we refer to Khot [14]. It has been proved that approximate SVP within a quasi-polynomial factor is NP-hard under the randomized reduction.

Because lattice-based cryptography has been very active in recent years, some spacial structured lattices such as ideal lattices have been used for example in Gentry's fully homomorphic encryption scheme [11], collision-resistant hash functions [18] and multi-linear maps [12]. In particular principle ideal lattices in cyclotomic integer rings have been considered suitable for efficient implementation. Lattice based cryptography has been considered suitable for post-quantum cryptography because of the belief that there is no polynomial time quantum algorithm for approximate SVP problem (conjecture 1.2 in [19] and [11, 12, 15, 16, 16, 18, 19, 21, 22]).

Let ξ_n be a primitive n-th root of unit, the n-th cyclotomic polynomial Φ_n is defined as $\prod_{j=1,gcd(j,n)=1}^{n}(x - \xi_n^j)$. This is a monic irreducible polynomial in $\mathbf{Z}[x]$ of degree $\phi(n)$, where ϕ is the Euler function. The n-th cyclotomic field is $Q(\xi_n) = \mathbf{Q}[x]/(\Phi_n(x))$ and the ring of integers in $\mathbf{Q}(\xi_n)$ is exactly $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_n(x))$ (see [8, 23]). For example when $n = 2^k$, the n-th cyclotomic polynomial is $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$. When $n = p$ is an odd prime $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ and when $n = p^k$, $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}}) = (x^{p^{k-1}})^{p-1} + \cdots + x^{p^{k-1}} + 1$. Interestingly there have been many works on the forms of cyclotomic polynomials (see [20, 23]).

Let K be an algebraic number field and $\mathbf{O}_K$ is its ring of integers, it is well-known there is a positive definite inner product on the lattice $\mathbf{O}_K$ defined by $< u, v >= tr_{K/Q}(uv^*)$ where v^* is its complex conjugate (see [8, 15]). If we can find one generator of an ideal $\mathbf{I} \subset \mathbf{O}_K$, $\mathbf{I}$ is called a principle ideal. The following principle ideal problem is a main problem in computational number theory.

Principle Ideal Problem. Given a $\mathbf{Z}$-basis of a principle ideal $\mathbf{I}$, find one generator of this principle ideal.

This problem has been studied by many authors and we refer to [2, 3 , 4, 5, 6, 9, 13] for the latest development. It has been proved that there is a polynomial time quantum algorithm to solve the PIP for all algebraic number fields.

In this paper we will show the following results.

Reduction to PIP. Let p be a prime. For cyclotomic integer rings $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_n(x))$ where $n = p^k$, if a generator of a principle ideal $\mathbf{I} \subset \mathbf{Z}[\xi_n]$ has been found, then we find a lattice vector $\mathbf{v} \in \mathbf{I}$ of length within $(cd^4)^{\frac{d-1}{2d}}\lambda_1(\mathbf{I})$ by using at most d^2 operations in $\mathbf{Z}$. Here $d = \phi(n) = (p-1)p^{k-1}$ is the degree of the extension.

The following proposition is useful in this paper.

Proposition 1.1. *If $\mathbf{x} \in \mathbf{I} \subset \mathbf{Z}[\xi_n]$ is an element of an ideal in the ring of n-th cyclotomic integers. Then $(vol(\mathbf{I}))^{1/d} \leq ||\mathbf{x}||$. Here $d = \phi(n)$ is the degree of the degree of Φ_n. In particular $(vol(\mathbf{I}))^{1/d} \leq \lambda_1(\mathbf{I})$.*

Proof. It is clear $tr_{Q(\xi_n)/Q}(\mathbf{g}\mathbf{g}^*) = tr_{Q(\xi_n)/Q}(\mathbf{g}\xi_n^t\mathbf{g}^*(\xi_n^t)^*) = tr_{Q(\xi_n)/Q}(\mathbf{g}\mathbf{g}^*\xi_n^t(\xi_n^t)^*)$. Thus $\mathbf{g}, \mathbf{g}\xi_n, ..., \mathbf{g}\xi_n^{d-1}$ span a (full-rank) sub-lattice in $\mathbf{I}$ and $\prod_{t=0}^{d-1}||\mathbf{g}\xi^t|| = ||\mathbf{g}||^d \geq vol(\mathbf{I})$. The conclusion follows directly.

