On the Security of the Multivariate Ring Learning with Errors Problem

Carl Bootland, Wouter Castryck, Frederik Vercauteren

imec-COSIC, ESAT, KU Leuven
Kasteelpark Arenberg 10
3001 Heverlee, Belgium
carl.bootland@kuleuven.be, wouter.castryck@kuleuven.be,
frederik.vercauteren@kuleuven.be

Abstract. The Multivariate Ring Learning with Errors (m-RLWE) problem was introduced in 2015 by Pedrouzo-Ulloa, Troncoso-Pastoriza and Pérez-González. Instead of working over a polynomial residue ring with one variable as in RLWE, it works over a polynomial residue ring in several variables. However, care must be taken when choosing the multivariate rings for use in cryptographic applications as they can be either weak or simply equivalent to univariate RLWE. For example, Pedrouzo-Ulloa et al. suggest using tensor products of cyclotomic rings, in particular power-of-two cyclotomic rings. They claim incorrectly that the security increases with the product of the individual degrees. In this paper, we present simple methods to solve the search m-RLWE problem far more efficiently than is stated in the current literature by reducing the problem to the RLWE problem in dimension equal to the maximal degree of its components (and not the product) and where the noise increases with the square-root of the degree of the other components. Our methods utilise the fact that the defining cyclotomic polynomials share algebraically related roots. We use these methods to successfully attack the search variant of the m-RLWE problem for a set of parameters estimated to offer more than 2600 bits of security, and being equivalent to solving the bounded distance decoding problem in a highly structured lattice of dimension 16384, in less than two weeks of computation time or just a few hours if parallelized on 128 cores. Finally, we also show that optimizing module-LWE cryptosystems by introducing an extra ring structure as is common practice to optimize LWE, often results in a total breakdown of security.

1 Introduction

In 2010, Lyubashevsky, Peikert and Regev introduced the Ring Learning with Errors (RLWE) problem [12]. The main advantage of using this ring-variant of the original LWE problem is that the schemes are much more efficient and the size of the public keys is significantly smaller. Beginning in 2015, Pedrouzo-Ulloa, Troncoso-Pastoriza and Pérez-González introduced the Multivariate Ring Learning with Errors (m-RLWE) problem in a series of papers [14,15,16]. Essentially

this does to module-LWE what RLWE does to LWE – by adding more structure they are able to construct more efficient schemes with smaller key sizes.

In the simplest case of two variables they define the problem, which they call the Bivariate RLWE (2-RLWE) problem, as follows:

Problem 1. Let $R_q[x,y] = \mathbb{Z}_q[x,y]/(f(x),g(y))$ be a bivariate polynomial residue ring, with f,g monic irreducible polynomials over $\mathbb{Z}$ and an error distribution $\chi[x,y] \in R_q[x,y]$ that generates small-norm random bivariate polynomials in $R_q[x,y]$, distinguish between samples $(a_i, b_i = a_i \cdot s + e_i)$ and (a_i, u_i) where $a_i, u_i \leftarrow R_q[x,y]$ are chosen uniformly at random from the ring $R_q[x,y]$, and $s, e_i \leftarrow \chi[x,y]$ are drawn from the error distribution.

Although not explicitly stated in [14], f and g are taken to be two-power cyclotomics, i.e. $f(x) = x^{n_x} + 1$ and $g(y) = y^{n_y} + 1$ with n_x and n_y powers of two. They claim and give a sketch proof that the 2-RLWE problem above is equivalent to the RLWE problem in the ring $\mathbb{Z}_q[z]/(h(z))$ where $h(z) = z^{n_1 n_2} + 1$, however as will become obvious this is not true as we can solve the 2-RLWE far more easily. The flaw is that while $\mathbb{Q}[z]/(h(z))$ certainly contains isomorphic copies of $\mathbb{Q}[x]/(f(x))$ and $\mathbb{Q}[x]/(g(y))$ it is not the smallest number field which does so. If we assume $n_1 \geq n_2$ then in this specific case $\mathbb{Q}[x]/(f(x))$ itself has this property. This shows that we expect to be able to solve the 2-RLWE problem by solving $\max\{n_1, n_2\}$ dimensional problems, not dimension $n_1 n_2$. This logic can be made to work more generally with any cyclotomic fields, not just power of two cyclotomics, as detailed in Section 3.1.

The authors then construct a method for encrypted image processing whose security is based on the 2-RLWE problem. The sample parameters proposed for use being $n_1 = n_2 = 2^i$, $\lceil \log_2 q \rceil = 22 + 3i$ for $i = 7, 8, 9, 10$. Using the lower bound given in [11, Equation (5.2)] these instances are estimated to have bit security 2663, 10288, 38880 and 146675 respectively, though these parameters fall well outside the range of parameters for which the bound was derived so these security levels so are unlikely to be accurate; however, using the LWE-estimator of Albrecht et al. [1] gives even larger security estimates. Thus it is clear the authors believe these parameter suggestions give a very high security level. However, in light of our attack, which works here in dimension $n_1 = n_2$, the LWE-estimator gives the estimated security levels as 32, 33, 35 and 98 bits respectively.

