Security considerations for Galois (non-dual) RLWE families

Hao Chen*, Kristin Lauter, Katherine E. Stange

SAC conference, St John's, Canada

August 11, 2016

Microsoft Research

Plan

1. Background: Ring-LWE
2. Improved attack using cosets
3. Infinite family of vulnerable instances (for narrow errors)
4. Impossibility of our attack for 2-power cyclotomic fields

The (non-dual and discrete) Ring-LWE problem

Ring-LWE problem: introduced by Lyubashevskey, Peikert and Regev in 2010 ([LPR]).

The (non-dual and discrete) Ring-LWE problem

Ring-LWE problem: introduced by Lyubashevskey, Peikert and Regev in 2010 ([LPR]).

- $R = \mathbb{Z}[x]/(f(x))$, $f(x)$ a degree n polynomial.
- q an integer (the modulus), $R_q = \mathbb{Z}_q[x]/(f(x))$.
- a secret polynomial $s \in R_q$.
- an error distribution χ over R.
- a sample is

$$(a, b = as + e) \in R_q \times R_q,$$

where $a \in R_q$ uniformly, and $e \leftarrow \chi$.

The (non-dual and discrete) Ring-LWE problem

Ring-LWE problem: introduced by Lyubashevskey, Peikert and Regev in 2010 ([LPR]).

- $R = \mathbb{Z}[x]/(f(x))$, $f(x)$ a degree n polynomial.
- q an integer (the modulus), $R_q = \mathbb{Z}_q[x]/(f(x))$.
- a secret polynomial $s \in R_q$.
- an error distribution χ over R.
- a sample is
$$(a, b = as + e) \in R_q \times R_q,$$
where $a \in R_q$ uniformly, and $e \leftarrow \chi$.

Remark: [LPR] uses $s \in R_q^\vee$ and χ a continuous Gaussian distribution on $\mathbb{R}^n/qR^\vee$.

Security of Ring-LWE

One main security reduction theorem in [LPR] is...

Theorem (LPR)

Fix a number field K of degree n with ring of integers R. Assume $r \geq \omega(\sqrt{\ln n})$. If search-RLWE is easy for all continuous Gaussian errors bounded by r, then for all fractional ideals $\mathcal{I}$ of K, it is easy to sample a discrete Gaussian over $\mathcal{I}$ with width

$$\gamma = \frac{q}{r} \cdot const(\mathcal{I}).$$

Security of Ring-LWE

One main security reduction theorem in [LPR] is...

Theorem (LPR)

Fix a number field K of degree n with ring of integers R. Assume $r \geq \omega(\sqrt{\ln n})$. If search-RLWE is easy for all continuous Gaussian errors bounded by r, then for all fractional ideals $\mathcal{I}$ of K, it is easy to sample a discrete Gaussian over $\mathcal{I}$ with width

$$\gamma = \frac{q}{r} \cdot const(\mathcal{I}).$$

Remarks:
(1) sampling a discrete Gaussian over lattices has connections to other hard lattice problems.
(2) for cyclotomic rings, can replace the problem with GapSVP.

Security in practice

There are still some security-related open questions after [LPR]...

Security in practice

There are still some security-related open questions after [LPR]...

- What happens when the error size is below the [LPR] requirement (and/or the error is discrete)?

Security in practice

There are still some security-related open questions after [LPR]...

- What happens when the error size is below the [LPR] requirement (and/or the error is discrete)?
- What happens if one use R instead of $R^\vee$? (If $R^\vee$ is principal, then there is a bijection. In general it is unclear).

Security in practice

There are still some security-related open questions after [LPR]...

- What happens when the error size is below the [LPR] requirement (and/or the error is discrete)?
- What happens if one use R instead of $R^\vee$? (If $R^\vee$ is principal, then there is a bijection. In general it is unclear).
- How does the security level vary in terms of the shape of R, q and χ?

