On the tightness of the error bound in Ring-LWE

W. Castryck, I. Iliashenko and F. Vercauteren

Abstract

Since its introduction in 2010 by Lyubashevsky, Peikert and Regev, the Ring Learning With Errors problem (Ring-LWE) has been widely used as a building block for cryptographic primitives, due to its great versatility and its hardness proof consisting of a (quantum) reduction to ideal lattice problems. This reduction assumes a lower bound on the width of the error distribution that is often violated in practice. In this paper we show that caution is needed when doing so, by providing for any $\varepsilon > 0$, a family of number fields K of increasing degree n for which Ring-LWE can be broken easily as soon as the errors required by the reduction are scaled down by $|\Delta_K|^{\varepsilon/n}$ with Δ_K the discriminant of K.

1. *The Ring-LWE problem*

About a decade ago Regev [**18**] proposed a new hard problem for use in public-key cryptography, namely the learning with errors problem (LWE), which informally stated is about solving an approximate linear system

$$A \cdot \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \approx \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

for an unknown secret $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ over $\mathbb{Z}/q\mathbb{Z}$, with q some integer modulus. The entries of A have been selected independently and uniformly at random and the b_i's carry small error terms, obtained by sampling from a fixed Gaussian centered around 0 and reducing the outcome mod q. These errors are elements of $\mathbb{R}/q\mathbb{Z}$, but in practice they are rounded to the nearest element of $\mathbb{Z}/q\mathbb{Z}$. To recover $\mathbf{s}$ uniquely, the system has to be overdetermined, i.e. $m > n$. In fact in Regev's model an attacker is allowed to ask for new equations indefinitely, in the hope of gradually unveiling $\mathbf{s}$: hence the terminology *learning* with errors.

The LWE problem is being acclaimed for three reasons. Firstly it enjoys a 'hardness proof' in the form of a reduction to worst-case instances of certain well-established lattice problems [**2**, **17**, **18**], providing security guarantees that are lacking for classical hard problems such as integer factorization or discrete logarithm computation. Secondly, it seems that LWE would remain hard in a post-quantum world, unlike the classical problems [**19**]. Thirdly, LWE has proven to be very versatile for use in cryptography, enabling applications that were impossible before, such as homomorphic encryption [**1**, **3**]. Its major drawback however is that the key sizes of the resulting cryptosystems are impractically large: typically one needs the entire $(m \times n)$-matrix A.

One idea to address this [**3**, **16**] is to endow $(\mathbb{Z}/q\mathbb{Z})^n$ with a ring structure, for instance by identifying it with $\mathbb{Z}[x]/(q, f)$ for some monic degree n polynomial $f \in \mathbb{Z}[x]$ (using the

---

2000 *Mathematics Subject Classification* 11T71(primary), 11R04, 11R11, 11R18, 11T22(secondary).

This work was supported by the European Commission through the ICT programme under contracts H2020-ICT-2014-1 644209 HEAT and H2020-ICT-2014-1 645622 PQCRYPTO.

polynomial basis $1, x, x^2, \ldots, x^{n-1}$), and to replace A by the matrix $A_{\mathbf{a}}$ of multiplication by some ring element $\mathbf{a}$. This is often referred to as Polynomial-LWE. By storing $\mathbf{a}$ rather than $A_{\mathbf{a}}$ one gains a factor n, thereby addressing the key size issue. But restricting to multiplication matrices comes at the cost of giving up on the randomness, thereby invalidating the mentioned hardness proof, and in fact it is possible to cook up instances of the problem having certain flaws [**11**, **14**].

In [**16**] Lyubashevsky, Peikert and Regev tweaked this idea in a remarkable way by introducing Ring-LWE. To start with, one fixes a degree n number field K with ring of integers $R = \mathcal{O}_K$, and as before one chooses an integral modulus q. The central role is played by the codifferent $R^\vee$ of K, which is defined as the inverse (fractional) ideal of the different ideal $\partial \subset R$. Alternatively it can be viewed as the dual of R with respect to the trace pairing:

$$R^\vee = \{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(xR) \subset \mathbb{Z}\}. \tag{1.1}$$

The reductions of R and $R^\vee$ modulo q are denoted by R_q and $R_q^\vee$, respectively. The Ring-LWE problem is then about guessing a secret $\mathbf{s} \in R_q^\vee$ from an arbitrary number of approximate equations of the form

$$\mathbf{a} \cdot \mathbf{s} \approx \mathbf{b}, \tag{1.2}$$

where $\mathbf{a} \in R_q$ is chosen uniformly at random and $\mathbf{b}$ is known to carry a small error term $\mathbf{e}$ (that is, $\mathbf{b} = \mathbf{a} \cdot \mathbf{s} + \mathbf{e}$) sampled from a distribution that we will discuss in the next paragraph. After agreeing upon a $\mathbb{Z}$-basis of $R^\vee$ this can be rewritten as

$$A_{\mathbf{a}} \cdot \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \approx \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix},$$

where the s_i are the coordinates of $\mathbf{s}$, the b_i are the coordinates of $\mathbf{b}$, and $A_{\mathbf{a}}$ is the matrix of multiplication by $\mathbf{a}$ with respect to the chosen $\mathbb{Z}$-basis, all considered modulo q.

In analogy with LWE and Polynomial-LWE one might want each b_i to carry an error that was sampled independently from the same univariate Gaussian distribution. But that property depends on the chosen basis, and Lyubashevsky et al. opted for a more intrinsic distribution using the canonical embedding

$$\sigma : K \to \mathbb{C}^n : \alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha)),$$

where $\sigma_1, \ldots, \sigma_s$ are the real monomorphisms from K to $\mathbb{R}$ and $\sigma_{s+1}, \ldots, \sigma_{s+2t}$ are the complex monomorphisms from K to $\mathbb{C}$ (so that $n = s + 2t$), ordered such that $\sigma_{s+i} = \tau \circ \sigma_{s+t+i}$ for $i = 1, \ldots, t$, where $\tau : \mathbb{C} \to \mathbb{C} : z \mapsto \overline{z}$ denotes complex conjugation. Thus σ takes values in

$$H = \{\, (z_1, \ldots, z_n) \in \mathbb{C}^n \mid z_1, \ldots, z_s \in \mathbb{R} \text{ and } \overline{z}_{s+i} = z_{s+t+i} \text{ for } i = 1, \ldots, t \,\},$$

which when equipped with the Hermitian inner product $\langle \cdot, \cdot \rangle$ is seen to be isomorphic to the standard inner product space $\mathbb{R}^n$, by considering the basis given by the columns of the unitary matrix

$$B = \begin{pmatrix} I_{s \times s} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} I_{t \times t} & \frac{\mathbf{i}}{\sqrt{2}} I_{t \times t} \\ 0 & \frac{1}{\sqrt{2}} I_{t \times t} & -\frac{\mathbf{i}}{\sqrt{2}} I_{t \times t} \end{pmatrix}.$$

It is well-known that under this identification of H with $\mathbb{R}^n$, the image $\sigma(I)$ of a fractional ideal $I \subset K$ is a lattice of rank n, and that $\sigma(R^\vee)$ is the complex conjugate of the dual lattice

$$\sigma(R)^* := \{\, \alpha \in H \mid \langle \alpha, \sigma(R) \rangle \subset \mathbb{Z} \,\},$$

as is immediate from (1.1); more generally $\sigma(I)^* = \tau(\sigma(I^\vee))$ where $I^\vee = (\partial I)^{-1}$. Now consider a spherical Gaussian on $\mathbb{R}^n$, say with distribution function

$$\Gamma_r^n(\mathbf{x}) = \frac{1}{r^n} \exp\left(-\pi \frac{\|\mathbf{x}\|^2}{r^2}\right),$$

where we note that Γ_r^1 is a univariate Gaussian distribution with mean 0 and standard deviation $r/\sqrt{2\pi}$, and that

$$\Gamma_r^n = \Gamma_r^1 \times \Gamma_r^1 \times \cdots \times \Gamma_r^1.$$

We view Γ_r^n as a distribution on H through the above identification with $\mathbb{R}^n$. Pulling it back along the canonical embedding and wrapping it mod q results in a distribution Ψ_r on the torus

$$(R^\vee \otimes_{\mathbb{Z}} \mathbb{R})/qR^\vee,$$

from which the errors are to be sampled. This distribution lies at the heart of Ring-LWE. As with LWE, in practice one of course rounds the errors to $R^\vee/qR^\vee = R_q^\vee$, but for analytical reasons it is convenient not to do this.

In order to formulate Ring-LWE more formally, let $\mathfrak{U}(R_q)$ and $\mathfrak{U}(R_q^\vee)$ denote the uniform distributions on R_q and $R_q^\vee$, respectively. For $\mathbf{s} \in R_q^\vee$ and $r \in \mathbb{R}_{>0}$ we let $A_{\mathbf{s},r}$ be the distribution over

$$R_q \times (R_q^\vee \otimes_{\mathbb{Z}} \mathbb{R})/qR^\vee$$

obtained by sampling $\mathbf{a} \leftarrow \mathfrak{U}(R_q)$, $\mathbf{e} \leftarrow \Psi_r$ and returning $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + \mathbf{e})$.

Definition 1 (Ring-LWE). For a random but fixed choice of $\mathbf{s} \leftarrow \mathfrak{U}(R_q^\vee)$ the (search) *Ring-LWE* problem is to recover $\mathbf{s}$ with non-negligible probability from arbitrarily many independent samples from $A_{\mathbf{s},r}$.

In their seminal paper [**16**] Lyubashevsky, Peikert and Regev proved the following hardness result on Ring-LWE. For proof-technical reasons, they actually deal with a slight variant called the Ring-LWE$_{\leq r}$ problem. In this problem each sample is taken from $A_{\mathbf{s}(x),\mathbf{r}}$ for a new choice of $\mathbf{r}$ which is chosen uniformly at random from $\{(r_1, \ldots, r_n) \in (\mathbb{R}^+)^n \mid r_i \leq r \text{ for all } i\}$. The distribution $A_{\mathbf{s}(x),\mathbf{r}}$ is defined in exactly the same way as $A_{\mathbf{s}(x),r}$, except that the spherical Gaussian Γ_r^n is to be replaced by the elliptical Gaussian $\Gamma_{r_1}^1 \times \Gamma_{r_2}^1 \times \cdots \times \Gamma_{r_n}^1$. Let ω denote any superlinear function and think of the error width r and the modulus $q \geq 2$ as quantities that vary with n. Then the hardness result [**16**, Theorem 4.1] reads:

Theorem 1.1. *If $r \geq 2\omega(\sqrt{\log n})$ then for some negligible ε (depending on n) there is a probabilistic polynomial-time quantum reduction from* DGS$_\gamma$ *to* Ring-LWE$_{\leq r}$*, where*

$$\gamma : I \mapsto \max\left\{\eta_\varepsilon(I) \cdot (\sqrt{2}q/r) \cdot \omega(\sqrt{\log n}), \sqrt{2n}/\lambda_1(I^\vee)\right\}.$$

Here $\eta_\varepsilon(I)$ is the smoothing parameter of $\sigma(I)$ with threshold ε, and $\lambda_1(I^\vee)$ is the length of a shortest vector of $\sigma(I^\vee)$.

The statement involves the discrete Gaussian sampling problem DGS$_\gamma$, which is about producing samples from a spherical Gaussian in H with parameter r', discretized to the lattice $\sigma(I)$, for any given non-zero ideal $I \subset R$ and any $r' \geq \gamma(I)$. As discussed in [**16**] there are easy reductions from standard lattice problems to the discrete Gaussian sampling problem. As an intermediate step in their proof Lyubashevsky et al. obtain a classical (i.e. non-quantum) reduction from an instance of the bounded distance decoding problem in ideal lattices to Ring-LWE$_{\leq r}$; see [**16**, Lem. 4.5].

REMARK 1. We omit a precise statement of Regev's original hardness result on LWE, which can be found in [**18**], but note for the sake of comparison that it assumes that the errors were sampled from Γ_r^1 with $r > 2\sqrt{n}$. It may seem surprising that the latter bound is more restrictive than its Ring-LWE counterpart $r \geq \omega(\sqrt{\log n})$. However, this is only superficial: the secret space is much 'denser' in this case, and relative to this the Ring-LWE bound is considerably larger. This will be quantified more precisely in the next section.

