Compact Public-Key Encryption Using Learning with Rounding

Anupama Arjun Pandit and Arun Mishra

Abstract Data gathering from IoT devices could be the target of cyberattack in the Internet of things (IoT) systems that utilize data from the real world. Because of this, encryption-based defenses are becoming increasingly important. Compact public-key encryption (PKE) scheme provides encryption with minimum key size and low-computational complexity. Its goal is to broaden cryptography's uses on constrained devices. Therefore, in this paper, we proposed a lattice-based PKE scheme that is based on learning with rounding (LWR) problems. It is a derandomized version of learning with errors (LWE). In LWE, errors are introduced explicitly to mask their true value, whereas in LWR, errors are introduced implicitly by eliminating the least significant bits after performing the rounding operations. Rounding operation for number r could be defined as $\lfloor r \rceil$. Since this approach compresses the key size as compared to the learning with errors scheme. Therefore, it reduces bandwidth requirement for key exchange and increases the transmission speed.

Keywords Learning with errors · Learning with rounding · Post-quantum cryptography · Lattice-based cryptography · Public-key encryption

1 Introduction

The construction such as the public-key encryption (PKE) scheme and public-key infrastructure (PKI) is based on the hard problems of lattice such as shortest vector problem (SVP) [13] or closest vector problem (CVP) [14] has the possibility to replace the current construction techniques that are based on the assumed hardness of classical theoretic problems such as large integer factorization problem and discrete logarithm problem [21]. Classical cryptographic encryption schemes will not be secure in the quantum era since it is reliant on the huge integer factorization

A. A. Pandit (✉) · A. Mishra
Computer Science and Engineering, Defence Institute of Advanced Technology, Pune, India
e-mail: anupamapandit91@gmail.com

A. Mishra
e-mail: arunmishra@diat.ac.in

M. Tuba et al. (eds.), *ICT Systems and Sustainability*, Lecture Notes in Networks and Systems 516, https://doi.org/10.1007/978-981-19-5221-0_75

problems, which conventional computers cannot accomplish in polynomial time. This encryption scheme will not be quantum-safe since quantum algorithms like the Shor's algorithm [20] and Grover's algorithm [10] can solve these problems in polynomial time.

Lattice-based cryptography has drawn a huge interest in the theoretical world because the construction of cryptographic models was supported with security assurances based on the worst-case hardness of lattice problems [1]. Ajtai and Dwork [2] introduced the first lattice-based encryption algorithm. Regev further simplified and improved this approach in [16]. Regev's research was notable for introducing the intermediate problem, the Learning with errors (LWE) problem [17], that was reasonably easy to utilize in crypto constructs and at least as asymptotically difficult as the conventional lattice-based worst-case problems [9].

Banerjee et al. [5] presented the LWR problem. Independently, randomly generated error from LWE is substituted with a deterministic error by rounding as to a lower modulus p in the LWR problem [7]. LWR [4] offers the following benefits over LWE: It necessitates the development of less randomization since it is not required to generate the error component.

Our contribution: Compact public-key encryption using learning with rounding has been presented in this work. Proposed work has been devided into three parts which are as key generation, encryption, and decryption. The key generation function is getting compact by applying the rounding operation. Also this scheme uses number theoretic transform (NTT) [19] and Montgomery modulus reduction to speedup the multiplication and modulus operation.

2 Literature Review

Regev [18] devised a public-key encryption (RegPKE) approach with the formulation of the LWE problem as well as the justification of the LWE relevance to lattice-based worst-case problems, which is still a foundation for current lattice-based cryptographic schemes. The following is its definition [3], which uses a more reduced matrix syntax.

Definition

For the public-key encryption scheme RegPKE = (RegGen, RegEnc, RegDec), let m, n, χ, and q are the parameters of the scheme, where n is the dimension of the lattice, q is a prime. All additions are performed over $\mathbb{Z}_q$.

