A Combination of BB84 Quantum Key Distribution and An Improved Scheme of NTRU Post-Quantum Cryptosystem

El Hassane Laaji* and Abdelmalek Azizi

Mohammed First University, Oujda, Morocco
E-mail: e.laaji@ump.ac.ma; abdelmalekazizi@yahoo.fr
**Corresponding Author*

Received 15 March 2022; Accepted 06 September 2022;
Publication 03 December 2022

Abstract

The BB84 quantum key distribution (QKD) protocol is based on the no-cloning quantum physic property, so if an attacker measures a photon state, he disturbs that state. This protocol uses two channels: (1) A quantum channel for sending the quantum information (photons polarized). (2) And a classical channel for exchanging the polarization and the measurement information (base sets or filters). The BB84 supposes that the classical channel is secure, but it is not always right, because it depends on the methods used during the communication over this channel. If an eavesdropper gets the sender or the receiver filters or both of them, he can leak some or all bits of the constructed key. In this context, we contribute by creating a protocol that combines the BB84 protocol with an improved scheme of NTRU post-quantum cryptosystem, which will secure the transmitted information over the classical channel. NTRU is a structured lattice scheme, and it is based on the hardness to solve lattice problems in $\mathbb{R}^n$. Actually, it is one of the most important candidates for the NIST post-quantum standardization project.

Keywords: Quantum cryptography, post quantum cryptography, BB84, NTRU.

Journal of Cyber Security and Mobility, Vol. 11_5, 673–694.
doi: 10.13052/jcsm2245-1439.1152

1 Introduction

The research in quantum technology is very intense to build quantum computers, quantum communication systems [1, 2], and other devices based on this technology [3]. This technology can offer many advantages and new solutions to major problems in different scientific fields [4, 5].

But, such a development represents a big security problem, because the currently widely deployed public-key cryptosystems, as we mentioned earlier, will be easily broken in polynomial time by the enormous power of the quantum computer [6, 7].

The first quantum computer was made by the Canadian company D-WAVE systems [8]. While the classical computer encodes information in bits, with a state exclusively at (0) or (1), on the other hand, the quantum computer uses what is called $qubit$ to encode information that can be in the state (0) and (1) at the same time, according to the principle of "superposition" of quantum mechanics [9–11].

The principles on which quantum mechanics is based are (1) **Entanglement**: two distant particles can communicate with each other, and if the state of one changes the other also; (2) **Superposition**: At the subatomic level, particles can be in two different quantum states at the same time; (3) Heisenberg's uncertainty principle; (4) and the quantum property of non-cloning which confirms the impossibility of copying or modifying the state of a qubit without disturbing its state [12].

In terms of security, quantum cryptography was first proposed in 1984 by Bennet and Brassard, known by the **BB84 Quantum Key Distribution (QKD)** protocol [13–15]. Quantum cryptography is based on the theory of quantum mechanics. It is supposed to be the most effective way to resist quantum computer attacks.

Over the years, various other schemes have been proposed, including B92 (Bennet, Bessette, Brassard, Salvail and Smolin 1992), BBM92 (Lo and Chau, 1999), and EPR (Inamori, Rallam and Vedral, 2000). Their general goal is to construct a key and share it securely, for use by a robust symmetric cryptosystem [16].

The BB84 quantum cryptography protocol makes it possible to discover any indiscretion in order to obtain perfect quantum communication and perfect security of the shared key. According to the properties of quantum mechanics and Heisenberg's probabilistic theorem: *"It is impossible for an attacker to listen on a quantum channel and measure the state of a photon (quantum information) without disturbing this state and without being* *detected"* [16]. If Eve tries to intercept the exchanged key by measuring or copying the transmitted photons, she will disturb the states of those photons.

he BB84 QKD protocol uses the combination of two communication channels, a quantum channel to exchange qubits (quantum information in the form of polarized photons), and a classic channel to exchange measurement information and validate communication according to the rate of acceptable error as we will explain in the following sections.

To transmit a set of binary information (bits), BB84 polarizes them and transforms them into quantum information (qubits) by polarizing them according to a corresponding **basis set (filters)**. A **diagonal basis** $\bigotimes$ with two states $\{\nwarrow, \nearrow\}$, or **rectilinear basis** $\bigoplus$ with two states $\{\uparrow, \rightarrow\}$ to polarize a single photon $\bigodot$, as shown in Figure 1 below.

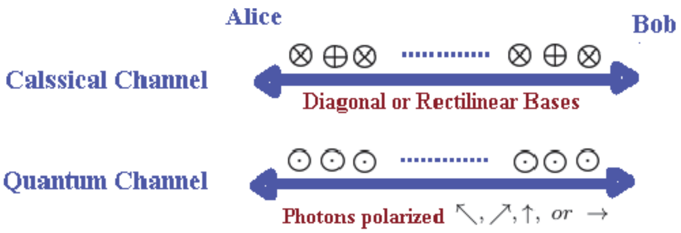

Figure 1 BB84 Quantum Key Distribution protocol using Classical channel and Quantum channel.

1.1 Outline

The remainder of our work is organized as follows:

Section 1: This introduction;
Section 2: We give a brief description of our contribution and related works;
Section 3: We Describe the BB84 Quantum Key Exchange protocol;
Section 4: A brief description of NTRU post-quantum cryptosystem. It is well described in Hoffstein et al. works [17, 18], and in Azizi et al. paper which describes an improved scheme of NTRU, namely "NTRUrobust" [19];
Section 5: We define our protocol that combines BB84 protocol and NTRUrobust to warrant security over quantum channels as well as over classical channels, and we give a discussion about the proposed solutions;
Section 6: Finally we give a conclusion and our future research orientation.

