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

(Binary) Ring-LWE Problem

Ring-LWE

The Ring-LWE problem:

- Is assumed as hard [Reg09, Pei09].
- Is promising, due to the provable security and high efficiency [LP11, Reg09].

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

- Public key encryption schemes [dCRVV15, LPR13],
- Digital signatures [BLN+16, WHZW12]
- Key Encapsulation Mechanisms (KEM) [BCNS15, AAB+17],
- Homomorphic encryptions [FV12, RKV16].

Internet of things (IoT) devices

Its implementation in software or hardware, specially in IoT devices, can be vulnerable to Side Channel Attacks [FV12, AOT18].

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 $\mathbf{a} \in \mathcal{R}_q$ uniformly at random, choosing $\mathbf{e} \rightarrow \chi_\sigma^n$, and outputting $(\mathbf{a}, \mathbf{b} = \mathbf{a}.\mathbf{s} + \mathbf{e})$.

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 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 $\mathbf{e} \rightarrow \{0,1\}^n$, 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 $\mathbf{s}$ [AOT18, BGG+16]

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

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

Recovering the secret s

Recovering the secret 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 $\mathbf{e}$:

$$\alpha = \frac{|\mathbf{e}_k| + |\mathbf{s}_k|}{|\mathbf{e}| + |\mathbf{s}|} \tag{1}$$

Recovering the secret s

We know that a Binary Ring-LWE instance $\mathbf{b} = \mathbf{a}.\mathbf{s} + \mathbf{e}$ 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 a system of equations

$$\mathbf{b}[i] = \sum_{j=0}^{i} \mathbf{a}[i-j].\mathbf{s}[j] - \sum_{j=i+1}^{n-1} \mathbf{a}[j].\mathbf{s}[n+i-j] + \mathbf{e}[i] \qquad \text{for } 0 \leq i \leq n-1 \qquad (2)$$

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

Recovering the secret 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:

$$|\mathbf{e}_u| + |\mathbf{s}_u| \leq n$$

$$|\mathbf{e}_u| \leq |\mathbf{s}_k| \qquad \text{because } |\mathbf{s}_k| + |\mathbf{s}_u| = n$$

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 (2) 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 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 [AOT18]) 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, 120009 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

- Our result was proved mathematically and experimentally where we need at least 50 % of random known bits of **s** and **e** to retrieve the actual value of the secret **s**.
- the hardness of the (Binary) Ring-LWE problem is to find **s**. There are some works focused on the protection of the secret **s** [AOT18] and the polynomial **e** is left out since **e** is only used one time (commonly in the KEYGEN process). We must be more careful with the noise polynomial **e** because the recovery of its coefficient makes the (Binary) Ring-LWE problem weaker.

References I

Erdem Alkim, Roberto Maria Avanzi, Joppe W. Bos, Léo Ducas, Antonio de la Piedra, Thomas Pöppelmann, and Peter Schwabe, Newhope algorithm specifications and supporting documentation, 2017.

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

Joppe W Bos, Craig Costello, Michael Naehrig, and Douglas Stebila, Post-quantum key exchange for the tls protocol from the ring learning with errors problem, 2015 IEEE Symposium on Security and Privacy, IEEE, 2015, pp. 553–570.

Johannes Buchmann, Florian Göpfert, Tim Güneysu, Tobias Oder, and Thomas Pöppelmann, High-performance and lightweight lattice-based public-key encryption, Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security, 2016, pp. 2–9.

Paulo SLM Barreto, Patrick Longa, Michael Naehrig, Jefferson E Ricardini, and Gustavo Zanon, Sharper ring-lwe signatures, Cryptology ePrint Archive (2016).

References II

- Ruan de Clercq, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede, Efficient software implementation of ring-lwe encryption, Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition (San Jose, CA, USA), DATE '15, EDA Consortium, 2015, p. 339–344.
- Junfeng Fan and Frederik Vercauteren, Somewhat practical fully homomorphic encryption, Cryptology ePrint Archive (2012).
- Richard Lindner and Chris Peikert, Better key sizes (and attacks) for lwe-based encryption, Topics in Cryptology – CT-RSA 2011 (Berlin, Heidelberg) (Aggelos Kiayias, ed.), Springer Berlin Heidelberg, 2011, pp. 319–339.
- Vadim Lyubashevsky, Chris Peikert, and Oded Regev, On ideal lattices and learning with errors over rings, J. ACM **60** (2013), no. 6.
- Chris Peikert, Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract, Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '09, Association for Computing Machinery, 2009, p. 333–342.

References III

- Oded Regev, On lattices, learning with errors, random linear codes, and cryptography, vol. 56, Association for Computing Machinery, sep 2009.
- Sujoy Sinha Roy, Angshuman Karmakar, and Ingrid Verbauwhede, Ring-lwe: applications to cryptography and their efficient realization, International conference on security, privacy, and applied cryptography engineering, Springer, 2016, pp. 323–331.
- Yanfang Wu, Zheng Huang, Jie Zhang, and Qiaoyan Wen, A lattice-based digital signature from the ring-lwe, 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content, 2012, pp. 646–651.