Security in practice

There are still some security-related open questions after [LPR]...

- What happens when the error size is below the [LPR] requirement (and/or the error is discrete)?
- What happens if one use R instead of $R^\vee$? (If $R^\vee$ is principal, then there is a bijection. In general it is unclear).
- How does the security level vary in terms of the shape of R, q and χ?

Our goals:

1. Explore the boundary of security for all types of RLWE problems (by exploring attacks using the ring-structure).

2. Clarify the security of the RLWE schemes used in practical applications.

Plan

Review the attack of [CLS15]

Fix a prime ideal $\mathfrak{q}$ above q in R. Let $\pi : R \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}$.

Review the attack of [CLS15]

Fix a prime ideal $\mathfrak{q}$ above q in R. Let $\pi : R \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}$.

Assume: $\pi(e)$ is distinguishable from uniform.
Goal: recover $\pi(s)$.

Review the attack of [CLS15]

Fix a prime ideal $\mathfrak{q}$ above q in R. Let $\pi : R \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}$.

Assume: $\pi(e)$ is distinguishable from uniform.
Goal: recover $\pi(s)$.

Algorithm:

1. For each g in $R/\mathfrak{q}$:
   - compute the "errors"

     $$e' = \pi(b) - \pi(a) \cdot g$$

     for all samples (a, b).
   - run a statistical test for uniform distribution on the set of e'. If non-uniform, return g.

Review the attack of [CLS15]

Fix a prime ideal $\mathfrak{q}$ above q in R. Let $\pi : R \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}$.

Assume: $\pi(e)$ is distinguishable from uniform.
Goal: recover $\pi(s)$.

Algorithm:

1. For each g in $R/\mathfrak{q}$:
   - compute the "errors"

     $$e' = \pi(b) - \pi(a) \cdot g$$

     for all samples (a, b).
   - run a statistical test for uniform distribution on the set of e'. If non-uniform, return g.

Coset improvement: assumptions

In [CLS15], we found several vulnerable Galois instances by searching. Recall that a number field of degree *n* is *Galois* if it has n automorphisms.

Coset improvement: assumptions

In [CLS15], we found several vulnerable Galois instances by searching. Recall that a number field of degree n is *Galois* if it has n automorphisms.

Galois number fields are nice for Ring-LWE because we have a *search-to-decision reduction*.

Coset improvement: assumptions

In [CLS15], we found several vulnerable Galois instances by searching. Recall that a number field of degree n is *Galois* if it has n automorphisms.

Galois number fields are nice for Ring-LWE because we have a *search-to-decision reduction*.

First we give an improved attack based on some extra assumptions.

Coset improvement: assumptions

In [CLS15], we found several vulnerable Galois instances by searching. Recall that a number field of degree n is *Galois* if it has n automorphisms.

Galois number fields are nice for Ring-LWE because we have a *search-to-decision reduction*.

First we give an improved attack based on some extra assumptions. Assume: there is a prime ideal $\mathfrak{q}$ over q such that

- $R/\mathfrak{q} \cong \mathbb{F}_{q^2}$.
- $e \mod \mathfrak{q}$ is more likely to lie in $\mathbb{F}_q$ than usual.

Coset improvement: assumptions

In [CLS15], we found several vulnerable Galois instances by searching. Recall that a number field of degree n is *Galois* if it has n automorphisms.

Galois number fields are nice for Ring-LWE because we have a *search-to-decision reduction*.

First we give an improved attack based on some extra assumptions. Assume: there is a prime ideal $\mathfrak{q}$ over q such that

- $R/\mathfrak{q} \cong \mathbb{F}_{q^2}$.
- $e \mod \mathfrak{q}$ is more likely to lie in $\mathbb{F}_q$ than usual.

Then we can use cosets to improve the χ^2 attack. This reduces runtime from $O(q^4)$ to $O(q^2)$.

