On Logical Operation for NTRU Cryptosystem

Sonika Singh
Department of Mathematics
Motilal Nehru National Institute of Technology
Allahabad-211004, India

ABSTRACT
Tripathi and Thakur proposed a new variant of NTRU cryptosystem [8] by using the Exclusive-OR operation. They proposed this system under the same general principles as that of the NTRU cryptosystem except the logical operators "Exclusive-OR" with the different bit size for encryption and decryption are used in place of truncated polynomial in NTRU cryptosystem. In this article we discuss some shortcomings of the scheme [8] and argue that the proposed scheme is not practical and secure.

Keywords
NTRU Cryptosystem, Logical XOR operation, Boolean Algebra.

1. INTRODUCTION
The original NTRU cryptosystem was proposed in the rump session at CRYPTO'96 in 1996, by Hoffstein, J. Pipher and Silverman [2], and was published in 1998 [3]. NTRU cryptosystem is based on polynomial rings over Z and the underlying problems are the shortest vector problem, and the closest vector problem of lattices. As compared to other well-known systems such as RSA [7] or ECC [5], the greatest advantage of NTRU is that it is based on a class of basic arithmetic operations whose complexity is low, amounting to O(N^2) in worst-case.

NTRU public key cryptosystem uses truncated polynomials [4, 6] with integer coefficients as its keys. The underlying algebraic structure of NTRU is n^{th} degree truncated polynomial ring (convolution polynomial rings). Let $R = \frac{(Z[x])}{(x^N - 1)}$ be the convolution polynomial ring. Let "*" denotes the multiplication of ring elements. If we use modulo p or modulo q, then it denotes that we are taking the coefficients of the polynomial in the range ($-p/2$, $p/2$] or (($-q/2$, $q/2$]. The main objects of this system are small polynomials with small coefficients. Many variants of NTRU came in picture based on different-different algebraic structures. One variant of them, was proposed by Tripathi and Thakur using exclusive-or (XOR) operation in 2015 [8]. We observed some shortcomings in that scheme and shown that the scheme is not practical and secure.

2. ORGANIZATION
The rest of the sections are organized as follows. In section III, we introduce the scheme proposed by Tripathi and Thakur [8] with an example to show the correctness of the scheme presented by the author. The estimation of time complexity is also presented in this section as given by the author. Next, we discuss our observed shortcomings of the scheme [8] in section IV. Finally, we conclude the article in the last section.

3. A LOGICAL OPERATION FOR NTRU CRYPTOSYSTEM
In this section we introduce the scheme proposed by Tripathi and Thakur [8]. The proposed scheme is based on some Boolean algebra's identities and laws [9, 1] as given below:

Let X is a binary code. Then,

- $X \oplus X = 0$ [Inverse Law]
- $X \oplus X^{-} = 1$ [Inverse Law]
- $X \oplus 0 = X$ [Identity Law]
- $X \oplus 1 = X^{-}$ [Complement Law]
- $X \oplus Y = Y \oplus X$ [Commutative Law]

3.1 Algorithm
Using the above logical operations author proposed their scheme as below:

3.1.1 Key Generation.
Step 1 - Bob randomly chooses two binary codes f and g where the binary codes f and g are private. He considers $f = X \oplus X$ and $g = X \oplus X^{-}$, where $X = A \oplus B$, A and B are some binary codes.

Step 2 - Bob's next step is to compute the inverse of f mod q which is f_q and f mod p which is f_p . Thus

$$f \oplus f_q = 1 \bmod q$$

$$f \oplus f_p = 1 \bmod p$$

Step 3 - Now Bob computes the product

$$H = p \oplus f_q \oplus g \bmod q.$$

H is the public key.

3.1.2 Encryption.
Step 1 - Alice wants to send a message to Bob using Bob's public key H. She first puts her message in the form of binary code M and its size is the same as private keys f and g.

Step 2 - To create the encrypted message, Alice chooses a random binary code of decimal $R = A.0$, where $A.0 = 0$ [Law of Intersection].

