Research Journal of Applied Sciences, Engineering and Technology 14(1): 35-39, 2017
DOI:10.19026/rjaset.14.3986
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2017 Maxwell Scientific Publication Corp.
Submitted: August 25, 2016 Accepted: November 15, 2016 Published: January 15, 2017

Research Article

A Secure and Efficient Authentication and Key Agreement Scheme for e-Health Platforms Using Lattices

Taoufik Serraj, Moulay Chrif Ismaili and Abdelmalek Azizi
ACSA Laboratory, Faculty of Sciences, Mohammed First University, Oujda 60000, Morocco

Abstract: In order to build a secure and an efficient scheme even in the presence of quantum computers, we propose an improved authenticated key agreement scheme based on NTRU for applications in e-health platforms. In fact, user authentication and key agreement are important cryptographic primitives that allow two entities to establish a secure and an authenticated channel over insecure networks. Currently, the security of the most of these primitives relies on RSA or ECC standards, which ensure high security levels. Unfortunately, all cryptosystems based on factorization problems (e.g., RSA) or the discrete logarithm problem in finite groups (e.g., ECC) will be vulnerable to quantum attacks in the next few years due to Shor's algorithm. Security and efficiency analysis show that the proposed scheme can resist various attacks, including quantum attacks while preserving efficiency.

Keywords: Authentication, e-health, key agreement, lattice, security

INTRODUCTION

Over the past two decades, information and communications technologies had changed our everyday life in different areas. New services are provided online, such as e-Commerce, e-Learning and e-Health.

To protect the sensitive data exchanged over public networks, many cryptographic techniques are used. Nowadays, the most dominant cryptosystems are based on the factorization problem (e.g., RSA (Rivest *et al*., 1978)) or on the discrete logarithm problem in some finite groups (e.g., Elliptic Curve Cryptography (ECC) (Koblitz, 1987; Miller, 1985).

In the last few years, Xie *et al*. (2013) proposed an authentication and key agreement scheme based on RSA for Telecare Medicine Information Systems (TMIS), while Xu *et al*. (2014) proposed another scheme using ECC. However, despite the current high security of cryptographic protocols based on RSA or ECC, these systems will be vulnerable to the quantum attacks in the future due to Shor's algorithm (Shor, 1997).

NTRU is a lattice-based public key cryptosystem, which provides encryption and digital signature schemes, it was proposed by Hoffstein *et al*. (1998). NTRU has recently standardized through IEEEP1363.1 (Whyte *et al*., 2008) and X9.98 (ANSI X9.98, 2010). In fact, the use of NTRU presents an alternative to RSA and Elliptic Curve Cryptography (ECC) to prevent quantum attacks. In addition, this choice provides more advantages compared to RSA or ECC, it is efficient and can be implemented in any environment.

In this study, we propose an authenticated key agreement scheme based on NTRU for applications in TMIS. The proposal enables two communicating parties in e-health platforms who share a simple password "pw" to generate a secret and authenticated session key, which will be used to secure subsequent communications through symmetric encryption cryptosystems, for example the Advanced Encryption Standard (AES).

MATERIALS AND METHODS

Definition and Notations: Let N, q and p be three positive integers, the ring R = Z [x]/(x^N -1) is called the ring of convolution polynomials. Similarly, we define the ring of convolution polynomials (mod q) as R$_q$ = Z$_q$[x]/(x^N - 1), where Z$_q$ = Z/qZ. We denote the convolution multiplication in R by '*'.

If f(x) = $\sum_{i=0}^{N-1} f_i x^i$ and g(x) = $\sum_{j=0}^{N-1} g_j x^j$are two polynomials in R, then h(x) = f(x)*g(x) is given by h(x) = $\sum_{k=0}^{N-1} h_k x^k$ where h$_k$ = $\sum_{i+j=k \bmod N} f_i\, g_j$.

For any positive integers d_1 and d_2, we let $T(d_1, d_2)$ be the set of polynomials $f(x) \in R$ which has d_1 coefficients equal to 1, d_2 coefficients equal to -1 and has all other coefficients equal to 0 .