Further, in [15] the same authors reformulate the m-RLWE problem in terms of the tensor product of number fields and consider the ring R now as the tensor product of the corresponding rings of integers. They proceed by generalising the security reductions of Lyubashevsky et al. from RLWE to standard problems on ideal lattices to the multivariate case, now reducing them to multivariate ideal lattice problems.

Finally, in [16] the same authors build upon the m-RLWE problem, this time specialised to power-of-two cyclotomics, and give a number of useful multi-dimensional signal processing operations and optimizations for use with their m-RLWE based homomorphic encryption scheme.

Although Pedrouzo-Ulloa et al. appear to have come up with the m-RLWE problem to deal with multidimensional signals the problem is natural in its own right. As mentioned above it is a rather natural optimization of module LWE (M-LWE), first introduced in [4] where it is called the General Learning with Errors (GLWE) problem. This module structure is used in cryptographic primitives such as the NIST submissions Saber [6] and Kyber[3]. For a ring R, samples from the module LWE distribution are of the form $(\mathbf{a}, b)$ where $\mathbf{a} \leftarrow R_q^n$ is uniformly sampled and $b = \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q$ where $e \leftarrow \chi$ is sampled from an error distribution and $\mathbf{s} \in R_q^n$ is the secret vector. LWE is the case when $R = \mathbb{Z}$ and RLWE is when $n = 1$ but now the ring R is a polynomial residue ring. Thus in going from LWE to RLWE we replace the inner product of vectors by the product of polynomials (modulo some polynomial modulus).

As such Module LWE bridges the gap between LWE and RLWE, but is still not as efficient as RLWE. It is thus tempting to replace the inner product in M-LWE by a product of polynomials, just like RLWE, but where now the coefficients are from a polynomial residue ring (in an independent variable) rather than simply integers. We thus reach the 2-RLWE problem and it is then straightforward to generalise to m-RLWE.

In this paper we give a simple assessment of the security of the m-RLWE problem and present an efficient attack when the polynomial moduli are related in a certain way. The basic idea of the attack is to apply a number of "smallness" preserving ring homomorphisms which reduce the problem to standard RLWE problems, of much lower dimension, and with a slightly larger error distribution. Solving the search variant in each case gives us enough information to recover the secret in the original m-RLWE problem. For example, for the 2-RLWE problem above with $n_1 \geq n_2$ the problem is reduced to n_2 instances of the RLWE problem in dimension n_1, the same modulus q and with the noise growing only by a factor of $\sqrt{n_2}$. This attack shows that the stated hardness of the problem is much lower than that asserted in the current literature coming from RLWE in dimension $n_1 n_2$.

The remainder of the paper is organised as follows: in Section 2 we recall the required background and in Section 3 we define the m-RLWE problem and show that in many cases it simply is the standard RLWE-problem. In Section 4 we present our attack on the remaining cases of m-RLWE and the results of our implementation, and in Section 5 we remark that the standard optimization trick going from LWE to RLWE, when applied to module-LWE often results in a total breakdown of security. Finally, Section 6 concludes the paper.

2 Preliminaries

Let $[n]$ denote the set $\{0, 1, 2, \ldots, n-1\}$. For a commutative ring R and an element $r \in R$ we denote by (r) the principal ideal of R generated by r; namely $(r) = \{rs \mid s \in R\}$.

2.1 Subgaussians

We also require the notion of a subgaussian random variable. We follow the approach in [13, Section 2.3] and say that, for any $\delta \geq 0$, a random variable X over $\mathbb{R}$ is δ-subgaussian with parameter $s > 0$ if for all $t \in \mathbb{R}$ we have

$$\mathbb{E}(e^{2\pi tX}) \leq e^{\pi s^2 t^2 + \delta}.$$

If $\delta = 0$ then we drop the refernce to this and say that the random variable X is subgaussian with parameter s. We also use the same notation for the probability distribution of X. It is a simple exercise to show that the sum of subgaussian distributions is also subgaussian:

Lemma 1. *Let $\delta_i, s_i \geq 0$ and suppose that we have random variables X_i which are δ_i-subgaussian with parameter s_i. Define X to be random variable that is the sum of the X_i and set $\delta = \sum_i \delta_i$ and $s = \left(\sum_i s_i^2\right)^{1/2}$ then X is δ-subgaussian with parameter s.*

We can also apply Markov's inequality to the δ-subgaussian random variable X with parameter s which shows that

$$\Pr(|X| \geq t) \leq 2e^{-\pi t^2/s^2 + \delta}.$$

2.2 RLWE variants

Here we also introduce the distinction between the so-called dual- and primal-RLWE problems as well as the polynomial RLWE problem. The starting point for the first two problems is a number field K and its ring of integers $\mathcal{O}_K$ and an integer modulus $q \geq 2$. Typically K is a cyclotomic number field but this need not be the case. Samples are of the form (a_i, b_i) where $b_i = a_i s + e_i$ and $a_i \in \mathcal{O}_K/q\mathcal{O}_K$ is sampled uniformly at random and e_i is sampled from an error distribution on $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$. The difference between the two cases is that in the dual-RLWE case the secret s is sampled from the dual fractional ideal $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$ while in the primal-RLWE case it is sampled from $\mathcal{O}_K/q\mathcal{O}_K$. Finally, in the PLWE case $a_i, s \in \mathbb{Z}_q[x]/(f)$ for some irreducible polynomial f and the error term is an element of $\mathbb{R}[x]/(f)$.