2 Reduction

Let $u_1 \leq u_2 \leq \cdots \leq u_s$ be s real numbers, the biggest positive difference of the closest non-equal u_i's is defined as $H_{u_1,...,u_s} = max\{u_2-u_1, ..., u_s-u_{s-1}\}$.

Theorem 2.1. *In a principle ideal $\mathbf{I}$ of the 2^k-th cyclotomic integer ring $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_{2^k}(x))$, if $\mathbf{g} = g_0 + g_1\xi_n + \cdots + g_{2^{k-1}-1}\xi_n^{2^{k-1}-1}$ is a generator of $\mathbf{I}$ satisfying the following condition.*
C) Set H the biggest positive difference of the closest non-equal g_i's and g_{i_0} is the smallest among $g_0, ..., g_{2^{k-1}-1}$. We suppose $-dH \leq g_{i_0} \leq dH$.
Then there exists a positive constant C such that $||\mathbf{g}|| \leq (Cd^3)^{\frac{d-1}{2d}} \cdot (vol(\mathbf{I}))^{1/d} \leq$

$(Cd^3)^{\frac{d-1}{2d}}\lambda_1(\mathbf{I})$ *where* $d = 2^{k-1}$ *is the degree of the extension.*

Proof. First of all in this cyclotomic ring $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_{2^k}(x)) = \mathbf{Z}[x]/(x^{2^{k-1}}+1)$, $1, \xi_n, ..., \xi_n^{2^{k-1}-1}$ is an orthogonal basis, since $tr_{Q(\xi_n)/Q}(\xi_n^t(\xi_n^t)^*) = 2^{k-1}$ and $tr_{Q(\xi_n)/Q}(\xi_n^{t_1}(\xi_n^{t_2})^*) = 0$ for two distinct indices t_1, t_2 in the set $\{0, 1, ..., 2^{k-1}-1\}$. We have a $\mathbf{Z}$-basis $\mathbf{g}, \mathbf{g}\xi_n = -g_{2_1^{k-1}} + g_0\xi_n + g_1\xi_n^2 + \cdots + g_{2^{k-1}-2}\xi_n^{2^{k-1}-1}$,..., $\mathbf{g}\xi_n^{2^{k-1}-1} = -g_1 - g_2\xi_n - \cdots - g_{2^{k-1}-1}\xi_n^{2^{k-1}-2} + g_0\xi_n^{2^{k-1}-1}$ of the ideal lattice $\mathbf{I}$. Without loss of the generality we can assume H can be expressed as $g_{2^{k-1}-1} - g_w$ for an index $w \in \{0, 1, ..., 2^{k-1}-1\}$.

