**A Practical Public Key Encryption Scheme Based on Learning Parity with Noise**

**Abstract:**

 To protect cyber security and privacy, it is critical to design security and practical public key encryption schemes. Today, big data and cloud computing bring not only unprecedented opportunities but also fundamental security challenges. Big data faces many security risks in the collection, storage and use of data and brings serious problems regarding the disclosure of private user data. It is challenging to achieve security and privacy protection in the big data environment. Thus, to meet the growing demand of public key encryption in this environment, we proposed a single-bit public key encryption scheme based on a variant of LPN (Learning Parity with Noise) and extended it to a multi-bit public key encryption scheme. We proved the correctness and CPA (Chosen Plaintext Attack) security of the proposed method. Our schemes solved encoding error rate problems of the existing public key schemes based on LPN, and the encoding error rate in our schemes is negligible.

**Architecture:**



**Introduction:**

 With the development and application of big data and cloud computing technology, the large data environment has put forward higher requirements for data encryption, and the design of a practical and secure public key encryption scheme has important practical significance. Considering data security in the big data environment, many valuable schemes have been put forward. They have been shown to be useful in applications such as protecting the privacy in machine learning, and protecting security in cloud computing. The main classical public key schemes were designed based on a number of difficult number theory problems, such as large number factorization and discrete logarithms. However, many traditional number theory assumptions on which the above schemes are based can be solved by quantum algorithms. That is, in the era of quantum computing, these public key encryption schemes have been broken. Therefore, in the post quantum era, new public key encryption schemes based on new difficult problems need to be designed and implemented for the new computing environments and applications.

**Exciting System:**

The creation and calculation of LPN instances are very simple, but it is very difficult to solve the DLPN problem. Therefore, it is very attractive to design cryptographic applications based on LPN. The LPN problem has been widely used in symmetric encryption but there has been little progress in the design of the public key scheme. Alekhnovich proposed a public-key encryption scheme based on a decisional LPN problem Subsequently, proposed not only a public key encryption scheme based on decisional LPN problem but also a public-key encryption scheme based on a ring-LPN problem. Damgård et al. proved the security of these schemes. Meanwhile, these schemes are practical. compared some practical public key encryption algorithms such as RSA for computational efficiency, public key size and ciphertext. Although the RSA algorithm does not have an anti-quantum However, non-negligible encoding error exists in all existing public key schemes based on an LPN variant. To solve this problem, we designed a new public-key encryption scheme. First, our issue will extend the LPN variant to a matrix LPN problem, and a new public key encryption scheme will be proposed based on an LPN variant. There are two advantages to the proposed scheme. First, we maintain the largest advantages of LPN, which are rapid instance generation, and rapid and efficient encryption and decryption computing; second, we solve the encoding error problem of existing public key encryption schemes.

**Proposed System:**

 In the post quantum era, the design of public key cryptography under the DLPN assumption is an important research direction. Such schemes have many advantages such as shorter public key and ciphertext, faster encryption and decryption. But the existing scheme is still having the problem of decryption error, which is not satisfactory. Based on the LPN variants problem, we proposed a single-bit and a multi-bit public key encryption scheme. Our scheme solved the decryption error problem of the existing public key encryption schemes based on DLPN. Compared to existing schemes, there is an increase in only a small amount of ciphertext space and computing overhead in our scheme. Our scheme not only is able to withstand quantum attack but also provides strong practical security at the same time. In the future, we will design a public key scheme based DLPN with high security, smaller public key and ciphertext size, and smaller computational overhead. Furthermore, designing public key cryptography that satisfies CCA security is also one of our future work.

**Modules:**

**Performance Analysis:**

Therefore, the multiplication and addition have the same overhead. Thus, the computational times in the table are the sum of the multiplication and addition results. Our scheme has the same public key size as in the Damgård scheme. Although our scheme increases slightly in ciphertext size and computational overhead, the decryption error can be negligible.

**Decisional LPN Problem:**

If the attacker can distinguish between a new sample (A,AS) and $ 2 (A,R) with non-negligible probability after obtaining enough samples; then, the attacker is able to solve the decisional LPN (DLPN) problem. Definition 2 (Decisional LPN Assumption) The probability of any probabilistic polynomial time (PPT) attacker to solve the decisional LPN problem with parameters is negligible.

