International Journal of Engineering Research and General Science Volume 3, Issue 6, November-December, 2015
ISSN 2091-2730

Message and Signature Conveyance System using NTRUSign

N. Sravan Kumar* P. Alee Mulla Khan#
*M.Tech Scholar, CSE Dept, Vignan's Institute of Information Technology, Visakhapatnam.
#Assistant Professor, CSE Dept, Vignan's Institute of Information Technology, Visakhapatnam.
*nagirisravankumar@gmail.com #p_aleekhan@yahoo.co.in

Abstract-Information Security is the investigation of hops that give the assurance of the data in the framework, mobiles and PDAs against unapproved access, use, change, and so forth. A Digital Signature is the condition utilized for stamping or marking an electronic file, by a procedure intended to be similar to paper marks, yet which makes utilization of an innovation known as open key cryptology. In this paper, we propose and test NTRU Signature the calendars for variable evaluated substance records, utilizing polynomial cryptosystems with a blend of the adjusted new cryptosystem. The algorithm exhibited in this paper can be utilized for both signature generation and for giving information classification not at all like a couple of different algorithms chipping away at polynomial arithmetic. NTRU Cryptosystems has passed on a few translations of the NTRU Algorithms, of which the essential algorithm was executed for this utilization.

Keywords-Authentication, Digital Signature, new cryptosystem, NSS, NTRU, PDA and polynomial.

I. INTRODUCTION

Information security (IS) is designed to protect the confidentiality, integrity and availability of system data from those with malicious purposes. Cryptography involves creating written or generated codes that allows information to be kept confidential. Cryptography converts data into a format that is unreadable for an unauthorized user, permitting it to be transmitted without anyone decoding it back into a readable format, therefore compromising the data.

Information security uses cryptography on several levels. The data cannot be read without a key to decipher it. The information keeps up its integrity during transportation and while being stored. Cryptography as well aids in non-renunciation. This implies that neither the creator nor the recipient of the data may claim they did not create or receive it.

Data Encryption is a process that applies operations or mathematical functions on data for difficult to understand it. Data encryption is very important to protect the various types of personal information and confidential information stored in the smartphone.

Data Authentication is the procedure of an overseer allowing the rights and the procedure of checking user account consents for access to information or data are both alluded to as approval.

The NTRU public key cryptosystem was developed in 1996 at Brown University by three mathematicians J. Hoffstein, J.Pipher and J.H. Silverman [6]. It is not that much popular cryptosystems like RSA, ECC and other traditional. The major advantages of NTRU cryptosystem are much faster generating key, encryption time and decryption time as compared to others [3][4].

It is easily compatible with mobile devices and other portable devices. It is theoretically proposed here. The Kid-RSA is a public-key cipher system proposed by Neal Koblitz [5] for pedagogic purposes and published in 1997. The new crypto-system is very simple.

II MOTIVATION

In any open cryptography, we need affirmed Public Key(s) and Private Key(s) to scramble/unscramble for any message at without fall flat. That infers there are various arrangements of Public Keys and Private Keys are required to encryption/interpret message(s) in this cryptosystem. Our objective is not to make various open keys with respect to related particular Private Keys. Our proposed calculation creates simply Public Key joined with Private Keys.

It sign the message once recipient not under any condition like other open crypto algorithm. If time "t" is required for encoding a message for each encryption procedure, out in the open crypto figuring, the total encryption time is N*t times for "N" number of recipients. This estimation needs just "t" time for any number of recipients.

The Recipient can translate message using their own accepted Private Key. The basic ideal position of our novel algorithm is to extra more encryption time and computational power. Thusly, the proposed, figuring is profitable and reasonable in regards to computational time.

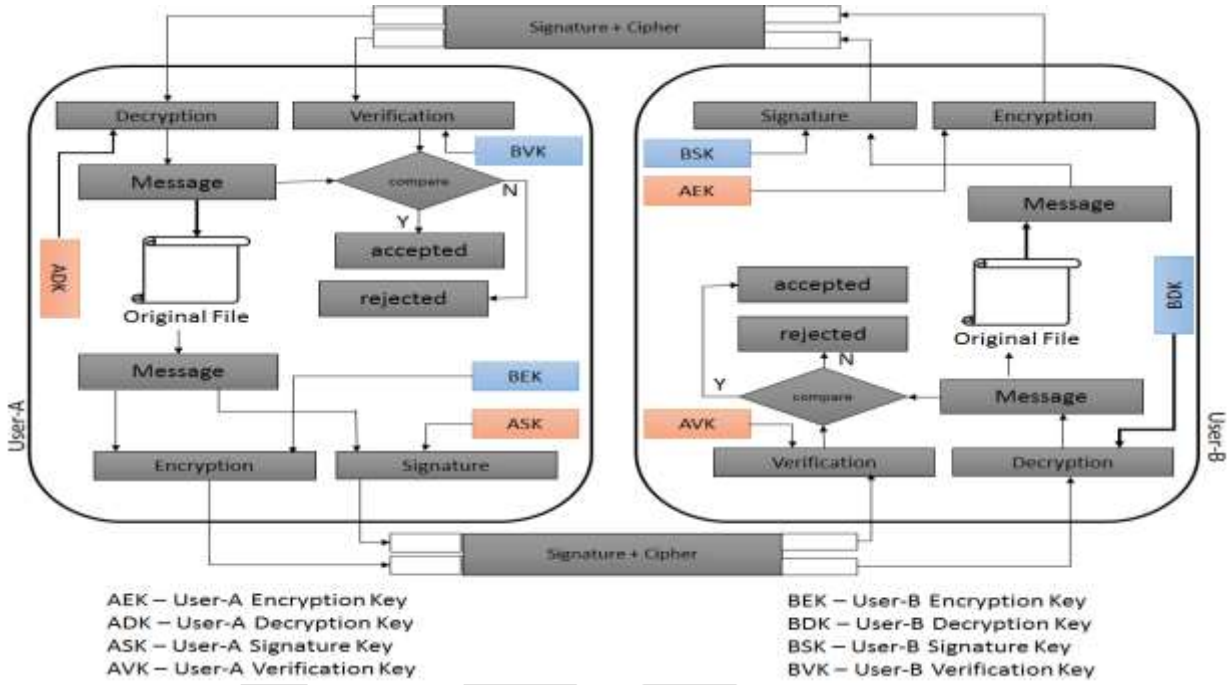

Fig. 1 Message, Signature Conveyance System Architecture

III. PROPOSED SYSTEM

NTRU Signature is defined similarly as set Of R polynomials of degree completely not as much as N and having entire number coefficients. The parameter N is settled. The vital operations on these polynomials are development and convolution duplication. Convolution expands * of two polynomials f and g is described by taking the coefficient of X^k in f*g to meet.

In more numerical terms, R is the quotient ring R = Z[X]/ (X^N-1). If one of the polynomials has all coefficients looked over the set {-1, 0, 1} we will insinuate the convolution as being twofold [7]. If coefficients of the polynomials are reduced modulo q for some q, we will suggest the convolution as being specific.

$$f(x) * g(x) = \sum_{i+j=1 \bmod N}^{\infty} (f(x).g(x)) \quad (0 \leq k < N)$$

We will likewise need to round numbers to the closest whole number and to take their partial parts. For any fits in with Q, let [a] mean the whole number nearest to a, and characterize {a} =a-[a]. On the off chance that A will be a polynomial with rational or (real) coefficients, let [A] and {A} be A with the showed operation connected to every coefficient [1].

The sender generates random large values for creating two keys for Encryption. The A new cryptosystem designed using a KID crypto system is modified for encryption by generating two extra-large two values (r_1, r2). The sender takes message which should be less than n. The sender sends message using receiver public key (d, n). The receiver decrypts cipher with his private key (e1, e2, n).The Entire system model is illustrated in the figure 1.

IV. IMPLEMENTATION

In our system, we propose two algorithms for signature and encryption process. In this one is NTRU Sign for Signature and another is a new cryptosystem for Encryption. Here, we compare the complexity and speed of the system in a practical way. Consider the two users (User-A, User-B), whose wants transfer the files using the message conveyance system.

NTRU Signature Scheme (NSS):

The key calculation incorporates the deviation between two polynomials. Let f(X) and g(X) be two polynomials in R. We are first lessening their coefficients modulo q to lie in the range between −q/2 to q/2, then we reduce their coefficients modulo p to lie in the degree between −p/2 and p/2. Let

$$f(X) = f_0+f_1X +\cdot\cdot\cdot+f_{N-1}X^{N-1} \text{ and}$$
$$g(X) = g_0+\cdot\cdot\cdot+g_{N-1}X^{N-1}$$

be these reduced polynomials. Then the deviation of a and b is Dev(f, g) = {i : $f_i \neq g_i$}. Intuitively, Dev(a, b) is the number of coefficients of a mod q and b mod q that differ modulo p.

Key Generation: User-A picks two polynomials f and g has the suitable form (2). He processes the opposite f^{-1} of f modulo q. The Weave's open verification key is the polynomial $h \equiv f^{-1} * g \bmod q$ and his private marking key is the pair(f, g)

Signing: User-A's document is a polynomial m modulo p. User-A chooses a polynomial w ∈ Fw of the form $w = m + w_1 + pw_2$, where w_1 and w_2 are small polynomials whose precise form we will describe later. He then computes $s \equiv f * w \pmod q$.User-A's signed message is the pair (m, s).

Verification: In order to verify User-A's signature s on the message m, User-B first checks that $s \neq 0$ and then User-B verifies the following two conditions:
(1) User-B compares s to $f_0 * m$ by checking if their deviation satisfies

$$D_{min} \leq Dev(s, f_0 * m) \leq D_{max}.$$

(2) User-B uses User-B's public verification key h to compute the polynomial

$$t \equiv h * s \pmod q,$$

putting the coefficients of t into the range [−q/2, q/2] as usual. She then checks if the deviation of t from $g_0 * m$ satisfies

$$D_{min} \leq Dev(t, g_0 * m) \leq D_{max}.$$

If a User-A's signature passes tests (1) and (2), then User-B accepts it as valid

New Cryptosystem:
Key Generation: The User-A generates random values as parameters such as x, y, P, Q, r1, r2 in secure way. By using these parameters the key generation algorithm computes private key and public key as following key generation algorithm.
Step 1: Start
Step 2: Read Random values x, y, P, Q
Step 3**:** Calculate constant = xy-1
Step 4: Calculate $m_1 = (P * constant) +x$
Step 5: Compute $m_2 = (Q * constant) +y$
Step 6: Calculate $n = ((m_1 * m_2) -1)/constant$
Step 7: $e1 = (m_1+r_1) \bmod n$ $(gcd (m_1+r_1, n) = 1 \bmod n)$
Step 8: $d = (m_2+r_2) \bmod n$ $(gcd (m_2+r_2, n) = 1 \bmod n)$
Step 9: $m = (r_1r_2+1+ m_1r_2+m_2r_1) \bmod n$
Step 10:$e2 = m^{-1} \bmod n$
Step 11: if gcd (m, n)! =1 mod n
Go to Step 7
Step 12: Public Key (d, n)
Step 13: Private Key (e_1, e_2, n)
Step 14: return Public Key, Private Key
Step 15: Stop

Encryption: The User-B wants to send message to User-A. The User-B computes the cipher text using the User-A's public key, i.e., (d, n) as following way.
Step 1: Start

Step 2: Read User-A public key (d, n)
Step 3**:** read message (message< n)
Step 4: Compute cipher text = (message * d) (mod n)
Step 5: return cipher text
Step 6: stop

Decryption: After User-A receives cipher text from the User-B, it needs to decipher the code word. The User-A decrypts the cipher text by using the User-A's private key, i.e., (e_1, e_2, n) as following way.
Step 1: Start
Step 2: Read User-A private key (e_1, e_2, n)
Step 4: Compute message = (cipher text * e_1 * e_2) (mod n)
Step 5: return cipher text
Step 6: stop

V. SECURITY ANALYSIS

NSS Analysis:
Test (1): The polynomial s that User-B tests is compatible to the product
s = f * w (mod q)
= (f_0 + pf1) (m + w_1 + p *w_2) (mod q)
= f_0 * m + f_0 * w_1 + pw_2 + pf_1 * w (mod q)

We see that i^{th} coefficients of s and f0 .m will concur modulo p unless one of the accompanying circumstances happens:
– The i^{th} coefficient of f_0 * w1 is nonzero.
– The i^{th} coefficient of f * w is outside the reach (- q/2, q/2], so varies from the i^{th} coefficient of s by some multiple of q.

