Recovering the Secret on Binary Ring-LWE problem with Random Known Bits

Reynaldo C. Villena & Routo Terada
reynaldo@ime.usp.br rt@ime.usp.br

Institute of Mathematics and Statistics
University of São Paulo
SP – Brazil

September, 2023

Summary I

1. (Binary) Ring-LWE Problem
2. Side Channel Attacks
3. Recovering the secret **s**
4. Experiments and Conclusions

(Binary) Ring-LWE Problem

Ring-LWE

The Ring-LWE problem:

- Is assumed as hard [Regev 2009, Peikert 2009].
- Is promising, due to the provable security and high efficiency [Lindner and Peikert 2011, Regev 2009].

The Ring-LWE problem is used as the basis of:

- Public key encryption schemes [de Clercq et al. 2015, Lyubashevsky et al. 2013],
- Digital signatures [Barreto et al. 2016, Wu et al. 2012]
- Key Encapsulation Mechanisms (KEM) [Bos et al. 2015, Alkim et al. 2017],
- Homomorphic encryptions [Fan and Vercauteren 2012, Roy et al. 2016].

Ring-LWE

The Ring-LWE problem:

- Is assumed as hard [Regev 2009, Peikert 2009].
- Is promising, due to the provable security and high efficiency [Lindner and Peikert 2011, Regev 2009].

The Ring-LWE problem is used as the basis of:

- Public key encryption schemes [de Clercq et al. 2015, Lyubashevsky et al. 2013],
- Digital signatures [Barreto et al. 2016, Wu et al. 2012]
- Key Encapsulation Mechanisms (KEM) [Bos et al. 2015, Alkim et al. 2017],
- Homomorphic encryptions [Fan and Vercauteren 2012, Roy et al. 2016].

Internet of things (IoT) devices

Its implementation in software or hardware, specially in IoT devices, can be vulnerable to Side Channel Attacks [Fan and Vercauteren 2012, Aysu et al. 2018].

Ring-LWE problem

The Ring-LWE problem:

- The Ring-LWE problem fixes a power of two n and modulus q.
- Let $\mathbb{Z}_q$ be the residue class ring modulo q.
- Let $\mathcal{R}_q = \frac{\mathbb{Z}_q[x]}{(x^n+1)}$ denote the polynomial ring modulo $x^n + 1$ where the coefficients are in $\mathbb{Z}_q$.

For $\mathbf{s} \in \mathcal{R}_q$ called as secret, the Ring-LWE distribution $A_{n,q,\mathbf{s},\chi_\sigma^n}$ over $\mathcal{R}_q \times \mathcal{R}_q$ is sampled by choosing a parameter $\mathbf{a} \in \mathcal{R}_q$ uniformly at random, choosing a noise polynomial $\mathbf{e} \to \chi_\sigma^n$, and outputting $(\mathbf{a}, \mathbf{b} = \mathbf{a}.\mathrm{s} + \mathbf{e})$.

Ring-LWE Oracle:

A Ring-LWE oracle $\mathcal{A}^{\text{R-LWE}}_{n,q,\mathbf{s},\chi_\sigma^n}$ is an oracle with outputs independent random samples according to the $A_{n,q,\mathbf{s},\chi_\sigma^n}$ distribution.

Search Ring-LWE problem:

Given access to a Ring-LWE oracle $\mathcal{A}^{\text{R-LWE}}_{n,q,\mathbf{s},\chi_\sigma^n}$, find the vector $\mathbf{s}$.

Binary Ring-LWE problem

The Binary Ring-LWE problem:

- The Ring-LWE problem fixes a power of two n and modulus q.
- Let $\mathbb{Z}_q$ be the residue class ring modulo q.
- Let $\mathcal{R}_q = \frac{\mathbb{Z}_q[x]}{(x^n+1)}$ denote the polynomial ring modulo $x^n + 1$ where the coefficients are in $\mathbb{Z}_q$.

