A Blind Digital Signature Protocol over NTRU

El Hassane LAAJI, [1,*],and *Abdelmalek AZIZI*[2]
[1] Department of Mathematic and Computer Sciences, Mohammed First University, Oujda, Morocco
[2] Department of Mathematic and Computer Sciences, Mohammed First University, Oujda, Morocco

Abstract. Actually, the NIST post-quantum cryptosystem standardization competition reached its third round with seven finalist candidates. And NIST invites the cryptographic community to analyzing the selected candidates. In this context, we contribute by creating a new blind digital signature protocol over our release of NTRU post-quantum cryptosystem. Our protocol can be a variant of FALCON digital signature scheme, which is among of those finalist candidates. Because of our NTRU release is additively homomorphic, we successfully blind and unblind the digital signature by adding a random message. We obtained good results; the speed performance of our protocol outperforms FALCON by a factor up to 27, with a stronger security level, and perfect correctness.

1 Introduction

Actually, the NIST post-quantum cryptosystem standardization project is still in process and the competition reached its third round in July 2020, with seven finalists candidates, and eight alternate candidates. The digital signature schemes selected for this round are " FALCON, RAINBOW, and CRYSTALS".

FALCON [1] is based on NTRU assumption, which is structured lattice and in its report [2], NIST states that the "structured lattice schemes appear to be the most promising general-purpose algorithms for public-key encryption/KEM and digital signature schemes ". For more details about FALCON and the others candidates, the reader can see NIST competition website.

The handwritten signatures on documents have long been used to prove the identity of their authors or at least the signatory's agreement with the content of the document. We would like to do the same with computers and communication networks during exchanges. Therefore, the digital signature mechanism makes it possible to guarantee the integrity of an electronic document and to authenticate the document author, by analogy with the handwritten signature of a paper document.

In this paper, we consider FALCON as our study case, and we create a new Bind Digital Signature Protocol over our NTRU release[3], which implements an improved NTT(Number Theoretic Transform) algorithm [4] for increasing the performance and uses the (SHA3-512) Keccak hash function [5] for increasing the security level.

The Blind and UnBlind of the digital signature down correctly, because NTRU is Additively Homomorphic.

The plan of this work is as below: the section.1 contains this introduction; in section.2, we give the preliminaries knowledge by describing briefly of the blind digital signature scheme over RSA, the FALCON signature scheme, the NTRU cryptosystem, and the Fully Homomorphic Encryption (FHE) ; the section.3 describes our Blind Digital Signature Protocol, namely **"NTRUblind_Sign"**; in section .4, we give a benchmarking and result of our NTRUblind_Sign compared to the FALCON signature scheme; and the latest section.5 concerns the conclusion and our future works.

2 Preliminaries

There are many examples and studies focused especially on the digital signature schemes and the blind digital signature schemes. In this section, we describe briefly how RSA implements the Blind signature [6]; we give an over view of the FALCON signature scheme [1] which is finalist candidate and which is our study case; we describe the NTRU post-quantum cryptosystem which our protocol is based on; and we describe the FHE (Fully Homomorphic Encryption) technique, which we are going to use for blinding the signature.

* Corresponding author: author@e-mail.org

2.1 Blind Signature with RSA

As in the literature of RSA, let be: $N = p * q$, e the public key, and d the private key, with $e * d = 1\ (mod\ N)$.

1. Alice sends a message *m* to Bob;
2. Bob receives *m* and sends a random message *r* to Alice;
3. Alice computes: $m' = (m * r)^e\ (mod\ N)$; and sends it to Bob;
4. Bob computes: $s' = (m')^d\ (mod\ N)$;
5. Bob unblinds the message by:
$$s = s' * r^{-1}\ (mod\ N).$$
6. Bob verify if *($m = s^e$ (mod N))*.

Alice performs the RSA blind signature in line.3 by multiplying his message *m* by the random message *r* received from Bob. And Bob unblind the signature by decrypting the message *m'* received from Alice and multiplying the result by the inverse of his random message *r*.