The norms of these vectors are the same $2^{k-1}(g_0^2 + \cdots + g_{2^{k-1}-1}^2)$. For any two different vectors in the basis, their inner product is $< \mathbf{g}\xi_n^{t_1}, \mathbf{g}\xi_n^{t_2} >= 2^{k-1}\Sigma \pm g_i g_{i+t_1-t_2}$. Then the difference $||\mathbf{g}\xi_n^{t_1}|| \cdot ||\mathbf{g}\xi_n^{t_2}|| \pm < \mathbf{g}\xi_n^{t_1}, \mathbf{g}\xi_n^{t_2} >= 2^{k-2}\Sigma(g_i \pm g_{i-t_1+t_2})^2 \geq 2^{k-2}(H)^2$. Actually if not all non-zero $g_0, ..., g_{2_1^{k-1}}$ are equal this is obvious. Therefore $\frac{|<\mathbf{g}\xi_n^{t_1}, \mathbf{g}\xi_n^{t_2}>|}{||\mathbf{g}\xi^{t_1}|| \cdot ||\mathbf{g}\xi^{t_2}||} \leq 1 - \frac{H^2}{g_0^2+\cdots+g_{2^{k-1}-1}^2} \leq 1 - \frac{1}{cd^3}$ from the condition in the Theorem if $H > 0$, since $g_0^2 + \cdots + g_{2^{k-1}-1}^2 \leq g_{i_0}^2 + (g_{i_0} + H)^2 + (g_{i_0} + 2H)^2 + \cdots + (g_{i_0} + (d-1)H)^2 \leq Cd^3H^2$ if $0 < g_{i_0}$ or $g_0^2 + \cdots + g_{2^{k-1}-1}^2 \leq g_{i_0}^2 + (g_{i_0} + h)^2 + (g_{i_0} + 2h)^2 + \cdots + (g_{i_0} + wh)^2 + \cdots + (g_{i_0} + wh + H) + \cdots + (g_{i_0} + wh + (d-1-w)H)^2 \leq C'd^3H^2$ if $g_{i_0} < 0$. Here h is the smallest positive difference of the closest non-equal g_i's, w is the biggest positive integer such that $g_{i_0} + wh < 0$ and C and C' are two universal constants.

If all these non-zero coefficients are equal it is clear $\frac{|<\mathbf{g}\xi_n^{t_1}, \mathbf{g}\xi_n^{t_2}>|}{||\mathbf{g}\xi^{t_1}|| \cdot ||\mathbf{g}\xi^{t_2}||} \leq 1 - \frac{ug^2}{(d'g^2)} \leq 1 - \frac{1}{d}$. Here g is the same non-zero coefficient and u, d' are two positive integers satisfying $0 \leq u \leq d' \leq d$.

Since the volume of the principle ideal lattice $\mathbf{I} = (\mathbf{g})$ can be computed from the Gram matrix $(tr_{Q(\xi_n)/Q}(\mathbf{g}\xi_n^{t_1}(\mathbf{g}\xi_n^{t_2})^*)$. We have $vol(\mathbf{I}))^2 \geq ||\mathbf{g}||^{2^{k-1}+1} \cdot det(G)$, where G is a $d \times d$ matrix with 1 at the diagonal entries and $1 - \frac{1}{cd^3}$ at the non-diagonal entries (from the following Lemma 2.1). Thus $(vol(\mathbf{I}))^2 \geq ||\mathbf{g}||^{2^k} \cdot (\frac{1}{Cd^3})^{d-1}$. The conclusion follows directly.

Lemma 2.1. *Let* $\mathbf{a}_1, ..., \mathbf{a}_n$ *be* n *linear independent vectors in* $\mathbf{R}^N$ *(*$N \geq n$*) with the same Euclid norms. If* $|\frac{<\mathbf{a}_i, \mathbf{a}_j>}{||\mathbf{a}_i|| \cdot ||\mathbf{a}_j||}| \leq cos\theta$ *where* $0 < \theta < \frac{\pi}{4}$*. Then the volume of the lattice spanned by* $\mathbf{a}_1, ..., \mathbf{a}_n$ *is bigger than or equal*

to the volume of the lattice spanned by $\mathbf{b}_1, ..., \mathbf{b}_n$ *satisfying* $||\mathbf{b}_1|| = \cdots = ||\mathbf{b}_n|| = ||\mathbf{a}_j||$ *and* $\frac{<\mathbf{b}_i, \mathbf{b}_j>}{||\mathbf{b}_i|| \cdot ||\mathbf{b}_j||} = cos\theta$.

