Quantum cryptography based on an algorithm for determining simultaneously all the mappings of a Boolean function

Koji Nagata,[1] Renata Wong,[2] Do Ngoc Diep,[3,4] and Tadao Nakamura[5]

[1] *Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea*
E-mail: ko_mi_na@yahoo.co.jp
[2] *Physics Division, National Center for Theoretical Sciences, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan (R.O.C.)*
[3] *TIMAS, Thang Long University, Nghiem Xuan Yem road, Hoang Mai district, Hanoi, Vietnam*
[4] *Institute of Mathematics, VAST, 18 Hoang Quoc Viet road, Cau Giay district, Hanoi, Vietnam*
[5] *Department of Information and Computer Science, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan*

(Dated: July 8, 2022)

Abstract

We study a quantum cryptography based on an algorithm for determining simultaneously all the mappings of a Boolean function using an entangled state. The security of our cryptography is based on the Ekert 1991 protocol, which uses an entangled state. Eavesdropping destroys the entanglement. Alice selects a secret function from the number of possible function types. Bob's aim is then to determine the selected function (a key) without an eavesdropper learning it. In order for both Alice and Bob to be able to select the same function classically, in the worst case Bob requires multiple queries to Alice. In the quantum case however, Bob requires just a single query. By measuring the single entangled state, which is sent to him by Alice, Bob can obtain the function that Alice selected. This quantum key distribution method is faster compared to the multiple queries that would be required in the classical case.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.Lx, 03.67.Ac, 02.10.-v
Keywords: Quantum cryptography, Quantum communication, Quantum computation, Quantum algorithms, Boolean algebra

I. INTRODUCTION

Quantum cryptography is synonymous with quantum key distribution (QKD) because much of the focus in the field lies on enabling secure key distribution using the principles of quantum mechanics. The two main encryption methods are the public and the private key. In the case of public keys, their security relies on the computational hardness of problems and some of those hard problems, such as integer factorization and discrete logarithms, have been shown to be efficiently solvable using quantum computational methods [1]. As such, quantum technology poses a direct threat to the Diffie-Hellman key distribution protocol widely in use today [2], as well as RSA, ECDSA and other asymmetric encryptions.

QKD uses quantum physics to distribute shared keys. It is not known to be able to break symmetric encrypton protocols such as AES-256, although Grover's search algorithm has been shown to weaken AES by a square root of the key space N [3]. The algorithm attacks block ciphers by searching for a key that matches a small number of plaintext-ciphertext pairs and requires $O(\sqrt{N})$ calls to the cipher [3].

In line with it being based on the laws of quantum mechanics, QKD is information-theoretically secure as physical laws cannot be violated.[2] This type of security is referred to as *unconditional security* and it has been proven in e.g. [4] and [5]. It is also discussed in [6]. Nonetheless, quantum key distribution faces certain issues in relation to practical conditions in which it is operated, which we discuss in Section VI.

Some of the developments in quantum algorithms relevant for the present work are as follows: The Bernstein–Vazirani algorithm [7, 8] for determining coefficients of a linear Boolean function, published in 1993, can be considered an extension of the Deutsch–Jozsa algorithm [9–11] for evaluating a Boolean function following queries. In 1994, algorithms were proposed by Simon [12] and by Shor [13]. In 1996, Grover [14] presented strong arguments for exploring the computational possibilities offered by quantum mechanics. Grover considers the problem of finding an object between some series of unodered objects. The algorithm is constructed by repeated use of Hadamard and query gates. The Grover search algorithm converges in square speed up in comparison with the classical counterpart

More precisely, Simon considers the problem of finding periods of a periodic Boolean function, which is solved by iterating some Hadamard, Fourier, and phase changing gates. This algorithm then is generalized by Shor for defining a discrete log algorithm. The idea comes back to the Grover search algorithm.

In 2020, a parallel computation for all of the combinations of values in variables of a logical function was proposed [15]. In 2021, concrete quantum circuits for addition of two numbers of arbitrary length were proposed [16].