At a first sight, there are two quite remarkable features about Ring-LWE, namely the 'canonical' error distribution Ψ_r and the 'dual' secret space $R_q^\vee$. We refer to [**16**, §3.3] for a discussion motivating these choices, but note that in the recent literature there has been some temptation to pick the secret from the smaller space R_q instead, for reasons of mathematical convenience. However, it is clear that one cannot expect the direct analogue of Theorem 1.1 to hold in this case. Indeed, because now the lattice $\sigma(R)$ may be very 'sparse' one should scale up the error parameter by a factor related to the covolume of $\sigma(R)$, which is $\sqrt{|\Delta|}$ where $\Delta = \Delta_K$ is the discriminant of K. As we will explain below, from the Ring-LWE point of view the natural choice of scaling factor is $|\Delta|^{1/n}$. For this choice we are unaware of classes of number fields for which the resulting non-dual Ring-LWE problem is easily solved (see [**10**] for a related discussion). But there is also a more aggressive Polynomial-LWE point of view, employed in [**5**, **6**, **12**] for instance, where one only scales up by the square root $|\Delta|^{1/2n}$.

We show that the latter choice may be problematic and that it may even be insufficient to scale up by $|\Delta|^{(1-\varepsilon)/n}$ for whatever fixed choice of $\varepsilon > 0$. In fact more interestingly, this observation also applies to the actual (i.e., dual) Ring-LWE problem: one cannot scale down the error parameter r in the statement of Theorem 1.1 by $|\Delta|^{\varepsilon/n}$ without invalidating it. Thus from a discriminant point of view the bound $r \geq 2\omega(\sqrt{\log n})$ is optimal, which is our main result in this article. A more precise formulation is as follows.

THEOREM 1.2. *Let $\rho : \mathbb{N} \to \mathbb{R}_{>0}$ be in* poly(n)*, let $(q_n)_{n\in\mathbb{N}}$ be any sequence of integer moduli, and let $\varepsilon \in \mathbb{R}_{>0}$ be fixed. Then there exists a family of number fields $(K_\ell)_{\ell\in\mathbb{N}}$ such that the following properties are satisfied:*

- *Each K_ℓ is Galois over $\mathbb{Q}$.*
- *The degree $n_\ell := [K_\ell : \mathbb{Q}]$ tends to infinity as ℓ does.*
- *The Ring-LWE problem in K_ℓ using error parameter $r = \rho(n_\ell)/|\Delta_{K_\ell}|^{\varepsilon/n_\ell}$ and modulus q_{n_ℓ} can be solved in time* poly$(n_\ell \cdot \log q_{n_\ell})$ *using $O(n_\ell)$ samples.*

Moreover, the same statement is true for non-dual Ring-LWE, upon replacement of the error parameter $r = \rho(n_\ell)/|\Delta_{K_\ell}|^{\varepsilon/n_\ell}$ by $r = \rho(n_\ell) \cdot |\Delta_{K_\ell}|^{(1-\varepsilon)/n_\ell}$.

The fields K_ℓ are constructed in such a way that the canonical embedding is extremely skew, which together with the fact that the errors were scaled down leads to certain linear equations in the secret $\mathbf{s}$ that carry negligible errors. Thus by rounding one obtains *exact* linear equations, and the secret can be recovered using elementary linear algebra over $\mathbb{Z}/q_{n_\ell}\mathbb{Z}$. This was also the observation behind [**4**], where in response to [**12**] we analyzed number fields defined by polynomials of the form $x^n + ax + b$. But the treatment given there was ad hoc, devoted to three concrete instantiations, and, moreover, number fields of the form $\mathbb{Q}[x]/(x^n + ax + b)$ are usually not Galois, which makes them less attractive (or at least less understood) from the Ring-LWE point of view. For instance it is known that in the Galois case the search version of Ring-LWE, as stated in Definition 1, is essentially equivalent to its decision version (which we did not state here); see [**5**, **11**, **16**].

2. *Dual versus non-dual Ring-LWE*

To allow for a comparison between dual and non-dual Ring-LWE we restrict our discussion to number fields K for which the different ideal ∂ is principal, say generated by $\theta \in R$, so that $R^\vee = R/\theta$. For instance this holds if K is monogenic, meaning that the ring of integers R is of the form $\mathbb{Z}[x]/(f)$, in which case one can take $\theta = f'(x)$. More generally ∂ is principal if and only if R is a so-called complete intersection, i.e. of the form $\mathbb{Z}[x_1, x_2, \ldots, x_n]/(f_1, f_2, \ldots, f_n)$, in which case one can take $\theta = |(\partial f_i/\partial x_j)_{i,j}|$; see [**9**].

Without loss of generality we can rewrite our sample (1.2) as

$$\mathbf{a} \cdot \frac{\mathbf{s}}{\theta} \approx \frac{\mathbf{b}}{\theta},$$

where now $\mathbf{s} \in R_q$ and $\mathbf{b}/\theta = \mathbf{a} \cdot \mathbf{s}/\theta + \mathbf{e}$ with $\mathbf{e}$ sampled from Ψ_r. Multiplying by θ then gives $\mathbf{b} = \mathbf{a} \cdot \mathbf{s} + \theta \cdot \mathbf{e}$. This way of rewriting Ring-LWE samples in terms of R also appears in [**7**], where θ is referred to as a tweaking factor. After fixing a $\mathbb{Z}$-basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ of R the foregoing reads

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + A_\theta \cdot M^{-1} \cdot B \cdot \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}, \tag{2.1}$$

where the s_i are the coordinates of $\mathbf{s}$, the b_i are the coordinates of $\mathbf{b}$, $A_{\mathbf{a}}$ is the matrix of multiplication by $\mathbf{a}$, A_θ is the matrix of multiplication by θ, and M is the matrix of the canonical embedding σ, all expressed with respect to the basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ and considered modulo q. The e_i are sampled independently from the univariate Gaussian Γ_r^1. Note that on average the factor $A_\theta \cdot M^{-1} \cdot B$ causes the errors to expand, because $|\det A_\theta| = \Delta$ and $|\det M| = \sqrt{|\Delta|}$; see [**13**]. Recall that B is unitary, so $|\det B| = 1$.