NB: It is possible that Alice encrypts the message *m* by Bob's public key and Bob decrypts it by using its private key.

2.2 FALCON

It is a lattice-based signature scheme over NTRU, inspired from Gentry et al. Lattice-Based signatures framework constructed by solving appSVP for obtaining secure lattice-based signature [9]. The FALCON obtains the trapdoor sampler by using fast Fourier sampling to construct hash-and-sign lattice-based signature scheme [1]. FALCON team creates two releases with sequences parameters satisfying the security level 3 and 5 claimed by NIST, respectively [2]. $Rq = \mathbb{Z}q[X] = (X^n + 1)$

It operates in the ring, and the polynomials are sampled according to Centered Binomial Distribution (sampCBD), by using SHAKE-256 Keccak hash function, inspired from Alkim et al. work [10].

2.3 NTRU post-quantum cryptosystem.

NTRU was created in 1996 by the three mathematicians J. Hofstein, J. Pipher, and J. H. Silverman, and published in 1998. It is the first cryptosystem that is completely structured lattices. NTRU is defined in the ring $Rq = \mathbb{Z}q[X] = (X^n - 1)$, with n is prime and $q = 2^k$, or in the ring $Rq = \mathbb{Z}q[X] = (X^n + 1)$ with $n = 2^k$, and q prime. The use of the ring structure reduces the key size and increases the speed performance that can be carried out [11]. The latest version is actually a candidate for the NIST PQC project, see [12].

2.4 Fully Homomorphic Encryption (FHE).

Rivest, et al. proposed the FHE method since 1978, but the creation of the first FHE scheme based on lattice scheme(Ring-LWE) was realized in 2009 by Gentry [13].

Our protocol Blind and UnBlind the digital signature by using the homomorphic encryption technique over our NTRU post-quantum cryptosystem release [14]. We give herein a brief definition of the homomorphic encryption.

Additive Homomorphic Encryption:
$$Dec(c_1 + c_2) = Dec(c_1) + Dec(c_2) = m_1 + m_2.$$

Multiplicative Homomorphic Encryption:
$$Dec(c_1 * c_2) = Dec(c_1) * Dec(c_2) = m_1 * m_2.$$

A cryptosystem is FHE, if it is additively and multiplicatively homomorphic. In our work, we used only additive homomorphic encryption for blinding the digital signature. For more information the reader can see the NIST report [15].

3 Our Blind Digital Signature over NTRU "NTRUblind_Sign"

3.1 NTRUblind_Sign Description.

NTRUblind_Sign protocol is inspired by our NTRU [3] release and it is defined in the polynomial ring $Rq = \mathbb{Z}q[X] = (Xn + 1)$. Its parameters satisfying the security level category 5 defined by NIST, and the polynomials are chosen according to Centered Binomial Distribution (sampCBD) [10], with the coefficients defined in [-3,…, 3], except the plain-text is codified in a binary polynomial. We note that the modulus q is the fourth prime number, which was first studied by Pierre Fermat [8].

The keys generation process of NTRU, begin by : (1) generating two polynomials *f* and *g* according to CBD; (2) computing a polynomial $F = pf + 1$ [16], and computing its inverse $invF = \frac{1}{F}\ (mod\ q)$; (3) computing the polynomial $H = g * invF\ (mod\ q)$; and for our protocol, we consider *F* as the public key and *H* as the private key .

So, the NTRU encryption function is defined by:
$$C = Encryption(H, M) = p(r * H) + M\ (mod\ q).$$
with r is a small polynomial chose randomly; and the decryption function is defined by:
$$= Decryption(F, C) = (F * C\ (mod\ q))\ (mod\ p).$$

In the literature [11] , the NTRU assumption of public key encryption (PKE) scheme is defined by: *"Having the public key $H = \frac{g}{F}(\ mod\ q)$, it is hard to find the private keys F and g"*

So we can define the NTRU assumption for the Digital Signature scheme by: *"Having the public key $F = \frac{g}{H}\ (mod\ q)$ it is hard to find H and g"*. Then in our digital signature scheme, we keep *H* and g as private keys and we consider *F* as the public key.