Quantum communication is the art of transferring a quantum state from one place to another. Traditionally, the sender is named Alice and the receiver Bob. The basic motivation is that quantum states code quantum information—called qubits in the case of two-dimensional Hilbert spaces—and that quantum information allows one to perform tasks that could only be achieved far less efficiently, if at all, using classical information. Quantum cryptography based on an algorithm for determining a function using qudit systems is studied by Nagata *et al.* [17] by using the idea of listing the possible mappings of a function and use it as encoded message for sending. Continuous-variable quantum computing and its applications to cryptography were proposed by Diep *et al.* [18] as some continuous-variable variants.

Here, we study a quantum cryptography based on an algorithm for determining simultaneously all the mappings of a Boolean function using an entangled state. The security of our cryptography is based on the Ekert 1991 protocol [19], which uses an entangled state. The entanglement is used as an essential point to make the algorithm applicable in quantum cryptology. Under this protocol, eavesdropping will destroy the entanglement. Our proposed cryptographic scheme is as follows: Alice selects a secret function from the possible function types. Bob's aim is then to determine the selected function (a key) without an eavesdropper learning it. In order for both Alice and Bob to be able to select the same function classically, in the worst case Bob would require multiple queries to Alice. In the quantum case however, Bob requires just a single query. By measuring the single entangled state that is sent to him by Alice, Bob can obtain the function that Alice selected. This quantum key distribution method is faster than the classical case, which would require multiple classical queries.

II. QUANTUM ALGORITHM FOR DETERMINING ALL THE 2 MAPPINGS OF A BOOLEAN FUNCTION

In this section, we propose a quantum cryptography based on an algorithm for determining a function using qubit systems. We consider the Boolean function $f : \{0, 1\} \to \{0, 1\}$. Alice knows all the 2 mappings $f(0)$ and $f(1)$ of the function, that is, $f(x)$ itself. Bob knows none of them. His aim is to obtain all of the mappings without an eavesdropper learning them. In the classical case, Bob needs two queries. In the quantum case, Bob needs just a single query. Hence, the quantum cryptography is faster than a classical cryptography by a factor of 2.

Quantum superposition is a fundamental feature of many quantum algorithms. It allows quantum computers to

evaluate simultaneously the mappings of a function $f(x)$ for many different values of x. Suppose that

$$f : \{0,1\} \to \{0,1\} \tag{1}$$

is a Boolean function with a one-bit domain and range. A convenient way of computing the function on a quantum computer is to consider a two-qubit quantum computer that starts with the state $|x,y\rangle$, where x and y are variables used in mapping f. The abbreviation $|x,y\rangle$ stands for $|x\rangle \otimes |y\rangle$.

Like in the Deutsch–Jozsa problem, we are given a black box quantum computer known as an oracle that implements some function $f : \{0,1\}^2 \to \{0,1\}$. For the quantum algorithms to work, the oracle computing $f(x)$ from x has to be a quantum oracle that doesn't decohere x. It also mustn't leave any copy of x lying around at the end of an oracle call. We have the function f implemented as a quantum oracle. The oracle maps the state $|x\rangle \otimes |y\rangle$ to $|x\rangle \otimes |y \oplus f(x)\rangle$, where $\oplus$ stands for addition modulo 2.

It is possible to transform the state $|x,y\rangle$ into

$$|x, y \oplus f(x)\rangle, \tag{2}$$

by applying the quantum oracle. Let U_f denote the transformation defined by the mapping

$$U_f|x,y\rangle = |x, y \oplus f(x)\rangle. \tag{3}$$

Here, (2) and (3) meet the category of Boolean algebras because their outcomes meet this category. Therefore, quantum computing meets the category of Boolean algebras.