- In RegPKE, the key generation function selects $\boldsymbol{A}$ matrix uniformly random from $\mathbb{Z}_q^{m \times n}$ and short vector, i.e., secret $\boldsymbol{s}$ chosen randomly from $\mathbb{Z}_q^n$. Selects error vector $\boldsymbol{e} < q/4$ independently from Gaussian distribution. The output sk (private keys) = $\boldsymbol{s}$ and pk(public key) = $(\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e})$.
- Encryption function selects m dimensional random vector $\boldsymbol{r}$ and encrypts message bit μ. The output of the fuction is u and u', where $u = \mathbf{A}\mathbf{r}$ and $u' = \boldsymbol{b}\boldsymbol{r} + \mu\lfloor q/2 \rceil$.

- The decryption fuction calculates $\mu' = u' - u \cdot s$. As error is less than $q/4$, check value of μ' if it is less than $q/4$, then decrypted value would be zero, else it would be one.

Lindner and Peikert encryption scheme [15]: In comparison with RegPKE, key sizes in Lindner and Peikert's encryption scheme are up till ten folds lesser [11] although providing a higher bit-security level, in which they conform to the parameters stated in [12]. The much more effective LWE-based public-key encryption strategy is the Lindner and Peikert's encryption technique, which is described as below.

Let m, χ, and q be parameters of the scheme and publically shared matrix $\mathbf{A}$ chosen uniformly random from $\mathbb{Z}_q^{m \times m}$.

- Key generation function, samples $\boldsymbol{e}$ and secret key $\boldsymbol{s}$ from χ distribution, and generate public key $\boldsymbol{p}$ is $\boldsymbol{As} + \boldsymbol{e}$.
- Lindner and Peikert's encryption function inputs the message $\mu \in 0, 1$ and public key $\boldsymbol{p}$. To encrypt message μ fuction samples vectors $\boldsymbol{s}'$, and error_1 with length m according to the distribution. Samples $\text{error}_2 \in \chi(\mathbb{Z})$. Computes $\boldsymbol{p}' =< \boldsymbol{s}', \boldsymbol{A} > + \text{error}_1$,
  $en_1 =< \boldsymbol{s}', \boldsymbol{p}' > + \text{error}_2$,
  $en_2 \leftarrow \text{encode}(\mu) + en_1$,
  return $c \leftarrow (\boldsymbol{p}', en_2)$
- Decryption function outputs the decoded value of $(en_2 - v) : v \leftarrow < \boldsymbol{p}', \boldsymbol{s} >$.

As of now, there is no algorithm exists, classical as well as quantum, which could break the lattice-based LWE algorithm in polynomial time. Therefore, LWE is quantum safe [17].

3 Preliminaries

3.1 Notations

In this paper, vectors are indicated by small case bold alphabets, and matrices are represented by capital bold alphabets.The rings $R = \mathbb{Z}[X]/(X^n + 1)$ and $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ are written as R and R_q, respectively, in which q and n be integers, and n is almost always 256. The standard dot product of two vectors is indicated by $< , >$. The sample x based on the distribution D is indicated by $x \leftarrow D$. Where D is a finite set, it represents uniform sampling. The rounding of real number r is represented by $\lfloor r \rceil$.

3.2 Post-quantum Cryptography

Quantum-resistant or quantum-safe cryptography is another name for post-quantum cryptography (PQC) [6]. The aim of PQC is to develop secure system against classical as well as quantum computers and could work with existing network infrastructure setup and protocols. The family of PQC comprises:

- Code-based cryptography
- Hash-based cryptography
- Multivariate quadratic cryptography
- Isogenies cryptography
- Lattice-based cryptography.

3.3 Lattice-Based Cryptography

Cryptographic constructions based on lattices are quantum safe as it uses very complex large dimensional geometric structures. The security of a lattice-based cryptosystem relies on the hardness of lattice problems. LWE [17] and LWR [5] are the most advanced lattice-based cryptosystems. The variant of LWE is ring LWE (RLWE). The decision LWE problem and LWR problem are the efficient primitives for lattice-based encryptions.