3.2 NTRUblind_Sign implementation .

In this subsection, we describe the NTRUblind_Sign blind digital signature protocol processes, which implements the NTT (Number Theoretic Transform)[4] to increase the polynomials multiplication performance of the cryptographic functions, and uses the SHA3-512 Keccak hash function to get a strong security level. For more details on how we implement the NTT algorithm in NTRU the reader can see [3].

In this work, we opted to use the additive homomorphic encryption technique to blind the signature, because it is very fast and warrants perfect correctness than the multiplicative homomorphic encryption technique.

As we describe above, the sender (Alice) generates her public key *F* for signing the message and the private key *H* for verifying the signature, and she sends *F* to Bob for verification of the digital signature.

The protocol processes are defined and described below in corresponding to Figure.1:

Firstly, Alice performs the keys generation process to compute the polynomial *H* and the polynomial *F*, she keeps *H* and publishes *F* (sends it to Bob). And the communication process between Alice and Bob begins by:

(1) Alice uses $Hash(.)$ function to hash the digital message *M* by $SHA3-512$ Keccak hash function and codify the result into a binary polynomial

$$Sig_0 = Hash(M) \text{ and send } M \text{ to Bob;}$$

(2) Bob uses the same hash function $Hash(.)$ to hash the digital message *M* by $SHA3-512$ Keccak hash function and codify the result into a binary polynomial

$$Sig_1 = Hash(M);$$

(3) Bob generates randomly a binary polynomial *B* (noise) according to the Centered Binomial Distribution $B = SampCBD(seed)$; and sends it to Alice for blinding the signature;

(4) Alice generates two polynomials r_1, r_2 by $SampCBD(.)$ function;

(5) She signs the hashed message Sig_0 into the first signature by the function:

$$S_1 = p(r_1 * H) + Sig_0 \ (mod\ q);$$

(6) She signs the random message B received from Bob into the second signature by the function:

$$S_2 = p(r_2 * H) + B \ (mod\ q);$$

(7) She blind the signatures by the addition of S_1 and S_2 into a polynomial : $S = S_1 + S_2 \ (mod\ q)$ and sends *S* to Bob.

In line **(8)** and **(9)** Bob receives the blinded signature S, and unblinds it by the verification function using the public key *F* to produce the polynomial verification:

$V = F * S \ (mod\ q)$, and reduce it into:

$V = V \ (mod\ p)$; And finally **(10)** he verifies if his signature $Sig_1 = V - B \ (mod\ p)$; that means the sender Alice is authenticated, else the process must be repeated.

Alice		Bob
1. $Sig_0 \leftarrow Hash(M)$	$- \rightarrow M$	2. $Sig_1 \leftarrow Hash(M)$
	$B \leftarrow -$	3. $B \leftarrow sampCBD(seed)$
4. $r_1, r_2 \leftarrow sampCBD(seed)$;		
5. $S_1 \leftarrow p(r_1 * H) + Sig_0 \pmod q$;		
6. $S_2 \leftarrow p(r_2 * H) + B \pmod q$;		
7. $S \leftarrow S_1 + S_2 \pmod q$;	$- \rightarrow S$	8. $V \leftarrow F * S \pmod q$ with $V_i \in \{\frac{-q-1}{2}, \frac{q-1}{2}\}$
		9. $V \leftarrow V \pmod p$;
		10. $If(Sig_1) == V - B \pmod p$ Then return *True*. Else *False*.

Figure 1. A Blind digital signature protocol using the additive homomorphic encryption technique.

Proof: Because of NTRUblind_sign is Additively homomorphic, we can write :

$$V = F * S \ (mod\ q) = F * S_1 + F * S_2 \ (mod\ q). \quad (1)$$

Then we obtain the equation:

$$V = F * S = Sig_0 + B \ (mod\ p). \quad (2)$$

Bob verifies the digital signature by comparing the signature $\boldsymbol{Sig_1}$ to $\boldsymbol{X = V - B (\mathbf{mod}\ p)}$.

If $Sig_1 = X \ (mod\ p)$, that means $\boldsymbol{Sig_0 = Sig_1}$, and the sender "Alice" is authenticated. For more details, the reader can see the implementation code at [17].

4 Benchmarking performance

In this section, we will present the performances of our NTRUblind_Sign release compared especially to the performances of the FALCON 1024 Digital signature release, with sequences parameters $\{n = 1024; q = 65537; p = 2\}$, and $\{n = 1024; q = 12289; p = 2\}$ respectively.

For increasing the performance of our protocol we implemented the NTT (Number Theoretic Transform) for speeding up the multiplication in $Rq = \mathbb{Z}q[X] = (X^n + 1)$. We note that we perform all implementations on the platform PC-TOSHIBA i7-2630QM, RAM 8GO, and C++ language on Windows-7.

The reader can find the NTRUblind_Sign software at [17] and FALCON 1024 software at [18]. We note that, our software implements SHA3-512 hash function, which allows us to sign directly the polynomial message into binary polynomial and increase the security performance.

The average results got after executing 100 times both software are reported in milliseconds (ms), as presented in Table.1 .

Table 1. Speed performance of NTRUblind Sign compared to FALCON

Schemes	KeysGen	Signature	Verification
FALCON	37.06	1.17	0.19
NTRUblind_Sign	1 .12	0.15	0.12
Gap	33 times	7.8 times	1.6 times

In this result, we remark that our NTRUblind_Sign achieves excellent performances as presented by Table.1,

Its keys generation function is 33 times faster, the Signature function is 7.8 times faster, and the Verification is 1.6 times faster. That means we did better by increasing the speed performance and our release outperforms the FALCON version by a factor of up to ***27 times*** for the complete cryptographic process.

In terms of the security performance, the researchers on structured lattice schemes use essentially the lattice reduction algorithms (LLL, BKZ, etc.) to check the robustness of the cryptosystems based on lattices[19]. BKZ is chosen by NIST and many researchers to check the complexity of solving the lattice problems (CVP, SVP, uSVP, etc).

Therefore, we used Albrecht et al.[20] tools and their proposed BKZ cost model to measure the security levels. The NTRUblind_Sign achieves 2^{216} security level for classical security level and 2^{196} security for quantum security level. The security level of our release is almost the same as the security of FALCON, and we improve the security of our NTRUblind_Sign by implementing the strong SHA3-512 Keccak hash function, unlike FALCON which uses SHAKE-256 hash function.

5 Conclusion

Our NTRUblind_Sign Blind Signature Protocol can be a variant of FALCON which is actually a finalist candidate to NIST post-quantum standardization project, it can be also an alternative to RSA digital signature schemes which is actually used for many applications in the industrial area. The RSA is considered as classical cryptosystem and it can't resist to eventual quantum computer attacks.

The performance of our protocol is obtained because of the use of the NTT algorithm optimized, and the blind and unblind the signature down correctly because of the NTRU post-quantum cryptosystem release which is Additively homomorphic.

The flexibility of NTRUblind_Sign, allows us to implement it for the payment system, credit card, and in software as well as in hardware.

In our future works, we will study the implementation of the multiplicative homomorphic encryption technique for blinding the signature and improving our protocol to use it for the banking systems.

References

1. J. Hofstein, C. Chen, D. Danba, A. Hulsing, J. Rijneveld, J.M. Schanck, P. Schwabe, W. Whyte, and Z. Zhang, *FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU*, NIST post-quantum standardization Project, Wilmington USA (2019)
2. G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey. L. Yi-Kai, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson . and D. Smith-Tone, USA *'NISTIR 8309- Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process'*, NIST, USA (2020)
3. E. LAAJI, and A. AZIZI, *New Efficient and robust NTRU post-quantum key-exchange release-"NTRUrobust"*, Journal of theorical and applied Information Technology, Vol. 98, No. 23, December (2020)
4. P.Longa, and M. Naehri, M. *Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography*, Microsoft Research, USA, (2019)
5. G.V. Assche, G. Bertoni, J. Daemen, P. Peters, and R. Van, *Keccak Hash algorithm* , (2016)
6. J. Quisquater, and B. Libert, *Identity based undeniable signatures*, Topics in Cryptology- CT-RSA, LNCS 2964 (2004)
7. G. Chen, S. Jordan, D. Moody, L. Yi-Kai, R. Peralta, R. Perlner, and D. Smith. *NISTIR 8105 -Report on Post-Quantum Cryptography*», NIST post-quantum standardization Project, Gaithersburg, Washington, USA (2016)
8. P. Ribenboim, *The New Book of Prime Number Records*, New York, Springer-Verlag, USA, (1996)
9. Y. Wang, and W. Wang, *CRPSF and NTRU Signatures over cyclotomic fields*, School of Mathematics, Shandong University, Jinan, Shandong, 250100, P.R. China (2018)
10. E. Alkim, L. Ducas, T. Poppelman, and P. Schwabe, *Post-quantum key exchange- "New Hope"*, Department of Mathematics, Ege University, NIST post-quantum standardization Project, USA, (2019)
11. J. Hofstein, J. Pipher, and J.H Silverman, *Introduction Mathematics and Cryptography, NTRU*, USA (1998)
12. C. Chen, O. Danba, J. Hofstein, A. Hulsing, J. Rijneveld, M. Schanck, B. Schwabe, W. Whyte, and Z. Zhang, *Algorithm Specifications And Supporting Doc-umentation,* ,NIST post-quantum standardization Project, Wilmington USA (2019)
13. C. Gentry, *A FULLY HOMOMORPHIC ENCRYPTION SCHEME*, STANFORD UNIVERSITY, USA (2009)
14. E. LAAJI, A. AZIZI, and T. SERRAJ, *An Efficient Homomorphic Encryption scheme over NTRUrobust "NTRUrobust_FHE",* International Journal of Theoretical and Applied Information Technology, Vol 99 N 5, (2021).
15. M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, J. Hofstein, K. Lauter, S. Lokam, D. Micciancio, M. Moody, T. Morrison, A. Sahai, V. Vaikuntanathan, *Homomorphic Encryption Standard*. NIST USA (2018)
16. R. Mamdikar, V. Kumar, and D. Ghosh, *Enhancement of NTRU public key*, National Institute of Technology. Durgapur, (2002)
17. E. LAAJI, and A. AZIZI, *Implementation link of New Blind digital Signature Protocol over NTRU* , https://drive.google.com/_le/d/1nYHG5Cj5f6N-mlvjerYwf2IVHlXq0tQS/view?usp=sharing

18. J. Hofstein, C. Chen, D. Danba, A. Hulsing, J. Rijneveld, J.M. Schanck, P. Schwabe, W. Whyte, and Z. Zhang, *FALCON implementation and document' at NIST website : https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions*
19. J. Hofstein, J. Pipher, J.M. Schanck, J.H. Silverman, W, Whyte, and Z. Zhang, *Choosing Parameters for NTRUEncrypt*, Wilmington ,USA, (2016)
20. M. Albrecht, R. Curtis, A. Deo, A. Davidson, R. Player, W. Postlethwaite, F. Virdia, and T. Wunderer, *Estimate all the {LWE, NTRU} schemes*, In Security and Cryptography for Networks - 11th International Conference, SCN, Lecture Notes in Computer Science, Springer, Vol. 11035, pp. 351-367, (2018).