We want to develop quantum algorithms that would allow for the ultimate parallel processing. The way to do it is to find the actual ultimate parallelism while keeping in mind the physical quantum phenomena. To that end, we insert an imaginary number i into the usual phase kickback formation and the mapping U_f, and define the following formulas:

$$\begin{aligned} &U_f|0\rangle(|0\rangle - i|1\rangle)/\sqrt{2} = +|0\rangle(|f(0)\rangle - i|\overline{f(0)}\rangle)/\sqrt{2} \\ &= \begin{cases} (-i)^{f(0)}|0\rangle(|0\rangle - i|1\rangle)/\sqrt{2} & \text{if} \quad f(0) = 0, \\ (-i)^{f(0)}|0\rangle(|0\rangle + i|1\rangle)/\sqrt{2} & \text{if} \quad f(0) = 1. \end{cases} \end{aligned} \tag{4}$$

$$\begin{aligned} &U_f|1\rangle(|0\rangle - |1\rangle)/\sqrt{2} = +|1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle)/\sqrt{2} \\ &= \begin{cases} (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)/\sqrt{2} & \text{if} \quad f(1) = 0, \\ (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)/\sqrt{2} & \text{if} \quad f(1) = 1, \end{cases} \end{aligned} \tag{5}$$

where $|\overline{1}\rangle = |0\rangle$ and $|\overline{0}\rangle = |1\rangle$.

The phase of the outcome of (4) is different from the phase of the outcome of (5). Adding (4) and (5) gives (7). A mathematical problem can be solved if the input state is defined as (7) because the mapping U_f is defined. Here we use a phase effect, which is a quantum phenomenon.

We define the following notations:

$$|-\rangle_y = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}, |+\rangle_y = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, |-\rangle_x = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{6}$$

We further define the input state as follows, using an imaginary number i:

$$|\psi_0\rangle = \alpha|0\rangle|-\rangle_y + \beta|1\rangle|-\rangle_x, \langle\psi_0|\psi_0\rangle = 1 \Leftarrow |\alpha|^2 + |\beta|^2 = 1, \alpha \neq 0, \beta \neq 0. \tag{7}$$

Applying $U_{f_i}, (i = 0, 1, 2, 2^{2^1} - 1)$, to $|\psi_0\rangle$, results in $U_{f_i}|\psi_0\rangle = |\psi_1\rangle_i$, therefore leaving us with one of 2^{2^1} cases, where the power 1 of 2^{2^1} indicates the case of one qubit:

$$\begin{aligned} |\psi_1\rangle_0 &= \alpha|0\rangle|-\rangle_y + \beta|1\rangle|-\rangle_x \quad \text{iff} \quad f_0(0) = 0, f_0(1) = 0, \\ |\psi_1\rangle_1 &= -i\alpha|0\rangle|+\rangle_y - \beta|1\rangle|-\rangle_x \quad \text{iff} \quad f_1(0) = 1, f_1(1) = 1, \\ |\psi_1\rangle_2 &= \alpha|0\rangle|-\rangle_y - \beta|1\rangle|-\rangle_x \quad \text{iff} \quad f_2(0) = 0, f_2(1) = 1, \\ |\psi_1\rangle_3 &= -i\alpha|0\rangle|+\rangle_y + \beta|1\rangle|-\rangle_x \quad \text{iff} \quad f_3(0) = 1, f_3(1) = 0. \end{aligned} \tag{8}$$

Once we have (8), we know simultaneously both $f(0)$ and $f(1)$ by measuring the single output state. How can we obtain (8)? Note that we cannot obtain it solely by using the usual phase kickback formation as this formation changes only the global phase and global phases are indistinguishable. For this reason, such a situation must be avoided.

Let us consider for distinguishing between the four states. Unfortunately, they are not orthogonal each other. Thus we might consider we cannot distinguish between the four states. In (8) the operations on the mapping look fine to us because the process here is based upon the phase that was obtained from the kickback formation. Therefore, the issue of orthogonality is not so essential here as we consider the phase of each state to be guaranteed.