Proof. If $n = 2$ the conclusion is obvious. We can adjust these vectors $\mathbf{a}_1, ..., \mathbf{a}_{n-1}$ in $\mathbf{R}^{n-1}$ (spanned by these vectors) to decrease the volume. Actually we can adjust $\mathbf{a}_1, ..., \mathbf{a}_{n-1}$ such that their angles are θ and keep the inner products of $< \mathbf{a}_n, \mathbf{a}_1 >$,...,$< \mathbf{a}_n, \mathbf{a}_{n-1} >$ the distance of $\mathbf{a}_n$ to the real subspace spanned by $\mathbf{a}_1, ..., \mathbf{a}_{n-1}$ unchanged. Then the Gram matrix of $\mathbf{a}_1, ..., \mathbf{a}_{n-1}$ is fixed and of the following $\mathbf{M}(\mathbf{1}, \mathbf{cos}\theta)$ form. The conclusion follows from the following fact and the volume decreasing if we only adjust $\mathbf{a}_n$.

We denote the following $s(\mathbf{M}) \times s(\mathbf{M})$ matrix by $\mathbf{M}(\mathbf{1}, \alpha)$. It is not hard to verify that the inverse of $\mathbf{M}(\mathbf{1}, \alpha)$ is of the form $c\mathbf{M}(\mathbf{1}, \beta)$ where $0 < \alpha < 1$, c is a positive constant and $\beta = -\frac{\alpha}{1+(s(\mathbf{M})-2)\alpha}$. From this simple computation the conclusion that adjusting only $\mathbf{a}_n$ will decrease the volume can be proved.

$$\begin{pmatrix} 1 & \alpha & \alpha & \cdots & \alpha \\ \alpha & 1 & \alpha & \cdots & \alpha \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha & \alpha & \alpha & \cdots & 1 \end{pmatrix}$$

Theorem 2.2. *Let* $n = p$ *be an odd prime. In a principle ideal* $\mathbf{I}$ *of the* p*-th cyclotomic integer ring* $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_p(x))$*, if* $\mathbf{g} = g_0 + g_1\xi_n + \cdots + g_{p-2}\xi_n^{p-2}$ *is a generator of* $\mathbf{I}$ *satisfying the following condition.*
C) Set H *the biggest positive difference of the closest non-equal* g_i*'s and* g_{i_0} *is the smallest among* $g_0, ..., g_{p-2}$*. We suppose* $-dH \leq g_{i_0} \leq dH$*.*
Then there exists a positive constant C *such that* $||\mathbf{g}|| \leq (Cd^4)^{\frac{d-1}{2d}} (vol(\mathbf{I}))^{1/d} \leq (Cd^4)^{\frac{d-1}{2d}} \lambda_1(\mathbf{I})$ *where* $d = p - 1$ *is the degree of the extension.*

Proof. It is clear $tr_{Q(\xi_n)/Q}(1) = p - 1$, $tr_{Q(\xi_n)/Q}(\xi_n^t) = -1$ for $t = 1, ..., p - 1$. In this cyclotomic ring $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_p(x)) = \mathbf{Z}[x]/(x^{p-1} + x^{p-2} + \cdots + x + 1)$, $1, \xi_n, ..., \xi_n^{p-2}$ is a $\mathbf{Z}$- basis. We have $tr_{Q(\xi_n)/Q}(\xi_n^t(\xi_n^t)^*) = p - 1$ and $tr_{Q(\xi_n)/Q}(\xi_n^{t_1}(\xi_n^{t_2})^*) = -1$ for two distinct indices t_1, t_2 in the set $\{0, 1, ..., p-2\}$. There is a $\mathbf{Z}$-basis of the ideal lattice $\mathbf{I}$, $\mathbf{g} = g_0 + g_1\xi_n + \cdots + g_{p-2}\xi_n^{p-2}$, $\mathbf{g}\xi_n$,..., $\mathbf{g}\xi_n^{p-2}$. We have $gg^* = g_0^2 + g_1^2 + \cdots + g_{p-2}^2 + \Sigma_{t=1}^{p-1}\xi_n^t(g_tg_0 + \cdots + g_{p-2}g_{p-2-t} + g_{p-1}g_{p-1-t} + g_0g_{p-t} + \cdots + g_{t-2}g_{p-2} + g_{t-1}g_{p-1})$. Here g_{p-1} can be understood as zero. Therefore