3.4 LWE Problem

LWE problem [18]: If the following distributions are (η, ϵ) indistinguishable, LWE problem would be (η, m, ϵ) hard:

- Arbitrary chosen sample $s \in \mathbb{Z}_r^n$ and output m pairs $(a_i, b_i) \in \mathbb{Z}_r^n \times \mathbb{Z}_r$, where $a_i's$ are independent and uniformly random $b_i =< a_i, s > + e \mod r$ for small random error e_i.
- Output m is independent and uniform pairs $(a_i, b_i) \in \mathbb{Z}_r^n \times \mathbb{Z}_p$.

Small error $e_i \in \mathbb{Z}$ is $\approx \alpha r$. If the hardness parameter is dimension n and error rate is α then as long as αr exceeds $\sqrt{n}$, LWE would be hard in worst case.

3.5 LWR Problem

LWR Problem [4]: The derandomised version of LWE is called LWR. In LWR, a slight error with $\boldsymbol{A} \cdot \boldsymbol{s} \in \mathbb{Z}_q$ may be used to mask their true value, which would be

multiplied by p/q for some $p < q$. If $q > p$ and $\boldsymbol{A} \cdot \boldsymbol{s}$ is a deterministic rounded version, the LWR problem would be hard. As a result, in this example, $\boldsymbol{b} = \lfloor \boldsymbol{A} \cdot \boldsymbol{s} \rceil = \lfloor p/q \cdot \boldsymbol{A} \cdot \boldsymbol{s} \rceil p$.

For the implementation aspect, we usually take the floor of this value. We are decreasing the result from mod q to mod p in this case. Other operations, such as encryption and decryption, will stay unchanged. LWR is at least as hard as LWE for the relevant parameters, and it provides a worst-case assurance for LWR [5]. It is claimed that the hardness of LWR [4] increases with a decrease in the ratio q/p. The advantage of LWR is that it eliminates the heavy error sampling process such as Gaussian error distribution.

4 Proposed Scheme

Most of the lattice-based public-key cryptography involve heavy computation in Gaussian sampling to sample errors for LWE and polynomial multiplication under ring. To achieve compact nature in lattice-based primitive, we use learning with rounding (LWR) problem instead of LWE. This removes one of the major computation costs of sampling errors in Gaussian distribution without affecting the security of the scheme.

The parameter for the proposed scheme is m, n, p, and q, where n represents lattice's dimension, m represents the no. of random independent uniform vectors, q and p are prime modulus, and prime rounding modulus, respectively, such that $p < q$. The following encryption scheme would be hard if $m > n \log q$.

A single bit LWR encryption scheme is as follows:

- Key_Generation (input_seed):
  - Sample secret key $sk \leftarrow \mathbb{Z}_q^n$
  - Sample $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$
  - Compute public key pk: $(\boldsymbol{A}, b = \lfloor \boldsymbol{A} \cdot \boldsymbol{s} \rceil p)$ where p is a rounding modulus $p < q$
  - return(sk, pk)
- Encryption(message_bit, pk):
  - Sample $x \leftarrow \mathbb{Z}_q^n$
  - Compute cipher $c = b \cdot \boldsymbol{x} +$ message_bit $\cdot (q/2)$
  - Compute cipher preamble $u = \boldsymbol{A}\boldsymbol{x}$
  - return(c, u)
- Decryption(c, u, sk):
  - Compute $c' = c - u \cdot sk$
  - If the coefficients of c' are in range $\left[-\frac{q}{4}, \frac{q}{4}\right]$, then message_bit would be 0 otherwise it would be 1.

The proposed scheme is also highly efficient since it is built on lattice-based cryptography, which is effective in the post-quantum era and consists of security proofs relies on worst-case hardness. It is also thought to be quantum-resistant as no attack on lattice-based encryption has been discovered to yet.