So, by measuring $|\psi_1\rangle_i$, we can determine simultaneously all the 2 mappings of $f_i(x)$ for all x. Interestingly, the quantum algorithm enables us to determine a perfect property of $f_i(x)$, namely, $f_i(x)$ itself, and does it faster than a classical apparatus would. Classically namely, at least 2 evaluations would be necessary to that end.

Based on the above, our cryptography is as follows:

- Alice randomly selects a function f_i.
- She applies U_{f_i} to $|\psi_0\rangle$ and obtains an entangled state $|\psi_1\rangle_i$.
- She sends the entangled state $|\psi_1\rangle_i$ to Bob.
- Bob compares (by measurement) the outcome state $|\psi_1\rangle_i$ with the input state and obtains all the 2 mappings with the respective values for the function f_i.
- Bob learns what function Alice selected.
- Alice and Bob compare their functions (a subset of the results).
- If Eve eavesdropped, Alice and Bob will each have a different function.
- If Eve did not eavesdrop, Alice and Bob will each have the same function.

Alice and Bob perform the protocol described above many times in order to obtain enough secret keys (functions) for a secure communication.

A. Concrete Example

We present a concrete example for a full and natural understanding of our quantum communication method. Let us consider the case where Alice selects a function f_1. Bob wants to know all the following mappings:

$$f(0) =?, f(1) =?. \tag{9}$$

In the classical case, Bob requires 2 evaluations. In the quantum case, Bob requires just one query.

Alice prepares the following input state:

$$|\psi_1\rangle_0 = \alpha|0\rangle|-\rangle_y + \beta|1\rangle|-\rangle_x \tag{10}$$

Next, Alice applies U_{f_1} to $|\psi_0\rangle$ to obtain $U_{f_1}|\psi_0\rangle = |\psi_1\rangle_1$. After that, she has the following output state:

$$|\psi_1\rangle_1 = -i\alpha|0\rangle|+\rangle_y - \beta|1\rangle|-\rangle_x \tag{11}$$

Bob enquires with Alice as to what phase factors of the quantum output state Alice has. In this example, the quantum phase factors of the output state are as follows:

$$-i, -1. \tag{12}$$

With this information, he then obtains simultaneously all the mappings of f_1:

$$f(0) = 1, f(1) = 1. \tag{13}$$

Finally, Bob learns that Alice selected a particular f_1. Again, this takes less than a classical apparatus would take, i.e. at least 2 evaluations. Likewise, Alice can select either of the 4 combinations of the mappings. That is, our argumentation is true for each fixed parameter i.

III. QUANTUM ALGORITHM FOR DETERMINING ALL THE 3 MAPPINGS OF A BOOLEAN FUNCTION

In this section, we propose a quantum cryptography based on an algorithm for determining a function using qutrit systems. Consider the Boolean function $f : \{0, 1, 2\} \to \{0, 1\}$. In our protocol, Alice will know all the 3 mappings $f(0)$, $f(1)$, and $f(2)$, that is, $f(x)$ itself. Bob will know none of them. His aim will therefore be to obtain all of them without an eavesdropper learning them. In the classical case, Bob needs three queries to learn all the mappings. In the quantum case, Bob needs just one single query. Hence, the quantum cryptography is faster than a classical cryptography by a factor of 3.

Quantum superposition is a fundamental feature of many quantum algorithms. It allows quantum computers to evaluate simultaneously the mappings of a function $f(x)$ for many different x. Suppose that

$$f : \{0, 1, 2\} \to \{0, 1\} \tag{14}$$

is a Boolean function known to Alice but not known to Bob. Bob's aim is therefore to determine all the mappings

$$f(0) =?, f(1) =?, f(2) =?, \tag{15}$$

that is, $f(x)$ itself. In the classical case, Bob requires 3 queries to establish all the mappings. In the quantum case, Bob requires just a single query. Therefore, the quantum communication is faster than a classical communication, which would require at least 3 queries.

In a qutrit system, Alice can select one of the 8 possible functions. Later we introduce a parameter $i = 0, 1, 2, ..., 7$ to distinguish between these functions.

Let us discuss our quantum cryptography using qutrit systems. We introduce the transformation U_f defined by the map

$$U_f|x\rangle|j\rangle = |x\rangle|(f(x) + j) \bmod 3\rangle. \tag{16}$$

From the map U_f, we insert an imaginary number i and define the following formulas:

$$\begin{aligned} &U_f|0\rangle(|0\rangle - i|1\rangle)/\sqrt{2} = +|0\rangle(|f(0)\rangle - i|f(0) + 1\rangle)/\sqrt{2} \\ &= \begin{cases} |0\rangle(|0\rangle - i|1\rangle)/\sqrt{2} & \text{if} \quad f(0) = 0, \\ |0\rangle(|1\rangle - i|2\rangle)/\sqrt{2} & \text{if} \quad f(0) = 1. \end{cases} \end{aligned} \tag{17}$$

$$\begin{aligned} &U_f|1\rangle(|0\rangle - |1\rangle)/\sqrt{2} = +|1\rangle(|f(1)\rangle - |f(1) + 1\rangle)/\sqrt{2} \\ &= \begin{cases} |1\rangle(|0\rangle - |1\rangle)/\sqrt{2} & \text{if} \quad f(1) = 0, \\ |1\rangle(|1\rangle - |2\rangle)/\sqrt{2} & \text{if} \quad f(1) = 1. \end{cases} \end{aligned} \tag{18}$$

We define a quantum state in a three-dimensional space $|\phi\rangle$ as follows:

$$|\phi\rangle = \frac{1}{\sqrt{3}}(\omega^3|0\rangle + \omega^2|1\rangle + \omega|2\rangle), \tag{19}$$

where $\omega = e^{2\pi i/3}$. We have the following formula by the phase kickback formation:

$$U_f|2\rangle|\phi\rangle = \omega^{f(2)}|2\rangle|\phi\rangle. \tag{20}$$

In fact, from the map U_f, we can define the following formulas:

$$\begin{aligned} &U_f|2\rangle\frac{1}{\sqrt{3}}(\omega^3|0\rangle + \omega^2|1\rangle + \omega|2\rangle) \\ &= |2\rangle\frac{1}{\sqrt{3}}(\omega^3|f(2)\rangle + \omega^2|f(2) + 1\rangle + \omega|f(2) + 2\rangle) \\ &= \begin{cases} |2\rangle\frac{1}{\sqrt{3}}(\omega^3|0\rangle + \omega^2|1\rangle + \omega|2\rangle) & \text{if} \quad f(2) = 0, \\ \omega|2\rangle\frac{1}{\sqrt{3}}(\omega^3|0\rangle + \omega^2|1\rangle + \omega|2\rangle) & \text{if} \quad f(2) = 1. \end{cases} \end{aligned} \tag{21}$$

Observe that

$$(U_f)^3|x\rangle|j\rangle = |x\rangle|(3f(x) + j) \bmod 3\rangle = |x\rangle|j\rangle. \tag{22}$$

Therefore, the map U_f is a cyclic transformation. Here, we define the normalized input state ($\langle\psi_0|\psi_0\rangle = 1$) as follows:

$$|\psi_0\rangle = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle,$$
$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1, \alpha \neq 0, \beta \neq 0, \gamma \neq 0. \tag{23}$$

Let us introduce a parameter i. Later, we will see that all the information for f_i is embedded into a single output state. This means that all the information for f_i can be learned from the single output state. This is the key of our quantum communication.

At the beginning of our communication protocol, Alice applies $U_{f_i}, (i = 0, 1, ..., 7)$ to $|\psi_0\rangle$, $U_{f_i}|\psi_0\rangle = |\psi_1\rangle_i$, the output state is one of 8 cases:

$$|\psi_1\rangle_0 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle$$
$$\text{iff} \quad f_0(0) = 0, f_0(1) = 0, f_0(2) = 0, \tag{24}$$

$$|\psi_1\rangle_1 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \omega\gamma|2\rangle|\phi\rangle$$
$$\text{iff} \quad f_1(0) = 0, f_1(1) = 0, f_1(2) = 1, \tag{25}$$

$$|\psi_1\rangle_2 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle$$
$$\text{iff} \quad f_2(0) = 0, f_2(1) = 1, f_2(2) = 0, \tag{26}$$

$$|\psi_1\rangle_3 = \alpha|0\rangle\left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right] + \omega\gamma|2\rangle|\phi\rangle$$
$$\text{iff} \quad f_3(0) = 0, f_3(1) = 1, f_3(2) = 1, \tag{27}$$

$$|\psi_1\rangle_4 = \alpha|0\rangle\left[\frac{|1\rangle - i|2\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle$$
$$\text{iff} \quad f_4(0) = 1, f_4(1) = 0, f_4(2) = 0, \tag{28}$$

$$|\psi_1\rangle_5 = \alpha|0\rangle\left[\frac{|1\rangle - i|2\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \omega\gamma|2\rangle|\phi\rangle$$
$$\text{iff} \quad f_5(0) = 1, f_5(1) = 0, f_5(2) = 1, \tag{29}$$

$$|\psi_1\rangle_6 = \alpha|0\rangle\left[\frac{|1\rangle - i|2\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle$$
$$\text{iff} \quad f_6(0) = 1, f_6(1) = 1, f_6(2) = 0, \tag{30}$$

$$|\psi_1\rangle_7 = \alpha|0\rangle\left[\frac{|1\rangle - i|2\rangle}{\sqrt{2}}\right] + \beta|1\rangle\left[\frac{|1\rangle - |2\rangle}{\sqrt{2}}\right] + \omega\gamma|2\rangle|\phi\rangle$$
$$\text{iff} \quad f_7(0) = 1, f_7(1) = 1, f_7(2) = 1. \tag{31}$$

Let us consider for distinguishing between the eight states. Unfortunately, they are not orthogonal each other. Thus we might consider we cannot distinguish between the eight states. In (24)-(31) the operations on the mapping look fine to us because the process here is based upon the phase that was obtained from the kickback formation. Therefore, the issue of orthogonality is not so essential here as we consider the phase of each state to be guaranteed.

By measuring the state $|\psi_1\rangle_i$ sent by Alice, Bob can determine simultaneously all the 3 mappings of $f_i(x)$ for all $x(= 0, 1, 2)$. Interestingly, the quantum communication gives us the ability to transmit a perfect property of $f_i(x)$, namely, $f_i(x)$ itself. Moreover, the quantum transmission is faster than a classical communication, which would require at least 3 queries.

With the above, our cryptography is as follows:

- Alice selects a function f_i at random.
- She applies U_{f_i} to $|\psi_0\rangle$ and obtains an entangled state $|\psi_1\rangle_i$.
- She sends the entangled state $|\psi_1\rangle_i$ to Bob.
- Bob compares (by measurement) the result state $|\psi_1\rangle_i$ with the input state and obtains all the 3 mappings with regards to the function f_i.
- Bob learns what function Alice selected.
- Alice and Bob compare their functions (a subset of the results).
- If Eve eavesdropped, Alice and Bob will each have a different function.
- If Eve did not eavesdrop, Alice and Bob will each have the same function.

Alice and Bob perform the protocol described above many times in order to obtain enough secret keys (functions).

A. Concrete Example

For a full and natural understanding of our quantum communication method, we present below a concrete example for a qutrit system. Let us consider the case where Alice selects a function f_1. Bob wants to know all the mappings

$$f(0) =?, f(1) =?, f(2) =?. \tag{32}$$

In the classical case, Bob requires 3 evaluations. In the quantum case, Bob requires just one query.

At the beginning, Alice prepares the following input state:

$$|\psi_0\rangle = \alpha|0\rangle \left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \gamma|2\rangle|\phi\rangle. \tag{33}$$

Next, Alice applies U_{f_1} to $|\psi_0\rangle$ obtaining $U_{f_1}|\psi_0\rangle = |\psi_1\rangle_1$. Her output state is

$$|\psi_1\rangle_1 = \alpha|0\rangle \left[\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right] + \beta|1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] + \omega\gamma|2\rangle|\phi\rangle. \tag{34}$$

Bob enquires with Alice as to what phase factors of the quantum output state Alice has. In this example, the quantum phase factors of the output state are as follows:

$$1, 1, \omega. \tag{35}$$

Then Bob obtains simultaneously all the mappings of f_1:

$$f(0) = 0, f(1) = 0, f(2) = 1. \tag{36}$$

Finally, Bob learns that Alice selected the mapping f_1. Again, the quantum method is faster than a classical apparatus, which would require at least 3 evaluations. Likewise, Alice can select any of the 8 combinations of the mappings. That is, our argumentation holds for each fixed parameter i.

IV. QUANTUM ALGORITHM FOR DETERMINING ALL THE 4 MAPPINGS OF A BOOLEAN FUNCTION

In this section, we propose a quantum cryptography based on an algorithm for determining a function using qubit systems. Consider the Boolean function $f : \{0,1\}^2 \to \{0,1\}$. Assume that Alice knows all the 4 mappings $f(0,0)$, $f(0,1)$, $f(1,0)$, and $f(1,1)$, that is, $f(x)$ itself. Assume further that Bob knows none of them. His aim is then to obtain all of these mapping values without an eavesdropper learning them. In the classical case, Bob needs four queries. In the quantum case, Bob needs just a single query. Thus, the quantum cryptography is faster than a classical cryptography by a factor of 4.

We propose a quantum algorithm for determining the 2^2 mappings of a function. Suppose that

$$f : \{0,1\}^2 \to \{0,1\} \tag{37}$$

is a Boolean function. We want to know simultaneously the 2^2 mappings $f(0,0), f(0,1), f(1,0)$, and $f(1,1)$. Later we will see a complete match between our results and a Boolean algebra F_2 [20]. In the Boolean algebra F_2, the functions are of two variables. For example, $f(x,y)$ is the function where x and y are variables used in mapping f. In what follows, the abbreviation $f(xy)$ will stand for $f(x,y)$.

We define the input state as follows using an application of (7):

$$|\psi_0\rangle = a_1|00\rangle|-\rangle_y + a_2|01\rangle|-\rangle_y + a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x,$$
$$\langle\psi_0|\psi_0\rangle = 1 \Leftarrow |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 = 1, a_1 \neq 0, a_2 \neq 0, a_3 \neq 0, a_4 \neq 0. \tag{38}$$

From the mapping U_f, we can define the following formulas:

$$U_f|00\rangle|-\rangle_y = \begin{cases} (-i)^{f(00)}|00\rangle|-\rangle_y & \text{if } \ f(00) = 0, \\ (-i)^{f(00)}|00\rangle|+\rangle_y & \text{if } \ f(00) = 1. \end{cases} \tag{39}$$

$$U_f|01\rangle|-\rangle_y = \begin{cases} (-i)^{f(01)}|01\rangle|-\rangle_y & \text{if } \ f(01) = 0, \\ (-i)^{f(01)}|01\rangle|+\rangle_y & \text{if } \ f(01) = 1. \end{cases} \tag{40}$$

$$U_f|10\rangle|-\rangle_x = \begin{cases} (-1)^{f(10)}|10\rangle|-\rangle_x & \text{if } \ f(10) = 0, \\ (-1)^{f(10)}|10\rangle|-\rangle_x & \text{if } \ f(10) = 1. \end{cases} \tag{41}$$

$$U_f|11\rangle|-\rangle_x = \begin{cases} (-1)^{f(11)}|11\rangle|-\rangle_x & \text{if } \ f(11) = 0, \\ (-1)^{f(11)}|11\rangle|-\rangle_x & \text{if } \ f(11) = 1. \end{cases} \tag{42}$$