Step 3 - Next Alice computes the encrypted message using R and Bob's public key as follows:

$$E = R \oplus H \oplus M \bmod q.$$

The binary code E is the encrypted message which Alice sends to Bob.

3.1.3 Decryption.

Step 1 - Now, Bob receives the encrypted message and decrypt it. Using his private binary code f , he computes the binary code $A = f \oplus E \bmod q$.

Step 2 – He next computes the binary code $B = A \bmod p$.

Step 3 - Finally, B is the decrypted ciphertext which should be equal to the original plaintext M.

3.2 Correctness.

To verify the proof of correctness, we have to show that $B = M$ so that its correctness can be proved as the same message send by the sender. The steps for the verification are as below:

$B = A \bmod p$
$B = (f \oplus E \bmod q) \bmod p$
$B = (f \oplus R \oplus H \oplus M \bmod q) \bmod p$
$B = (f \oplus R \oplus p \oplus f_q \oplus g \oplus M \bmod q) \bmod p$
$B = (p \oplus f \oplus f_q \oplus R \oplus 1 \oplus M \bmod q) \bmod p$
$B = p \oplus 1 \oplus R \oplus 1 \oplus M \bmod p$
$B = p \oplus 1 \oplus 1 \oplus R \oplus M \bmod p$
$B = p \oplus 0 \oplus R \oplus M \bmod p$
$B = p \oplus R \oplus M \bmod p$
$B = p \oplus A.0 \oplus M \bmod p$
$B = p \oplus 0 \oplus M \bmod p$
$B = p \oplus M \bmod p$
$B = p \pmod p \oplus M \pmod p$
$B = 0 \oplus M \bmod p$
$B = M \bmod p$.

3.3 A Toy Example.

The example for key generation, encryption and decryption for proposed design with randomly chooses value given by the authors is as follows –

3.3.1 Key generation –

Let $A = 10010011$ and $B = 10010100$.

Let parameters are $p = 91$ and $q = 127$.

$$X = A \oplus B = 10010011 \oplus 10010100 = 00100111$$

$$f = X \oplus X = 00000000, \quad g = X \oplus \bar{X} = 11111111.$$

$$f_q = f^{-1} \bmod 127 = 11111111 \bmod 127 = 00000001 \pmod{127}.$$

So, $f \oplus f_q = 00000000 \oplus 00000001 = 00000001$.

Now, Bob generates the public key H as

$$H = 01011011 \oplus 00000001 \oplus 00000001 = 01011011.$$

The private key is f with f_q and H is the public key.

3.3.2 Encryption –

Now, suppose Alice want to send the message M to Bob.

Let $M = 00000001$ and $R = A.0 = 00000000$.

Then,

$E = R \oplus H \oplus M \bmod q$

$E = 00000000 \oplus 01011011 \oplus 00000001 \bmod 127$

$E = 01011100 \bmod 127$

Hence, $E = 01011100$ is the ciphertext.

3.3.3 Decryption –

Bob has received the encrypted message from Alice. He computes –

$A = f \oplus E \bmod q$
$A = 00000000 \oplus 01011100 \bmod 127$
$A = 01011100 \bmod 127$
$A = 01011100$

Now, the second step is to compute

$B = A \bmod p$
$B = 01011100 \bmod 91$
$B = 00000001 \bmod 91$
$B = 00000001 = M$

3.3.4 Time Complexity Calculation.

As per the author the time complexity of the proposed scheme is discussed as below. The time complexity of binary to decimal, decimal to binary and binary to string conversion is $O(\log_2(N))$. The time complexity of length of the binary string is $O(N)$ because i varies from 1 to N. Also the time complexity of inverse of any binary number is $O(1)$. The time complexity of addition of two binary numbers is, Multiplication of two binary numbers is $O(N^2)$. Therefore the total time complexity of the proposed scheme is

$$O(\log_2(N)) + O(N) + O(1) + O(N^2) = O(\log_2(N)).$$

4. COMMENTS ON LOGICAL OPERATION FOR NTRU CRYPTOSYSTEM

The observed shortcomings/comments are given step by step as below:

Step 1 - In key-generation step, the author took $f = X \oplus X$ and $g = X \oplus \bar{X}$ as the private keys. If we use the given Boolean laws (Inverse laws), then $X \oplus X = 0$ and $X \oplus \bar{X} = 1$. That means $f = 0$ and $g = 1$ always. Then, there is no meaning of the secrecy of f and g. These values are always known to attacker as $f = 0$ and $g = 1$.

