Analyzing subrings for some R-LWE and NTRU instances

Zhenfei Zhang
zzhang@securityinnovation.com

Security Innovation Inc.
Wilmington MA, US
Oct 31, 2016

1 Overview

We assume some familiarity with lattice based cryptography over the ring, in particular R-LWE [9] and NTRU [8]. In some of those ideal lattice-based cryptosystems, one usually uses a polynomial ring of $\mathcal{R}_q = \mathbb{Z}_q/F$ over $F = x^N + 1$ with N a power of 2. For fast implementation purposes, the modulus q is usually

1. either one plus a multiple of $2N$, i.e, $q = 12289$ (such as BLISS [7] and NewHope [2]);
2. or a power of 2, i.e., 2^{32} (such as FHEW [6] and YaSHE [4]).

In the first case there exist structured subrings. In the second case, it is possible to convert the original rings into those that admit subrings using modulus switching techniques [5]. This is perhaps the first time modulus switching is used in a destructive way to the best knowledge of the author.

The purpose of this report is to study the interesting property of those subrings using lattices. The results in this report are mainly negative: "*we have tried this and that methods and we failed.*" It does not suggest any of the parameters/schemes are broken, nor does it suggest that the existence of subrings is a potential weakness by design (and hence suggests non-subring designs shall be in favor). In fact it shows that all lattice attacks (if possible) considered in this report are less efficient than the attacks over the original rings. And the result also implies that if parameters are derived from the provable secure R-LWE theorem [9], the shortest vector is totally lost during the mapping into the subring and therefore makes the subring attack impossible.

An interesting observation, though, is that for some parameters/schemes (not driven from the provable secure theorem), by moving into a subring, one can still preserve the uniqueness of the shortest non-zero vector. Those unique vectors in the new lattices are unfortunately too close to Gaussian heuristic length to be recovered via any lattice reduction technique. To this extend the results in this report is similar to those of the subfield attacks on NTRU [1] where the uniqueness of the shortest vectors is preserved, however the root Hermite factor is reduced more significantly (in some cases, beyond the reach of known lattice reduction techniques).

We have also considered a few ad-hoc non-lattice method, such as combinatorial searching for short vectors in the lattice over the subring, but none of those seems to be able to exploit the sub-ring better than a lattice attack. We did not include those analysis in this report. At the moment we are unable to improve the results in the report. We wrote this report in the hope of inspiring new and improved cryptanalysis using subrings.

Another interesting observation is on the constructive side of subrings: the analysis of subrings allows for a possible connection between an R-LWE instance with binary secrets in the original ring (with a larger dimension) and an R-LWE instance with integer secrets in the subring (with a smaller dimension).

2 Modulus switching

For the rest of the report, we use the letter q to denote modulus that is "*one plus a multiple of* $2N$", and Q to denote modulus that is "*a power of* 2". Those are two common choices for lattice-based cryptography. They are interchangeable via the modulus switching technique. For example, when Q is sufficiently large, i.e., $Q = 2^{32}$, one is able to move from $\mathcal{R}_Q = \mathbb{Z}_Q[x]/F(x)$ into $\mathcal{R}_q = \mathbb{Z}_q[x]/F(x)$ as follows[1]:

Let s be an R-LWE secret, and $(A, B) \in \mathcal{R}_Q^2$ be an R-LWE instance, where

$$As + e = B \bmod x^N + 1 \bmod Q \tag{1}$$

for some error vector e. Then,

$$As + e = B + Qc \bmod x^N + 1$$

for some unknown c. Since both s and e are small, c is also small (see Section 5.1 for the analysis of the smallness of c). Let $q \equiv 1 \bmod 2N$ be the target modulus that is smaller than Q, and $r \equiv Q \bmod q$, then we have

$$as + e = b + rc \bmod x^N + 1 \bmod q$$

where $(a, b) = (A, B) \bmod q$. Note that s, e and c are unchanged, so long as $\|s\|_\infty$, $\|e\|_\infty$ and $\|rc\|_\infty$ are smaller than q. Hence, we obtain a new equation

$$as + (e - rc) = b \bmod x^N + 1 \bmod q \tag{2}$$

where the attacker knows $(a, b) \in \mathcal{R}_q^2$ and is asked to find s. It is again an R-LWE instance, over the new ring $\mathcal{R}_q$ now. Compared to the original one, the noise term is increased by rc.

Example: let $Q = 2^{32}$, $q = 2^{16} + 1 = 65537$, then $r = 1$. Other candidate (q, r) couples are $(1689601, 1554)$, $(429496321, 4086)$. Those candidates allow for a larger q but they increase the noise too much.

[1] It is also feasible to move from the other direction when $q > Q$. It is irrelevant to the cryptanalysis in this report.

In the rest we have two typical qs, namely $q = 12289$ used in BLISS and NewHope, which is the smallest possible $2kN + 1$ for $N = 512$ or 1024; and $q = 65537$ for FHEW and YaSHE where $Q = 2^{32}$. Moving towards this modulus has minimum impact on rc, and $q = 65537$ has some very nice roots (power of 2s).

3 Move into the subrings

We analyze the following ring $\mathcal{R}_q = \mathbb{Z}_q[x]/F(x)$ for $F(x) = x^N + 1$, N a power of 2, and q one plus a multiple of $2N$. Note that $q \equiv 1 \bmod 2N$ enables fast NTT. A special feature of this choice of $F(x)$ is that $F(x)$ has exactly N roots modulo q. I.e.,

$$F(x) = x^N + 1 = \prod_{i=1}^{N}(x - r_i) \bmod q \tag{3}$$

In addition, $F(x)$ has many binomial factors, such as

$$\begin{aligned} x^N + 1 \equiv & (x^{N/2} - 1479)(x^{N/2} - 10810) \\ \equiv & (x^{N/4} - 4043)(x^{N/4} - 5146)(x^{N/4} - 7143)(x^{N/4} - 8246) \mod 12289 \end{aligned}$$

where each of the factors defines a subring. For example, $\mathcal{R}_1 = \mathbb{Z}_q[x]/F_1(x)$ where $F_1 = (x^{N/2} - q_1)$ with $q_1 = 1479$.

More generally speaking, let $F_1 = (x^M - q_1)$ be a factor of F where $M = N/k$ is a power of 2. (The above example is the case where $k = 2$.) Then $\{x^M - q_1^{2i+1}\}_{i=1}^{k}$ are all factors of F, and

$$q_1 \geq (q-1)^{1/k} \tag{4}$$

There are some cases where the equality holds, for example, when $q = 2^{16} + 1$, we have $q_1 = \pm 2^8$ for $k = 2$, and $q_1 = \pm 2^4$ for $k = 4$.

Operations over the original ring are homomorphic in the subrings. For example, let h be an NTRU public polynomial such that

$$fh = g \bmod F \bmod q,$$

for some short f and g, then

$$\bar{f}\bar{h} = \bar{g} \bmod F_1 \bmod q,$$

where $\bar{f} \equiv f \bmod F_1$ is the image of f in $\mathcal{R}_1$.

Example: Let $f_2 = f \bmod x^{N/2}$ and $f_1 = (f - f_2)/x^{N/2}$ be the lower/higher parts of f, i.e.,

$$f = x^{N/2} f_1 + f_2$$

Also denote g_1 and g_2 for higher/lower parts of g. Then we know:

$$f \equiv q_1 f_1 + f_2 \bmod F_1$$

$$g \equiv q_1 g_1 + g_2 \bmod F_1$$

therefore

$$(q_1 f_1 + f_2)\bar{h} = (q_1 g_1 + g_2) \bmod F_1 \bmod q \tag{5}$$

This is another NTRU lattice with half of the dimension but much larger $\|\bar{f}\|$ and $\|\bar{g}\|$.

In the more general case where $F_1 = (x^M - q_1)$ for $M = N/k$, let f be a polynomial in $\mathcal{R}$ that can be segmented into k polynomials of degree less than M:

$$f = f_0 + f_1 x^M + f_2 x^{2M} + \cdots + f_{k-1} x^{(k-1)M},$$

then,

$$\bar{f} \equiv f_0 + q_1 f_1 + q_1^2 f_2 + \cdots + q_1^{k-1} f_{k-1} \bmod F_1$$

For all possible ks, $k = 2$ gives the minimum l_∞ norm for $\bar{f}$, in which case

$$\|\bar{f}\|_\infty \approx (q_1 + 1)\|f\|_\infty = q_1 + 1 \geq \sqrt{q-1},$$

assuming f is a trinary polynomial and $\|f\|_\infty = 1$.

As an example, with $q = 2^{16} + 1 = 65537$ we have $q_1 = 2^8 = \sqrt{q-1}$. We have "$\approx$" rather than "$=$" because it is possible that f_1 and f_2 do not overlap each other at all when they are extremely sparse.

However, for an R-LWE lattice or an NTRU lattice, over the subring $\mathcal{R}_1 = \mathbb{Z}_q[x]/(x^M - q_1)$, i.e.,

$$L = \begin{bmatrix} qI & 0 \\ \star & I \end{bmatrix}$$

the determinant of the lattice is q^M, and the dimension is $2M$, hence the Gaussian heuristic length in this lattice is estimated by

$$GH \approx \sqrt{\frac{dim}{2\pi e}} det^{\frac{1}{dim}} = \sqrt{\frac{Mq}{\pi e}}, \tag{6}$$

while the l_2 norm of the target vector $\|(\bar{f}, \bar{g})\|_2$ is around $\sqrt{2M} q_1 \geq \sqrt{2Mq}$, if $(\bar{f}, \bar{g})$ *has uniform coefficients less than* q_1. In this case the classical lattice attack is strictly impossible.

Nevertheless, in some of the settings, f and g are fairly sparse, making the l_2 norm a little smaller. With a few tricks we can preserve the uniqueness of the shortest vector.

4 The $q = 12289$ case

We analyze the following ring $\mathcal{R}_q = \mathbb{Z}_q[x]/F(x)$ for $F(x) = x^{512} + 1$ and $q = 12289$ with a subring $\mathcal{R}_1 = \mathbb{Z}_q[x]/F_1(x)$ with $q_1 = 1479$ and $F_1 = x^{256} - q_1$. This is the setting for BLISS-II. BLISS uses NTRU type of (f, g) that are trinary with pre-fixed number of ± 1s. For NewHope a different $N = 1024$ is used. NewHope also has Gaussian like "(s, e)" which makes the shortest non-zero

vector disappear after mapping to the subring. Compared to NewHope, BLISS is an easier example to analysis.

Let h be an NTRU public polynomial such that

$$fh = g \bmod F \bmod q,$$

for some short f and g, also denote

$$\bar{h} = h \bmod F_1,$$

and $\bar{H}$ the matrix formed by the "cyclic rotation" of $\bar{h}$ over $\mathcal{R}_1$, then from previous section we have

$$(q_1 f_1 + f_2)\bar{h} = (q_1 g_1 + g_2) \bmod F_1 \bmod q$$

One can define two lattices:

$$L_1 = \begin{bmatrix} qI & 0 \\ \bar{H} & I \end{bmatrix}$$

where one can look for

$$(q_1 g_1 + g_2, q_1 f_1 + f_2) \in L_1$$

Alternatively,

$$L_2 = \begin{bmatrix} qI & 0 & 0 \\ q_1\bar{H} & I & 0 \\ \bar{H} & 0 & I \end{bmatrix}$$

where one can look for

$$(q_1 g_1 + g_2, f_1, f_2) \in L_2.$$

4.1 Analyzing second lattice

The second lattice is not well balanced because

- $(q_1 g_1 + g_2)$ itself is not well balanced; and
- $\|(f_1, f_2)\|_\infty$ is significantly smaller than $\|(q_1 g_1 + g_2)\|_\infty$.