$$tr_{Q(\xi_n)/Q}(gg^*) = (p-1)(g_0^2 + \cdots + g_{p-2}^2) -$$
$$\Sigma_{t=1}^{p-1}\xi_n^t(g_tg_0 + \cdots + g_{p-2}g_{p-2-t} + g_{p-1}g_{p-1-t} + g_0g_{p-t} + \cdots + g_{t-2}g_{p-2} + g_{t-1}g_{p-1})$$
$$tr_{Q(\xi_n)/Q}(gg^*\xi_n^{-t}) = -(g_0^2 + \cdots + g_{p-2}^2) +$$
$$(p-1)(g_tg_0 + \cdots + g_{p-2}g_{p-2-t} + g_{p-1}g_{p-1-t} + g_0g_{p-t} + \cdots + g_{t-2}g_{p-2} + g_{t-1}g_{p-1}))$$
$$-\Sigma_{j\neq t, j=1}^{p-1}(g_jg_0 + \cdots + g_{p-2}g_{p-2-j} + g_{p-1}g_{p-1-j} + g_0g_{p-j} + \cdots + g_{j-2}g_{p-2} + g_{j-1}g_{p-1})$$

Then

$$tr_{Q(\xi_n)/Q}(gg^*) - tr_{Q(\xi_n)/Q}(gg^*\xi_n^{-t}) = p[g_{t-1}^2 + g_{p-1-t}^2]$$
$$+p[\tfrac{(g_t-g_0)^2}{2} + \cdots + \tfrac{(g_{p-2}-g_{p-2-t})^2}{2}$$
$$+\tfrac{(g_0-g_{p-t})^2}{2} + \cdots + \tfrac{(g_{p-2}-g_{t-2})^2}{2}]$$

We have $tr_{Q(\xi_n)/Q}(gg^*) - tr_{Q(\xi_n)/Q}(gg^*\xi^{-t}) \geq (p-1)(H)^2$.

On the other hand

$$tr_{Q(\xi_n)/Q}(gg^*) + tr_{Q(\xi_n)/Q}(gg^*\xi^{-t}) =$$
$$\tfrac{p}{2}||\mathbf{g} + Shift_t(\mathbf{g})||^2 - 2(g_0 + \cdots + g_{p-2} + g_{p-1})^2 =$$
$$\tfrac{1}{2}(\Sigma_{i\neq j}(g_i + g_{i+t} - g_j - g_{t+j})^2)$$

where $||a||$ is the ordinary Euclid norm and $\mathbf{g} = (g_0, ..., g_{p-2}, g_{p-1}) \in \mathbf{R}^p$ and $Shift_t(\mathbf{g}) = (g_t, ..., g_{p-1}, g_0, ..., g_{t-1})$ is the shift of the vector $\mathbf{g}$. The last equality comes from the identity $m(a_1^2 + \cdots + a_m^2) - (a_1 + \cdots + a_m)^2 = \Sigma_{i\neq j}(a_i - a_j)^2$.

Then $tr_{Q(\xi_n)/Q}(gg^*) + tr_{Q(\xi_n)/Q}(gg^*\xi^{-t}) \geq \frac{1}{2}(H')^2$. Here H' is a the the biggest positive difference of the closest non-equal $g_i + g_{i-t}$'s.

Since $tr_{Q(\xi_n)/Q}(gg^*) \leq c(p-1)^4(H)^2$ and $tr_{Q(\xi_n)/Q}(gg^*) \leq c(p-1)^4(H')^2$ from the condition in Theorem 2.2, $|\frac{tr_{Q(\xi_n)/Q}(gg^*) - tr_{Q(\xi_n)/Q}(gg^*\xi_n^{-t})}{tr_{Q(\xi_n)/Q}(gg^*)}| \leq 1 - \frac{1}{cd^4}$, where $d = p-1$ is the degree of the extension. The conclusion follows from Lemma 2.1 similarly.

Corollary 2.1. *Let p be an odd prime and k be a positive integer. In a principle ideal $\mathbf{I}$ of the $n = p^k$-th cyclotomic integer ring $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_p(x^{p^{k-1}}))$, if $\mathbf{g} = g_0 + g_1\xi_n + \cdots + g_{p-2}\xi_n^{p^k - p^{k-1} - 1}$ is a generator of*

$\mathbf{I}$ *satisfying the following the condition.*
C). Set H *the biggest positive difference of the closest non-equal* g_i*'s and* g_{i_0} *is the smallest among* $g_0, ..., g_{(p-1)p^{k-1}-1}$*. We suppose* $-dH \leq g_{i_0} \leq dH$*.*
Then there exists a positive constant C *such that* $||\mathbf{g}|| \leq (Cn^4)^{\frac{d-1}{2d}}(vol(\mathbf{I}))^{1/d} \leq (Cd^4)^{\frac{d-1}{2d}}\lambda_1(\mathbf{I})$ *where* $d = p^k - p^{k-1}$ *is the degree of the extension.*

Main Theorem. *If* $n = p^k$ *where* p *a prime for any principle ideal lattice* $\mathbf{I}$ *in the* n*-th cyclotomic integer ring, if a generator of* $\mathbf{I}$ *has been found, then we can can find a generator of* $\mathbf{I}$ *satisfying the condition in Theorem 2.1, 2.2 and Corollary 2.1 with at most* d^2 *operations in the integer ring* $\mathbf{Z}$*. Thus we can find a lattice vector* $\mathbf{v} \in \mathbf{I}$ *satisfying* $||\mathbf{v}|| \leq (Cd^4)^{\frac{d-1}{2d}}\lambda_1(\mathbf{I})$ *with most* d^2 *operations in the integer ring* $\mathbf{Z}$*. Here* $d = \phi(n)$ *is the degree of the extension.*

Proof. If $\mathbf{g} = g_0 + g_1\xi_n + \cdots + g_{d-1}\xi_n^{d-1}$ is a generator of $\mathbf{I}$ and g_{i_0} is the smallest among all coefficients, we have $g_i < 0$ if $g_{i_0} < -dH$. Thus we get a generator of $\mathbf{I}$ satisfying $g_i > 0$ with one operation in $\mathbf{Z}$. From now on we assume that $g_i > 0$ for all $i = 0, ..., d-1$. We can get another generator $\mathbf{g}\xi_n = g_0\xi_n + g_1\xi_n^2 + \cdots + g_{d-2}\xi_n^{d-1} + g_{d-1}\xi_n^d$. If $n = 2^k$, then $\mathbf{g}\xi = -g_{d-1} + g_0\xi_n + \cdots + g_{d-2}\xi_n^{d-1}$. It is obvious that this generator satisfies the condition in Theorem 2.1 since it has both positive and negative coefficients. If $n = p$, we can assume that g_{d-1} is not the biggest among all coefficients (with at most d operations in $\mathbf{Z}$). Then $\mathbf{g}\xi_n = -g_{d-1} + (g_0 - g_{d-1})\xi_n + \cdots + (g_{d-2} - g_{d-1})\xi_n^{d-1}$ has positive and negative coefficients. If $n = p^k$ a similar argument give us the desired generator.

Remark. 1) The above reduction can be extended to principle ideal lattices in other cyclotomic integer rings. We will give the detail in our future paper.

2) The main result in [9] showed that under the condition if there is a "short" generator of a principle ideal lattice $\mathbf{I} \subset \mathbf{Z}[\xi_{p^k}]$, then given any generator of this principle ideal, this "short" generator can be found effectively by the using of BDD. Our result showed that given any generator of a principle in $\mathbf{I} \subset \mathbf{Z}[\xi_{p^k}]$, a generator of length with in $cd^2\lambda_1(\mathbf{I})$ can be found with simple reduction

3) In zeroizing attack to multilinear maps of [6] if the generator is found, our reduction gives the "short" vector needed in the attack in [6]. Thus

combining with the polynomial time quantum algorithm for PIP, [7] and our result it is clear the multilinear maps in [12] is not secure in quantum computing setting.

Acknowledgement. The author is grateful to Phong Q. Nguyen for introducing him to this subject.

3 References

[1] M. Ajtai, The shortest vector problem in L_2 is NP-hard for randomized reduction, STOC 1998, 10-19.

[2] D. Bernstein, A subfield-logarithm attack in against some ideal lattices, http://blog.cr.yp.to/20140213-ideal.html.

[3] J.-F. Biasse and C. Fieker, Sub-exponential class group and uint group computation in large degree number fields, LMS J. Comput. Math., 17 (suppl. A), 385-403, 2014.

[4] J.-F. Biasse, Subexponential time relations in the class group of large degree number fields, Adv. Math. Commun., 8(4), 407-425, 2014.

[5] J.-F. Biasse and F. Song, A polynomial time quantum algorithm for computing class groups an solving the principle ideal problem in arbitrary degree number fields, http:// www.lix.polytechnique.fr/Labo/Jean-Francois.Biasse/.2015.

[6] P. Campbell, M. Grovers and D.Shepherd, Soliloquy: A cautionary tale, http://docbox.etsi.org/2014/201410-Crypto/S07-systems-and-Attacks/S07-Grovers-Annex.pdf.

[7] Jung Hee Cheon and Changmin Lee, cryptanalysis of multilinear map on ideal lattices, iacr e-print.

[8] H.Cohen, A Course in computational algebraic number theory, Graduate Texts in Mathematics 238, Springer-Verlag, 1993.

[9] R. Cramer, L. Ducas, C. Peikert and O.Regev, Recovering short generators of principle ideals in cyclotomic rings, iacr e-print 2015.

[10] K. Eisentrager, S. Hallgren, A. Kutaev and F. Song, A quantum algorithm for computing the unit group of an arbitrary degree number field, 46th ACM STOC, 293-302, 2014.

[11] C. Gentry, Fully homomorphic encryption using ideal lattices, S-TOC 2009, 167-178.

[12] S. Garg, C. Grag and S. Halevi, Candidate multilinear maps from ideal lattices, Eurocrypt 2013, 1-17.

[13] S. Hallgren, Polynomial-time quantum algorithms for Pell's equation and the principle ideal problem, Journal of ACM, vol.54(2005), no.1, 34:1-34:33.

[14] S. Khot, Hardness of approximating the shortest vector problem, Journal of ACM, vol.52 (2005), 789-808.

[15] V. Lyubashevsky and C. Peikert and O. Regev, On ideal lattices and learning with errors over rings, J. ACM, 60(6), 1-43, nov., 2013, preliminary version, Eurocrypt 2010.

[16] A. Langlois, D. Stehle and R. Steinfeld, Gghlite: More efficient multilinear maps from ideal lattices, Eurocrypt 2014, 239-256.

[17] D. Micciancio and S. Goldwasser, Complexity of lattice problems,A cryptographic perspective, Kluwer Academic Publishers.

[18] D. Micciancio, Generalized compact knapsaks, cyclic lattices and efficient one-way functions, Computational Complexity, 16(4), 365-411, 2007.

[19] D. Micciancio and O. Regev, Lattice-based cryptography, Book chapter in Post-quantum Cryptography, D. J. Bernstein and J. Buchmann (eds.), Springer (2008).

[20] A. Migotti, Zur Theorie der Kreisteilungsgleichung, Sitzber. Math. Naturwiss. Classe der Kaiser. Akad. der Wiss. 87(1883) 7-14.

[21] T. Plantard and M. Schneider, Creating a challenge for ideal lattices, iacr e-print.

[22] N. Smart and F. Vercauteren, Fully homomorphic encryption scheme with relatively small key size and ciphertext sizes, PKC 2010.

[23] L. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics 83, Springer-Verlag 1997.