The actual problems come in two variants, a decision version where one has to determine whether the second component of the samples is computed correctly or chosen randomly as in Problem 1, and a search version where one is asked to find s.

It has been shown by Ducas and Durmas [7] for cyclotomic fields, and by Rosca, Stehlé, and Wallet [17] more generally, that one can reduce dual-RLWE to primal-RLWE with only a limited growth in the error term. Also in [17] they show that the reduction can be extended from primal-RLWE to PLWE. Since cyclotomic number fields are monogenic, that is the ring of integers is generated by one element over $\mathbb{Z}$, and we are primarily interested in the cyclotomic case, for simplicity, we will not worry too much about distinguishing the various problems.

2.3 Search RLWE as a BDD problem

In this section we recall a simple and well-known lattice attack on the search variant of the RLWE problem by considering it as a special case of the bounded distance decoding problem (BDD). The attack works given enough samples and is practical for low dimensional problems.

Suppose we are given ℓ samples $\{(a_i, b_i)\}_{i\in[\ell]}$ from the $\mathrm{RLWE}_{q,\Psi}$ distribution and suppose we are working in the ring $R = \mathbb{Z}_q[x]/(f(x))$, $\deg(f) = n$. Then we know that if s is the secret polynomial we have $b_i = sa_i + e_i$ for some e_i with small coefficients. We can rewrite this as a vector-matrix equation by replacing the elements of R by their (row) vector of coefficients (with respect to the standard power basis in x) which we denote in bold; if M_{a_i} is the matrix of multiplication by a_i then we have $\mathbf{b}_i = \mathbf{s}M_{a_i} + \mathbf{e}_i$. Since s is the same for each sample we can concatenate all of the samples into one equation:

$$\left(\mathbf{b}_1 \cdots \mathbf{b}_\ell\right) = \mathbf{s}\left(M_{a_1} \cdots M_{a_\ell}\right) + \left(\mathbf{e}_1 \cdots \mathbf{e}_\ell\right).$$

This is an instance of the bounded distance decoding (BDD) problem in the q-ary lattice $\mathcal{L}$ spanned by the rows of $(M_{a_1} \cdots M_{a_\ell})$ (with entries taken as integers) and $qI_{n\ell}$; the target vector being $\mathbf{v} = (\mathbf{b}_1 \cdots \mathbf{b}_\ell)$. Any BDD-solver, such as Kannan's embedding technique [10] or Babai's nearest plane algorithm [2], can thus be used to solve search RLWE. Two samples will in practice uniquely define s and the more samples one has the better the chance of solving the problem. Since we will use the BDD-solver as a black box in our algorithm, we simply refer to the excellent tool of Albrecht et al. [1] which can be used to estimate the running time of these algorithms.

3 The m-RLWE Problem

In [15] the authors define the multivariate RLWE distribution, in its dual formulation, in terms of a tensor product of number fields $K = \bigotimes_{i\in[\ell]} K_i$ where each K_i is a cyclotomic field; not necessarily distinct. The ring R used is now the tensor product, $R = \bigotimes_{i\in[\ell]} \mathcal{O}_{K_i}$, where $\mathcal{O}_{K_i}$ is the ring of integers of the number field K_i. Further, one defines an integer modulus $q \geq 2$ and denotes by $R^\vee$ the dual fractional ideal of R, then $\mathbb{T} = K_\mathbb{R}/R^\vee$.

Definition 1 (Multivariate RLWE distribution). *For $s \in R_q^\vee$ and an error distribution ψ over $K_\mathbb{R}$, a sample from the m-RLWE distribution $A_{s,\psi}$ over $R_q \times \mathbb{T}$ is generated by $a \leftarrow R_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b = (a \cdot s)/q + e \bmod R^\vee)$.*

One can then define the multivariate RLWE search and decision problems in the standard way.

Definition 2 (Multivariate RLWE Search Problem). *Let Ψ be a family of distributions over $K_\mathbb{R}$. Denote by m-$\mathrm{RLWE}_{q,\Psi}$ the search version of the m-RLWE problem: given access to arbitrarily many independent samples from $A_{s,\Psi}$ for some fixed uniformly random $s \in R_q^\vee$ and $\psi \in \Psi$, find s.*

Definition 3 (Multivariate RLWE Decision Problem). *Let Γ be a distribution over a family of error distributions, each over $K_{\mathbb{R}}$. The average-case-decision version of the m-RLWE problem, denoted by m-R-DLWE$_{q,\Gamma}$, is to distinguish with non-negligible advantage between arbitrarily many independent samples from $A_{s,\phi}$, for a random choice of $(s,\psi) \leftarrow U(R_q^\vee) \times \Gamma$, and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.*

Here $U(R)$ denotes the uniform distribution on R.