2 Our Contribution and Related Works

2.1 Our Contribution

So, we find that there are many vulnerabilities in the existing model of the BB84 protocol for its security on the public channel to ensure perfect security and build the quantum secret key (Shared Key).

For this objective, our work comes to solve this problem, by implementing the Azizi et al. **NTRUrobust** post-quantum cryptosystem [19] over the classical channel (inspired from NTRU scheme actually under standardization process) [18].

To do so, we are going to use **NTRUrobust-KEM** post-quantum key exchange primitive to ensure the exchange of thebasis series (filters), and the **NTRUrobust-PKE** public-key encryption primitive to ensure the measurement and validation information of the constructed key. For more details, the reader can read the paper [18, 19].

We discuss two solutions, which can be adopted alternatively according to the targeted security and the desired choice of the user [14].

1. The first solution concerns the use of two different basis sets (filters), one by the sender (Alice) to polarize the quantum information, and the other by the receiver (Bob) to measure the quantum information. In this case, the key reconciliation rate should be about (50%) of the transmitted key size without any attacks, and about (25%) in the case where there is an attack by an eavesdropper (Eve);
2. The second solution concerns the use of the same basis set (filter) randomly generated by (Alice) for the polarization that will be used by (Bob) to carry out his measurements of the states of the photons. In this case, they should obtain perfectly correlated bits, the key reconciliation rate must be (100%), without an attack by (Eve), and not less than (50%) in the case where an attack exists.

2.2 Related Works

There are several works that implement quantum key distribution protocols to achieve unconditional security and to improve the performance and reliability of implemented technologies for quantum communication devices and quantum systems.

Advances in research in this area allow the implementation and integration and combination of QKD with different communication protocols and with different cryptography schemes. Here we cite a few examples:

Rimitha Shajahan et al. [20], proposed a new approach to implement the BB84 QKD protocol, which can be combined with a traditional cryptosystem like RSA. The challenge is to secure communication over the classical channel. The author's protocol used the RSA cryptosystem for authentification of the sender and the receiver and the encryption-decryption of the key pairs exchanged by using a file manager system, and in the file transfer phase, the author uses the AES symmetric cryptosystem with SHA hash function for exchanging the encrypted files (the file can be an image, a video, or a text). For more details of this work, the reader can see the paper [20].

The work of Elboukhari et al. [21] presents a new approach to combining a quantum key distribution protocol with classical security protocols, and defines how they integrate QKD into the TLS protocol. Using the BB84 protocol, they have defined an extended TLS protocol that enhances the security of the TLS protocol as described in RFC5246. This work gives a new diagram illustrating this method for integrating QKD into the TLS protocol by providing more details. The mechanism of key distribution is established by QKD, and this shared key is modified at each new connection, which increases security.

In Ammar Odeh et al. work [22], the authors improve the quantum key distribution protocol by using the public key algorithm (RSA). They propose a three-party key distribution protocol.

Alice and Bob want to communicate securely with each other and require a secret key to secure their communication channel from a trusted third party.

This protocol involves three or more parties in the key distribution process, the objective of which is to improve the key distribution system by applying certain classical concepts and quantum techniques.

By applying public key concepts, the authors improve the user authentication process and data integrity. The proposed algorithm achieves a high percentage of correct bases by performing two phases:

1. User authentication and distribution of quantum bases;
2. Quantum Channel Data Transfer.

In Chainika Singhal et al. work [23], the authors propose a new security algorithm for distributing a key over the quantum channel. In this algorithm, it is assumed that two quantum channels between sender and receiver use diagonal basis $\bigotimes$ and rectilinear basis $\bigoplus$.

The sender sends the same data using two channels. The receiver measures data on the first channel using diagonal basis set and uses rectilinear basis set for the second channel.

By measuring both channels, the receiver cancels any measured bit that has a lower probability of 1. By this strategy, the parties agree on the quantum bases in order to transmit the data.

3 BB84 Protocol Description

The BB84 Quantum Key Distribution protocol was first created by Charles Bennett and Gilles Brassard in 1984 [13, 14]. It is the oldest and most important quantum cryptography protocol, and researchers in this field claim that quantum cryptography holds promise for exchanging secret keys.

Quantum cryptography, or "Quantum Key Distribution" as known by the cryptographic community, is used to produce and distribute a $K = \{0.1\}^n$ key, which can be used afterward by any symmetric cryptosystem chosen to encrypt and decrypt messages.

3.1 How BB84 Works

Assuming two interlocutors Alice and Bob who want to build a shared key using the BB84 QKD protocol, the process is described by the following steps:

1. First, Alice sends a sequence of quantum bits (qubits or photons) to Bob over a quantum channel, polarized respectively according to a basis set **(filter)** selected randomly;
2. Bob measures the qubits received respectively with his basis set **(filter)** which he has chosen randomly too;
3. Then Alice and Bob exchange their two **filters** respectively over the classical channel, in order to agree or not on the reconciliation between the bits sent and received to adjust the sequence of bits;
4. Finally, for verification and validation of the constructed key, Bob sacrifices a few bits and sends them to Alice over the classical channel to check for eavesdropping. For that, Bob takes for example a part of the key (for example (10%)) and sends it to Alice. If EVE was listening, Alice will find a few bit mismatches, so the whole key will be discarded, otherwise, the constructed key is valid.

This procedure can be repeated several times in order to make some error corrections to form a secret key.