5 Implementation and Result

SHAKE-256 [8] is utilized in the implementation to supply a 256-bit initial value to the LWR key generation function, which generates the encryption keys. The encryption function will utilize this key to encrypt the input bit into the cipher vector as shown in the Sect. 4. This scheme chose the number theoretic transform (NTT) [19] for fast multiplication since it conducts point-wise multiplication of integer numbers and to speedup the modulus operation, the Montgomery modulus reduction approach is employed as it transforms modulus operation into a shift operation.

The scheme has been implemented in C language using Visual Studio 2019 IDE on Windows 10 operating system. Figure 1 is a snapshot of the encrypted result of the input bit '0' for the proposed LWR-based algorithm.

Figure 2 shows the snapshot of the decrypted output, which is the same as the original bit. The decrypted bit is representing by 256 values as proposed approach is using a polynomial with 256 coefficients. The single bit encryption is simply showing the working process of LWR encryption scheme.

For the multi-bit encryption needs to compute cipher c_i as follows:

$$c_i = \left(\sum_{i=1}^{256} b_i \cdot x_i + \text{message\_bit}_i * \frac{q}{2} \right) \mod q.$$

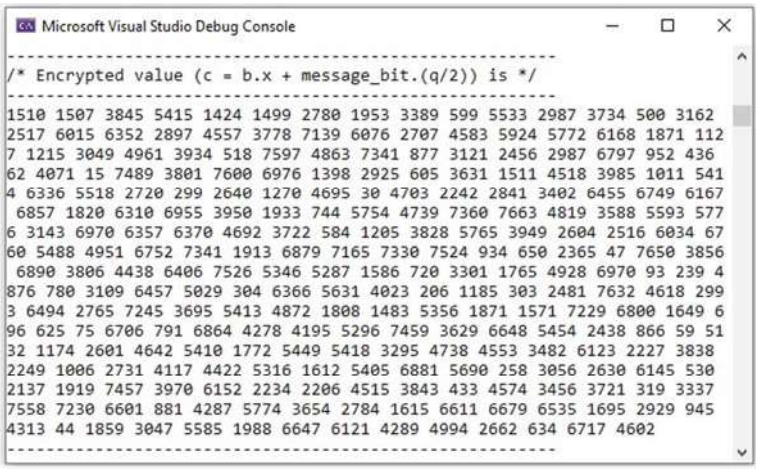

Fig. 1 Encrypted result of single bit

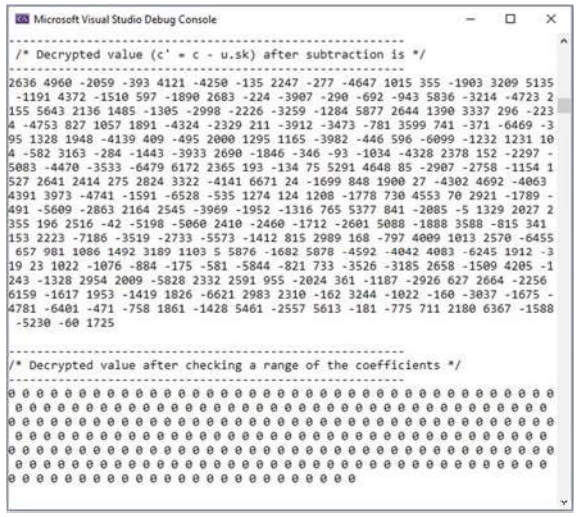

Fig. 2 Decrypted result of single bit

Now, the above approach would be capable to encrypt message_bit$_i$ into c_i. Hence, it will produce plain text → cipher text → decrypted/plain text would be of same length.

6 Conclusion

In this paper, we have discussed the LWE-based encryption schemes and proposed compact public-key encryption using learning with rounding. It has been found that all these schemes are cryptographically secure, but the proposed scheme is more compact than LWE-based schemes. The advantage of LWR is that it eliminates the heavy error sampling process. Proposed scheme is also quantum safe as there is no quantum algorithm exists which could break the LWR problem in polynomial time.