3.1 Decomposition of m-RLWE and the compositum field

It is well known that the n-th cyclotomic ring (respectively field) can be split using the Chinese Remainder Theorem (CRT) into a tensor product of prime-power cyclotomic rings (respectively fields), these prime powers being those appearing in the factorisation of n. In the case of rings, if we denote the j-th cyclotomic polynomial by Φ_j, we have that if the prime power factorisation of n is $n = p_1^{e_1} \cdots p_\ell^{e_\ell}$ then,

$$\frac{\mathbb{Z}[x]}{(\Phi_n(x))} \cong \frac{\mathbb{Z}[x]}{(\Phi_{p_1^{e_1}}(x))} \otimes \cdots \otimes \frac{\mathbb{Z}[x]}{(\Phi_{p_\ell^{e_\ell}}(x))}.$$

If ψ is the isomorphism from the right hand side to the left, and we have an instance of the m-RLWE problem in the right hand tensor product of rings modulo q then lifting the coefficients to $\mathbb{Z}$, applying ψ and reducing modulo q will give an instance of the RLWE problem since $\psi(q) = q$ and ψ is a linear map when considering the rings as $\mathbb{Z}$-lattices. Furthermore, this map is "smallness" preserving so the resulting error distribution is still a distribution of small elements, though possibly with some degradation in precisely how small. As a result we obtain the following: the m-RLWE problem for cyclotomic fields with defining polynomials Φ_{n_i} is only distinct from the RLWE problem when the n_i are not all pairwise coprime.

Going back to the more general case of arbitrary number fields K_i the way to view the problem is via the notion of the compositum of fields, in our case this is the smallest number field which contains isomorphic copies of each K_i. Then there is a natural algebra homomorphism from the tensor product of the K_i to the compositum. We can then distinguish two cases: the first case is the so called *linearly disjoint* case: the map is injective (and as such automatically bijective in our case) and so the tensor product and the compositum are isomorphic. We remark this is only true in terms of number fields themselves and not the corresponding rings of integers. However, only when this map is not injective is the m-RLWE problem distinct to the RLWE problem and this is the crux of the flaw in the reduction from m-RLWE to RLWE given in [15]. Instead of having to solve a lattice problem in the tensor product of fields whose dimension is the product of the degrees of the defining polynomials one can work in the compositum field where the lattice problem now has dimension the degree of the compositum as a number field which can be much smaller. For well behaved number fields which

can be used in advanced cryptographic primitives such as somewhat homomorphic encryption the natural linear map from the tensor product of the K_i to the compositum is again somewhat "smallness" preserving so that the corresponding RLWE problems in the compositum field may still have small enough error polynomials to be able to mount an attack against them.

Since the RLWE problem is widely deemed to be a hard problem in large dimensions, we will only be interested in the case when the fields K_i are not linearly disjoint. The simplest case of this for cyclotomic fields is when $m = 2$ and the two fields are prime-power cyclotomic fields for the same prime. In particular we will focus on the prime 2 as this is a very popular choice.

4 Attacks

4.1 A distinguishing attack

Our attack is inspired by the "evaluation at one" attack and its variants on non-standard decisional RLWE problems [8,9,5]. These attacks work if the defining polynomial f of the ring $R = \mathbb{Z}[x]/(f(x))$ has a small root modulo q, say $f(\theta) \equiv 0 \mod q$. Then evaluation at $x = \theta$ is well defined and guessing the value of $s(\theta)$ one can test if $e(\theta) = b(\theta) - a(\theta)s(\theta)$ is distributed according to the error distribution evaluated at θ. This requires $e(\theta)$ to be distinguishable from uniform, which it is if $e(\theta)$ remains small enough, hence θ should also be small, e.g. $\theta = \pm 1$.

Note that evaluation at θ is equivalent to reduction modulo the ideal generated by $x - \theta$ and on further reduction by q the ring is non-trivial if and only if $f(\theta)$ and q are not coprime. To stand any chance of distinguishing though, $f(\theta)$ and q should have a large common factor so that the quotient ring is not too small; this is the case when $f(\theta) \equiv 0 \mod q$. More generally, for the attack to succeed we really only need that $\mathbb{Z}[x]/(f(x), q, x - \theta) = \mathbb{Z}/(f(\theta), q)$ is large enough to distinguish the distribution of $e(\theta)$ from uniform.

In our setting the ring R is equal to $\mathbb{Z}[x, y]/(f(x), g(y))$ so we look for an ideal $\mathcal{I}$ of R such that $\mathcal{I}$ and (q) are not coprime. In particular, viewing R as $\mathbb{Z}[x]/(f(x))[y]/(g(y))$ we can try to find a root of $g(y)$ modulo q in the ring $\mathbb{Z}[x]/(f(x))$. If such a root $\theta(x)$ exists one can try to distinguish between $e(x, \theta(x)) = b(x, \theta(x)) - a(x, \theta(x))s(x, \theta(x))$ coming from genuine m-RLWE samples and $e(x, \theta(x))$ coming from uniformly random samples.