BB84 works great if the communication over the classical channel is guaranteed unless a spy perfectly predicts the sender (Alice) on her

random filter and uses it to measure qubits and re-send to the recipient (Bob).

The BB84 is based on the transmission of polarized photons (one by one successively). Each photon is randomly polarized either by an orthogonal basis denoted $\bigoplus$ or by a diagonal basis denoted $\bigotimes$ and for each basis, there are two possible polarization states of a photon, as described below:

1. The basis $\bigoplus$ uses two rectilinear polarization, horizontal and vertical presented respectively by $\{\rightarrow, \uparrow\}$ which correspond respectively to the quantum notations $|0\rangle\ and\ |1\rangle$. We therefore consider the notation of the orthogonal basis and its polarization states by: $\bigoplus = \{\rightarrow),\ \uparrow\}$ which will respectively correspond to the binary codes 0 and 1.
2. The basis $\bigotimes$ uses two diagonal polarization presented by $\{\nwarrow, \nearrow\}$ which correspond to the quantum notations respectively $|+\rangle\ and\ |-\rangle$ with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\ rank)$. We therefore consider the notation of the diagonal basis and its polarization states by $\bigotimes = \{\nwarrow,\ \nearrow\}$ which will correspond respectively to the binary codes 0 and 1.

3.2 BB84 Protocol Process to Transmit One BIT

We assume that Alice takes a bit of information from a random number generator, $Bit \in \{0.1\}$, and wants to transmit it over the quantum channel. The process is described as follows in correspondence with Figure 2:

1. If information bit $Bit = 0$:
   (a) If Alice's quantum system uses the rectilinear basis $\bigoplus$, then the binary information is polarized into quantum information $\{\rightarrow\}$ and transmitted to Bob over the quantum channel;
   (b) If Bob's measurement basis is $\bigoplus$, then the quantum information received from Alice will be $\{\rightarrow\}$, otherwise, if the measurement basis is diagonal $\bigotimes$, the quantum information obtained will be probabilistic with 50% polarized at $\{\nwarrow\}$ and 50% polarized at $\{\nearrow\}$.
   (c) If Alice's quantum system uses the diagonal basis $\bigotimes$, the binary information will be polarized into quantum information $\{\nwarrow\}$ and transmitted to Bob over the quantum channel;
   (d) If Bob's measurement base is $\bigotimes$, the quantum information received from Alice will be $\{\nwarrow\}$, otherwise, if the measurement basis is rectilinear $\bigoplus$, the quantum information obtained will be probabilistic with 50% polarized at $\{\rightarrow\}$ and 50% polarized at $\{\uparrow\}$.

2. If bit information $Bit = 1$:
   - (a) If Alice's quantum system uses the rectilinear basis $\bigoplus$, the binary information will be polarized into quantum information $\{\uparrow\}$ and transmitted to Bob over the quantum channel;
   - (b) If Bob's measurement basis is $\bigoplus$, the quantum information received from Alice will be $\{\uparrow\}$, otherwise, if the measurement basis is diagonal $\bigotimes$, the quantum information obtained will be polarized into $\{\nwarrow\}$ or $\{\nearrow\}$ with an equal probability of 50%.
   - (c) If Alice's quantum system uses the diagonal basis $\bigotimes$, the binary information will be polarized into quantum information $\{\nearrow\}$ and transmitted to Bob over the quantum channel;
   - (d) If Bob's measurement basis is $\bigotimes$, the quantum information received from Alice will be $\{\nearrow\}$, otherwise, if the measurement basis is rectilinear $\bigoplus$, the quantum information obtained is probabilistic, it can be polarized into $\{\rightarrow\}$ or $\{\uparrow\}$ with a probability equal to 50%.

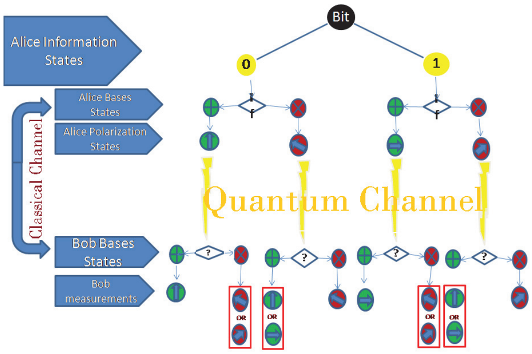

Figure 2 BB84 Quantum Key Distribution protocol using Classical channel and Quantum channel.

3.3 Full Transmission Process of BB84 Protocol

The description of the complete BB84 process in correspondence to Figure 3:

(1) Quantum transmissions (first phase)

1. (a) Alice generates randomly her series of bits $d \in \{0, 1\}^n$, and a basis set (or filter) $A \in \{\bigoplus, \bigotimes\}^n$, with $n > k$. k is the length of the final key we want to build.