**Single-Bit Public Key Encryption Scheme:**

In this section, we first give a single-bit public key encryption scheme based DLPN, and then we prove the correctness and security of the scheme. Second, we extend a single-bit scheme to the multi-bit public key encryption scheme and prove its correctness and security.

**Multi-Bit Public key Encryption Scheme:**

In our single-bit and multi-bit schemes, even if we choose a larger parameter 1/ n , it can also ensure that the decryption error can be ignored. Therefore, under the promise of security, the size of the public key is smaller than in Damgård’s scheme. Meanwhile, total encryption and decryption time of our algorithms is greatly reduced. The remainder of this paper is organized as follows. preliminary knowledge will be given. we propose a single-bit and a multi-bit public key encryption scheme. Then, we give the comparison between our scheme and the existing scheme.

**Algorithms:**

**BKW algorithm:**

The BKW algorithm was proposed by Blum, Kalai and Wasserman as a method for solving the LPN problem, with sub-exponential complexity, requiring 2O(n/ log n) samples and time. The algorithm can be adapted for tackling Search- and Decision-LWE, with complexity 2O(n) , when the modulus is taken to be polynomial in n.

**Discrete logarithms:**

Discrete logarithms are quickly computable in a few special cases. However, no efficient method is known for computing them in general. Several important algorithms in public-key cryptography base their security on the assumption that the discrete logarithm problem over carefully chosen groups has no efficient solution.The discrete logarithm problem is considered to be computationally intractable. That is, no efficient classical algorithm is known for computing discrete logarithms in general.

**Example for Implementing Algorithm:**

**1.**

|  |  |
| --- | --- |
| **Type of bit parity** | **Successful transmission scenario** |
| Even parity | A wants to transmit: 1001A computes parity bit value: 1+0+0+1 (mod 2) = 0A adds parity bit and sends: 10010B receives: 10010B computes parity: 1+0+0+1+0 (mod 2) = 0B reports correct transmission after observing expected even result. |
| Odd parity | A wants to transmit: 1001A computes parity bit value: 1+0+0+1 (mod 2) = 0A adds parity bit and sends: 1001**1**B receives: 10011B computes overall parity: 1+0+0+1+1 (mod 2) = 1B reports correct transmission after observing expected odd result. |

**2.** The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the [key](https://en.wikipedia.org/wiki/Key_%28cryptography%29)):

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

**Future Work:**

In the post quantum era, the design of public key cryptography under the DLPN assumption is an important research direction. Such schemes have many advantages such as shorter public key and ciphertext, faster encryption and decryption. But the existing scheme is still having the problem of decryption error, which is not satisfactory. Based on the LPN variants problem, we proposed a single-bit and a multi-bit public key encryption scheme. Our scheme solved the decryption error problem of the existing public key encryption schemes based on DLPN. Compared to existing schemes, there is an increase in only a small amount of ciphertext space and computing overhead in our scheme. Our scheme not only is able to withstand quantum attack but also provides strong practical security at the same time. In the future, we will design a public key scheme based DLPN with high security, smaller public key and ciphertext size, and smallercomputational overhead. Furthermore, designing public key cryptography that satisfies CCA security is also one of our future work.

**Conclusion:**

In the post quantum era, the design of public key cryptography under the DLPN assumption is an important research direction. Such schemes have many advantages such as shorter public key and ciphertext, faster encryption and decryption. But the existing scheme is still having the problem of decryption error, which is not satisfactory. Based on the LPN variants problem, we proposed a single-bit and a multi-bit public key encryption scheme. Our scheme solved the decryption error problem of the existing public key encryption schemes based on DLPN. Compared to existing schemes, there is an increase in only a small amount of ciphertext space and computing overhead in our scheme. Our scheme not only is able to withstand quantum attack but also provides strong practical security at the same time. In the future, we will design a public key scheme based DLPN with high security, smaller public key and ciphertext size, and smallercomputational overhead. Furthermore, designing public key cryptography that satisfies CCA security is also one of our future work.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV or Later Version

➢ RAM - 4 GB (min)

➢ Hard Disk - 40 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP or Later Version
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL