ISSN No:-2456-2165

Linear Polarization of Keys (Public and Private) for Increased RSA Security

KABEYA TSHISEBA Cedric
Associate Professor at DRC Pedagogic National University
Faculty of Sciences Department of Mathematics and Computing Science

Abstract:- Quantum cryptography consists of using the properties of quantum physics to establish cryptography protocols that achieve levels of security that are proven or conjectured not achievable using only classical phenomena. An important example of quantum cryptography is the quantum distribution of keys, which we have been able to present in this reflection, more in relation to the RSA protocol, by proposing to increase its security by using these principles of quantum cryptography for the distribution of the private key.

Keyswords:- *Cryptologie, cryptographie, cryptanalyse, cryptographie quantique.*

I. INTRODUCTION

Among the current hot topics, we note the security of data. This question is a permanent issue in many areas of private or public life, and represents a strategic issue for not only companies, but all organizations within them that use new technologies. The protocols used today for the encryption and decryption of messages use increasingly complex mathematical codes with increasingly long public keys, as the power of (classical) computers capable of breaking them increases. Talking today about the computer and quantum algorithms requires the use of other mechanisms, thus improving the security of current data security protocols, which in this situation can easily be compromised.

In cryptography or quantum computing, the bits of cryptography or classical computing are replaced by quantum bits (Qbits or Qubits), which have the particularity of being random, unlike classical bits which are deterministic. These qubits constitute keys, which are then used in conventional encryption protocols. Since it is impossible to clone quantum information without it being destroyed, or to measure a quantum state without modifying it, the reading of the information by an intruder would be immediately detected by the recipients of the message.

In this quantum context, the preferred medium for sending qubits over great distances is the photon, which has the particularity of allowing the encoding of information on observable variables such as the polarization of light, something that we have wanted presented in this article, precisely by illustrating through the above behavior, the inviolability of the RSA private key considered here as a quantum object.

The RSA protocol through a trivial example:

- **Definition**
  By cryptographic protocol RSA, we mean is a cryptographic system (cryptosystem), for public key encryption. It is often used for securing confidential data, especially when transmitted over an insecure network like the Internet.

  RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of MIT (Massachusetts Institute of Technology). Public key encryption, also called asymmetric encryption, uses two different but mathematically related keys, one public and the other private. The public key can be shared with anyone, while the private key must be kept secret. In RSA encryption, both the public key and the private key can be used to encrypt a message. In this case, it is the key opposite to that used for encryption that is used for decryption. It is notably thanks to this characteristic that RSA has become the most widely used asymmetric algorithm: it offers a method for ensuring the confidentiality, integrity, authenticity and non-repudiability of electronic communications and data storage.

  It is important to note today that many protocols, such as SSH, OpenPGP, S/MIME and SSL/TLS rely on RSA for their encryption and digital signature functions. This algorithm is also used in software: browsers are a clear example, because establishing a secure connection on an insecure network such as the Internet or validating a digital signature are part of their attributions. RSA signature verification is one of the most common operations performed in computing.

- **Drawing**
  In order to better understand the algorithm on which the RSA protocol is based, we will in the lines below, approach an extremely trivial example, which will thus allow us to verify the operation of this said system.

  Take for example the following binary numbers:
  - 11(binary) which correspond to 3(decimal system) and ;
  - 101(binary) which correspond to 5(decimal system).

ISSN No:-2456-2165

Let's assume in view of what is said above that p = 3 and q = 5. We therefore find the following:

A. Key calculation (private and public)

- n = p×q = 15
- (p-1)×(q-1) = 8.

In this case, e = 3 is prime with 8. We can choose d = 3 since e×d = 3×3 = 9 = 8×1 + 1

B. Message encryption

If for example the number to encrypt A is equal to 2,we therefore have $A^e = 2^3 = 8$, therefore A^e is congruent to 8 modulo 15. The coded number is therefore B is equal to 8.

C. Decryption of the coded message

To decipher, we take the remainder from the division of B^d by n. $B^d = 8^3 = 512$. By making the Euclidean division of 512 by 15, we obtain: $B^d = 512 = 34×15 + 2$. The remainder is therefore 2, that is to say A, the number that we have ciphered at the beginning.

- **The polarization**
  As we already know, light is an electromagnetic wave, where an electric field oscillates in a plane perpendicular to that where the magnetic field oscillates. The direction of light propagation follows the intersection of these two planes, as shown below.

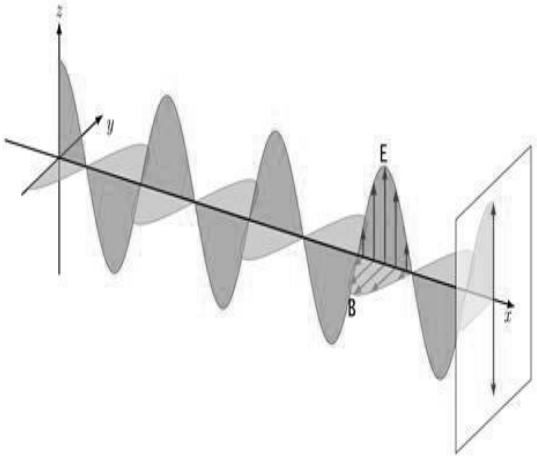

Fig. 1: Vertically polarized light

Our figure above illustrates the linear polarization of light, which we can define as the direction in which its electric field oscillates.

In reality, all the photons that make up a ray of light have their own polarizations. When these have polarizations aligned in the same direction, the light is said to be linearly polarized. Light can be polarized in all directions: horizontally, vertically, diagonally, and even not polarized at all. In the latter case, the photons that constitute this light all have polarizations that do not point in a particular direction. The light that surrounds us, like that which comes to us from the sun, tends not to be polarized.

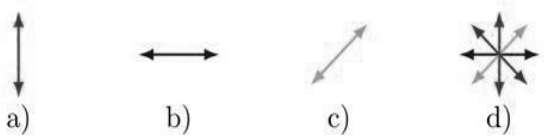

Fig. 2: Directions of polarization of light

However, polarized light can be created, for example, by using a polarizing filter also called a polarizer. The light that succeeds in passing through a polarizing filter is necessarily polarized in the direction imposed by the axis of the polarizer. In below, the axis of the polarizer is indicated by a double gray arrow. We can see such a filter as a sieve formed by vertical slits while the photons are flat pieces. Only photons whose polarization is aligned with the slits can pass. Inbelow, the polarizing filter passes the vertically polarized photons (3a) and absorbs the horizontally polarized photons (3b). By turning the polarizing filter, one turns by this very fact the polarization of the photons which can cross it 3c.

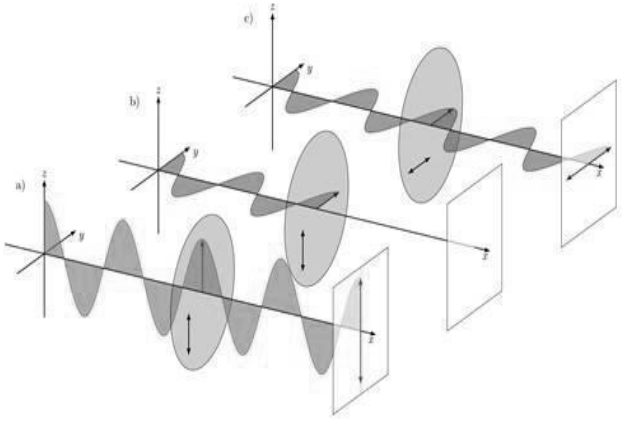

Fig. 3: Polarization filter

What happens if we send a photon with a 45° polarization on a polarizing filter that only lets through the vertical polarization? From the point of view of the filter, this photon is both vertically and horizontally polarized: it is in superposition of states! This is possible because polarization is a quantum property of light. This photon being in equal superposition of the horizontal and vertical polarizations, the filter must know its polarization to decide if it lets it pass or not. For this it must actually measure the state of polarization. If the photon is measured with vertical polarization, it will pass completely through the filter. However, it will be absorbed if measured with horizontal polarization.

Below figure shows the fact that these two results are possible with a hatched wave: sometimes the photon passes, sometimes it does not. For a 45° polarization, the photon has a 50% chance of passing the filter. If this happens, then it will have perfectly vertical polarization. Then, if we modify the angle between the polarization of the photon and the polarizer, the probabilities that the photon will pass will change according to Malus' law. And since it's quantum, only probabilities can be inferred, and the end result is quite impossible to predict!

ISSN No:-2456-2165

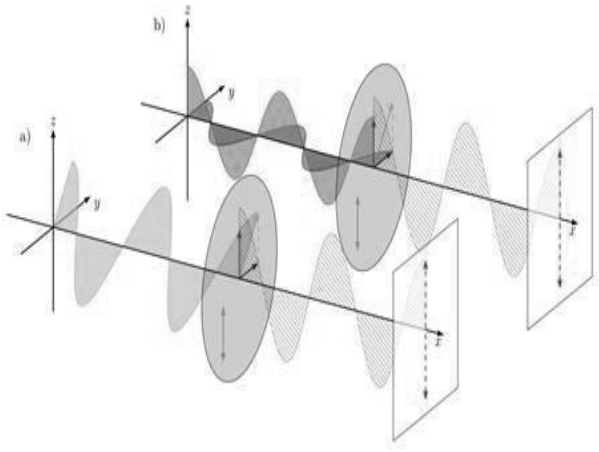

Fig 4: Photon passing probabilities

What happens if we send light that contains several photons all polarized in the same way through a polarizer? Each of the photons has the same probability of passing the filter, a probability which is given by the angle between this polarization and the axis of the polarizer. Thus, the fraction of the number of photons that pass is given by this probability. The intensity of the light beam passing through the filter therefore decreases as a function of the angle between the initial polarization of the light and that of the polarizer.

II. LINEAR POLARIZATION OF RSA KEYS

Consider two people wishing to communicate securely, and needing to share an encryption key (In this case the private key, e or d depending on the case, the one supposed to be secret).

After the calculation of the keys e and d as illustrated above and the encryption, the use of quantum technology occurs when we share our two keys (no problem for the public key). For the sharing of the private key deemed quantum, the transmitter will send a series of photons to the receiver, and for each of these photons, it will randomly draw both a base (+ or x) and a bit (0 or 1). Each photon will therefore be randomly one of these 4 states: 0+, 1+, 0x or 1x.

Source base	**+**	**x**	**X**	**+**	**+**	**+**	**x**	**+**	**…**
Bits transmitted	0	0	1	1	0	1	1	0	…
Quantum states	0+	0x	1x	1+	0+	1+	1x	0+	…

Table 1: Quantum distribution of the secret key

The receiver sees the photons arrive and for each of them it must measure the polarization. But he must choose a basis of measurement. For each he draws it at random: + or x, and notes the result of his measurement.

If for a given photon, the receiver has chosen the "good" base, i.e. the same as the transmitter, it will certainly obtain the correct bit, 0 or 1, sent by the transmitter. If, on the other hand, he has chosen the other base, he will obtain 0 or 1 at 50% probability. And in this case, he will get the "bad" result once out of 2 on average.

Example:

Source base	**+**	**x**	**X**	**+**	**+**	**+**	**x**	**+**	**…**
Bits transmitted	0	0	1	1	0	1	1	0	…
Quantum states	0+	0x	1x	1+	0+	1+	1x	0+	…
Destination basis	+	+	X	+	x	x	x	+	…
Bits measured	0	0 ou 1	1	1	0 ou 1	0 ou 1	1	0	…

Table 2: Polarization measurement

Once the transmission of the photons has been carried out, the transmitter and the receiver communicate "publicly" (without a particular secure channel) the list of bases that they have used for each of the photons. And they throw from their list all the photons for which the bases are different.

For all the remaining photons, they used the same base and are therefore certain to have the same bits: 0 or 1. This series of bits will constitute the encryption key which is, in fact, known to both of them.

At the end of the process specified above, it is important to focus on the photons for which the emitter and the receiver have chosen the same base, since the others will be discarded anyway. Like the receiver, any ill-intentioned person who is not supposed to have access to the key will have to choose for each photon a base of measurement + or x. In 50% of cases it will be correct. But in the remaining 50% it will choose a base different from the base of the emitter and the receiver, for example it chooses x while the emitter and the receiver have chosen +.

III. CONCLUSION

In this article, we have proposed a reflection on improving the complexity of the security of the RSA cryptosystem, by using quantum cryptography to secure the private key, which is supposed to remain inviolable in the eyes of any malicious person, wanting to thus recovering in an illicit manner the RSA key produced at the source level, eg jeopardizing its security, up to its destination.

ISSN No:-2456-2165

REFERENCES

[1.] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel et Hugo Zbinden, « Quantum cryptography », *Reviews of Modern Physics*, vol. 74, nº 1, 8 mars 2002, p. 145–195

[2.] Samuel J. Lomonaco, « A Quick Glance at Quantum Cryptography », *Cryptologia*, vol. 23, 1999, p. 1-41

[3.] Dagmar Bruss, Gábor Erdélyi, Tim Meyer et Tobias Riege, « Quantum cryptography: A survey », *ACM Computing Surveys (CSUR)*, vol. 39, nº 2, 6 juillet 2007, p. 6

[4.] Gilles Brassard, Norbert Lütkenhaus, Tal Mor et Barry C. Sanders, « Limitations on Practical Quantum Cryptography », *Physical Review Letters*, vol. 85, nº 6, 7 août 2000, p. 1330–1333

[5.] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus et John Preskill, « Security of quantum key distribution with imperfect devices », *Quantum Information & Computation*, vol. 4, nº 5, 1er septembre 2004, p. 325–360

[6.] Stephen Wiesner, « Conjugate coding », *ACM SIGACT News*, vol. 15, nº 1, 1er janvier 1983, p. 78–88

[7.] Sebastian Nauerth, Martin Fürst, Tobias Schmitt-Manderbach et Henning Weier, « Information leakage via side channels in freespace BB84 quantum cryptography », *New Journal of Physics*, vol. 11, nº 6, 2009, p. 065001