For $\mathbf{s} \in \{0,1\}^n$ called as secret, the Binary Ring-LWE distribution $A'_{n,q,\mathbf{s}}$ over $\mathcal{R}_q \times \mathcal{R}_q$ is sampled by choosing $\mathbf{a} \in \mathcal{R}_q$ uniformly at random, choosing $\mathbf{e} \to \{0,1\}^n$, and outputting $(\mathbf{a}, \mathbf{b} = \mathbf{a}.\mathbf{s} + \mathbf{e})$.

Binary Ring-LWE Oracle:

A Binary Ring-LWE oracle $\mathcal{A}^{\text{BR-LWE}}_{n,q,\mathbf{s}}$ is an oracle with outputs independent random samples according to the $A'_{n,q,\mathbf{s}}$ distribution.

Search Binary Ring-LWE problem:

Given access to a Binary Ring-LWE oracle $\mathcal{A}^{\text{BR-LWE}}_{n,q,\mathbf{s}}$, find the vector $\mathbf{s}$.

Side Channel Attacks

Side Channel Attacks

A Side Channel Attack (SCA) is any attack based on Side Channel Information that is obtained when protocols or schemes are executed. Some examples are:

- execution time
- power consumption
- electromagnetic leaks
- sound

and other information that is that is produced during the running process.

These Side Channel Information can be applied to retrieve (hints about) the values of some coefficients (bits) of the secret $\mathbf{s}$. [Aysu et al. 2018, Buchmann et al. 2016]

Applying the same concepts, the recovery of bits of noise polynomial $\mathbf{e}$ is feasible.

The recovery of some bits of $\mathbf{s}$ and $\mathbf{e}$ is feasible.

Recovering the secret $\mathbf{s}$

Recovering the secret $\mathbf{s}$

Let us define:

- $\mathbf{s}_u$ be the set of unknown coefficients in $\mathbf{s}$
- $\mathbf{s}_k$ be the set of known coefficients in $\mathbf{s}$
- $\mathbf{e}_u$ be the set of unknown coefficients in $\mathbf{e}$
- $\mathbf{e}_k$ be the set of known coefficients in $\mathbf{e}$

where $|\mathbf{s}_u| + |\mathbf{s}_k| = |\mathbf{s}| = n$ and $|\mathbf{e}_u| + |\mathbf{e}_k| = |\mathbf{e}| = n.$

Let α be the percentagem of known bits of $\mathbf{s}$ and $\mathbf{e}$:

$$\alpha = \frac{|\mathbf{e}_k| + |\mathbf{s}_k|}{|\mathbf{e}| + |\mathbf{s}|}$$

then

$$|\mathbf{e}_k| + |\mathbf{s}_k| = \alpha.2n$$

Recovering the secret s

We know that a Binary Ring-LWE sample $\mathbf{b} = \mathbf{a}.\mathbf{s} + \mathbf{e}$ can be written as matrix operations.

$$\begin{bmatrix} \mathbf{b}[0] \\ \mathbf{b}[1] \\ \vdots \\ \mathbf{b}[n-1] \end{bmatrix} = \begin{bmatrix} \mathbf{a}[0] & -\mathbf{a}[n-1] & \dots & -\mathbf{a}[1] \\ \mathbf{a}[1] & \mathbf{a}[0] & \dots & -\mathbf{a}[2] \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}[n-1] & \mathbf{a}[n-2] & \dots & \mathbf{a}[0] \end{bmatrix} \begin{bmatrix} \mathbf{s}[0] \\ \mathbf{s}[1] \\ \vdots \\ \mathbf{s}[n-1] \end{bmatrix} + \begin{bmatrix} \mathbf{e}[0] \\ \mathbf{e}[1] \\ \vdots \\ \mathbf{e}[n-1] \end{bmatrix}$$

Each $\mathbf{b}[i]$ can be expressed as an equation

$$\mathbf{b}[i] = \sum_{j=0}^{i} \mathbf{a}[i-j].\mathbf{s}[j] - \sum_{j=i+1}^{n-1} \mathbf{a}[j].\mathbf{s}[n+i-j] + \mathbf{e}[i] \qquad \text{for } 0 \leq i \leq n-1. \qquad (1)$$

It results in n equations with $2n$ variables (bits of $\mathbf{s}$ and $\mathbf{e}$) that results hard to solve. However, some bits of $\mathbf{s}$ and $\mathbf{e}$ are known.