Balance $(q_1 g_1 + g_2)$: Let r_1 be an integer such that $|r_1 q_1 \bmod q| \approx |r_1|$. Denote $r_2 = r_1 q_1 \bmod q$. Example, for $r_1 = 740$ we have $r_2 = 740 \times 1479 \equiv 739 \bmod 12289$. Let

$$v = x - q_1 = x - 1479 \bmod 12289$$

be an example vector, then

$$740v = 740x - 739 \bmod 12289.$$

This effectively reduces the l_2-norm by approximately $\sqrt{2}$. I.e,

$$\|v\| = \sqrt{1479^2 + 1} \approx 1479,$$

$$\|740v\| = \sqrt{740^2 + 739^2} \approx 1039.5 \approx 1479/\sqrt{2}$$

Therefore from

$$(q_1 f_1 + f_2)\bar{h} = (q_1 g_1 + g_2) \bmod F_1 \bmod q$$

we know

$$f_1(r_2\bar{h}) + f_2(r_1\bar{h}) = (r_2 g_1 + r_1 g_2) \bmod F_1 \bmod q \tag{7}$$

Balance (f_1, f_2): Let a be a balance integer whose value is to be determined later. From Eq. (7) we already construct a lattice

$$L_2' = \begin{bmatrix} qI & 0 & 0 \\ r_2\bar{H} & I & 0 \\ r_1\bar{H} & 0 & I \end{bmatrix}$$

To balance the weight for (f_1, f_2), we look at a lattice

$$L_3 = \begin{bmatrix} qI & 0 & 0 \\ r_2\bar{H} & aI & 0 \\ r_1\bar{H} & 0 & aI \end{bmatrix}$$

which contains $(r_2 g_1 + r_1 g_2, af_1, af_2)$ for some balance integer a.

L_3 has a larger dimension $= 3N/2$ than L_1 (with dimension $= N$). But for L_3 with certain parameter a, it is still possible to maintain the shortness of $(r_2 g_1 + r_1 g_2, af_1, af_2)$.

Parameters In BLISS-I/II, f and g are both trinary polynomials with 70% of 0s, 15% of ± 1s each. That means within $r_2 g_1 + r_1 g_2$,

- 49% of coefficients are 0;
- 42% of coefficients are $\pm r_1$ or $\pm r_2$;
- 4.5% of coefficients are $\pm|r_1 - r_2|$;
- 4.5% of coefficients are $\pm|r_1 + r_2|$.

Also, we know $r_1 = 740$ and $r_2 = 739$. So the norm of $(r_1 g_1 + r_2 g_2)$ is expected:

$$\begin{aligned}\|r_1 g_1 + r_2 g_2\| \approx & (256 \times 0.42 \times 740^2 + 256 \times 0.045 \times 1^2 + 256 \times 0.045 \times 1479^2)^{1/2} \\ \approx & 9196.4\end{aligned}$$

On the other hand the norm of (af_1, af_2) is expected as $a\sqrt{512 \times 0.3}$. The norm of the target vector is therefore

$$(9196.4^2 + 153.6a^2)^{1/2}$$

The Gaussian expected length in L_3 is:

$$\sqrt{3N/4\pi e}(q^{N/2}a^N)^{2/3N} \approx 154.7a^{2/3}$$

For the attack to be optimal, we need to maximize

$$154.7a^{2/3} - (9196.4^2 + 153.6a^2)^{1/2}.$$

When $a = 1053$ this value is maximized, resulting a shortest vector of length 15951 within lattice L_3, with a Gaussian expected length of 16017; although there is no known method that is capable of recovering this shortest vector due to the extremely small root Hermite factor

$$(16017/15951)^{2/(3N)} \approx 1.004^{1/768} \approx 1.000005.$$

This is way smaller than the root Hermite factor for the original lattice (1.006). It is very likely that even though the dimension is smaller than the original lattice, the attack over the subring lattice is much less efficient.

4.2 Analyzing first lattice

Recall that

$$L_1 = \begin{bmatrix} qI & 0 \\ \bar{H} & I \end{bmatrix}$$

L_1 has a smaller dimension, N, compared to $2N$ for original lattice, and $3N/2$ for L_3. But the expected short vector in L_1 is $\sqrt{\frac{Nq}{2\pi e}}$ that is significantly less than q_1. So a direct lattice attack is not feasible. Some potential way to exploit this subring is via meet-in-the-middle/combinatorial attacks when f and/or g are very sparse trinary polynomials; or when $r_2 f_1$ and $r_1 f_2$ has some overlapping that reduces the search spaces.

5 The $q = 65537$ cases

There are some schemes that use very large modulus rather than $2kN + 1$ cases. For example, FHEW (fully homomorphic encryption in the west) and YASHE (yet another somewhat homomorphic encryption) use $Q = 2^{32}$ and $N = 1024$. This choice of Q makes modular operation is implicit in implementation. As we have shown in Section 2, we can simplify the equation by

$$as + d = b \bmod x^N + 1 \bmod q \tag{8}$$

where $d = e - rc$.

To recover s and d from a and b one tries to find the shortest vector in the lattice

$$\begin{bmatrix} qI & 0 & 0 \\ a & I & 0 \\ b & 0 & 1 \end{bmatrix}$$

which will be $(d, -s, 1)$. Following same notation for d_1, d_2, s_1, s_2 and $\bar{a}$, $\bar{b}$. Let $F_1 = (x^{N/2} - q_1)$ then,

$$\bar{a}(q_1 s_1 + s_2) + (q_1 d_1 + d_2) = \bar{b} \bmod F_1 \bmod q \tag{9}$$

Applying the same technique in section 4 we obtain two new lattices, namely

$$L_4 = \begin{bmatrix} qI & 0 & 0 \\ \bar{A} & I & 0 \\ \bar{b} & 0 & 1 \end{bmatrix}$$

where $(q_1 d_1 + d_2, -q_1 s_1 - s_2, 1) \in L_4$; and

$$L_5 = \begin{bmatrix} qI & 0 & 0 & 0 \\ q_1\bar{A} & q_1 I & 0 & 0 \\ -\bar{A} & 0 & q_1 I & 0 \\ \bar{b} & 0 & 0 & 1 \end{bmatrix}$$

where $(q_1 d_1 + d_2, q_1 s_1, q_1 s_2, 1) \in L_5$. As per previous analysis, L_5 is easier to attack than L_4.

Note that $q_1 \approx q^{1/2}$. The Gaussian expected length of L_5 is approximately

$$\sqrt{(3N/2+1)/(2\pi e)}(q^{N/2} q_1^N)^{1/(3N/2+1)} \approx \sqrt{3N/(4\pi e)} q^{2/3} \tag{10}$$

$$\approx \sqrt{90} q^{2/3}, \tag{11}$$

while the shortest vector is close to a small multiple of $q_1 \approx q^{1/2}$, where the "small multiple" depends on the distribution of s, e and c.

Asymptotically, this is very nice, as the Gaussian heuristic length is on the order of $q^{2/3}$ while the target vector is on the order of $q^{1/2}$, which creates a gap of $q^{1/6}$, asymptotically. However, as we shall see in next subsection, the hidden constant for $q^{1/2}$ is a polynomial in N, which is too large to break any practical parameters. The only possible scenarios that $(q_1 d_1 + d_2, q_1 s_1, q_1 s_2, 1)$ remains the shortest vector in L_5 are that

- either both s and e are *very sparse trinary polynomials* as in BLISS-I/II;
- or q is very large, potentially (sub-)exponential in N.

Even so, it is not likely that this vector is recoverable from lattice reductions, as we saw in the BLISS example. In addition, it is not likely such q even exists for a given Q that allows for both small r in modulus switching and smallish q_1 in subrings. Lastly, when such large q does exist, it is likely the the original lattice has already have a huge gap so one does not gain anything (other than reduced dimension) by moving to the sub-ring.

5.1 Asymptotic parameters

Let s and e be sampled from N dimensional discrete Gaussian distribution χ_σ^N with mean 0 and deviation σ. Then we have $\|s\|_2 \approx \|e\|_2 \approx \sqrt{N}\sigma$.

To approximate the length of c is trickier. Since each coefficient of c is "the number of wraparounds over q" of an accumulation of N different $a_i s_j$ terms, where a_i is random in $\mathbb{Z}_q$ and s_j follows χ_σ, the distribution of c is also a Gaussian

$\chi^N_{\sqrt{N}\sigma/2}$. Therefore we approximate the norm $\|rc\|_2 \approx rN\sigma/2$. Then, d follows $\chi^N_{(r\sqrt{N}/2+1)\sigma}$ and $\|d\|_2 \approx (rN/2+\sqrt{N})\sigma$. Therefore we estimate that

$$\|(q_1d_1+d_2, q_1s_1, q_1s_2, 1)\|_2 \approx ((q_1+1)^2(rN/4+\sqrt{N/2})^2\sigma^2 + q_1^2N\sigma^2+1)^{1/2} \tag{12}$$

$$\approx \frac{q_1\sigma}{4}\left(r^2N^2 + 4\sqrt{2}rN^{\frac{3}{2}} + 8N\right)^{1/2} \tag{13}$$

Combining Eq. (10) and (13), the uniqueness of the shortest vector is preserved, if only

$$\frac{q_1\sigma}{4}\left(r^2N^2 + 4\sqrt{2}rN^{\frac{3}{2}} + 8N\right)^{1/2} < \sqrt{3N/(4\pi e)}q^{2/3} \tag{14}$$

Ignoring all constants we require

$$q > N^3r^6\sigma^6$$

5.2 Practical parameters

For $N = 1024$, $q = 65537$, we have $r = 1$. The norm of shortest vector is estimated by:

$$\|(q_1d_1+d_2, q_1s_1, q_1s_2, 1)\|_2 \approx 280q_1\sigma$$

For $\sigma = 8$ as in YASHE, we have

$$\|(q_1d_1+d_2, q_1s_1, q_1s_2, 1)\|_2 \approx 573440$$

This is a lot greater than Gaussian Heuristic $\sqrt{90}q^{2/3} \approx 15421$, which implies that the attack is no longer feasible.

In order for the attack to be successful, we require

$$\sqrt{90}q^{2/3} > 280q^{1/2}\sigma$$

That is

$$q > (29.5\sigma)^6$$

6 R-LWE with Binary secret

For now let us assume that f is a binary polynomial over a ring $\mathcal{R}_q = \mathbb{Z}_q/F$ with q one plus a power of 2. Also $F_1 = x^M - q_1$ be a binomial factor of F, with $M = N/k$ for some k. Then, there exist a mapping from $\mathcal{R}_q$ to $\mathcal{R}_1$ that maps a binary polynomial f into a degree $M-1$ polynomial with integers coefficients of t-bits.

Example: let

$$f = (f_0 + f_1x + f_2x^2 + \cdots + f_{15}x^{15})$$

$$+(f_{16} + f_{17}x + f_{18}x^2 + \cdots + f_{31}x^{15})x^{16}$$
$$\vdots$$
$$+(f_{112} + f_{113}x + f_{114}x^2 + \cdots + f_{127}x^{15})x^{112}$$

be a binary polynomial over the ring with $F = x^{128} + 1$ and $q = 2^{16} + 1$. Then

$$F_1 = x^{16} - 2$$

defines a subring, and

$$\begin{aligned}\bar{f} = f \bmod F_1 =&(f_0 + 2f_{16} + 2^2 f_{32} + \cdots + 2^7 f_{112})\\ &+(f_1 + 2f_{17} + 2^2 f_{33} + \cdots + 2^7 f_{113})x\\ &\vdots\\ &+(f_{15} + 2f_{31} + 2^2 f_{47} + \cdots + 2^7 f_{127})x^{15}\end{aligned}$$

Interestingly, when each of f_i is randomly chosen from $\{0, 1\}$, $\bar{f}$ becomes a random degree 15 polynomial with integer coefficients uniformly randomly in $[0, 2^8)$.