In the non-dual Ring-LWE version where the secret is taken directly from R, the multiplication-by-θ step is left out. But as we remarked in the previous section, merely removing A_θ leaves us with $M^{-1} \cdot B$ which causes the errors to shrink on average by a factor $\mathrm{covol}(\sigma(R)) = |\det M| = \sqrt{|\Delta|}$. So for a given choice of r, which in view of Theorem 1.1 we prefer to think of as depending on n only, it is straightforward to find number fields K for which several errors become negligible, resulting in exact equations in the secret $\mathbf{s}$ that can be solved using linear algebra: just let K have a huge discriminant. In order to fix this one should scale up the errors. In view of (2.1) the natural choice of scalar would be $|\det A_\theta|^{1/n} = |\Delta|^{1/n}$:

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + |\Delta|^{1/n} \cdot M^{-1} \cdot B \cdot \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}. \tag{2.2}$$

This compensates at least determinant-wise for the removal of A_θ. Equivalently, one can also just sample the errors e_i from $\Gamma_{|\Delta|^{1/n} \cdot r}$. If A_θ happens to be a scalar matrix itself then (2.1) and (2.2) are of course equivalent. For instance this is the case if K is the 2^m-th cyclotomic field for some $m \geq 2$, where one can take $\theta = 2^{m-1} = n$.

Note that switching to another basis of R boils down to multiplying both sides of (2.1) and (2.2) from the left by the same element of $\mathrm{GL}_n(\mathbb{Z})$, and similarly for taking another generator θ of ∂. Thus the resulting equations in $\mathbf{s}$ are equivalent.

Example 1. To illustrate these different flavors of Ring-LWE, we analyze a simple example that will act as one of the building blocks in our main theorem. Let $d \equiv 1 \bmod 4$ be a positive squarefree integer and consider the real quadratic field $K = \mathbb{Q}(\sqrt{d})$. It has discriminant d and

its ring of integers $R = \mathbb{Z}[(1+\sqrt{d})/2]$ admits the integral basis $1, (1+\sqrt{d})/2$. The different ideal ∂ is the principal ideal generated by $\theta = \sqrt{d}$. With respect to this basis one has

$$A_\theta = \begin{pmatrix} -1 & \frac{-1+d}{2} \\ 2 & 1 \end{pmatrix}, \qquad M^{-1} = \frac{1}{\sqrt{d}} \begin{pmatrix} \frac{-1+\sqrt{d}}{2} & \frac{1+\sqrt{d}}{2} \\ 1 & -1 \end{pmatrix}, \qquad B = I_{2\times 2}.$$

So a Ring-LWE sample reads

$$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + A_\theta \cdot M^{-1} \cdot \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + \begin{pmatrix} \frac{-1+\sqrt{d}}{2} & \frac{-1-\sqrt{d}}{2} \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} e_1 \\ e_2 \end{pmatrix},$$

while a non-dual Ring-LWE sample with scaling factor $|\Delta|^{1/n}$ reads

$$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + \sqrt{d} \cdot M^{-1} \cdot \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + \begin{pmatrix} \frac{-1+\sqrt{d}}{2} & \frac{1+\sqrt{d}}{2} \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}.$$

We will refer to this example in the next section. □

Let us also compare with the Polynomial-LWE approach where one considers (2.1) with the *entire* matrix product $A_\theta \cdot M^{-1} \cdot B$ replaced by a scalar. Note that unlike the previous variants, the resulting problem is no longer invariant under basis change. In view of the foregoing discussion the most natural choice of scalar would be $|\det A_\theta \cdot M^{-1}|^{1/n} = |\Delta|^{1/2n}$:

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + \sqrt{|\Delta|}^{1/n} \cdot \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}. \tag{2.3}$$

This appears to be conservative when compared to cryptographic practice, where one often simply *removes* the scalar and lets the errors depend on n only. This may be motivated by the error bound in Regev's original work on LWE [**18**] where there is no number field into play (see Remark 1), and by NTRU where the errors are even taken constant. Taking small errors has some advantages towards the efficiency of the resulting cryptosystems, but the security risks of doing so are not fully understood.

Nevertheless, this could tempt one into making similarly aggressive choices for (dual or non-dual) Ring-LWE. The analogue of removing the scalar in (2.3) would be to scale down the errors in (2.1) and (2.2) by $|\Delta|^{1/2n}$, as is done in [**5**, **6**, **12**]. But as announced in the previous section, we will show that even scaling down by $|\Delta|^{\varepsilon/n}$ for whatever fixed choice of $\varepsilon > 0$ leads to weak instances of (dual and non-dual) Ring-LWE.

Remark 2. We certainly do not claim that *all* number fields become vulnerable after scaling down the errors: the fields K_ℓ that will be constructed in the next section are very special. In particular our findings do not seem to apply to cyclotomic number fields, which are the main candidates for making their way to daily-life cryptography. Furthermore, for the conservative choices of scalars made in (2.2) and (2.3) we are unaware of number fields for which the non-dual Ring-LWE problem resp. the Polynomial-LWE problem is weak, even though these problems are not backed-up by a hardness statement of the kind of Theorem 1.1. It is an interesting open problem to show that the scalars in (2.2) and (2.3) are sufficient to obtain an equivalent hardness result.