Recovering the secret $\mathbf{s}$

One condition to have the solution of a system of equations is that the number of variables must be lower than or equal to the number of equations:

$$\begin{aligned} |\mathbf{e}_u| + |\mathbf{s}_u| &\leq n \\ |\mathbf{e}_u| &\leq |\mathbf{s}_k| \qquad\qquad \text{because } |\mathbf{s}_k| + |\mathbf{s}_u| = n, \end{aligned}$$

Recovering the secret $\mathbf{s}$

One condition to have the solution of a system of equations is that the number of variables must be lower than or equal to the number of equations:

$$\begin{aligned} |\mathbf{e}_u| + |\mathbf{s}_u| &\leq n \\ |\mathbf{e}_u| &\leq |\mathbf{s}_k| \qquad\qquad \text{because } |\mathbf{s}_k| + |\mathbf{s}_u| = n¸ \end{aligned}$$

The above condition is always accomplished since we can set $|\mathbf{e}_u| = 0$.

Recovering the secret $\mathbf{s}$

One condition to have the solution of a system of equations is that the number of variables must be lower than or equal to the number of equations:

$$\begin{aligned} |\mathbf{e}_u| + |\mathbf{s}_u| &\leq n \\ |\mathbf{e}_u| &\leq |\mathbf{s}_k| \qquad\qquad \text{because } |\mathbf{s}_k| + |\mathbf{s}_u| = n, \end{aligned}$$

The above condition is always accomplished since we can set $|\mathbf{e}_u| = 0$.
One way to get $|\mathbf{e}_u| = 0$ is discarding all equations in Equations (1) where the value of $\mathbf{e}[i]$ is unknown,

$$\mathbf{b}[i] = \sum_{j=0}^{i} \mathbf{a}[i-j].\mathbf{s}[j] - \sum_{j=i+1}^{n-1} \mathbf{a}[j].\mathbf{s}[n+i-j] + \mathbf{e}[i] \qquad \text{if } \mathbf{e}[i] \text{ is known}$$

resulting in $|\mathbf{e}_k|$ equations and $|\mathbf{s}_u|$ variables. This new system of equations needs $|\mathbf{e}_k| \geq |\mathbf{s}_u|$ to be solved.

Recovering the secret $\mathbf{s}$

We need $|\mathbf{e}_k| \geq |\mathbf{s}_u|$.

$$\begin{aligned} |\mathbf{e}_k| + |\mathbf{s}_k| + \geq |\mathbf{s}_u| + |\mathbf{s}_k| & \qquad \text{because } |\mathbf{e}_k| \geq |\mathbf{s}_u| \\ |\mathbf{e}_k| + |\mathbf{s}_k| \geq n & \qquad \text{because } |\mathbf{s}_k| + |\mathbf{s}_u| = n \\ \alpha.2n \geq n & \qquad \text{because } |\mathbf{s}_k| + |\mathbf{e}_k| = \alpha.2n \\ \alpha \geq \frac{1}{2} & \end{aligned}$$

Recovering the secret s

We need $|\mathbf{e}_k| \geq |\mathbf{s}_u|$.

$$\begin{aligned} |\mathbf{e}_k| + |\mathbf{s}_k| + \geq |\mathbf{s}_u| + |\mathbf{s}_k| && \text{because } |\mathbf{e}_k| \geq |\mathbf{s}_u| \\ |\mathbf{e}_k| + |\mathbf{s}_k| \geq n && \text{because } |\mathbf{s}_k| + |\mathbf{s}_u| = n \\ \alpha.2n \geq n && \text{because } |\mathbf{s}_k| + |\mathbf{e}_k| = \alpha.2n \\ \alpha \geq \frac{1}{2} && \end{aligned}$$

In other words, we need at least 50 % of bits of **s** and **e** to retrieve all unknown bits of **s**, allowing us to know the actual value of the secret **s**.

Experiments and Conclusions

Experiments

Experiments:

- An algorithm was implemented in 20 lines of code using sageMath. This algorithm contains the Gaussian Elimination method to solve equations.
- It was executed on a processor Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz with 3 Mb of cache and 8 GB of DDR4 Memory.

Our experiments

- we work with parameters $n = 256, q = 256$ (parameters defined in [Aysu et al. 2018]) and $\alpha \in [49, 60]$.
- For each value of α, 100 public keys $\langle \mathbf{b}, \mathbf{a} \rangle$ were generated and for each public key, 100 samples were generated with α percentage of random known bits of $\mathbf{s}$ and $\mathbf{e}$. In total, 120000 experiments were executed.
- For all experiments, the method Gaussian Elimination was applied and the unknown bits of the secret $\mathbf{s}$ were successfully retrieved since $\alpha \geq 50\%$.
- Each experiment takes at most 6 seconds.

Conclusions

- The recovery of coefficients of the noise polynomial **e** makes the (Binary) Ring-LWE problem weaker.
- We need at least 50 % of random known bits of **s** and **e** to retrieve the actual value of the secret **s**.

References I

- Alkim, E., Avanzi, R. M., Bos, J. W., Ducas, L., de la Piedra, A., Pöppelmann, T., and Schwabe, P. (2017).
  Newhope algorithm specifications and supporting documentation.

- Aysu, A., Orshansky, M., and Tiwari, M. (2018).
  Binary ring-lwe hardware with power side-channel countermeasures.
  In 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), pages 1253–1258. IEEE.

- Barreto, P. S., Longa, P., Naehrig, M., Ricardini, J. E., and Zanon, G. (2016).
  Sharper ring-lwe signatures.
  Cryptology ePrint Archive.

- Bos, J. W., Costello, C., Naehrig, M., and Stebila, D. (2015).
  Post-quantum key exchange for the tls protocol from the ring learning with errors problem.
  In 2015 IEEE Symposium on Security and Privacy, pages 553–570. IEEE.

- Buchmann, J., Göpfert, F., Güneysu, T., Oder, T., and Pöppelmann, T. (2016).
  High-performance and lightweight lattice-based public-key encryption.
  In Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security, pages 2–9.

References II

de Clercq, R., Roy, S. S., Vercauteren, F., and Verbauwhede, I. (2015).
Efficient software implementation of ring-lwe encryption.
In Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, DATE '15, page 339–344, San Jose, CA, USA. EDA Consortium.

Fan, J. and Vercauteren, F. (2012).
Somewhat practical fully homomorphic encryption.
Cryptology ePrint Archive.

Lindner, R. and Peikert, C. (2011).
Better key sizes (and attacks) for lwe-based encryption.
In Kiayias, A., editor, Topics in Cryptology – CT-RSA 2011, pages 319–339, Berlin, Heidelberg. Springer Berlin Heidelberg.

Lyubashevsky, V., Peikert, C., and Regev, O. (2013).
On ideal lattices and learning with errors over rings.
J. ACM, 60(6).

References III

Peikert, C. (2009).
Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract.
In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, STOC '09, page 333–342, New York, NY, USA. Association for Computing Machinery.

Regev, O. (2009).
On lattices, learning with errors, random linear codes, and cryptography.
volume 56, New York, NY, USA. Association for Computing Machinery.

Roy, S. S., Karmakar, A., and Verbauwhede, I. (2016).
Ring-lwe: applications to cryptography and their efficient realization.
In International conference on security, privacy, and applied cryptography engineering, pages 323–331. Springer.

Wu, Y., Huang, Z., Zhang, J., and Wen, Q. (2012).
A lattice-based digital signature from the ring-lwe.
In 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content, pages 646–651.