Current Quantum Cryptography Algorithm Is Optimal: A Proof

1st Oscar Galindo
2nd Vladik Kreinovich
Department of Computer Science
University of Texas at El Paso
El Paso, Texas, USA
ogalindomo@miners.utep.edu
vladik@utep.edu

3rd Olga Kosheleva
Department of Teacher Education
University of Texas at El Paso
El Paso, Texas, USA
olgak@utep.edu

***Abstract*—One of the main reasons for the current interest in quantum computing is that, in principle, quantum algorithms can break the RSA encoding, the encoding that is used for the majority secure communications – in particular, the majority of e-commerce transactions are based on this encoding. This does not mean, of course, that with the emergence of quantum computers, there will no more ways to secretly communicate: while the existing non-quantum schemes will be compromised, there exist a quantum cryptographic scheme that will enables us to secretly exchange information. In this scheme, however, there is a certain probability that an eavesdropper will not be detected. A natural question is: can we decrease this probability by an appropriate modification of the current quantum cryptography algorithm? In this paper, we show that such a decrease is not possible: the current quantum cryptography algorithm is, in some reasonable sense, optimal.**

***Index Terms*—quantum cryptography, quantum computing, optimality**

I. Formulation of the Problem

Why quantum computing. In many practical problems, we need to process large amounts of data in a limited time. To be able to do it, we need computations to be as fast as possible. While computations are already fast, there are many important problems for which we still cannot get the results on time. For example, it has been shown that, in principle, we can predict with a reasonable accuracy where the tornado will go in the next 15 minutes, but at present, the corresponding computations take days on the fastest existing high performance computer.

One of the main limitations on the speed of modern computers is the fact that, according to modern physics, the speed of all the processes is limited by the speed of light $c \approx 3 \cdot 10^5$ km/sec; see, e.g., [1], [5]. As a result, for example, for a typical laptop of size ≈ 30 cm, the fastest we can send a signal across the laptop is $\dfrac{30\text{ cm}}{3 \cdot 10^5\text{ km/sec}} \approx 10^{-9}$ sec – during this time, a usual few-Gigaflop laptop performs quite a few operations. To further speed up computations, we thus need to further decrease the size of the processors. To be able to fit Gigabytes of data – i.e., billions of cells – within a small area, we need to attain a very small cell size. At present, a typical cell consists of several dozen molecules. As we decrease the size further, we get to a few-molecule size, at which stage we need to take into account the fact that for molecules and atoms, physics is different: quantum effects become dominant; see, e.g., [1], [5].

At first, quantum effects were mainly viewed as a nuisance. For example, one of the features of quantum world is that its results are usually probabilistic. So, if we simply decrease the cell size but use the same computer engineering techniques, then, instead of getting the desired results all the time, we will start getting other results with some probability – and this probability of undesired results increases as we decrease the size of the computing cells.

However, researchers found out that by appropriately modifying the corresponding algorithms, we can often not only avoid the probability-related problem but, even better, make computations faster. The resulting algorithms are known as algorithms of *quantum computing*; see, e.g., [2], [6].

Quantum computing will enable us to decode all traditionally encoded messages. One of the spectacular algorithms of quantum computing is Shor's algorithm for fast factorization of large integers; see, e.g., [2]–[4].

The importance of this algorithm comes from the fact that in the modern world, most encryption schemes – e.g., schemes that underlie https, the backbone of the online commerce – as based on the RSA algorithm, the algorithm whose crypto applications are based on the difficulty of factorizing large integers. To form an at-present-unbreakable code, the user selects two large prime numbers P_1 and P_2 – that will form his private code – and transmits to everyone their product $n = P_1 \cdot P_2$ that everyone can use to encrypt their messages. At present, the only way to decode this message is to know the values P_i.

Shor's algorithm allows quantum computers to effectively find P_i based on n and thus, to read practically all the secret messages that have been sent so far. This algorithm is one of the main reasons why governments throughout the world are

This work was supported in part by the US National Science Foundation grant HRD-1242122 (Cyber-ShARE Center of Excellence).

investing in the design of quantum computers.

Quantum cryptography: an unbreakable alternative to the current cryptographic schemes. The fact that RSA-based cryptographic schemes can be broken by quantum computing does not mean that there will be no secrets: researchers have invented a quantum-based encryption scheme that cannot be thus broken. This scheme, by the way, is already used for secret communications.

Remaining problems and what we do in this paper. In addition to the current cryptographic scheme, one can propose its modifications which also serve the same purpose. This possibility raises a natural question: which of these scheme is the best?

In this paper, we show that the current cryptographic scheme is, in some reasonable sense, optimal.

II. Quantum Cryptography: Main Idea

Quantum physics: possible states. One of the main ideas behind quantum physics is that in the quantum world, in addition to the regular states, we can also have linear combinations of these states, with complex coefficients; such combinations are known as *superpositions* [1], [5].

Quantum states: case of a 1-bit memory cell. For a single 1-bit memory cell, which in the classical physics can only have states 0 and 1 – these states are denoted by $|0\rangle$ and $|1\rangle$ – we can also have superpositions $c_0 \cdot |0\rangle + c_1 \cdot |1\rangle$, where c_0 and c_1 are complex numbers.

Measurements in quantum physics. What will happen if we try to measure the bit in the superposition state $c_0 \cdot |0\rangle + c_1 \cdot |1\rangle$? According to quantum physics, as a result of this measurement, we get 0 with probability $|c_0|^2$ and 1 with probability $|c_1|^2$.

After the measurement, not only we get the measurement result, but the state also turns, correspondingly, into either $|0\rangle$ or $|1\rangle$:

- if the measurement result is 0, the state will turn into $|0\rangle$, and
- if the measurement result is 1, the state will turn into $|1\rangle$.

Comment. Since we can get either 0 or 1, the corresponding probabilities should add up to 1.

So, for the expression $c_0 \cdot |0\rangle + c_1 \cdot |1\rangle$ to represent a physically meaningful state, the coefficients c_0 and c_1 must satisfy the condition $|c_0|^2 + |c_1|^2 = 1$.

Operations on quantum states. In addition to usual operations with bits, we can also perform *unitary* operations, i.e., linear transformations that preserve the property

$$|c_0|^2 + |c_1|^2 = 1.$$

Walsh-Hadamard transformation and its geometric meaning. A simple example of a unary transformation is *Walsh-Hadamard (WH)* transformation that transforms $|0\rangle$ into

$$|0'\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle$$

and $|1\rangle$ into

$$|1'\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \cdot |0\rangle - \frac{1}{\sqrt{2}} \cdot |1\rangle;$$

see, e.g., [2], [6].

What is the geometric meaning of this transformation? By linearity, the above formulas enables us to describe a linear combination $c'_0 \cdot |0'\rangle + c'_1 \cdot |1'\rangle$ of the new 0 and 1 states $|0'\rangle$ and $|1'\rangle$ in terms of the original 0 and 1 states $|0\rangle$ and $|1\rangle$:

$$c'_0 \cdot |0'\rangle + c'_1 \cdot |1'\rangle =$$

$$c'_0 \cdot \left(\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle\right) + c'_1 \cdot \left(\frac{1}{\sqrt{2}} \cdot |0\rangle - \frac{1}{\sqrt{2}} \cdot |1\rangle\right) =$$

$$\left(\frac{1}{\sqrt{2}} \cdot c'_0 + \frac{1}{\sqrt{2}} \cdot c'_1\right) \cdot |0\rangle + \left(\frac{1}{\sqrt{2}} \cdot c'_0 - \frac{1}{\sqrt{2}} \cdot c'_1\right) \cdot |1\rangle.$$

Thus,

$$c'_0 \cdot |0'\rangle + c'_1 \cdot |1'\rangle = c_0 \cdot |0\rangle + c_1 \cdot |1\rangle,$$

where

$$c_0 = \frac{1}{\sqrt{2}} \cdot c'_0 + \frac{1}{\sqrt{2}} \cdot c'_1 \text{ and } c_1 = \frac{1}{\sqrt{2}} \cdot c'_0 - \frac{1}{\sqrt{2}} \cdot c'_1.$$

If we represent each of the two pairs (c_0, c_1) and (c'_0, c'_1) as a point in the 2-D plane (x, y), then the above transformation resembles the formulas for a clockwise rotation by an angle θ:

$$x' = \cos(\theta) \cdot x + \sin(\theta) \cdot y;$$

$$y' = -\sin(\theta) \cdot x + \cos(\theta) \cdot y.$$

Specifically, for $\theta = 45^\circ$, we have $\cos(\theta) = \sin(\theta) = \frac{1}{\sqrt{2}}$ and thus, the rotation takes the form

$$x' = \frac{1}{\sqrt{2}} \cdot x + \frac{1}{\sqrt{2}} \cdot y;$$

$$y' = -\frac{1}{\sqrt{2}} \cdot x + \frac{1}{\sqrt{2}} \cdot y.$$

In these terms, can see that the WH transformation from (c'_0, c'_1) and (c_0, c_1) is a rotation by 45 degrees followed by a reflection with respect to the x-axis: $(c_0, c_1) \to (c_0, -c_1)$.

Comment. One can check that if we apply WH transformation twice, then we get the same state as before. Indeed, due to linearity,

$$\text{WH}(0') = \text{WH}\left(\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle\right) =$$

$$\frac{1}{\sqrt{2}} \cdot WH(|0\rangle) + \frac{1}{\sqrt{2}} \cdot WH(|1\rangle) =$$

$$\frac{1}{\sqrt{2}} \cdot \left(\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle\right) + \frac{1}{\sqrt{2}} \cdot \left(\frac{1}{\sqrt{2}} \cdot |0\rangle - \frac{1}{\sqrt{2}} \cdot |1\rangle\right) =$$

$$|0\rangle$$

and similarly, $\text{WH}(|1'\rangle) = |1\rangle$.

Measurements of quantum states of 1-bit systems. According to the above description of the measurement process, if we measure the bit 0 or 1 in each of the states $|0'\rangle$ or $|1'\rangle$, then we will get 0 or 1 with equal probability $1/2$. So, if we measure 0 or 1, then:

- if we are in the state $|0\rangle$, then the state does not change and we get the measurement result 0 with probability 1;
- if we are in the state $|1\rangle$, then the state does not change and we get the measurement result 1 with probability 1;
- if we are in one of the states $|0'\rangle$ or $|1'\rangle$, then:
  - with probability $1/2$, we get the measurement result 0 and the state changes into $|0\rangle$; and
  - with probability $1/2$, we get the measurement result 1 and the state changes into $|1\rangle$.

In addition to measuring whether we are in the state $|0\rangle$ or in the state $|1\rangle$, we can also measure whether we have $|0'\rangle$ or $|1'\rangle$. In this case, similarly:

- if we are in the state $|0'\rangle$, then the state does not change and we get measurement result $0'$ with probability 1;
- if we are in the state $|1'\rangle$, then the state does not change and we get measurement result $1'$ with probability 1;
- if we are in one of the states $|0\rangle$ or $|1\rangle$, then:
  - with probability $1/2$, we get the measurement result $0'$ and the state changes into $|0'\rangle$; and
  - with probability $1/2$, we get the measurement result $1'$ and the state changes into $|1'\rangle$.

Main idea of quantum cryptography. The sender – who, in cryptography, is usually called Alice – sends each bit

- either as $|0\rangle$ or $|1\rangle$ (this orientation is usually denoted by $+$)
- or as $|0'\rangle$ or $|1'\rangle$ (this orientation is usually denoted by $\times$).

The receiver – who, in cryptography, is usually called Bob – tries to extract the information from the signal that Alice has sent.

Extracting numerical information from a physical object is nothing else but measurement. Thus, to extract the information from Alice's signal, Bob needs to perform some measurement on this signal.

Since Alice uses one of the two orientations $+$ or $\times$, it is reasonable for Bob to also use one of these orientations.

Sender and receiver must use the same orientation. Let us show that if for some bit, Alice and Bob use the same orientation, then Bob will get the exact same signal that Alice has sent.

For example, let us consider the case when Alice and Bob use the same $+$ orientation and Alice sends the bit 0. In the $+$ orientation, this bit is sent as the state $|0\rangle$. Bob measures this state with respect to the basis corresponding to the same $+$ orientation, i.e., with respect to the basis consisting of the states $|0\rangle$ and $|1\rangle$. According to the above general description of quantum measurement process, this means that we represent the measured state as a linear combination of basic states, in this case as

$$|0\rangle = 1 \cdot |0\rangle + 0 \cdot |1\rangle.$$

Then:

- with probability $|1|^2 = 1$, Bob will measure 0 (and the resulting after-measurement state will be $|0\rangle$), and
- with probability $|0|^2 = 0$, Bob will measure 1 (and the resulting after-measurement state will be $|1\rangle$).

Probability 1 means that, in this case, Bob always get the 0 bit that Alice sent.

Similarly, if they use the same $+$ orientation and Alice sends the bit 1, Bob will always get 1.

Let us now consider the case when Alice and Bob use the same $\times$ orientation and Alice sends the bit 0. In the $\times$ orientation, this bit is sent as the state $|0'\rangle$. Bob measures this state with respect to the basis corresponding to the same $\times$ orientation, i.e., with respect to the basis consisting of the states $|0'\rangle$ and $|1'\rangle$. According to the above general description of quantum measurement process, this means that we represent the measured state as a linear combination of basic states, in this case as

$$|0'\rangle = 1 \cdot |0'\rangle + 0 \cdot |1'\rangle.$$

Then:

- with probability $|1|^2 = 1$, Bob will measure 0 (and the resulting after-measurement state will be $|0'\rangle$), and
- with probability $|0|^2 = 0$, Bob will measure 1 (and the resulting after-measurement state will be $|1'\rangle$).

Probability 1 means that, in this case, Bob always get the 0 bit that Alice sent.

Similarly, if they use the same $\times$ orientation and Alice sends the bit 1, Bob will always get 1.

The situation is completely different if Alice and Bob use different orientations. For example, assume that Alice sends a 0 bit in the $\times$ orientation, i.e., sends the state $|0'\rangle$, and Bob uses the $+$ orientation to measure the signal. In this case, if we represent the measured state $|0'\rangle$ as a linear combination of Bob's basis states $|0\rangle$ and $|1\rangle$, as

$$|0'\rangle = \frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle,$$

then, according to the general description of quantum measurement: :

- with probability $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$, Bob will measure 0 (and the resulting after-measurement state will be $|0\rangle$), and
- with probability $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$, Bob will measure 1 (and the resulting after-measurement state will be $|1\rangle$).

The same results, with the same probabilities, will happen if Alice sends a 1 bit in the $\times$ orientation, i.e., sends the state $|1'\rangle$. Thus, by observing the measurement result, Bob will not be able to tell whether Alice send 0 or 1: the information will be lost.

Similarly, the information will be lost if Alice uses a $+$ orientation and Bob uses a $\times$ orientation. So, the only possibility for Alice and Bob to successfully communicate is when they select the same orientation for each of the message's bits.

What if we have an eavesdropper? What will happen if, in addition to Alice and Bob, an eavesdropper – who, in cryptography, is usually called Eve – also gains access to the same communication channel? In non-quantum eavesdropping, if Eve has access to the corresponding communication channel, she can measure each bit that Alice sends and thus, get the whole message. In non-quantum physics, measurement does not change the signal; thus, Bob gets the same signal that Alice has sent – and so, neither Alice not Bob will know that somebody eavesdropped on their communication.

In quantum physics, the situation is different. One of the main features of quantum physics is that measurement, in general, changes the signal. If Eve does not know in which of the two orientations each bit is sent, she can select the wrong orientation for her measurement. As a result, e.g., if Alice and Bob agreed to use the $\times$ orientation for transmitting a certain bit, but Eve selects a $+$ orientation, then Eve's measurement will change Alice's signal – and Bob will only get the distorted message.

For example, if Alice sent $|0'\rangle$, then, after Eve's measurement, the signal will become either $|0\rangle$ or $|1\rangle$, with probability 1/2 of each of these options. In each of the options, when Bob measures the resulting signal ($|0\rangle$ or $|1\rangle$) by using his agreed-upon $\times$ orientation, with the basis $(|0'\rangle, |1'\rangle)$, Bob will get 0 or 1 with probability 1/2 – instead of the original signal that Alice has sent.

Quantum cryptography helps to detect an eavesdropper. If there is an eavesdropper, then, with certain probability, the signal received by Bob will be different from what Alice sent. Thus, by comparing what Alice sent with what Bob received, we can see that something was interfering – and thus, we will be able to detect the presence of the eavesdropper.

Let us describe how this idea is implemented in the current quantum cryptography algorithm.

III. Current Quantum Cryptography Algorithm: Reminder

Sending a preliminary message. Before Alice sends the actual message, she needs to check that the communication channel is secure, that there is no eavesdropping.

For this purpose, Alice uses a random number generator to select n random bits $b_1, \ldots, b_n$ – each of which is equal to 0 or 1 with probability $1/2$. These bits will be sent to Bob.

Alice also selects n more random bits $r_1, \ldots, r_n$. Based on these bits, Alice sends the bits b_i as follows:

- if $r_i = 0$, then the bit b_i is sent by using the $+$ orientation, i.e., Alice sends $|0\rangle$ if $b_i = 0$ and $|1\rangle$ if $b_i = 1$;
- if $r_i = 1$, then the bit b_i is sent by using the $\times$ orientation, i.e., Alice sends $|0'\rangle$ if $b_i = 0$ and $|1'\rangle$ if $b_i = 1$.

Receiving the preliminary message. Independently, Bob selects n random bits $s_1, \ldots, s_n$ that determine how he measures the signal that he receives from Alice:

- if $s_i = 0$, then Bob measures whether the i-th received signal is $|0\rangle$ or $|1\rangle$;
- if $s_i = 1$, then Bob measures whether the i-th received signal is $|0'\rangle$ or $|1'\rangle$.

Checking for eavesdroppers. After this, for k out of n bits, Alice openly sends to Bob her bits b_i and her orientations r_i, and Bob sends to Alice his orientations s_i and the signals b'_i that he measured.

In half of the cases, the orientations r_i and s_i should coincide, in which case, if there is no eavesdropper, the signal b'_i measured by Bob should coincide with the signal b_i that Alice sent. So, if $b'_i \neq b_i$ for some i, this means that there is an eavesdropper.

If there is an eavesdropper, then with probability $1/2$, Eve will select a different orientation. In half of such cases, the eavesdropping with change the original signal. So, for each bit, the probability that we will have $b'_i \neq b_i$ (and thus, that the eavesdropper will be detected) is equal to $1/4$. Thus, the probability that the eavesdropper will not be detected by this bit is $1 - 1/4 = 3/4$. The probability that Eve will not be detected in all $k/2$ cases is thus equal to the product of $k/2$ such probabilities, i.e., to $(3/4)^{k/2}$. For a sufficiently large k, this probability of not-detecting-eavesdropping is very small.

Thus, if $b'_i = b_i$ for all k bits i, this means that with high confidence, there is no eavesdropping: the communication channel between Alice and Bob is secure.

Preparing to send a message. Now, for each of the remaining $(n - k)$ bits, Alice and Bob openly exchange orientations r_i and s_i. For half of these bits, these orientations must coincide. For these bits, since there is no eavesdropping, Alice and Bob know that the signal b'_i measured by Bob is the same as the signal b_i sent to Alice. So, there are $B \stackrel{\text{def}}{=} (n - k)/2$ bits $b_i = b'_i$ that they both know but no one else knows.

Sending the actual message. Now, Alice takes the B-bit message $m_1, \ldots, m_B$ that she wants to send, forms the encoded message $m'_i \stackrel{\text{def}}{=} m_i \oplus b_i$, where $\oplus$ means addition modulo 2 (or, equivalently, exclusive or), and openly sends the encoded message m'_i.

Receiving the actual message. Upon receiving the message m'_i, Bob reconstructs the original message as $m_i = m'_i \oplus b_i$.

IV. A General Family of Quantum Cryptography Algorithms: Description

In the current quantum cryptography algorithm, Alice selects one of the possible two orientations $+$ and $\times$ with probability 0.5. Similarly, Bob selects one of the two possible orientations $+$ and $\times$ with probability 0.5.

It is therefore reasonable to consider a more general scheme, in which:

- Alice selects the orientation $+$ with some probability a_+ (which is not necessarily equal to 0.5) and, correspondingly, the other orientation $\times$ with the remaining probability $a_\times = 1 - a_+$; and

- Bob select the orientation $+$ with some probability b_+ (which is not necessarily equal to 0.5) and, correspondingly, the other orientation $\times$ with the remaining probability $b_\times = 1 - b_+$.

A natural question is: which probabilities a_+ and b_+ should they choose to make the connection maximally secure, i.e., to maximize the probability of detecting the eavesdropper?

V. Proving That the Current Quantum Cryptography Algorithm Is Optimal

What do we want to maximize? We want to maximize the probability of detecting an eavesdropper. The eavesdropper also selects one of the two orientations $+$ or $\times$. Let e_+ be the probability with which the eavesdropper (Eve) select the orientation $+$, then Eve will select $\times$ with the remaining probability $e_\times = 1 - e_+$.

As we have seen from the description of the current algorithms, Alice and Bob can only use bits for which their selected orientations coincide, because in this case, the message bit remains unchanged. If in this case, it so happens that Eve selects the same orientation, then her observation will also not change this bit, and thus, we will not be able to detect the eavesdropping.

The only case when we can detect the eavesdropping is when Alice and Bob have the same orientation, but Eve has a different one. There are two such cases:

- the first case is when Alice and Bob select $+$ and Eve selects $\times$;
- the second case is when Alice and Bob select $\times$ and Eve selects $+$.

Alice, Bob, and Eve act independently, thus, the probability p_1 of the first case is equal to the product of the probabilities that Alice selects $+$, that Bob selects $+$, and that Eve selects $\times$:

$$p_1 = a_+ \cdot b_+ \cdot e_\times.$$

Similarly, the probability p_2 of the second case is equal to the product of the probabilities that Alice selects $\times$, that Bob selects $\times$, and that Eve selects $+$:

$$p_2 = a_\times \cdot b_\times \cdot e_+.$$

These two cases are incompatible, so the overall probability p of detecting the eavesdropper is equal to the sum of the above two probabilities:

$$p = a_+ \cdot b_+ \cdot e_\times + a_\times \cdot b_\times \cdot e_+.$$

Taking into account that $a_\times = 1 - a_+$, $b_\times = 1 - b_+$, and $e_\times = 1 - e_+$, we conclude that this detection probability takes the form

$$p = a_+ \cdot b_+ \cdot (1 - e_+) + (1 - a_+) \cdot (1 - b_+) \cdot e_+. \quad (1)$$

This probability depends on Eve's selection e_+. As typical in game-theoretic situations, we would like to maximize the probability of detection in the worst case for us, when Eve uses her best strategy. Eve's strategy is to minimize the detection probability (1). So, we want to find the values a_+ and b_+ for which the minimum of the expression (1) over all possible values e_+ is the largest possible. In other words, we want to maximize the following expression:

$$J = \min_{e_+ \in [0,1]} \{a_+ \cdot b_+ \cdot (1 - e_+) + (1 - a_+) \cdot (1 - b_+) \cdot e_+\}. \quad (2)$$

Let us analyze the resulting optimization problem. One can easily see that, once the values a_+ and b_+ are fixed, the expression (1) that Eve wants to minimize is a linear function of e_+: namely, it can be described as

$$p = a_+ \cdot b_+ - a_+ \cdot b_+ \cdot e_+ + (1 - a_+) \cdot (1 - b_+) \cdot e_+ =$$

$$a_+ \cdot b_+ + e_+ \cdot ((1 - a_+) \cdot (1 - b_+) - a_+ \cdot b_+).$$

We want to minimize this expression over all possible values of e_+ from the interval $[0, 1]$. It is known that a linear function on an interval always attains its smallest possible value at one of the endpoints. Thus, to find the minimum of the above expression over e_+, it is sufficient to consider the two endpoints $e_+ = 0$ and $e_+ = 1$ of this interval, and takes the smallest of the resulting two values.

For $e_+ = 0$, the expression (1) becomes $a_+ \cdot b_+$. For $e_+ = 1$, the expression (1) becomes $(1 - a_+) \cdot (1 - b_+)$. Thus, the minimum (2) of the expression (1) can be equivalently described as:

$$J = \min\{a_+ \cdot b_+, (1 - a_+) \cdot (1 - b_+)\}. \quad (3)$$

We need to find the values a_+ and b_+ for which this quantity attains its largest possible value.

Let us first, for each a_+, find the value b_+ for which the expression (3) attains its maximum possible value. In the formula (3), the first of the two expressions, namely, the expression $a_+ \cdot b_+$, is increasing from 0 to a_+ as b_+ goes from 0 to 1. The second expression $(1 - a_+) \cdot (1 - b_+)$ decreases from $1 - a_+$ to 0 as b_+ goes from 0 to 1. Thus:

- for small b_+, the first of the two expressions is smaller, thus for these b_+, the function (3) is equal to the first expression $J = a_+ \cdot b_+$ and is, thus, increasing with b_+;
- for larger b_+, the second of the two expressions is smaller, thus for these b_+, the function (3) is equal to the second expression $J = (1 - a_+) \cdot (1 - b_+)$ and is, thus, decreasing with b_+.

Since the expression (3) first increases and then decreases, its maximum is attained at a point when the expression (3) switches from increasing to decreasing, i.e., at a point b_+ at which the two products that form the expression (3) are equal:

$$a_+ \cdot b_+ = (1 - b_+) \cdot (1 - a_+).$$

If we open the parentheses, we conclude that

$$a_+ \cdot b_+ = 1 - a_+ - b_+ + a_+ \cdot b_+.$$

Subtracting $a_+ \cdot b_+$ from both sides of this equality, we get $0 = 1 - a_+ - b_+$, thus $b_+ = 1 - a_+$.

Substituting this expression for b_+ into the formula (3), we conclude that

$$J = \min\{a_+ \cdot (1 - a_+), (1 - a_+) \cdot a_+\},$$

i.e., that $J = a_+ \cdot (1 - a_+)$. We want to find the value a_+ that maximizes this expression. To find this value, we differentiate this expression with respect to a_+ and equate the resulting derivative to 0. As a result, we get the equation $1 - 2a_+ = 0$, hence $a_+ = 0.5$. Since $b_+ = 1 - a_+$, we get

$$b_+ = 1 - 0.5 = 0.5.$$

Thus, the current quantum cryptography algorithm is indeed optimal.

Comment. Similar arguments show:

- that the best is to use 45 degrees rotation, and
- that the best is to have 0s and 1s in b_i with probability 0.5.

ACKNOWLEDGMENTS

The authors are thankful to the anonymous referees for valuable suggestions.

REFERENCES

[1] R. Feynman, R. Leighton, and M. Sands, *The Feynman Lectures on Physics*, Addison Wesley, Boston, Massachusetts, 2005.

[2] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[3] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, New Mexico, November 20–22, 1994.

[4] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *SIAM J. Sci. Statist. Comput.*, 1997, Vol. 26, pp. 1484-ff.

[5] K. S. Thorne and R. D. Blandford, *Modern Classical Physics: Optics, Fluids, Plasmas, Elasticity, Relativity, and Statistical Physics*, Princeton University Press, Princeton, New Jersey, 2017

[6] C. P. Williams and S. H. Clearwater, *Ultimate Zero and One*, Copernicus, New York, 2000.