Example 1. As a small example let us take $f(x) = x^4 + 1$ and $g(y) = y^2 + 1$. We look for a solution to $y^2 + 1 \equiv 0 \mod q$ in the ring $\mathbb{Z}[x]/(x^4 + 1)$. It is easy to see that a solution is $y = x^2$, hence we have found a root. Thus the mapping $a(x, y) \mapsto a(x, x^2)$ is a ring homomorphism from $\mathbb{Z}[x, y]/(x^4 + 1, y^2 + 1)$ to $\mathbb{Z}[x]/(x^4+1)$. The error polynomials will be sampled coefficient-wise with respect to the standard power basis $x^i y^j$ which we use throughout this paper. Thus writing $e(x, y) = \sum_{i=0}^{3} \sum_{j=0}^{1} e_{i,j} x^i y^j$ we see that under this homomorphism the error polynomial $e(x, y)$ is mapped to

$$\sum_{i=0}^{3} \sum_{j=0}^{1} e_{i,j} x^{i+2j} = (e_{0,0} - e_{2,1}) + (e_{1,0} - e_{3,1})x + (e_{2,0} + e_{0,1})x^2 + (e_{3,0} + e_{1,1})x^3.$$

We thus see that the image of the error polynomial also has small coefficients as they are just a signed sum of two of the original coefficients and is in particular distinguishable from random for large enough q. This means a distinguishing attack can be successfully mounted against the decisional m-RLWE problem in this setting.

We can in fact go a step further in the above example as $y = -x^2$ is another solution to $y^2 + 1 \equiv 0 \bmod q$. This may not seem to add much but using this second solution we can perform an attack on the search variant of the problem making the attack much more powerful. More generally, having multiple roots may make a direct attack on the search variant feasible.

4.2 Multiple roots

Take the example of the 2-RLWE problem of Problem 1 with $f(x) = x^{n_1} + 1$ and $g(y) = y^{n_2} + 1$ for n_1 and n_2 powers of two so that without loss of generality we can assume that $n_2 \mid n_1$ and let $k = n_1/n_2$. Here we have many roots of $g(y)$ in $\mathbb{Z}[x]/(f(x))$ even before reducing modulo q. Namely we have $g(x^{(2i+1)k}) = 0$ for $i \in [n_2]$ and each of the roots is distinct. We can thus define the map

$$\begin{aligned}\Theta\colon \mathbb{Z}[x,y]/(f(x),g(y)) &\to (\mathbb{Z}[x]/(f(x)))^{n_2} \\ a(x,y) &\mapsto (a(x,x^k), a(x,x^{3k}), \ldots, a(x,x^{(2n_2-1)k})).\end{aligned}$$

This map is essentially the canonical embedding of $\mathbb{Z}[y]/(y^{n_2}+1)$ where instead of mapping into $\mathbb{Z}[e^{\pi i/n_2}]^{n_2} \subset \mathbb{C}^{n_2}$ each component maps into the ring of integers of the compositum of fields which is isomorphic to $\mathbb{Z}[x]/(x^{n_1}+1)$ in our case, and extend this mapping to homomorphically in x. Thus we see that Θ is a ring homomorphism. We denote by Θ_i the i'th component of Θ which is again a ring homomorphism.

Just like the canonical embedding, the map Θ is injective. Write $a(x,y) = \sum_{j=0}^{n_2-1} a_j(x)y^j$ and let $\mathbf{a}$ be the vector of coefficients with respect to the power basis in y: $\mathbf{a} = (a_0(x), \ldots, a_{n_2-1}(x))$. Then we have

$$\Theta(a(x,y)) = \mathbf{a}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x^k & x^{3k} & \cdots & x^{(2n_2-1)k} \\ x^{2k} & x^{6k} & \cdots & x^{(2n_2-1)2k} \\ \vdots & \vdots & \ddots & \vdots \\ x^{(n_2-1)k} & x^{3(n_2-1)k} & \cdots & x^{(2n_2-1)(n_2-1)k} \end{pmatrix}.$$

The matrix appearing above is a Vandermonde matrix and thus has determinant $\prod_{0\le i<j<n_2}(x^{(2j+1)k} - x^{(2i+1)k})$ which is non-zero as the $x^{(2i+1)k}$ are distinct for $i \in [n_2]$. Hence Θ is injective and can thus be inverted. Further, for $n_2 > 2$, the absolute value of this determinant is a square root of the discriminant of the number field $\mathbb{Q}(e^{\pi i/n_2})$. It is well known, see for example [19, Proposition 2.1], that the discriminant is $n_2^{n_2}$ so that the determinant is one of $\pm n_2^{n_2/2}$. Hence for

odd q the corresponding map Θ modulo q which we denote by $\bar{\Theta}$, where the bar denotes reduction modulo q, is also invertible, here we mean the map

$$\begin{aligned}\bar{\Theta}\colon \mathbb{Z}_q[x,y]/(f(x),g(y)) &\to (\mathbb{Z}_q[x]/(f(x)))^{n_2}\\ a(x,y) &\mapsto (a(x,x^k), a(x,x^{3k}), \ldots, a(x,x^{(2n_2-1)k})).\end{aligned}$$

The inverse mapping from the image of Θ (or $\bar{\Theta}$ if it exists) is given by multiplying by the inverse of the Vandermonde matrix on the right. Denoting the Vandermonde matrix by $T = (T_{i,j})_{i,j\in[n_2]}$ then its inverse is given by $U = (U_{i,j})_{i,j\in[n_2]}$ where $U_{i,j} = \frac{1}{n_2}x^{-2jk}T_{j,n_2-i} = \frac{1}{n_2}x^{-j(2i+1)k}$ where the indices are taken modulo n_2. To see this we compute

$$\begin{aligned}(TU)_{i,j} &= \sum_{m=0}^{n_2-1} T_{i,m}U_{m,j} = \sum_{m=0}^{n_2-1} x^{i(2m+1)k}\tfrac{1}{n_2}x^{-j(2m+1)k}\\ &= \frac{1}{n_2}\sum_{m=0}^{n_2-1} x^{(i-j)(2m+1)k} = \delta_{i,j}.\end{aligned}$$

We now look at how large the coefficients of t-th component of $\Theta(e(x,y))$, denoted $\Theta_t(e(x,y))$, are if $e(x,y)$ is sampled from the m-RLWE error distribution. We suppose that this error distribution has coefficients, with respect to the basis x^iy^j, sampled independently from a distribution that is subgaussian with parameter σ so writing $e(x,y) = \sum_{i=0}^{n_2-1}\sum_{j=0}^{n_1-1} e_{i,j}x^jy^i$ each $e_{i,j}$ is an independent subgaussian random variable with parameter σ. Then applying Θ_t for some $t \in [n_2]$ gives

$$\Theta_t(e(x,y)) = \sum_{i=0}^{n_2-1}\sum_{j=0}^{n_1-1} e_{i,j}x^{j+i(2t+1)k} = \sum_{j=0}^{n_1-1}\left(\sum_{i=0}^{n_2-1}(-1)^{q_{i,j}}e_{i,r_{i,j}}\right)x^j$$

where we define $q_{i,j}$ and $r_{i,j}$ as the quotient and remainder of $j - i(2t+1)k$ on division by n_1 (which depends on t): $j - i(2t+1) = q_{i,j}n_1 + r_{i,j}$ with $r_{i,j} \in [n_1]$.

Thus we see that the coefficients of $\Theta_t(e(x,y))$ are the sum of n_2 subgaussians with parameter σ and so are themselves subgaussian with parameter $\sqrt{n_2}\sigma$.

4.3 Our Attack

Here we present a simple attack on the 2-RLWE problem. It combines both the simple lattice attack and the distinguishing attack. We stress that the attack is much more powerful that the distinguishing attack alone as firstly it solves a search rather than a decisional problem and secondly there is no need for any guessing during the attack.

We start with a number of samples $\{(a_j(x,y), b_j(x,y))\}_{j\in[\ell]}$ where $b_j(x,y) = a_j(x,y)s(x,y) + e_j(x,y)$. The attack starts by computing the map $\bar{\Theta}$ on each sample, we define $\alpha_{i,j}(x) := \bar{\Theta}_i(a_j(x,y))$ and $\beta_{i,j}(x) := \bar{\Theta}_i(b_j(x,y))$. We note

that since $\bar{\Theta}$ is a ring homomorphism we have, on defining $\epsilon_{i,j}(x) := \bar{\Theta}_i(e_j(x,y))$ and $\sigma_i(x) = \bar{\Theta}_i(s(x,y))$, that

$$\beta_{i,j}(x) = \alpha_{i,j}(x)\sigma_i(x) + \epsilon_{i,j}(x) \qquad \text{for } i \in [n_2],\ j \in [\ell].$$

Our first goal is to find the $\sigma_i(x)$ and to do this we use the simple lattice attack from Section 2.3 since for a fixed i the samples $(\alpha_{i,j}(x), \beta_{i,j}(x))$ follow a $\mathrm{RLWE}_{q,\sqrt{n_2}\Psi}$ distribution. This means we need to simply solve n_2 instances of an RLWE problem in dimension n_1 with noise distribution that is $\sqrt{n_2}$ times wider than for the m-RLWE problem; each instance is independent so can be solved in parallel. If this succeeds we have computed the image of $s(x,y)$ under $\bar{\Theta}$ and since $\bar{\Theta}$ is invertible for odd q we can compute $s(x,y)$ and solve the 2-RLWE problem.

We implemented and tested our attack in SageMath [18], using the NTL library for lattice reduction. We tested our attack on the smallest parameter set given in [14], namely for $n_1 = n_2 = 128$ and q being the smallest prime larger than 2^{42}. The secret polynomial is sampled from the error distribution which samples coefficients independently from a discrete Gaussian with $\sigma = 3.19$, larger than the stated $\sigma = 1$ in the paper [14]. We were able to successfully recover the secret polynomial with just one sample using BKZ reduction with block size 10 to solve the BDD problem instances. This clearly shows that the estimated security level of over 2500 bits, is grossly overestimated. We can see from the estimates given by the LWE estimator [1] that also the parameter set with $n_1 = n_2 = 256$ and $n_1 = n_2 = 512$ offers little to no security (33 and 35 bits respectively) while that for $n_1 = n_2 = 1024$ offers at most 98 bits.

In Table 1 we ran our attack with $n_1 \geq n_2$ and q of the form $2^p + 1$ for $p \in \mathbb{N}$. The secret polynomial s we try to find is chosen uniformly at random from $\mathbb{Z}_q[x,y]/(x^{n_1}+1, y^{n_2}+1)$ so the minimum number of 2-RLWE samples possible to recover s is two. We give the minimum q of the stated form for which the attack succeeded with the stated number of samples; here we used the embedding approach combined with BKZ reduction to attempt to solve the BDD instances. Further, the coefficients of the error polynomials were sampled independently using a discrete Gaussian sampler with $\sigma = 3.19$. The results are heuristic as we only attempted to solve a limited number of instances for each choice of n_1, n_2 and q. It is certainly possible to find the secret for smaller q by increasing the block size used, and in specific instances this may not even be necessary.

In Table 2 we performed the same attack but this time with the coefficients of the secret polynomial taken from the uniform distribution on $\{-1, 0, 1\}$, hence it is now possible for a successful attack with only one sample.

5 Optimizing module based cryptosystems

We take the example of Kyber [3] which when reduced to its simplest form has a public key which is a module-LWE sample where the secret $\mathbf{s}$ is a small element of the module R_q^k where $R = \mathbb{Z}[x]/(x^n+1)$ with n a power of two. Such a

Table 1. The number of samples $\ell \leq 3$ and the minimal $p \in \mathbb{N}$, $p \approx \log_2(q)$ for which our attack succeeded in each of the stated number of attempts for the stated block size, given n_1, n_2 and $q = 2^p + 1$, and where the secret polynomial is sampled uniformly at random in R_q.

		n_1											
		4		8		16		32		64		128	
instances		100		100		100		10		1		1	
block size		30		30		30		30		10		10	
		ℓ	p	ℓ	p	ℓ	p	ℓ	p	ℓ	p	ℓ	p
n_2	4	2	13	2	13	2	13	2	13	2	15	2	21
		3	9	3	10	3	10	3	11	3	13	3	20
	8			2	13	2	13	2	14	2	17	2	22
				3	10	3	10	3	11	3	15	3	20
	16					2	14	2	15	2	18	2	23
						3	11	3	12	3	16	3	22
	32							2	15	2	19	2	24
								3	12	3	17	3	22
	64									2	20	2	31
										3	18	3	24

public key is then a pair $(\mathbf{A}, \mathbf{b})$ with $\mathbf{A}$ a $k \times k$ matrix whose entries are chosen uniformly at random from R_q and $\mathbf{b} \in R_q^k$ with $\mathbf{b} = \mathbf{As} + \mathbf{e}$ for some small error element $\mathbf{e} \in R_q^k$. This means a public key consists of $k(k+1)$ elements of R_q. One might be tempted to use a structured matrix, such as an anti-circulant one, instead of a uniformly random one; after all this is essentially how one goes from LWE to its ring based counterpart RLWE and with our current understanding this latter optimization only incurs a negligible deterioration in security.

Let us fix some parameters and observe what happens. The suggested "paranoid" parameters from [3] are to take $k = 4$ and $n = 256$ and $q = 6781$ which gives a (post-quantum) security level of 218 bits, the largest given by the authors. Taking the matrix $\mathbf{A}$ to be anti-circulant means only having 5 elements of R_q define the public key instead of 20. Further, the scheme can be interpreted as adding a ring structure on top of R_q in a new variable y satisfying $y^4 + 1$ and replacing matrix multiplication by ring multiplication. Hence, we are in the m-RLWE setting and working in the tensor product of two power-of-two cyclotomic fields of degrees 256 and 4 respectively. We can thus apply our attack with $n_1 = 256$ and $n_2 = 4$ which shows that we can recover $\mathbf{s}$ by solving four RLWE problems in dimension 256 from one sample where the error distribution has variance twice that of the original error distribution. The LWE-estimator [1] results in a security of this basic version of "multivariate-Kyber" of at most 107 bits, essentially halving the security. Thus there is a huge difference in terms of security between going from LWE to RLWE and going from module-LWE to m-RLWE if one is not careful.