2. (b) Alice prepares each information (d_i), which will be polarized according to the corresponding basis $A_i \in \{\bigoplus, \bigotimes\}$ and transformed into a quantum information a_{ij} with $a_{ij} \in \{\nwarrow, \nearrow, \rightarrow, \uparrow\}$ with $j \in \{0, 1, 2, 3\}$, and sends it to Bob over the quantum channel.
3. (c) Bob randomly generates his basis set (or filter) $B \in \{\bigoplus, \bigotimes\}^n$, with $n > k$. And begins to measure the quantum information a_{ij} sent by Alice, according to the basis B_i that is $\bigoplus$ *or* $\bigotimes$, to get a series of bits $d' \in \{0, 1\}^n$;

(2) Classical Channel transmission (Second Phase)
Alice and Bob communicate on the public channel, in order to agree or disagree with the bits received from Bob as follows:

1. Alice and Bob exchange the two filters A and B (Alice sends A to Bob and Bob sends B to Alice), using an information exchange system;
2. Bob performs a comparison of the two filters A and B (Resp. Alice as well), $if\ A_i \neq B_i$ the d'_i bit will be discarded;
3. Bob then obtains a subset K of the remaining bits, formed by the bits d'_i which verify $A_i = B_i$. So the common secret key constructed by the remaining bits is $K = \{0, 1\}^k$;
4. Then, Alice and Bob communicate via a classic channel without disclosing the result of the measurement for the correlation of the key to be built. If the rate of matching bits is less than the predefined threshold, both parties conclude that an attacker (Eve) is listening on the quantum channel and the communication must be interrupted and the whole process must be started again.
5. Alice and Bob, sacrifice some bits to verify the correctness of the sharing key. Bob will randomly select a small number of bits from his key, send them to Alice to verify them against her key, and eventually validate the process.

Thus, by constructing a long key, a sufficient security level can be achieved by sacrificing a few bits for verification and validation of the reconciliation key.

3.3.1 Discussion

If Alice and Bob use the same filter, the length of the constructed key will be obtained completely with a probability rate of 100% (without Eve attack). On the other hand, if they use two different filters, when the measurement is carried out on the wrong basis, Bob does not obtain any information because the result of the measurement is not correlated with Alice's filter.

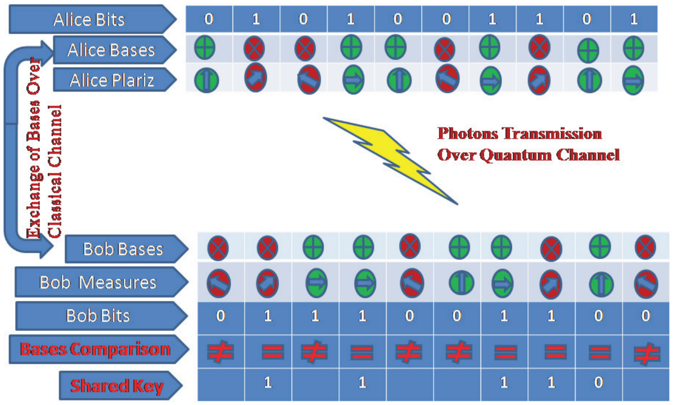

Figure 3 BB84 Algorithm process for subset of bits information.

It depends on the desired threshold if the error rate is below the threshold, error correction and privacy enhancement procedures are used to achieve a secure communication bit rate. "The uncertainty principle was applied in this experiment instead of mathematical modeling" [13, 14].

We want the filters exchanged over the classic channel to be very secure, because if an attacker (**Eve**) succeeds in recovering the Alice's or Bob's filter, he can construct the same keys without disturbing the communication. This is why we propose the post-quantum cryptosystem NTRUrobust [19] to guarantee confidentiality on the classical channel.

3.4 Description of Transmission in the Presence of An Eavesdropper

If an attacker EVE has access to the quantum channel and wants to measure the photons transmitted by Alice to Bob. EVE will randomly choose his filter too, and he will read the photon states emanating from Alice and relay them to Bob. For the cases where the measurement filters of Alice, Bob, and EVE are equal there will be no disturbance, and Alice and Bob will not feel anything, on the other hand, if the filter of EVE is different from the filters of Alice and Bob, the latter will detect the inconsistency and conclude that an attacker is listening on the quantum channel.

To detect Eve's attack, Alice and Bob test eavesdropping. The idea is that the bits where the filters of Alice and Bob are equal $(A_i = B_i)$, must also match $(d_i = d_i')$, otherwise an external disturbance is produced or there is noise in the quantum channel.

All disturbances are supposed to be caused by Eve, in this case even if two bases of Alice and Bob match each other, the measurement will be false as we describe in the process below: Alice and Bob will find that in some cases even if they used the same bases the results are not good. Positions 2, and 9 in the series present disturbances, even if the bases of Alice and Bob are equal, Bob will find that the photon polarization is wrong.

So in summary, the result will be as follow:

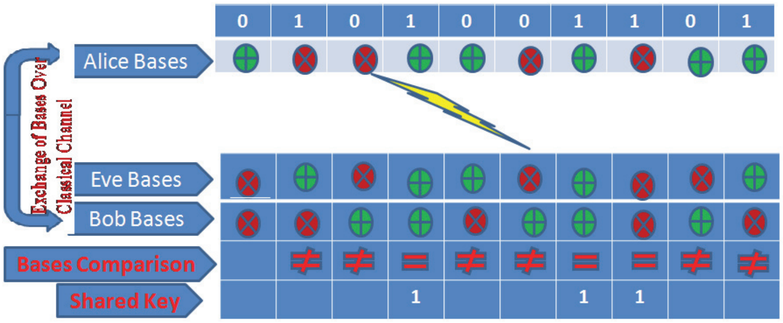

Figure 4 BB84 Algorithm process with disturbance performed by Eve.

If Alice and Bob are using two different filters, then the key length will be constructed by 25% of the original key transmitted by Alice. The example of Figure 4 above, reflects this case, we see that we obtained only $3bits$ of $10bits$ transmitted by Alice after the disturbance caused by EVE.

In the second case where the two filters of Alice and Bob are equal, the key length will be 50% of the original key transmitted by Alice.