3. *Proof of the main theorem*

PROOF OF THEOREM 1.2: Fix an $\ell \geq 2$ and pick prime numbers $p_1, \ldots, p_\ell$ congruent to 1 mod 4 such that

$$m_\ell := p_1 p_2 \cdots p_\ell \geq \frac{1}{\log(\varepsilon/2)} \cdot \log(2\sqrt{n_\ell}\rho(n_\ell)\sqrt{\log n_\ell}). \tag{3.1}$$

For each p_i consider the corresponding quadratic field $K_{\ell,i} = \mathbb{Q}(\sqrt{p_i})$. It has discriminant p_i and ring of integers $R_{\ell,i} = \mathbb{Z}[(1+\sqrt{p_i})/2]$, which we equip with the basis $\alpha_{i,1} = 1$, $\alpha_{i,2} = (1+\sqrt{p_i})/2$. We will analyze Ring-LWE in the field compositum

$$K_\ell = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_\ell}) \cong K_{\ell,1} \otimes_{\mathbb{Q}} K_{\ell,2} \otimes_{\mathbb{Q}} \cdots \otimes_{\mathbb{Q}} K_{\ell,\ell},$$

which is clearly of degree $n_\ell := 2^\ell$. Because the discriminants p_i of $\mathbb{Q}(\sqrt{p_i})$ are mutually coprime this tensor structure carries over to the integral elements [**20**, Thm. 2.6], i.e. the ring R_ℓ of integers in K_ℓ reads

$$R_\ell = \mathbb{Z}[(1+\sqrt{p_1})/2, (1+\sqrt{p_2})/2, \ldots, (1+\sqrt{p_\ell})/2] \cong R_{\ell,1} \otimes_{\mathbb{Z}} R_{\ell,2} \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} R_{\ell,\ell}.$$

Please do not confuse this notation with our previous notation R_q for the reduction of R mod q (in fact the modulus will not play an important role in the proof). Note that R_ℓ is a complete intersection, so the different ideal $\partial_\ell \subset R_\ell$ is generated by $\theta_\ell = \sqrt{p_1}\sqrt{p_2}\cdots\sqrt{p_\ell} = \sqrt{m_\ell}$. Therefore the codifferent reads

$$R_\ell^\vee = \frac{1}{\sqrt{m_\ell}}\mathbb{Z}[(1+\sqrt{p_1})/2, (1+\sqrt{p_2})/2, \ldots, (1+\sqrt{p_\ell})/2] \cong R_{\ell,1}^\vee \otimes_{\mathbb{Z}} R_{\ell,2}^\vee \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} R_{\ell,\ell}^\vee,$$

i.e. it is again naturally compatible with the tensor structure of K_ℓ.

Towards breaking Ring-LWE we assume that the samples are expressed with respect to the product basis

$$\{\alpha_{1,i_1}\alpha_{2,i_2}\cdots\alpha_{\ell,i_\ell}\}_{\iota \in \{1,2\}^\ell}, \tag{3.2}$$

where ι abbreviates $(i_1, i_2, \ldots, i_\ell)$. With respect to this basis a Ring-LWE sample reads:

$$(b_\iota)_\iota^t = \mathbf{A}_{\mathbf{a}} \cdot (s_\iota)_\iota^t + A_{\theta_\ell} \cdot M^{-1} \cdot (e_\iota)_\iota^t. \tag{3.3}$$

Here $A_{\mathbf{a}}$ and A_{θ_ℓ} are the matrices of multiplication by $\mathbf{a}$ resp. $\theta_\ell = \sqrt{m_\ell}$ and M^{-1} is the canonical embedding matrix. The e_ι's are sampled independently from Γ_r^1 with $r = \rho(n_\ell)/|\Delta_K|^{\varepsilon/n_\ell}$, and the whole expression is considered modulo q_{n_ℓ}. Note that $B = I_{n_\ell \times n_\ell}$ can be left out because K_ℓ is totally real.

Because we work with respect to the product basis, the matrix $A_{\theta_\ell} \cdot M^{-1}$ arises as the Kronecker product of the corresponding matrices for the quadratic fields $K_{\ell,i}$, which by Example 1 are given by

$$\begin{pmatrix} \frac{-1+\sqrt{d}}{2} & \frac{-1-\sqrt{d}}{2} \\ 1 & 1 \end{pmatrix}.$$

Note that

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{-1+\sqrt{d}}{2} & \frac{-1-\sqrt{d}}{2} \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \end{pmatrix}, \tag{3.4}$$

so through the Kronecker product we find that

$$\begin{pmatrix} 0 & 0 & \ldots & 1 \end{pmatrix} \cdot A_{\theta_\ell} \cdot M^{-1} = \begin{pmatrix} 1 & 1 & \ldots & 1 \end{pmatrix},$$

where the row vector on the left has 0's everywhere, except at index $\iota = (2, 2, \ldots, 2)$ where it has a 1.

Thus given a Ring-LWE sample (3.3), we can multiply both sides from the left by the row vector $(0\ 0\ \ldots\ 1)$ in order to end up with a single linear equation in the secret $\mathbf{s} = (s_\iota)_\iota$,

perturbed by an error of the form

$$\begin{pmatrix}1 & 1 & \dots & 1\end{pmatrix} \cdot (e_\iota)_\iota^t,$$

which behaves as if it were sampled from a univariate Gaussian $\Gamma^1_{r'}$ with $r' = \sqrt{n_\ell} \cdot r$. Now our primes p_i have been chosen in such a way that this error is most likely negligible. More precisely, our bound (3.1) on m_ℓ implies that

$$r' = \frac{\sqrt{n_\ell} \cdot \rho(n_\ell)}{|\Delta_K|^{\varepsilon/n_\ell}} = \frac{\sqrt{n_\ell} \cdot \rho(n_\ell)}{\sqrt{m_\ell}^{\varepsilon}} \leq \frac{1}{2\sqrt{\log n_\ell}},$$

whose absolute value is less than $1/2$ with overwhelming probability, so a mere rounding results in an *exact* linear equation in the secret. In fact by the lemma below, with very high probability we can successfully repeat this during n_ℓ consecutive rounds, to end up with an exact linear system of n_ℓ equations in the n_ℓ unknowns s_ι. This system is likely to have full rank (if not we can simply query a few more samples), so that the secret can be recovered using standard linear algebra over $\mathbb{Z}/q_{n_\ell}\mathbb{Z}$. This concludes the proof in the case of dual Ring-LWE.

