台灣大學 電機工程學系
密碼學

Term Project

組別：A3

組員 1：林仕倫

組員 2：林士鈞

授課教授：雷欽隆教授

日期：2019/1/14

1.Description of the paper

1.1 Abstract

In this work, a new public-key cryptosystem whose security is based on the computational intractability of the following problem: Given a Mersenne number p = 2n −1, where n is a prime, a positive integer h, and two n-bit integers T, R, find two n-bit integers F, G each of Hamming weight at most h such that T = F ·R+G modulo p, under the promise that they exist.

1.2 Introduction

Shor [Sho97] gave a quantum algorithm that solves the abelian hidden subgroup problem and as a result solves both discrete logarithms and factoring. Although quantum computers are far from being a reality, there is serious effort in both the industry and the scientific community to make information security systems resistant to quantum computing.

In the recent years, some presumably quantum-safe public-key cryptosystems have been proposed in the literature. Perhaps the most promising among these are those based on the hardness of lattice problems like Learning with Errors (LWE) based cryptosystems, Ring-LWE based cryptosystems and NTRU. While these cryptosystems have so far resisted any classical or quantum attacks, it cannot be excluded that such attacks are possible in the future. Thus, it is desirable to come up with other promising proposals for public-key cryptosystems.

1.3 Problem addressed by the paper

Nowadays, most public-key cryptosystems based on the hardness of discrete logarithms or factoring integers will be solved by the quantum algorithm after quantum computers being invented. Therefore, the paper gives an algorithm of a public-key cryptosystem which may resist quantum attacks with more efficiency than other existing algorithm that can resist quantum attacks.

1.4 Related work

Ntru cryptosystem family [HPS98, Reg09, LPR10, MTSB13] work with elements in a ring which are hidden by adding some small noise.

1.5 Solutions or techniques

This paper uses Mersenne’s prime number as module, which can speed up the operation during addition and multiplication, to make the encryption and decryption

more efficient than than the other existing algorithm that can resist quantum attacks.

1.6 Comparisons with existing approaches

The complexity of this system is O(N), based on the addition. The length of N is extremely larger than existing approaches like RSA. As the result, the time of encryption and decryption is much longer than RSA.

1.7 Conclusion

This paper proposes a simple new public-key encryption scheme, which security relies on an unproven assumption. Since the proposed cryptosystem is based on a relatively new assumption, it requires more cryptanalytic effort before one can become reasonably confident about its security.

2.Our comments about the paper

Although this paper is to propose a new scheme about the post-quantum crypto, the core concept is similar to other approaches like LWE. So even though it's a new system, it suffers from same problems of existing approach.

3.Recent development of the topic

3.1 attack analysis

3.1.1 meet in the middle attack

published soon after this paper, claim to attack with asymptotic $O(\sqrt{\binom{n}{w}})$

3.1.2 challenge to the LHW assumption

LLL algorithm may break this cryptosystem

3.2 other approach

lattice, LWE, Hash-based cryptography

4.Ideas/suggestions to improve the approach

physically:
Do it on chip or on gpu to speed up the add operation, approach would be much faster because there is a lot parallel computation.

5.Our comments and conclusion about the topic

The approaches nowadays suffers from efficiency. But we think that there is no need to do quantum resist mechanic to daily use. And for higher secure required

applications, the speed is not that important so it's ok. Also, there are a lot of improvements could apply such as table look-up, computational speed will not be a problem.

6.Description of our implementation

6.1 Introduction

In this cryptosystem, the encryption and the decryption only contain addition, multiplication and some bitwise operation 'like shifting', 'and' , 'or' and 'xor' . Besides operation, it needs error correcting code to correct the errors which generated during the encryption and decryption.

6.2 Specification and functionalities

The length of plaintext = lambda.
The hamming weight of several random-choosing strings = h = lambda.
The length of ciphertext = n , where n is a Mersenne's prime number.
The relation between h and n: $10 * h^2 < n < 16 * h^2$.
KeyGen function generates n bit public key and secret key.
Encryption function uses error-correcting-code to transform message from h bits to n bits and then do several operations.
Decryption function does several operations and the recovers the message to h bits with error-correcting-code.

6.3 Scenario of the system

```
KeyGen ( plaintext.size )
{
    //Random generate n bit string
    //    with hamming weight h : f , g
    // hamming weight h = plaintext.size
    // set hamming weight
    for( i = 0 ; i < plaintext.size ; i++ )
        f[i] , g[i] = 1
    random shuffle (f) , random shuffle (g)
    //Random generate n bit string : r
    Compute t = f * r + g
    public_key = (r , t)
    secret_key = f
    return    public_key ,    secret_key
```

```
}
Encrypt ( public_key , plaintext )
{
        // Random generate n bit string
        //    with hamming weight h : a , b1 , b2
        c1 = a * r + b1
        c2 = (a * t + b2)  ⊕  ECC ( plaintext )
        ciphertext = (c1 , c2)
        return    ciphertext
}
Decrypt ( secret_key , ciphertext )
{
        Compute d = DECC( (f * c1)  ⊕  c2 )
        return d
}
```

6.4 Evaluation of our implementation

length of n, h	n = 11213	n = 44497	n = 216091
	h = 32	h = 64	h = 128
ECC Repeat times	350	695	1688
Max error	10	12	680
Average error	1	2	320
Max error rate	2.9%	1.7%	40.3%
Average error rate	0.3%	0.3%	19.0%
Time consume	0.35 sec	2.5 sec	25 sec

7.Reference

https://eprint.iacr.org/2017/481.pdf

https://arxiv.org/pdf/quant-ph/9508027.pdf

https://pdfs.semanticscholar.org/dc4e/75107be82e774409a9998d4b93f5e98e554c.pdf

https://link.springer.com/chapter/10.1007/978-3-319-79063-3_5