Coset improvement: idea

Fix a set of coset representatives $\{t_i\}$ of $\mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Assume $\pi(s) = s_0 + t_j$, with $s_0 \in \mathbb{F}_q$.

Coset improvement: idea

Fix a set of coset representatives $\{t_i\}$ of $\mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Assume $\pi(s) = s_0 + t_j$, with $s_0 \in \mathbb{F}_q$.

Algorithm:

For each i:

For each sample (a, b):

Compute

$$m_i(a, b) := \frac{\pi(b)^q - \pi(b) - (\pi(a)t_i)^q + \pi(a)t_i}{\pi(a)^q - \pi(a)}.$$

Run a statistical uniform test on the $m_i(a, b)$. If non-uniform, let s_0 be the element with highest frequency, and return $s_0 + t_i$.

Coset improvement: idea

Fix a set of coset representatives $\{t_i\}$ of $\mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Assume $\pi(s) = s_0 + t_j$, with $s_0 \in \mathbb{F}_q$.

Algorithm:

For each i:

For each sample (a, b):

Compute

$$m_i(a, b) := \frac{\pi(b)^q - \pi(b) - (\pi(a)t_i)^q + \pi(a)t_i}{\pi(a)^q - \pi(a)}.$$

Run a statistical uniform test on the $m_i(a, b)$. If non-uniform, let s_0 be the element with highest frequency, and return $s_0 + t_i$.

Why it works: If $i = j$, $m_j(a, b) = s_0$ happens with probability the same as the probability that $e \in \mathbb{F}_q$; otherwise the result is uniform.

Table: attacks in [CLS15] improved by using cosets

Table: Vulnerable instances under our improved attack

n	q	r_0	no. samples	old time (min)	new time (min)
40	67	2.51	22445	209	3.5
60	197	2.76	3940	63	2.4
60	617	2.76	12340	8.2×10^5 (est.)	21.3
80	67	2.51	3350	288.6	0.5
90	2003	3.13	60090	6.6×10^4 (est.)	305
96	521	2.76	15630	4.5×10^3 (est.)	21.7
100	683	2.76	20490	1.6×10^4(est.)	36.5
144	953	2.51	38120	342.6	114.5

Plan

1. Background: Ring-LWE
2. Improved attack using cosets
3. Infinite family of vulnerable instances (for narrow errors)
4. Impossibility of our attack for 2-power cyclotomic fields

Infinite family: a sketch

As another improvement to [CLS15], we construct an infinite family of vulnerable Galois number fields with moduli of residue degree 2.

Infinite family: a sketch

As another improvement to [CLS15], we construct an infinite family of vulnerable Galois number fields with moduli of residue degree 2.

Define the *relative error rate* as

$$r_0 = \frac{r}{|\Delta_K|^{\frac{1}{2n}}}.$$

Our family allows the relative error rate to grow to infinity.

Infinite family: a sketch

As another improvement to [CLS15], we construct an infinite family of vulnerable Galois number fields with moduli of residue degree 2.

Define the *relative error rate* as

$$r_0 = \frac{r}{|\Delta_K|^{\frac{1}{2n}}}.$$

Our family allows the relative error rate to grow to infinity.

Remark: independently, Castryck et al. constructed another infinite family, which is vulnerable to an *errorless LWE* attack as long as $r = O(|\Delta_K|^{\frac{1-\epsilon}{n}})$.

Infinite family: some details

The family of rings: take $R = \mathbb{Z}[\zeta_p, \sqrt{d}]$ where

Infinite family: some details

The family of rings: take $R = \mathbb{Z}[\zeta_p, \sqrt{d}]$ where

p : an odd prime.

d: an integer, such that d is coprime to p and $d \equiv 2, 3 \mod 4$.

Infinite family: some details

The family of rings: take $R = \mathbb{Z}[\zeta_p, \sqrt{d}]$ where

p : an odd prime.

d: an integer, such that d is coprime to p and $d \equiv 2, 3 \mod 4$.