Much research on the BB84 protocol negligee security over the classic channel which is used for exchanging the sets between Alice and Bob.

If Alice and Bob exchange their two filters **before** the transmission of photons on the quantum channel, it is assumed that EVE succeeds in hacking the communication on the classical channel and recovers Bob's set of filters, and uses it to measure the photon states transmitted by Alice, then he retransmits them to Bob. Alice and Bob won't feel anything and EVE will get the whole key.

But if Alice and Bob exchange their filters **after** the transmission of the photons on the quantum channel, we suppose that EVE listening on the quantum channel using its own filter, and at the same time it succeeds in recovering the filters of Alice and Bob. After EVE will analyze the result of the photon states obtained by using his filter and the filters of Alice and Bob;

finally he will retain the bits where the three filters match. From where EVE will recover at least 25% of the bits of the final key built by Alice and Bob, which reduces the complexity of an exhaustive attack on the build keys of 25%.

4 NTRU

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 [17].

NTRU was presented as an alternative to RSA, ECDH and ECC. NTRU releases have also been standardized by the IEEE P1363.1 standard in April 2011, and by the X9.98 standard.

Its domain of computation is the ring of the polynomials $\mathbf{R_q} = Z_q[X]/(X^N - 1)$, where N is a prime number and q is power of two, or in the ring of the form $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ with N power of two and q prime number.

Since its first creation there are several versions, the latest NTRU is now a candidate for NIST's post-quantum standardization project, and it is selected amount the four the third finalist public key encryption/KEM schemes. This is an exciting field of research and one of the most promising candidates for post-quantum cryptography. In terms of security, NTRU resisted more than 20 years of cryptanalysis.

The security of NTRU is based on the hardness of the SVP (Short Vector Problem), and the best tool used to prove the security is Lattice reduction by using the algorithms (Gram-Schmidt, LLL, BKZ algorithms) and Meet-in-The-Middle attack (MIM) algorithm [30].

According to the NIST experts' analysis, "NTRU provided two different cost models for estimating the security of its parameter sets: a local and a non-local model. The non-local model is most similar to the CoreSVP metric used by the other lattice-based submissions, and in this model, the NTRU submission lacks a category 5 parameter set proposal" [18,24,25].

In this work, we are going to implement an improved scheme of NTRU over a classical channel to combine it with BB84 protocol. This scheme is proposed by Azizi et al. namely **NTRUrobust** [19], it is inspired by NTRU release which is a candidate for NIST post-quantum standardization project [18].

NTRUrobust is presented in two primitives: NTRUrobus-KEM key exchange primitive and NTRUrobust-PKE public-key encryption primitive.

In order to increase the performance of those primitives, the authors used the NTT (Number Theoretic Transform) algorithm [26, 27] and FMMA (Fast Modular Multiplication Algorithm) [28]. The speed performance of NTRUrobust by using those algorithms is greater by a factor more than $\times 90$ compared to the use of convolution multiplication. For more details, the reader can read the authors' paper [19].

In terms of the security of NTRUrobust, it is based on the same NTRU assumption "Having the public key $H = G * F^{-1} \pmod q$ it is hard to find the private keys $G\ and\ F$ in the ring of the form $R_q = \mathbb{Z}_q[X]/(X^n + 1)$".

We obtained the result below by using Albrecht et al. Estimator described in their paper titled "Estimate all the LWE, NTRU schemes" [31]. Our NTRUrobust achieves 2^{216} for classical security level and 2^{196} for quantum security level, and we also improve its security by implementing the strong Keccak hash function SHA3-512.

Our release implementation provides perfect correctness of the decryption, the failure probability is ZERO. We obtained this result by using the python script developed by Hoffstein et al. [32], and executed by using SAGE software, for more information about decryption failure see [33] and [34].

5 BB84_NTRUrobust Protocol

The mixture of quantum cryptography and post-quantum cryptography will surely improve security and build more reliable keys. For this reason, we propose the combination of the BB84 and NTRUrobust protocol to secure both communications on the quantum channel and on the classical (or public) channel.

The quantum channel will take care of the transmission of quantum information on a quantum medium, and the classic channel will be responsible for transmitting the information of polarization, measurement, and reconciliation.

Therefore, we will use the two NTRUrobust primitives on the classic channel. The first NTRUrobust-KEM will be used to exchange the two filters of the sender (Alice) and the receiver (Bob) used respectively for polarization and measurement, and the second NTRUrobust-PKE will be used to encrypt the shared key and the validation information, as described in [19].

We will implement the complete process with the same parameters defined for both primitives $\{n = 1024, q = 65537, p = 2\}$, and we use the Keccak hash function $SHA3 - 512$ to build the two filters used by Alice and Bob.

The description of the complete process in correspondence with Figure 5, is as follows:

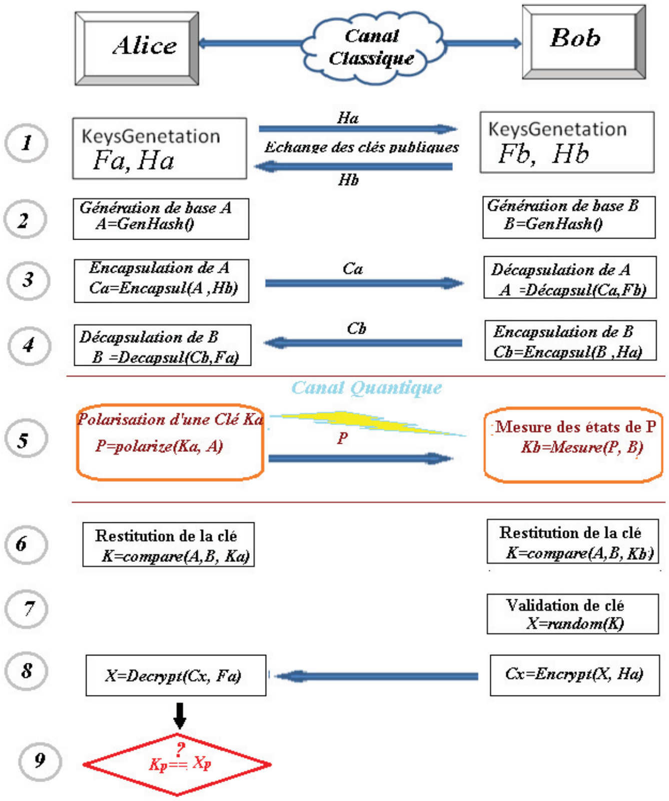

Figure 5 BB84 Algorithm process combined with NTRUrobust.

For the generated keys (public keys and private keys), they will be the same used for both NTRUrobus-KEM and the NTRUrobust-PKE. As in NTRU literature, we will designate Alice's and Bob's keys respectively by (F_a, H_a) and (F_b, H_b), with F_* the private key and H_* the public key.

For NTRUrobus-KEM we designate the Encapsulation and Decapsulation function respectively by **Encapsult, Decapsult**, and for NTRUrobus-PKE we designate the Encryption and Decryption functions respectively by **Encrypt, Decrypt**.

The $GenHash()$ function generate a polynomial and hashes it with the SHA3-512.

It is considered that two partners Alice and Bob want to build a shared key by using BB84 protocol on the quantum channel and NTRUrobust (NTRUrobust-KEM, NTRUrobust-PKE) on the classical channel:

1. Alice and Bob generate their keys (F_a, H_a) and (F_b, H_b) respectively, then they publish their public keys H_a and H_b;
2. Alice and Bob randomly generate two polynomials of dimension $n = 1024$ in $R_q = \mathbb{Z}_q[X]/(x^n + 1)$, then they apply the SHA3-512 hash function to obtain two series of bits A and B of dimension 512 to serve as basis series (filters). Let $A = GenHash()$ and $B = GenHash(.)$ respectively used for polarization by Alice and for measurement by Bob, whose coefficients will be coded by: 0 will correspond to the filter $\bigoplus$ and 1 will correspond to $\bigotimes$;
3. Alice encapsulates her filter A by the encapsulation function of NTRUrobust-KEM in an encrypted polynomial $C_a = Encapsul(A, H_b)$, and sends it to Bob who will use the decapsulation function of NTRUrobust-KEM to obtain the decrypted polynomial $A = Decapsul$ (C_a, F_b);
4. Bob encapsulates his filter B by the encapsulation function of NTRUrobust-KEM in an encrypted polynomial that is $C_b = Encapsul(B, H_a)$, and sends it to Alice who will use the decapsulation function of NTRUrobust-KEM to obtain the decrypted polynomial $B = Decapsul(C_b, F_a)$;
5. (a) In this phase of communication over the quantum channel, Alice will randomly generate a key K in the form of a series of "Bits" of dimension $n' = 512$, then she will polarize them into a series of quantum information "Qbits" according to the basis $\bigoplus$ or $\bigotimes$ by using her filter A (see Figure 3): $P = polarize(K_a, A)$. Bob, on the other side of quantum communication, measures the photons received by his filter B, to obtain a series of bits $K_b = Measure(P, B)$;
   (b) Then they make their comparisons each on their side of the two filters A and B, they reject the bits where the filters do not correspond and they retain the rest either: Alice obtains $K = compare(A, B, Ka)$ and Bob gets $K = compare(A, B, Kb)$ (So they get the same key if there is no attack performed by an eavesdropper EVE);
6. Once the transmission of quantum information on the quantum channel is complete, Bob selects randomly a small part X (10% of the key K for

example) of the key K, by also designing their positions in the series. This part X of the bits of the key K will be sacrificed to ensure that there was no eavesdropping on the quantum channel by an attacker (Eve);

7. Bob encrypts the series of bits X with their positions in the key K by the Encryption function of NTRUrobust-PKE, $C_x = Encrypt(X, Ha)$, and sends it to Alice who will decrypt it using the Decryption function of NTRUrobust-PKE, $X = Decrypt(C_x, F_a)$;
8. Finally, Alice compares the sample X and its key K, if the bits match the process confirms the establishment of the key K; if not, we conclude that an attacker is listening on the quantum channel to steal some information on the key or the whole key.

5.1 Discussion

In the case where the filters of Alice and Bob are different, and with the parameters used for NTRUrobust in particular the dimension of the network $n = 1024$ and Keccak hash function SHA3-512 [29]. We can build a key of $256bits$, because the generation of a polynomial of degree 1024 which corresponds to a message of $1024bits$, will be condensed by the hash function SHA3-512 into a string of $512bits$, and since we used this case where the filters are different, then we will obtain a probability of 50% match between Alice's and Bob's filters, so the key will be approximate of size $256bits$.

In the case where the filters of Alice and Bob are the same, and with the parameters used for NTRUrobust, in particular, the dimension of the lattice $n = 1024$ and the hash function SHA3-512, we can build a key of $512bits$, because the generation of a binary polynomial of degree 1024, will be condensed by the hash function SHA3-512 into a string of $512bits$, and since we used the same filter, then we will obtain a probability of 100% match between Alice's and Bob's filters, so the key will be approximate of size $512bits$.