In general, let

$$as + e = b \bmod F \bmod q \tag{15}$$

be an R-LWE instance in $\mathcal{R}_q$ where both s and e are random binary vectors, then, one can convert this instance into a new R-LWE instance

$$\bar{a}\bar{s} + \bar{e} = \bar{b} \bmod F_1 \bmod q, \tag{16}$$

where $\bar{s}$ and $\bar{e}$ are small integer vector uniformly distributed over $\mathbb{Z}_{2^k}$. Hence,

1. if one can solve R-LWE w.r.t. (15) then he can also solve the R-LWE w.r.t (16);
2. if one can solve R-LWE w.r.t. (16), in addition, if he can also recover a from $\bar{a}$. then he can also solve the R-LWE w.r.t (15);

The first point is straightforward, as given a, b and F, one can compute $\bar{a}, \bar{b}$ and F_1. In fact, the map from a to $\bar{a}$ is surjective; the map from f to $\bar{f}$ was supposed to be surjective too, but the restriction of binary coefficients reduces the space, and indeed makes it bijective. Hence, one is not able to reserve the reduction, as from $\bar{a}$ and $\bar{b}$ there exists many potential as and bs.

This result does not suggest the existence of "provable secure" instances of R-LWE with binary coefficients.

7 Conclusion and further thoughts

In this report we have looked at some of possible ways to attack the rings that contain very nice subrings. In section 2 we have shown that even if present ring does not admit those nice subrings, one can still using modulus switching to obtain nice sub-rings.

We then show in Section 3 that, in general, those attacks does not break any existing schemes. However, it is still interesting to see that

– for some schemes (such as BLISS-II) one can still preserve the uniqueness of the shortest non-zero vector, although this vectors are too close to Gaussian heuristic length to be recovered by any known algorithm;
– for some other settings, one can expect a unique shortest vector asymptotically.

We then show that in both cases those lattice attacks are no better than lattice attack over original rings due to the extremely small root Hermite factors.

We believe that it is safe to conclude that subring *lattice* attacks are in general less efficient than lattice attacks over the original ring. However, this report does not rule out the possibility that there exist other types of attacks that exploit the subring structure better than lattice attacks.

There are some ideas to which the author do not have the knowledge to explore further at the moment. For example, in the case of $q = 2^{16} + 1$, there are many different subrings $x^M - q_1$ with $q_1 = 2^t$ a power of 2. This is a highly structured q_1 and it is not too optimistic to assume that it is exploitable.

References

1. Martin R. Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encoding schemes. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, pages 153–178, 2016.
2. Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 327–343, 2016.
3. Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU prime. *IACR Cryptology ePrint Archive*, 2016:461, 2016.
4. Joppe W. Bos, Kristin E. Lauter, Jake Loftus, and Michael Naehrig. Improved security for a ring-based fully homomorphic encryption scheme. In *Cryptography and Coding - 14th IMA International Conference, IMACC 2013, Oxford, UK, December 17-19, 2013. Proceedings*, pages 45–64, 2013.
5. Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *FOCS*, pages 97–106, 2011.
6. Léo Ducas and Daniele Micciancio. FHEW: bootstrapping homomorphic encryption in less than a second. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, pages 617–640, 2015.
7. Lo Ducas, Alain Durmus, Tancrde Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In Ran Canetti and JuanA. Garay, editors, *Advances in Cryptology CRYPTO 2013*, volume 8042 of *Lecture Notes in Computer Science*, pages 40–56. Springer Berlin Heidelberg, 2013.
8. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *ANTS*, pages 267–288, 1998.
9. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6):43, 2013.