Modulus: take q a prime such that

$$(1)\ q \text{ is one modulo } p, \text{ and } (2)\ d \text{ is not a square in } \mathbb{F}_q.$$

Infinite family: some details

The family of rings: take $R = \mathbb{Z}[\zeta_p, \sqrt{d}]$ where

p : an odd prime.

d: an integer, such that d is coprime to p and $d \equiv 2, 3 \mod 4$.

Modulus: take q a prime such that

$$(1)\ q \text{ is one modulo } p\text{, and } (2)\ d \text{ is not a square in } \mathbb{F}_q.$$

Reason for vulnerability: there is a nice basis for R where the shorter half basis elements reduce to the prime field $\mathbb{F}_q$, and the longer half are much longer.

Table of successful attacks

Table: New vulnerable Galois RLWE instances

p	d	q	r_0	no. samples	time (sec)
31	4967	311	8.94	3110	144.92
43	4871	173	8.97	1730	6.44
61	4643	367	8.84	3670	205.28
83	4903	167	8.94	1670	5.74
103	4951	619	8.94	6190	579.77
109	4919	1091	8.94	10910	1818.82
151	100447	907	14.08	9070	1394.18
181	100267	1087	14.11	10870	1973.47

Table of successful attacks

Table: New vulnerable Galois RLWE instances

p	d	q	r_0	no. samples	time (sec)
31	4967	311	8.94	3110	144.92
43	4871	173	8.97	1730	6.44
61	4643	367	8.84	3670	205.28
83	4903	167	8.94	1670	5.74
103	4951	619	8.94	6190	579.77
109	4919	1091	8.94	10910	1818.82
151	100447	907	14.08	9070	1394.18
181	100267	1087	14.11	10870	1973.47

Remark: interpreted in the classical RLWE setting in [LPR], our attack corresponds to $\chi =$ an elliptic Gaussian with the largest width $r = \Omega(\frac{1}{p^{1/2}d^{1/4}})$.

Plan

Impossibility of our attack on 2-power cyclotomic rings

Goal: we want to prove that our attack does **not** work for 2-power cyclotomic rings, even if the width r is very small.

Impossibility of our attack on 2-power cyclotomic rings

Goal: we want to prove that our attack does **not** work for 2-power cyclotomic rings, even if the width r is very small.

Set up:
m = a power of 2, $R = \mathbb{Z}[\zeta_m]$, and $n = m/2$, we choose q to be a prime which is 1 modulo m.

Impossibility of our attack on 2-power cyclotomic rings

Goal: we want to prove that our attack does **not** work for 2-power cyclotomic rings, even if the width r is very small.

Set up:
$m =$ a power of 2, $R = \mathbb{Z}[\zeta_m]$, and $n = m/2$, we choose q to be a prime which is 1 modulo m.

We approximate discrete Gaussians on R with

$$e = \sum_{i=0}^{n-1} e_i \zeta_m^i,$$

with each e_i sampled from a *shifted binomial distribution* $B(k, 1/2) - k/2$.

$e \mod \mathfrak{q}$ is close to uniform

Theorem

Let q, m be positive integers such that q is a prime, m is a power of 2, $q \equiv 1 \mod m$ and $q < m^2$. Let $\beta = \frac{1+\frac{\sqrt{q}}{m}}{2} \in (0,1)$. Then for any prime ideal $\mathfrak{q}$ above q, we have

$$\Delta(e \mod \mathfrak{q}, \textit{uniform}) \leq \frac{q-1}{2}\beta^{\frac{km}{4}}.$$

Table: statistical distances from uniform

Fixing $k = 2$ (roughly corresponds to $r = \sqrt{2\pi}/3$), we obtained ...

m ($n = m/2$)	q	$\log(\Delta(e \mod \mathfrak{q}, \text{uniform}))$
64	193	-40
128	1153	-97
256	3329	-194
512	10753	-431

Thank you!