To obtain the analogous result for non-dual Ring-LWE using scaling factor $|\Delta_{K_\ell}|^{(1-\varepsilon)/n_\ell}$, one repeats the foregoing reasoning with $A_{\theta_\ell} \cdot M^{-1}$ replaced by $|\Delta_{K_\ell}|^{1/n} \cdot M^{-1}$. The analogue of (3.4) reads

$$\begin{pmatrix}0 & 1\end{pmatrix} \cdot \begin{pmatrix}\frac{-1+\sqrt{d}}{2} & \frac{1+\sqrt{d}}{2} \\ 1 & -1\end{pmatrix} = \begin{pmatrix}1 & -1\end{pmatrix},$$

leading to

$$\begin{pmatrix}0 & 0 & \dots & 1\end{pmatrix} \cdot |\Delta_{K_\ell}|^{1/n} \cdot M^{-1} = \left((-1)^{\eta(\iota)}\right)_\iota,$$

where $\eta(\iota)$ denotes the number of 2's appearing in $\iota \in \{1,2\}^\ell$. The right-hand side is again a norm $\sqrt{n_\ell}$ vector, which is the main ingredient needed for the rest of the proof to apply. □

LEMMA 3.1. *Let P_n denote the probability that n independent samples from the univariate Gaussian $\Gamma^1_{1/2\sqrt{\log n}}$ are all at most $1/2$ in absolute value. Then $P_n \to 1$ as $n \to \infty$.*

Proof. Write $r = 1/2\sqrt{\log n}$ and let z be sampled from Γ^1_r. Then P_n equals

$$\left(1 - 2P\left(z > \frac{1}{2}\right)\right)^n = \left(1 - \frac{2}{r}\int_{1/2}^{\infty} \exp\left(-\pi\frac{x^2}{r^2}\right)\right)^n \geq \left(1 - \frac{2}{r}\int_{1/2}^{\infty} 2x\exp\left(-\pi\frac{x^2}{r^2}\right)\right)^n$$

so

$$P_n \geq \left(1 - \frac{\exp\left(-\pi\log n\right)}{\pi\sqrt{\log n}}\right)^n,$$

where the right hand side is seen to converge to 1 using l'Hôpital's rule. □

REMARK 3. The fields K_ℓ that were constructed in the above proof are totally real, but this is not essential. Indeed, if we would also allow primes $p_i \equiv 3 \bmod 4$ and instead consider the field

$$K_\ell = \mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*}, \dots, \sqrt{p_\ell^*}),$$

where

$$p_i^* = (-1)^{\frac{p_i-1}{2}} p_i,$$

then the same conclusions would have followed.

4. *A cyclotomic point of view*

The fields K_ℓ constructed in the previous section are abelian, more precisely they are Galois with Galois group

$$\mathrm{Gal}(K_\ell/\mathbb{Q}) \cong C_2 \times C_2 \times \cdots \times C_2,$$

where C_2 denotes the group of order two. So by the Kronecker-Weber theorem it should be a subfield of some cyclotomic field. The following lemma shows that it is a subfield of $K := \mathbb{Q}(\zeta_{m_\ell})$. We identify the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ with $G := (\mathbb{Z}/(m_\ell))^\times$, where $a \in G$ acts on K as $\zeta_{m_\ell} \mapsto \zeta_{m_\ell}^a$.

LEMMA 4.1. *Let G^2 be the subgroup of squares in G. Then K_ℓ is the subfield of K fixed by G^2.*

Proof. Denote the subfield of K fixed by G^2 as K^{G^2}. For each $c \in G/G^2$ consider

$$w_c = \mathrm{Tr}_{K/K^{G^2}}(\zeta_{m_\ell}^c) = \sum_{h \in G^2} \zeta_{m_\ell}^{hc} \ \in \ K^{G^2}.$$

By the Chinese remainder theorem (CRT) we have the isomorphism

$$G \cong \mathbb{F}_{p_1}^\times \times \mathbb{F}_{p_2}^\times \times \cdots \times \mathbb{F}_{p_\ell}^\times,$$

according to which the w_c's can be decomposed as follows:

$$w_c = \sum_{h \in G^2} \zeta_{m_\ell}^{hc} = \sum_{\substack{h_1 \in (\mathbb{F}_{p_1}^\times)^2 \\ \cdots \\ h_\ell \in (\mathbb{F}_{p_\ell}^\times)^2}} \zeta_{p_1}^{h_1 c} \zeta_{p_2}^{h_2 c} \cdots \zeta_{p_\ell}^{h_\ell c} = \prod_{i=1}^{\ell} \sum_{h \in (\mathbb{F}_{p_i}^\times)^2} \zeta_{p_i}^{hc}. \tag{4.1}$$

Every sum in the last product is a so-called Gaussian period, where the exponents run through either the quadratic residues or the quadratic non-residues modulo p_i. As all p_i's are congruent to 1 modulo 4, such sums result in

$$\beta_{i,1} := \frac{-1+\sqrt{p_i}}{2}, \quad \text{resp.} \quad \beta_{i,-1} := \frac{-1-\sqrt{p_i}}{2}$$

(see [**8**]). One sees that $\{w_c\}_c$ is the product basis of K_ℓ obtained by equipping the $R_{\ell,i}$'s with the $\mathbb{Z}$-bases $\beta_{i,1}, \beta_{i,-1}$ rather than $\alpha_{i,1}, \alpha_{i,2}$. In particular the w_c's generate K_ℓ, so $K_\ell \subset K^{G^2}$ and the lemma follows by comparing degrees. □

As a byproduct of the above proof, we obtain that the w_c's form a $\mathbb{Z}$-basis of R_ℓ, which is a special case of a more general statement [**15**, Prop. 6.1]. This kind of 'trace basis' is also used in the recent work on Ring-LWE by Chen, Lauter and Stange [**5**], an example of which we will analyze later in this section. It is interesting to have a quick look at our proof of Theorem 1.2, where now we express the samples with respect to the basis $\{w_c\}_c$, instead of (3.2). Here the factors in the Kronecker product decomposition of $A_{\theta_\ell} \cdot M^{-1}$ read

$$\begin{pmatrix} \frac{-1-p_i}{2} & \frac{-1+p_i}{2} \\ \frac{1-p_i}{2} & \frac{1+p_i}{2} \end{pmatrix} \cdot \frac{1}{\sqrt{p_i}} \begin{pmatrix} \frac{1-\sqrt{p_i}}{2} & \frac{-1-\sqrt{p_i}}{2} \\ \frac{-1-\sqrt{p_i}}{2} & \frac{1-\sqrt{p_i}}{2} \end{pmatrix} = \begin{pmatrix} \frac{1-\sqrt{p_i}}{2} & \frac{1+\sqrt{p_i}}{2} \\ \frac{-1-\sqrt{p_i}}{2} & \frac{-1+\sqrt{p_i}}{2} \end{pmatrix}.$$