Table 2. The number of samples $\ell \leq 2$ and the minimal $p \in \mathbb{N}$, $p \approx \log_2(q)$ for which our attack succeeded in the stated number of instances and with the stated block size, given n_1, n_2 and $q = 2^p + 1$, and where the secret polynomial is sampled coefficient-wise with each coefficient uniformly random in $\{-1, 0, 1\}$.

		n_1											
		4		8		16		32		64		128	
instances		100		100		100		10		1		1	
block size		30		30		30		30		10		10	
		ℓ	p	ℓ	p	ℓ	p	ℓ	p	ℓ	p	ℓ	p
n_2	4	1	11	1	12	1	12	1	13	1	14	1	22
		2	9	2	9	2	10	2	11	2	13	2	20
	8			1	13	1	13	1	14	1	15	1	22
				2	10	2	10	2	11	2	14	2	21
	16					1	14	1	14	1	17	1	22
						2	11	2	12	2	15	2	21
	32							1	15	1	18	1	23
								2	12	2	16	2	22
	64									1	20	1	25
										2	17	2	23

We note this "multivariate-Kyber" would also be weak with the "light" parameter set where $k = 2$ but for the standard parameters where $k = 3$ the above attack does not apply as 3 is not a power of two.

6 Conclusion

In this paper we reconsidered the m-RLWE problem and its security. We showed that, with a combination of simple evaluation and lattice attacks, the security of the m-RLWE problem is dramatically less than estimated in the current literature. We would therefore not recommend using 2-RLWE for values of n_1 or n_2 less than those used in standard RLWE based schemes for cryptographic purposes. More generally, we conclude that the m-RLWE problem using number fields with a small degree compositum field is insecure. Finally, this paper should also serve as a warning to implementers of module-LWE based cryptosystems to not blindly apply the standard optimization trick that is used to transform LWE into RLWE.

Acknowledgements

This work was supported in part by the Research Council KU Leuven grants C14/18/067 and STG/17/019 as well as by the Research Foundation Flanders (FWO) through the WOG Coding Theory and Cryptography. The first author was also supported PhD fellowship of the Research Foundation Flanders (FWO).

References

1. M. R. Albrecht, R. Player, and S. Scott. On the concrete hardness of Learning with Errors. *Journal of Mathematical Cryptology*, 9(3):169–203, 2015.
2. L. Babai. On lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.
3. J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. In *2018 IEEE European Symposium on Security and Privacy*, pages 353–367, 2018.
4. Z. Brakerski, C. Gentry, and V. Vaikuntanathan. Fully Homomorphic Encryption without Bootstrapping. Cryptology ePrint Archive, Report 2011/277, 2011. `https://eprint.iacr.org/2011/277`.
5. W. Castryck, I. Iliashenko, and F. Vercauteren. Provably Weak Instances of Ring-LWE Revisited. In *EUROCRYPT 2016*, pages 147–167. Springer-Verlag, 2016.
6. J.-P. D'Anvers, A. Karmakar, S. Sinha Roy, and F. Vercauteren. Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM. In A. Joux, A. Nitaj, and T. Rachidi, editors, *AFRICACRYPT 2018*, pages 282–305. Springer International Publishing, 2018.
7. L. Ducas and A. Durmus. Ring-LWE in Polynomial Rings. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *PKC 2012*, pages 34–51. Springer Berlin Heidelberg, 2012.
8. K. Eisenträger, S. Hallgren, and K. Lauter. Weak Instances of PLWE. In A. Joux and A. Youssef, editors, *SAC 2014*, pages 183–194. Springer International Publishing, 2014.
9. Y. Elias, K. E. Lauter, E. Özman, and K. E. Stange. Provably Weak Instances of Ring-LWE. In R. Gennaro and M. Robshaw, editors, *CRYPTO 2015*, pages 63–92. Springer Berlin Heidelberg, 2015.
10. R. Kannan. Minkowski's Convex Body Theorem and Integer Programming. *Mathematics of Operations Research*, 12(3):415–440, 1987.
11. R. Lindner and C. Peikert. Better Key Sizes (and Attacks) for LWE-Based Encryption. In A. Kiayias, editor, *CT-RSA 2011*, pages 319–339. Springer Berlin Heidelberg, 2011.
12. V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors over Rings. In H. Gilbert, editor, *EUROCRYPT 2010*, pages 1–23. Springer Berlin Heidelberg, 2010.
13. V. Lyubashevsky, C. Peikert, and O. Regev. A Toolkit for Ring-LWE Cryptography. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT 2013*, pages 35–54. Springer Berlin Heidelberg, 2013.
14. A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González. Multivariate lattices for encrypted image processing. In *IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 1707–1711. IEEE, 2015.
15. A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González. On Ring Learning with Errors over the Tensor Product of Number Fields. `https://arxiv.org/abs/1607.05244`, 2016.
16. A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González. Multivariate Cryptosystems for Secure Processing of Multidimensional Signals. *CoRR*, abs/1712.00848, 2017.
17. M. Rosca, D. Stehlé, and A. Wallet. On the Ring-LWE and Polynomial-LWE Problems. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018*, pages 146–173. Springer International Publishing, 2018.

18. The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.5.1)*, 2017. `http://www.sagemath.org`.
19. L. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics. Springer New York, 1997.