References

1. Ajtai M (1996) Generating hard instances of lattice problems. In: Proceedings of the annual ACM symposium on theory of computing, part F129452, pp 99–108. https://doi.org/10.1145/237814.237838
2. Ajtai M, Dwork C (1997) Public-key cryptosystem with worst-case/average-case equivalence. In: Conference proceedings of the annual ACM symposium on theory of computing, pp 284–293. https://doi.org/10.1145/258533.258604
3. Akavia A, Goldwasser S, Vaikuntanathan V (2009) Simultaneous hardcore bits and cryptography against memory attacks. In: Theory of cryptography conference. LNCS, vol 5444, pp 474–495. https://doi.org/10.1007/978-3-642-00457-5_28

4. Alwen J, Krenn S, Pietrzak K, Wichs D (2013) Learning with rounding, revisited: new reduction, properties and applications. In: Annual cryptology conference. LNCS, vol 8042(PART 1), pp 57–74. https://doi.org/10.1007/978-3-642-40041-4_4
5. Banerjee A, Peikert C, Rosen A (2012) Pseudorandom functions and lattices. In: Annual international conference on the theory and applications of cryptographic techniques. LNCS, vol 7237, pp 719-737. https://doi.org/10.1007/978-3-642-29011-4_42
6. Bernstein DJ, Johannes B, Dahmen E (2009) In: Bernstein DJ, Johannes B, Dahmen E (eds) Post-quantum cryptography. Springer, Berlin. https://doi.org/10.1007/978-3-540-88702-7
7. Brakerski Z, Langlois A, Peikert C, Regev O, Stehlé D (2013) Classical hardness of learning with errors. In: Proceedings of the annual ACM symposium on theory of computing, pp 575–584. https://doi.org/10.1145/2488608.2488680
8. Dworkin MJ (2015) SHA-3 standard: permutation-based hash and extendable-output functions. https://doi.org/10.6028/NIST.FIPS.202
9. Gentry C, Peikert C, Vaikuntanathan V (2008) Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the annual ACM symposium on theory of computing, pp 197–206. https://doi.org/10.1145/1374376.1374407
10. Grover LK (1996) A fast quantum mechanical algorithm for database search. In: Proceedings of the annual ACM symposium on theory of computing, part F1294, pp 212–219. https://doi.org/10.1145/237814.237866
11. Lindner R, Peikert C (2011) Better key sizes (and attacks) for LWE-based encryption. In: Cryptographers' track at the RSA conference, pp 319–339. https://doi.org/10.1007/978-3-642-19074-2_21
12. Micciancio D, Regev O (2008) Lattice-based cryptography. In: Post-quantum cryptography. Springer. https://link.springer.com/chapter/10.1007/978-3-540-88702-7_5
13. Micciancio D (n.d.) Shortest vector problem. Retrieved 16 Dec 2021, from http://turing.wins.uva.nl/peter/
14. Micciancio D, Goldwasser S (2002) Closest vector problem. In: Complexity of lattice problems, pp 45–68. https://doi.org/10.1007/978-1-4615-0897-7_3
15. Peikert C (2009) Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the annual ACM symposium on theory of computing, pp 333–342. https://doi.org/10.1145/1536414.1536461
16. Regev O (2003) New lattice based cryptographic constructions. J ACM 51(6):899–942. https://doi.org/10.1145/1039488.1039490
17. Regev O (2010) The learning with errors problem. In: Proceedings of the annual IEEE conference on computational complexity, vol 3(015848), pp 191–204. https://doi.org/10.1109/CCC.2010.26
18. Regev O (2005) On lattices, learning with errors, random linear codes, and cryptography. In: STOC'05, vol 56(6). https://doi.org/10.1145/1568318.1568324
19. Scott M (2017) A note on the implementation of the number theoretic transform. In: IMA international conference on cryptography and coding. LNCS, vol 10655, pp 247–258. https://doi.org/10.1007/978-3-319-71045-7_13
20. Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput 26(5):1484–1509. https://doi.org/10.1137/S0097539795293172
21. Yan SY (2017) Integer factorization based cryptography. In: Computational number theory and modern cryptography, pp 293–336. https://doi.org/10.1002/9781118188606.CH7