One sees that

$$\begin{pmatrix} 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1-\sqrt{p_i}}{2} & \frac{1+\sqrt{p_i}}{2} \\ \frac{-1-\sqrt{p_i}}{2} & \frac{-1+\sqrt{p_i}}{2} \end{pmatrix} = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

So expanding the Kronecker product gives

$$(J(\iota))_\iota \cdot A_{\theta_\ell} \cdot M^{-1} = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}, \tag{4.2}$$

where ι runs over all tuples $(i_1, i_2, \dots, i_\ell) \in \{1, -1\}^\ell$ and

$$J(\iota) = J(i_1, i_2, \dots, i_\ell) = \prod_{j=1}^{\ell} i_j$$

(this formula explains why we indexed the β_i's by ± 1 rather than $1, 2$). The row vector $(1\ 1\ \dots\ 1)$ on the right-hand side of (4.2) has norm $\sqrt{n_\ell}$, so as before this can be used to obtain linear equations in the coordinates of the secret $\mathbf{s}$ that carry negligible error terms, allowing one to recover $\mathbf{s}$ by means of simple linear algebra.

Remark 4. As before, the same claims apply to non-dual Ring-LWE and/or to the setting where we allow primes $p_i \equiv 3 \bmod 4$, upon replacement of every appearance of $\sqrt{p_i}$ by $\sqrt{p_i^*}$.

Remark 5. The letter J refers to the Jacobi-symbol. Indeed, through the CRT we have

$$G/G^2 \cong \frac{\mathbb{F}_{p_1}^\times}{(\mathbb{F}_{p_1}^\times)^2} \times \frac{\mathbb{F}_{p_2}^\times}{(\mathbb{F}_{p_2}^\times)^2} \times \dots \times \frac{\mathbb{F}_{p_\ell}^\times}{(\mathbb{F}_{p_\ell}^\times)^2} = \{\pm 1\} \times \{\pm 1\} \times \dots \times \{\pm 1\},$$

where if $c \in G/G^2$ corresponds to $\iota = (i_1, i_2, \dots, i_\ell) \in \{1, -1\}^\ell$, then $w_c = \beta_{1,i_1}\beta_{2,i_2}\cdots\beta_{\ell,i_\ell}$ and $J(\iota) = (c/m_\ell)$. Thus if we prefer to think of the rows and columns of the matrices A_θ and M as being indexed by $c \in G/G^2$ rather than $\iota \in \{1, -1\}^\ell$, then (4.2) becomes

$$\left(\left(\tfrac{c}{m_\ell}\right)\right)_c \cdot A_{\theta_\ell} \cdot M^{-1} = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix},$$

an identity which we found remarkable at first sight.

To conclude this article, we note that more generally, the presence of factors of the form $\mathbb{Z}[(1+\sqrt{d})/2]$ for some $d \equiv 1 \bmod 4$ may lead to unexpectedly short linear combinations of the rows of $A_\theta \cdot M^{-1}$, and thus to weaker instances of Ring-LWE than one might hope (for an aggressive choice of scaling factor).

For instance, let us analyze the first example listed in [**5**, §5.1]; the other examples admit a similar analysis. Here Chen et al. let $m = 2805 = 3 \cdot 5 \cdot 11 \cdot 17$ and they consider the fixed field $K^{G'}$ of $K = \mathbb{Q}(\zeta_m)$ under the action of

$$G' := \langle 1684, 1618 \rangle \subset G = \mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/(m))^\times.$$

Under the CRT decomposition $(\mathbb{Z}/(m))^\times \cong \mathbb{F}_3^\times \times \mathbb{F}_{11}^\times \times (\mathbb{Z}/(85))^\times$ this subgroup corresponds to $\{1\} \times \{1\} \times G'_{85}$ where G'_{85} denotes the index two subgroup of elements having Jacobi symbol 1. We again work with respect to the trace basis

$$w_c = \sum_{h \in G'} \zeta_m^{hc} = \zeta_3^c \cdot \zeta_{11}^c \cdot \sum_{h \in G'_{85}} \zeta_{85}^{hc},$$

where $c \in G/G'$. The latter sum equals $\beta_1 := (1+\sqrt{85})/2$ or $\beta_{-1} := (1-\sqrt{85})/2$ depending on whether $\left(\frac{c}{85}\right) = 1$ or not. So we conclude similarly as before that the ring of integers equals

$$R := \mathcal{O}_{K^{G'}} = \mathbb{Z}[\zeta_3, \zeta_{11}, (1+\sqrt{85})/2] \cong \mathbb{Z}[\zeta_3] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{11}] \otimes_{\mathbb{Z}} \mathbb{Z}[(1+\sqrt{85})/2]$$

and that $\{w_c\}_c$ is the product basis

$$\{\zeta_3^i \zeta_{11}^j \beta_k\}_{\substack{i=1,2 \\ j=1,2,\dots,10 \\ k=1,-1}}.$$

As in [**5**], let us have a look at non-dual Ring-LWE with scaling factor $|\Delta|^{1/2n}$, where $\Delta = \Delta_{K^{G'}} = (-3) \cdot (-11^9) \cdot 85$ and $n = [K^{G'} : \mathbb{Q}] = 40$. Let M denote the matrix of the canonical embedding of $K^{G'}$ with respect to the above basis. Then the last Kronecker factor of $|\Delta|^{1/2n} \cdot M^{-1} = |\Delta|^{1/80} \cdot M^{-1}$ is given by

$$\frac{1}{\sqrt[4]{85}} \cdot \begin{pmatrix} \frac{1+\sqrt{85}}{2} & \frac{-1+\sqrt{85}}{2} \\ \frac{-1+\sqrt{85}}{2} & \frac{1+\sqrt{85}}{2} \end{pmatrix}.$$