In the event that the required variables and test spaces are selected appropriately, then there will be in any event D_{min} and at most D_{max} deviations between s mod p and m mod p. Subsequently User-A's mark breezes through test.

Test (2): The polynomial t is given by t = h * s = (f^{-1} * g) * (f *w) =g * w (mod q):
Since g has the same structure as f, the same thinking with respect to test (1) demonstrates that t will finish test (2).

New Cryptosystem Analysis:
At Encryption side, User-B uses User-A's public key (d, n). In cryptosystem, d equals to the m_2+r_2 and multiply with message.

Cipher = (Message * d) mod n

At Decryption side, User-A uses his private key (e_1, e_2, n). In cryptosystem, e_1 equals to the m_1+r_1 and multiply with cipher.

(Cipher * e1*e2) mod n = (Message *d *e1*e2) mod n
= Message

VI. EXPERIMENTAL RESULTS

We have implemented NSS, new cryptosystem in Java and run it on various platforms. The Figure (2), (3) describes the performance of NSS and new cryptosystem respectively, on a desktop machine which has the features such Intel i3 4th generation with speed of 1.70 GHz and cache size 3.0MB.

For NSS, we are using the basic parameters like that N= 157 (Highest degree of polynomial). The p and q are must be follows the gcd(p,q) = 1. Hence, the values of p and q are 256 and 29 respectively. The experimental results of signature generation and verification are shown in Table (1) graphically evaluated in figure 2.

NSS Signature Time for process		
File Size (kb)	Signature (m.Sec)	Verification (m.Sec)
0.25	3	2
0.5	6	3

1	7	4
2	8	5
10	10	6

Table 1: NSS time space evaluation

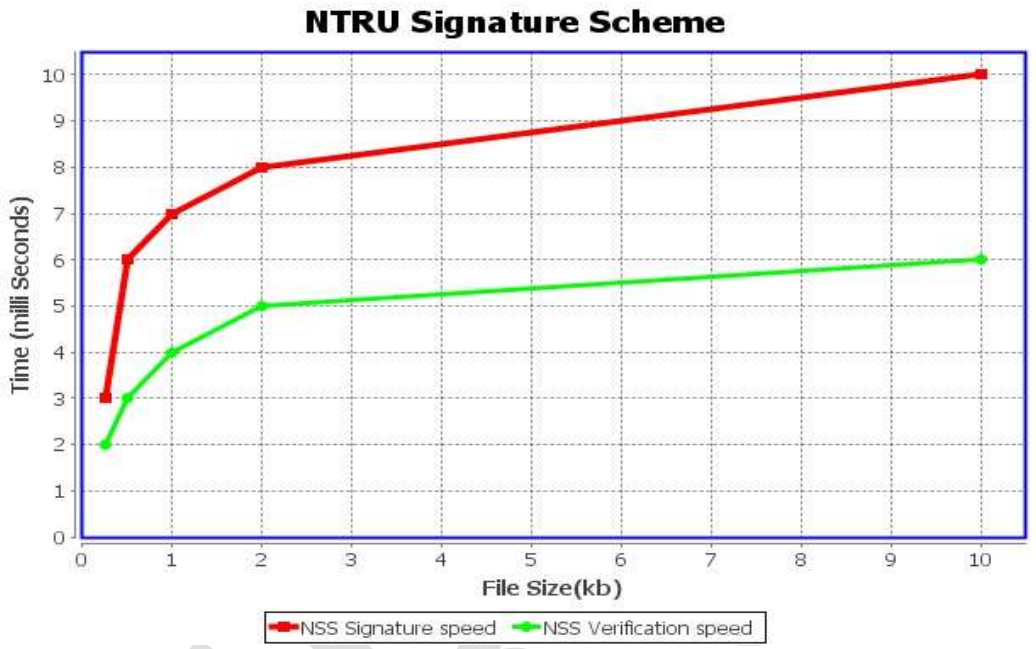

Fig. 2 Graph for time space of NSS Signing, verifying

For new cryptosystem, we consider the parameters random BigInteger (with Bit Length of 512). In our proposed system, it consider the block size 128 bytes. The Results are shown in the Table (2) and graphically evaluated in figure 3.

Encryption Time for Process		
File Size (kb)	Encryption (m.Sec)	Decryption (m.Sec)
0.25	2	1
0.5	3	1
1	5	3
2	14	7
10	65	15

Table 2: New Cryptosystem time space evaluation

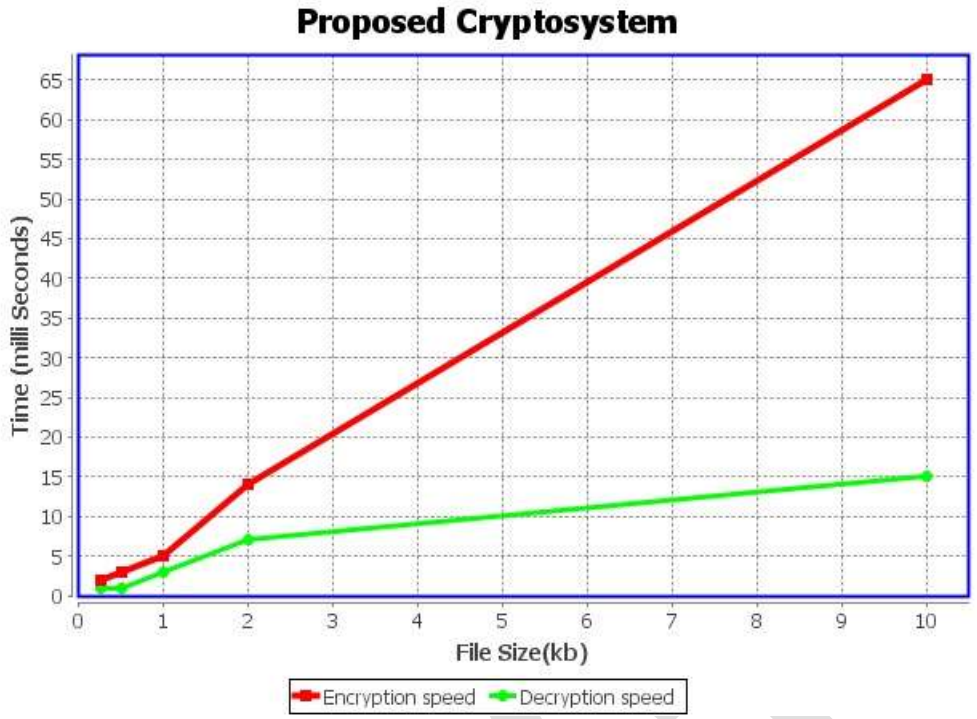

Fig. 3 Graph for time space of New Proposed System Encryption, Decryption

VI. CONCLUSION

The NSS calculation exhibited in this paper can be used for both sides signature generation and for giving data security not in any manner like several unique counts taking a shot at polynomial number juggling. In this paper, security and capability examination showed that the NTRU Signature estimation with blend of new encryption system. Here proposed new encryption algorithm give the security, versatile quality. In this way, our computation is a good contender for the security of records. Finally, the movements of the use of this calculation are illuminated. Lattice is one of the existing quantum-secure cryptographic primitive.

REFERENCES:

[1] Jeff Hoffstein, Nick Howgrave-Graham, Jill Pipher, William Whyte "Practical lattice based cryptography: NTRU Encrypt and NTRU Sign", part of series Information Security and Cryptography pp 349-390
[2] Amandeep Kaur Gill, Charanjit Singh "Implementation of NTRU Algorithm for the Security of N-Tier Architecture" in volume4 pp 417-462
[3] Divyajyothi M G, Rachappa, Dr. D H Rao "Techniques of Lattice Based Cryptography Studied on a Pervasive Computing Environment" in Vol.5, No.4, August 2015
[4] Ranjeet Ranjan, Dr. A. S. Baghel, Sushil Kumar "Improvement of NTRU Cryptosystem" Volume 2, Issue 9, September 2012
[5] http://www.usna.edu/Users/math/wdj/_files/documents/sm473-capstone/sm473-crypto-lecture-notes.pdf pp 63-65
[6] http://en.wikipedia.org/wiki/NTRU_Cryptosystems,_Inc
[7] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman "NSS: The NTRU Signature Scheme" Advances in Cryptology—Eurocrypt, 2001 – Springer