Step 2 - In encryption process, the sender has to use a random value R to maintain randomization or blinding the information. But, in this scheme, the author took $R = A.0 = 0$ by the law of intersection of Boolean algebra. Here, first of all the operation "." is not defined. Secondly, the used random value R is 0 in all cases. Then, how can the system be randomized as we know $R = 0$ always. So, there is no randomization at all.

Step 3 - In the example given by the author to show the correctness of the algorithm, the author took the message M is 1 i.e. 00000001. But the message can be anything. It is not necessary that message is 1. If we take another message, then the given system does not work.

For example, Suppose the sender wants to send the message $M = 10001010$ i.e. $M = 138$. We are using the same values as given in the example , we are changing only the message M .

So, f = 00000000 , g = 00000001, f_q = 000000, H = 01011011, R = 00000000, M = 10001010

$$E = R \oplus H \oplus M \bmod q$$

$$E = 00000000 \oplus 01011011 \oplus 10001010 \bmod 127$$

$$E = 11010001$$

Now,

$$A = f \oplus E \bmod q$$

$$A = 00000000 \oplus 11010001 \bmod 127$$

$$A = 11010001.$$

Next,

$$B = A \bmod p$$

$$B = 11010001 \bmod 91$$

$$B = 00011011 .$$

It is clear here that $B \neq M$, i.e decryption is not verified in this case.

Step 4 - In the time complexity calculation step, author said that the time complexity of finding inverse is $O(1)$, whereas the time complexity of finding inverse should be $O(N^2)$. The second thing is, according to the author, the total of time complexities of the proposed scheme is - $O(\log_2(N)) + O(N) + O(1) + O(N^2) = O(\log_2(N))$, where as , according to us, this should be $O(N^2)$ in place of $O(\log_2(N))$.

At last, the scheme in [8] is definitely not viewed as a variation of NTRU. It has no relation to the intractable problems over lattices.

5. CONCLUSION

In this article we introduced the scheme proposed by Tripathi and Thakur [8] and highlighted some shortcomings of the proposed scheme. Under these shortcomings we conclude that the scheme proposed by Tripathi and Thakur is not practical and secure.

6. REFERENCES

[1] Eldon, J. W., 2010. Boolean Algebra and its Application. Springer.

[2] Hoffstein, J. , Pipher, J. and Silverman, J. H. 1996. NTRU: a new high speed public key cryptosystem. Preprint; presented at the rump session of Crypto96.

[3] Hoffstein, J., Pipher, J. and Silverman, J. H . 1998. NTRU: a ring based public key cryptosystem. In Proc. of ANTS, LNCS Springer, 1423, 267-288.

[4] Hoffstein, J., Lieman, D. and Silverman, J. 1999. Polynomial Rings and Efficient Public Key Authentication. In Proceeding of CryptTCS'99, City University of Hong-Kong Press, 7-19.

[5] Koblitz, N. 1987. Elliptic curve cryptosystem. Mathematics of Computation, 48, 203-209.

[6] Roja, P. P., Avadhani, P.S. and Prasad, E .V . 2006. An Efficient Method of Shared Key Generation Based on Truncated Polynomials. International Journal of Computer Science and Network Security, 6.(8B, 156-161.

[7] Rivest, R. L., Shamir, A. and Adleman, L. 1978. A Method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21, 120-126.

[8] Tripathi, B.P. and Thakur, K. 2015. A logical XOR operation for NTRU Cryptosystem, International Journal of Computer Applications, 126 , 0975-8887.

[9] Steven, G. and Paul , H. 2009. Introduction to Boolean Algebras. Springer-Verlag.