Corresponding Author: Taoufik Serraj, ACSA Laboratory, Faculty of Sciences, Mohammed First University, Oujda 60000, Morocco

Polynomial in $T(d_1, d_2)$ are called ternary polynomials. We propose the use of the Non-Adjacent Form (NAF) of some chosen integers to build coefficients defining such polynomials.

The NTRU encrypt/decrypt scheme: In this section, we describe the NTRU cryptosystem. The NTRU parameters are the positive integers: N, p, q and d, where N and p are primes, $q > (6d + 1)p$ and $\gcd(N, q) = \gcd(p,q) = 1$:

- In the keys generation phase, Alice chooses the public parameters (N, p, q, d) satisfying the security requirement described in Hoffstein *et al.* (2015). Alice chooses randomly two polynomials $f(x) \in T(d+1,d)$ and $g(x) \in T(d, d)$. Alice computes the inverses $F_q(x) = f^1(x)$ in R_q and $F_q(x) = f^1(x)$ in R_q. Next, Alice computes $h(x) = F_q(x)*g(x)$ in R_q. The polynomial h(x) is Alice's public key. Her private key is f(x).
- In the encryption phase, Bob's plaint text is a polynomial $m(x) \in R$ whose coefficients satisfy-$1/2p < m_i \leq ½\, p$. Next, Bob chooses a random polynomial $r(x) \in T(d,d)$ and computes: $c(x) \equiv ph(x) * r(x) + m(x) \bmod q$
  Bob's cipher text is the polynomial c(x).
- In the decryption phase, Alice decrypts the encrypted message c(x) using f(x) by computing $a(x) \equiv f(x) * c(x) \bmod q$, the message m(x) is obtained from $a(x)$ by reducing the coefficients of $F_p(x) * a(x)$ modulo p, as follows:

  $a(x) \equiv f(x) * c(x) \bmod q$
  $a(x) \equiv f(x) * (ph(x)*r(x) + m(x)) \bmod q$
  $a(x) \equiv pg(x) * r(x) + f(x) * m(x) \bmod q$
  Now, Alice computes $F_p(x) *a(x) \bmod p$ and $b(x) \equiv F_p(x) *a(x) \bmod p$
  $b(x) \equiv F_p(x) * (pg(x)*r(x)+f(x)*m(x)) \bmod p$ $b(x) \equiv m(x) \bmod p$.

We note that the condition q>(6d+ 1) pis necessary for the decryption process.

Description of the proposed scheme: The server *S* in e-health platforms allows a user *U* to register once. After that, *U* can access to the server *S* anytime and anywhere using his/her password denoted "pw" without further registrations. After the registration step, *U* and *S* share a common password "*pw*", they also agree on: the NTRU parameters (N, p, q, d) certified by a trusted party, the server's and the user's public keys pk_S and pk_U, the NTRU encryption (NTRUEnc) and decryption (NTRUDec) functions, a random number generator, a message authentication code MAC and a secure hash function *H*. The proposed scheme is depicted in Table 1, it can be performed as follows:

Table 1: The NTRU-AKA scheme for e-health platforms

User		Server
(pk_U, sk_U)		(pk_S, sk_S)
$r \leftarrow_R [1,n]$		$s \leftarrow_R [1,n]$
$X = H(pw)^r$		$Y = H(pw)^s$
$X^* = NTRUEnc(X, pk_S)$		
$Y^* = NTRUEnc(Y, pk_U)$		
	X^*	
	$\rightarrow$	
	Y^*	
	$\leftarrow$	
$Y = NTRUDec(Y^*, sk_U)$		$X = NTRUDec(X^*, sk_S)$
$K_U = Y^r$		$k_S = X^s$
	$k_U = k_S = H(pw)^{rs}$	
$S_k = H(U,S, X^*, Y^*, k_U)$		$S_k = H(U,S, X^*, Y^*, k_S)$
	$S_k = k_{enc} \Vert k_{mac}$	
$u = MAC(k_{mac}, Y^*)$		$v = MAC(k_{mac}, X^*)$
	u	
	$\rightarrow$	
	v	
	$\leftarrow$	
Abort if *v* is invalid		Abort if *u* is invalid

- The user (resp. The server) randomly chooses *r* (resp. *s*) in [1, n], for a chosen *n*.
- The user (resp. The server) computes $X = H(pw)^r$ (resp.$Y = H(pw)^s$), encrypts it through NTRUEnc using the server's public key pk_S (resp. the user's public key pk_U) and sends the encrypted value X^* (resp.Y^*) to the server (resp. the user).
- On receiving Y^* (resp. X^*), the user (resp. the server) recovers Y (resp. X) by decrypting under its private key sk_U (resp.sk_S), they both compute$Y^r = X^s = H(pw)^{rs}$.
- The user and the server individually derive the session key material through the hash function *H* using their identities *U* and *S* concatenated with the values of X^*, Y^* and $H(pw)^{rs}$.

The session key generated between *U* and *S*, denoted S_k is $H(U, S, X^*,Y^*, H(pw)^{rs}) = k_{enc} \Vert k_{mac}$.

- The user (resp. the server) computes: $u = MAC(k_{mac}, Y^*)$ (resp. $v = MAC(k_{mac}, X^*)$) and sends *u* (resp.*v*) to the server (resp. the user). Each party checks the others MAC and reports a failure in case of a mismatch.
- Now, both parties explicitly confirm knowledge of the session key S_k.

We highlight that sk_S and sk_U are static keys, while S_k is an ephemeral key generated at the end of each scheme execution.

Design choices for the proposed scheme: In real world applications, cryptographic protocols should provide an optimal trade-off Security/Efficiency. According to IEEE 1363.1 (Whyte *et al.*, 2008), X9.98 (ANSI X9.98,

2010) and NIST (Chen *et al*., 2016) standards, the NTRU based cryptosystems appear to be more practical and use small keys, making it ideal for all environments and more suitable for embedded and mobile systems. Consequently, to ensure the currently required security level k = 128, we choose our scheme parameters as follows:

- N = 613,
- q = 2048,
- p = 3,
- d = 55,
- The choice of *n* do not affect the security since NTRU secures the exchange, for efficiency purpose, we can choose a small *n*.
- RNG is a (pseudo-) random number generator of class DRG.3,
- *H* is the SHA-224 hash function,
- MAC is a Message Authentication Code.

Experimental parameters: To analyze the execution time of cryptographic operations, we compare the total computational cost in the login and the authentication phases of Xie *et al*. (2013) and Xu *et al*. (2014) and our proposed scheme. We use PARI/GP systems in the environment (CPU: 2.16 GHz and RAM: 2GB), with the required security parameters for RSA and ECC (Lochter and Merkle, 2010) defined as follows:

For RSA we take:

- p_{RSA}= 160120 36164 5344 79271 6955 177235 31391 61031 61853 6375 20131 69227 5166 255922 9053261 98153 286480 258678 43690 747669 52180450 689139 78708 12211 1790700 94231042661171255671305168105512878939643 22897304469783315661048359317377457938232 27478687778052731633173755999016012036164 53447927169551772353139161031618536375201 31692275166255922905326198153286480258678 43690747669521804506891397870812211179070 09423104266117125567130516810551287893964 32289730446978331566104835931737745793823 22747868777805273163317375599900412103059 81588112522647836074493467269213460684054 08815570101;
- q_{RSA} = 231739 47692 244170 874190 268460 68 19600 43663868 14065 772370 87630 9438730 39680 9151560 3956 117767 1355 1132699 815837 9214 8923 8462 8696 42721 8148 589290 3522 8973 46704 58237 58717 901579 331180 0640 58180 8686 3778 73901 397994 191590 1671910 270531 71759 2478020 278781818 94694284 747993 126133 99545501 4695250 68959 7594 12769812939430909303900 9;
- e_{RSA}= 65537;

For ECC we take:

- p_{ECC} = 22721622932454352787552537995 9 109280733407321459449923044354729413 11;
- a_{ECC}= 11020 7252 7262 57423 61946 4808330 143440 15343 4569186684560615890015 10723;
- b_{ECC} = 394960 66260 533740 307879 2645769 51397 6611844 29460 52311 411513528958987;
- P_x= 14283 6492 7244 2017 2643 1498 2074 754 8649 69930 6726 7318 5208 44137 448783997;
- P_y = 933755 5360 4488 2322 7812410 7531774 6863 12155 58779020518084752618816205;

RESULTS AND DISCUSSION

In this section, we present and discuss our results in the light of the works of Stehlé and Steinfeld (2011) and Hoffstein *et al.* (2015) and the recent NIST technical report on post-quantum cryptosystems (Chen *et al*., 2016).

Security of the proposed scheme: The security of NTRUEnc relies on the presumed hardness of the "Short Vector Problem" (SVP) in some lattices. Stehlé and Steinfeld (2011) proposed a modified version of NTRUEnc to make it provably secure in the standard model by assuming the quantum intractability of standard worst-case lattice problem in very special lattices.

Recently, Hoffstein *et al*. (2015) reviewed attacks on NTRUEnc and discussed how can we prevent such attacks by a good choice of security parameters. In this scope and in the aim of avoiding the following attacks, it suffices that:

- **Hidden collisions attack (Vaudenay, 1996):** To ensure that no back doors exist in the NTRU parameters, the parameter generation algorithm must be published and certified by a certification authority, using Public Key Infrastructures (PKI).
- **Coppersmith-Shamir and lattice reduction attacks:** The attack of Coppersmith and Shamir attack (Coppersmith and Shamir, 1997) is based on the construction of a lattice L from the parameters N, q, d combined with reduction algorithms (Lenstra *et al*., 1982) to find the private key. These attacks can be avoided by choosing a prime number N of sufficiently bigger size (e.g., N = 613).
- **How grave-Graham attack (Howgrave-Graham, 2007):** The polynomials used in the cryptosystem as keys and messages, should be ternary polynomials and the probability p_s that a correct guess in the meet-in-the-middle stage must be determined mathematically. In addition, parameters must be chosen so that the expected work to recover both the private key f(x) (from the public key h(x)) and the plaintext m(x) (from the cipher text c(x)), is at least 2^k (for a security level k = 128).
- **Decryption failures attack (Howgrave-Graham et al., 2003):** The probability of decryption failures must be at most 2^{-k} for a security level k = 128 (i.e., $q > (6d + 1)\,p$).

Table 2: Computational cost comparisons

Schemes	Xie *et al*. (2013)	Xu *et al*. (2014)	Ours
Operations	$8T_H+6T_E+T_S$	$11T_H+6T_M$	$6T_H+4T_{NTRU}$
Time	2928 ms	90 ms	20 ms

The parameters specified by Hoffstein *et al*. (2015) meet all the security requirements to secure the NTRUEnc function.

- **Additional security requirements:** The message authentication code MAC should be unforgeable against adaptively chosen message attacks. In addition, the hash function *H* and the random number generator must ensure a random uniformly distributed value in the output.

The proposed scheme satisfies the following additional security properties:

- **Resistance against replay attacks:** An attacker can intercept X^* and Y^*, but he cannot compute *X* or *Y*. Generally, he cannot deduce k_{mac}. Therefore, he fails to compute a correct message authentication code. Consequently, the proposed scheme can resist the impersonation and the replay attacks.
- **Secure mutual authentication:** Under the assumption that the message authentication code MAC is unforgeable against adaptively chosen message attacks, each entity confirms the knowledge of the session key and it is sure that it shares the correct session key with the right partner. Therefore, the proposed scheme ensure a secure mutual authentication.
- **Forward quantum-resistance:** Data exchanged in public networks today are encrypted using RSA or ECC, the encrypted information can be stolen and stored until quantum computers will be available. Attackers will be able to recover all previous messages. Since NTRU is secure against quantum attacks, the encrypted information using NTRU will remain secure in the future.

Efficiency of the proposed scheme: Using the following notations:

- T_H : The time cost of a hash operation;
- T_E : The time cost of a modular exponentiation;
- T_M : The time cost of the scalar multiplication in ECC;
- T_S: The time cost of a symmetric encryption or decryption operation.
- T_{NTRU}: The time cost of NTRU encryption or decryption operation.

We get $T_M \approx 15$ms, $T_E \approx 488$ms and $T_{NTRU} \approx 5$ms. Also, we note that T_H and T_S are negligible compared to T_E or T_M.

Table 2 summarizes the total time cost of Xie *et al*. (2013) and Xu *et al*. (2014) and our proposed scheme.

Results in Table 2 show that NTRU is a fast public key cryptosystem compared to RSA or ECC. The polynomial convolution product is done with simple operations on small coefficients of sizes almost 11bits, while RSA (resp. ECC) requires complex exponentiations (resp. scalar multiplications) with integers of size that can reach 2048 bits (resp. 224 bits) for the same security level (128 bits).

In the NIST report (Chen *et al*., 2016), AES is considered as a post-quantum encryption scheme, therefore, we propose the combination of our scheme with AES-128 (or AES-256) to preserve the forward quantum-resistance.

CONCLUSION

Using NTRU cryptosystem, we have proposed a scheme to authenticate users and to generate strong session keys in e-health platforms. The proposal ensures many interesting security features such as confidentiality of session keys, perfect forward secrecy and mutual authentication. Finally, the use of NTRU combined with AES and SHA hash functions provides an efficient and a quantum-resistant alternative to schemes based on RSA or ECC against quantum attacks.

REFERENCES

ANSI X9.98, 2010. Lattice–based polynomial public key establishment algorithm for the financial services industry. Technical Report: X9.98, American National Standards Institute (ANSI).

Chen, L., S. Jordan, Y.K. Liu, D. Moody, R. Peralta, R. Perlner and D. Smith-Tone, 2016. Report on post-quantum cryptography. Internal Report: 8105, National Institute of Standards and Technology (NIST).

Coppersmith, D. and A. Shamir, 1997. Lattice Attacks on NTRU. Proceeding of the 16th Annual International Conference on the Theory and Application of Cryptographic Techniques. Konstanz, Germany, May. 11-15, pp: 52-61.

Hoffstein, J., J. Pipher and J.H. Silverman, 1998. NTRU: A ring-based public key cryptosystem. Proceeding of the 3rd International Symposium on Algorithmic Number Theory. Springer-Verlag London,, June 21-25, pp: 267-288.

Hoffstein, J., J. Pipher, J.M. Schanck, J.H. Silverman, W. Whyte and Z. Zhang, 2015. Choosing parameters for NTRUEncrypt. Cryptology ePrint Archive, Report: 2015/708.

Howgrave-Graham, N., 2007. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. Proceeding of the 27th Annual International Cryptology Conference. Santa Barbara, CA, USA, August 19-23, pp: 150-169.

Howgrave-Graham, N., P.Q. Nguyen, D. Pointcheval, J. Proos, J.H. Silverman, A. Singer and W. Whyte, 2003. The impact of decryption failures on the security of NTRU encryption. Proceeding of the 23rd Annual International Cryptology Conference. Santa Barbara, California, USA, August 17-21, pp: 226-246.

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48(177): 203-209.

Lenstra, A.K., H.W. Lenstra and L. Lovász, 1982. Factoring polynomials with rational coefficients. Math. Ann., 261(4): 515-534.

Lochter, M. and J. Merkle, 2010. Elliptic Curve Cryptography (ECC) brainpool standard curves and curve generation. Internet Engineering Task Force (IETF), RFC 5639.

Miller, V.S., 1985. Use of elliptic curves in cryptography. Proceeding of the Conference on the Theory and Application of Cryptographic Techniques. Santa Barbara, CA, USA, August 18-22, pp: 417-426.

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM., 21(2): 120-126.

Shor, P.W., 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26(5): 1484-1509.

Stehlé, D. and R. Steinfeld, 2011. Making NTRU as secure as worst-case problems over ideal lattices. Proceeding of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tallinn, Estonia, May 15-19, pp: 27-47.

Vaudenay, S., 1996. Hidden collisions on DSS. Proceeding of the 16th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara, California, USA, August 18-22, pp: 83-88.

Whyte, W., N. Howgrave-Graham, J. Hoffstein, J. Pipher, J. Silverman and P. Hirschhorn, 2008. Draft standard for public-key cryptographic techniques based on hard problems over lattices. Technical Report: IEEE P1363.1, Institute of Electrical and Electronics Engineers (IEEE).

Xie, Q., J. Zhang and N. Dong, 2013. Robust anonymous authentication scheme for telecare medical information systems. J. Med. Syst., 37(2): 9911.

Xu, X., P. Zhu, Q. Wen, Z. Jin, H. Zhang and L. He, 2014. A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. J. Med. Syst., 38(1): 9994.