But if we still want to opt for the first case, we can repeat the execution of the protocol several times. For example, if we run it twice we will get a key of $512bis$.

On the other hand, if we opt for the second case, we will gain both in terms of security and in terms of performance, because we will not need to do the two generations and exchanges of the filters. Only Alice will generate her filter A and exchange it with Bob.

But, it should also be noted that one needs to sacrifice some 5% bits (for example), or more for the verification phase if a spy was listening on the quantum channel, as explained in steps 6, 7, and 8 of Figure 5. So for the first case, there will remain $256 - 5\% * 256 = 243bits$ of the constructed key; and for the second case, there will remain about $426bits$ of the build.

Table 1 Performance comparison of case 1 and case 2, where Alice and Bob's filters are different or equal in (ms) respectively

Schemes	Cas 1	Cas 2
NTRUrobust-KEM	4.68	2.34
NTRUrobust-PKE	4.06	2.03
Total	8.74	4.37

Note that in the second case where Alice's and Bob's filters are equal, it is more efficient. So the protocol in this case runs in $4.4+\alpha$ ms with (α) the time needed for the process of the BB84 protocol on the quantum channel which includes biasing, transmission, and measurement. And adopting the first case will cost more, about $8.8 + \alpha$ ms.

The reader can see JAVA implementation of BB84 protocol at [35] on the Github website, and the NTRUrobust C++ implementation at [36], on our Google drive website.

We note that all the tests are performed on the platform PC-TOSHIBA – Satellite, Processor Intel, Core$^{\text{TM}}$i7-2630QM CPU, 2GHz, RAM 8GO, under Windows 7-32 bits, Dev-C++ 4.9.9.2, and JavaBeans environments.

6 Conclusion

The quantum computer and quantum communication technologies are in continuous evolution. Actually, China had set up a number of quantum communication networks, and it could have a global quantum communication network in the 2030s [15].

But when the quantum computer will be ready, the cryptosystems actually deployed like RSA, ECC, and ECDH will not resist quantum computer attacks. Then we should construct robust and efficient new post-quantum and quantum cryptosystems.

Therefore in this work, we increase the security of BB84 protocol, by using the NTRUrobust post-quantum cryptosystem over the classical channel, to exchange the polarization and measurement information of the sender and the receiver respectively to construct their quantum shared key.

The NTRU is appreciated by NIST experts and many researchers in the world. It is considered the best candidate submitted to NIST post-quantum standardization project, and it can be standardized a few years later and replace the actual classical cryptosystems.

Our work can be very useful for improving the protocol of Rimitha et al. [20] (cited in the related work section 2.2), by implementing our NTRUrobust post-quantum cryptosystem in place of the RSA cryptosystem.

This combination of quantum cryptography and post-quantum cryptography can allow the users of the Internet network to be more sure of their security life against eventual quantum computer attacks when it will be generalized.

For our future work, we will improve and adapt our protocol for implementing it in the real world, like a banking system.

We hope that our work can be interesting for cryptographic community researchers.

References

[1] Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei- Yue Liu, Shuang-Lin Li, Rong Shu, Yong-Mei Huang, Lei Deng, Li Li, Qiang Zhang, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Xiang-Bin Wang, Feihu Xu, Jian-Yu Wang, Cheng-Zhi Peng, Artur K. Ekert, and Jian-Wei Pan. *Entanglement-based secure quantum cryptography over 1,120 kilometres.* Nature, 582: 501–505, 06 2020.

[2] A. Abd EL-Latifab, B. Abd-El-AttyaSalvador E. Venegas-Andracac, W. Mazurczykd. Efficient quantum-based security protocols for information sharing and data protection in 5G networks. *Future Generation Computer Systems Volume 100, November 2019, Pages 893–906*, 2019.

[3] François Guillier. *La physique quantique au secours de la protection informatique*, Novembre 2020.

[4] B. Abd-El-Atty, A. Abd El-Latif, E. Venegas-Andraca. An encryption protocol for NEQR images based on one-particle quantum walks on a circle. *Quantum Information Processing September 2019* https://doi.org/10.1007/s11128-019-2386-3, 2019.

[5] B. Abd-El-Atty, A. M. Iliyasu, A. Alanezi, A A. Abd El-latif. Optical image encryption based on quantum walks, *Optics and Lasers in Engineering. Volume 138, 2021, 106403, ISSN 0143-8166*, https://doi.org/10.1016/j.optlaseng.2020.106403., 2021

[6] Eleni Diamanti. “Progrés et défis pour la cryptographie quantique”. Photoniques, 91:33–37, 05 2018.

[7] Lily Chen, StephenJordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith “NISTIR 8105 – Report on post-quantum cryptography”, Gaithersburg, Washington, USA 2016.

[8] Etienne Thierry-Aymé, https://www.science-et-vie.com/technos-et-futur/voici-le-nouvel-ordinateur-quantique-le-plus-rapide-au-monde-7668, le 6 février 2017.

[9] Joseph Iosue. “Math and proofs for the quantum algorithms implemented in the code”, note de cours, February 2, 2018.

[10] Patrick J. Coles et al. “Quantum Algorithm Implementations for Beginners”. Los Alamos National Laboratory, Los Alamos, New Mexico, USA, 2018.

[11] Fleur Brosseau, “Un ordinateur quantique de plus de 5000 qubits lancé en Europe”, https://trustmyscience.com/ordinateur-quantique-5000-qubits-lance-europe/, 21 janvier 2022.