So multiplying from the left by $(1 \ -1)$ leads to the row vector $(1 \ 1)/\sqrt[4]{85}$ of norm ≈ 0.4658, which is 'unexpectedly short'. The other Kronecker factors correspond to cyclotomic fields and have less surprising behavior. Here taking the first row (for instance) of each factor leads to norms $\sqrt{2}/\sqrt[4]{3} \approx 1.0746$ and $\sqrt{10}/\sqrt[20]{11^9} \approx 1.0750$, respectively. Thus multiplying $|\Delta|^{1/80} \cdot M^{-1}$ from the left by

$$(1, 0) \otimes (1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \otimes (1, -1)$$

yields a row vector of norm $\approx 1.0746 \cdot 1.0750 \cdot 0.4658 \approx 0.5381$. Since Chen et al. let $r = 1$, this results in a linear equation in the secret $\mathbf{s}$ carrying an error term sampled from $\Gamma^1_{0.5381}$, roughly. By taking other rows of the cyclotomic parts one in fact finds 20 independent such equations. This is insufficient to break this concrete instance of non-dual Ring-LWE using mere rounding (a substantial number of equations will carry an error that exceeds $1/2$ in absolute value), but it is tight, so it provides an explanation why this was indirectly helpful for Chen et al. to successfully apply their χ^2-analysis.

5. *Conclusion*

In this paper we have shown, by explicitly constructing a family of counterexamples, that the lower bound on the noise in the hardness result for Ring-LWE by Lyubashevsky, Peikert and Regev [**16**] is tight in a very natural sense: scaling down the noise even by a factor $|\Delta_K|^{\varepsilon/n}$, for any ε, invalidates the hardness result. Our proof also implies that one cannot simply use non-dual Ring-LWE without scaling up the noise by a factor that depends explicitly on Δ_K, which is often violated in practice. Our results can also be seen as further evidence that the original construction using the dual $R^\vee$ really is the most natural. Finally, we note that our counterexamples implicitly exploit the structure of the Galois group, which raises the question to what extent the structure of the Galois group can be exploited further in the analysis of the hardness of Ring-LWE.

References

1. J. Bos, K. Lauter, J. Loftus, M. Naehrig, 'Improved security for a ring-based fully homomorphic encryption scheme', 14*th IMA Conference on Cryptography and Coding* (2013)

2. Z. Brakerski, A. Langlois, C. Peikert, O. Regev and D. Stehlé, 'Classical hardness of learning with errors', *ACM Symposium on the Theory of Computing – STOC '13*, pp. 575-584 (2013)

3. Z. Brakerski, V. Vaikunthanathan, 'Fully homomorphic encryption from Ring-LWE and security for key dependent messages', *Advances in Cryptology – CRYPTO '11*, Lecture Notes in Computer Science 6841, pp. 505-524 (2011)

4. W. Castryck, I. Iliashenko, F. Vercauteren, 'Provably weak instances of Ring-LWE revisited', to appear in *EUROCRYPT '16*, Lecture Notes in Computer Science (2016)

5. H. Chen, K. Lauter, K. Stange, 'Attacks on search RLWE', Cryptology ePrint Archive 2015/971 (2015)

6. H. Chen, K. Lauter, K. Stange, 'Vulnerable Galois RLWE families and improved attacks', Cryptology ePrint Archive 2016/193 (2016)

7. E. Crockett, C. Peikert, 'Λ ∘ λ: A functional library for lattice cryptography', Cryptology ePrint Archive 2015/1134 (2015)

8. H. Davenport, *Multiplicative number theory*, 2nd edition (revised by H. Montgomery), Graduate Texts in Mathematics 74 (Springer, 2000)

9. B. de Smit, 'A differential criterion for complete intersections', *Journées Arithmétiques* 1995, Collectanea Mathematica 48 (1-2), pp. 85-96 (1997)

10. L. Ducas, A. Durmus, 'Ring-LWE in polynomial rings', *Public Key Cryptography – PKC '12*, Lecture Notes in Computer Science 7293, pp. 34-51 (2012)

11. K. Eisenträger, S. Hallgren, K. Lauter, 'Weak instances of PLWE', *Selected Areas in Cryptography – SAC 2014*, Lecture Notes in Computer Science 8781, pp. 183-194 (2014)

12. Y. Elias, K. Lauter, E. Ozman, K. Stange, 'Provably weak instances of Ring-LWE', *Advances in Cryptology – CRYPTO '15*, Lecture Notes in Computer Science 9215, pp. 63-92 (2015)

13. A. Fröhlich, M. Taylor, *Algebraic number theory*, Cambridge Studies in Advances Mathematics 27, (Cambridge University Press, 1991)

14. C. Gentry, 'Key recovery and message attacks on NTRU-Composite', *EUROCRYPT '01*, Lecture Notes in Computer Science 2045, pp. 182-194 (2001)

15. H. Johnston, 'Notes on Galois modules', Notes accompanying the course 'Galois Modules' given in Cambridge (2011)

16. V. Lyubashevsky, C. Peikert, O. Regev, 'On ideal lattices and learning with errors over rings', *Journal of the ACM* 60(6), article 43, 35 pp. (2013)

17. C. Peikert, 'Public-key cryptosystems from the worst-case shortest vector problem', *ACM Symposium on the Theory of Computing – STOC '09*, pp. 333-342 (2009)

18. O. Regev, 'On lattices, learning with errors, random linear codes, and cryptography', *Journal of the ACM* 56(6), article 34, 40 pp. (2009)

19. P. Shor, 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer', *SIAM Journal of Computing* 26(5), pp. 1484-1509 (1997)

20. L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics 83 (Springer, 1982)

Wouter Castryck
KU Leuven ESAT/COSIC and iMinds
Kasteelpark Arenberg 10
B-3001 Leuven-Heverlee
Belgium

Vakgroep Wiskunde, Universiteit Gent
Krijgslaan 281/S22, B-9000 Gent
Belgium

wouter.castryck@esat.kuleuven.be

Frederik Vercauteren
KU Leuven ESAT/COSIC and iMinds
Kasteelpark Arenberg 10
B-3001 Leuven-Heverlee
Belgium

Open Security Research
Fangda 704, 11 Kejinan 12th road
518000 Shenzhen
China

frederik.vercauteren@esat.kuleuven.be

Ilia Iliashenko
KU Leuven ESAT/COSIC and iMinds
Kasteelpark Arenberg 10
B-3001 Leuven-Heverlee
Belgium

ilia.iliashenko@esat.kuleuven.be