[12] Michel Le Bellac. “Physique quantique”, livre 2ème édition, SAVOIRS ACTUELS, EDPSciences/CNRS ÉDITIONS, 2007.

[13] Charles H. Bennett et Gilles Brassard, “Quantum cryptography: Public key distribution and coin tossing”, Theoretical Computer Science, vol. 560, p: 7–11, 1984.

[14] BB84 Quantum Key Distribution Protocol https://fr.wikipedia.org/wiki/Protocole_BB84.

[15] François Guillier. Revue bibliographique – protocoles de cryptographie quantique et mise en place pratique en milieu aqueux. 07 2020.

[16] Maanav Seth et Amit Yadav, “Principes fondamentaux de la distribution de clés quantiques – Protocoles BB84, B92 et E91”, https://ichi.pro/fr/principes-fondamentaux-de-la-distribution-de-cles-quantiques-protocoles-bb84-b92-et-e91-247627336138413, 2020.

[17] J. Hoffstein, J. Pipher, and J.H. Silverman. Introduction Mathematics and Cryptography NTRU. Wilmington USA, 1998.

[18] Cong Chen, Oussama Danba, Jeffrey Hofstein, Andreas Hülsing, Joost Rijneveld, John. Schanck, Peter Schwabe, William Whyte, Zhenfei Zhang “Algorithm Specifications And Supporting Documentation” March 30, 2019.

[19] E. Laaji and A. Azizi, New Efficient and robust NTRU post-quantum key-exchange release – “NTRUrobust”. Department of Mathematics, Mohammed First University, Oujda, Morocco. *Journal of Theoretical and applied Information Technology, Vol 98 N 23 December 2020.*

[20] Rimitha Shajahan, Suchithra S. Nair. “Simulation of BB84 Protocol over Classical Cryptography Channel for File Transfer”, *International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 09*, Sep 2020.

[21] Mohamed Elboukhari, Mostafa Azizi and Abdelmalek Azizi. “Improving TLS Security by Quantum Cryptography”. International Journal of Network Security & Its Applications (IJNSA), Vol. 2, No. 3, July 2010. University Mohamed Ist, Oujda, Morocco.

[22] Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah. “Quantum Key Distribution by Using Public Key Algorithm (RSA)” – Department of Computer Science & Engineering University of Bridgeport Bridgeport, USA.

[23] Chainika Singhal, Ravinder Kr. Gautam, Lakshman Das, Manoj Kumar Mishra. “Enhancement of Quantum Key Distribution Protocol”. International Journal of Engineering Science and Researches. VIET, Ghaziabad. 2012.

[24] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta Ray Perlner, Angela Robinson, Daniel Smith-Tone: “Status Report NISTIR 8240 on the First Round of the NIST Post-Quantum Cryptography Standardization Process” USA 2019.

[25] 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, NISTIR 8309- Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST, USA (2020).

[26] Nayuki Project, Number-Theoric-Transform (Integer DFT), website Link: https://www.nayuki.io/page/number-theoretic-transform-integer-dft

[27] Alkim, E. Ducas, Poppelman, T. and Schwabe, P. Post-quantum key exchange – “New Hope”. Department of Mathematics, Ege University, USA, 2019.

[28] E. Laaji, A. Azizi and T. Serraj, New Fast Modular Multiplication Algorithm applied to Ring-LWE scheme, Department of Mathematics, Mohammed First University, Oujda, Morocco. *International Journal of Theoretical and Applied Information Technology, Vol 99 N 7, April 2021*.

[29] G.V. Assche, G. Bertoni, J. Daemen, P. Peters, and R. Van. *Keccak Hash algorithm*, Radboud University, Nederlands, 2016.

[30] J. Hoffstein, J. Pipher, J.M. Schanck, J.H. Silverman, W. Whyte, and Z. Zhang. *Choosing Parameters for NTRUEncrypt*. Wilmington USA 2016.

[31] 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 2018, volume 11035 of Lecture Notes in Computer Science, Springer* (2018), 351–367.

[32] J. Scham and NTRU team, "Decryption failure script" link: https://github.com/jschanck/ntru-ephem-dfr.

[33] N. Howgrave-Graham, Q. Nguyen, D. Pointcheval, J. Proos, H. Silverman, A. Singer and W. Whyte, The Impact of Decryption Failures on the Security of NTRU Encryption, NTRU Cryptosystems Burlington, CNRS France, University of Waterloo, Canada (2018).

[34] Daniel J. Bernstein, "Comparing proofs of security for lattice-based encryption", Department of Computer Science, University of Illinois at Chicago, Chicago, IL 60607-7045, USA, Horst Gortz Institute for IT Security, Ruhr University Bochum, Germany djb.at.cr.yp.to

[35] A. Azizi, E. Laaji, Quantum Key Distribution Java Implementation. https://github.com/hlaaji/MPU-MORROCO

[36] El Hassane LAAJI, abdelmalek AZIZI, Link Google drive of our NTRUrobust implementation: https://drive.google.com/file/d/1Cbe0fTFphfxzEvMCLTQjdIerlaEsc6cm/view?usp=sharing Mohammed first University Oujda, Morocco, 2020.

Biographies

El Hassane Laaji. Engineer in Science computer and Ph.D student at Mohammed First University Oujda Morroco, Science Faculty, Arithmetic, Science computation and Application Laboratory (ASCAL).

Abdelmalek Azizi. Professor and Director of Arithmetic, Science computation and Application Laboratory (ASCAL), Science Faculty, Mohammed First University Oujda Morroco.