Applying $U_{f_i}, (i = 0, 1, 2, ..., 2^{2^2} - 1)$, to $|\psi_0\rangle$ gives $U_{f_i}|\psi_0\rangle = |\psi_1\rangle_i$ and leaves us with one of the 2^{2^2} cases:

$$|\psi_1\rangle_0 = a_1|00\rangle|-\rangle_y + a_2|01\rangle|-\rangle_y + a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x$$
$$\text{iff } \ f_0(00) = 0, f_0(01) = 0, f_0(10) = 0, f_0(11) = 0, \tag{43}$$

$$|\psi_1\rangle_1 = a_1|00\rangle|-\rangle_y + a_2|01\rangle|-\rangle_y + a_3|10\rangle|-\rangle_x - a_4|11\rangle|-\rangle_x$$
$$\text{iff } \ f_1(00) = 0, f_1(01) = 0, f_1(10) = 0, f_1(11) = 1, \tag{44}$$

$$|\psi_1\rangle_2 = a_1|00\rangle|-\rangle_y + a_2|01\rangle|-\rangle_y - a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x$$
$$\text{iff } \ f_2(00) = 0, f_2(01) = 0, f_2(10) = 1, f_2(11) = 0, \tag{45}$$

$$|\psi_1\rangle_3 = a_1|00\rangle|-\rangle_y + a_2|01\rangle|-\rangle_y - a_3|10\rangle|-\rangle_x - a_4|11\rangle|-\rangle_x$$
$$\text{iff } \ f_3(00) = 0, f_3(01) = 0, f_3(10) = 1, f_3(11) = 1, \tag{46}$$

$$|\psi_1\rangle_4 = a_1|00\rangle|-\rangle_y - ia_2|01\rangle|+\rangle_y + a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x$$
$$\text{iff } \ f_4(00) = 0, f_4(01) = 1, f_4(10) = 0, f_4(11) = 0, \tag{47}$$

$$|\psi_1\rangle_5 = a_1|00\rangle|-\rangle_y - ia_2|01\rangle|+\rangle_y + a_3|10\rangle|-\rangle_x - a_4|11\rangle|-\rangle_x$$
$$\text{iff } \ f_5(00) = 0, f_5(01) = 1, f_5(10) = 0, f_5(11) = 1, \tag{48}$$

$$|\psi_1\rangle_6 = a_1|00\rangle|-\rangle_y - ia_2|01\rangle|+\rangle_y - a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x$$
$$\text{iff } \ f_6(00) = 0, f_6(01) = 1, f_6(10) = 1, f_6(11) = 0, \tag{49}$$

$$|\psi_1\rangle_7 = a_1|00\rangle|-\rangle_y - ia_2|01\rangle|+\rangle_y - a_3|10\rangle|-\rangle_x - a_4|11\rangle|-\rangle_x$$
$$\text{iff } \ f_7(00) = 0, f_7(01) = 1, f_7(10) = 1, f_7(11) = 1, \tag{50}$$

$$|\psi_1\rangle_8 = -ia_1|00\rangle|+\rangle_y + a_2|01\rangle|-\rangle_y + a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x$$
$$\text{iff } \ f_8(00) = 1, f_8(01) = 0, f_8(10) = 0, f_8(11) = 0, \tag{51}$$

$$|\psi_1\rangle_9 = -ia_1|00\rangle|+\rangle_y + a_2|01\rangle|-\rangle_y + a_3|10\rangle|-\rangle_x - a_4|11\rangle|-\rangle_x$$
$$\text{iff} \quad f_9(00) = 1, f_9(01) = 0, f_9(10) = 0, f_9(11) = 1, \tag{52}$$

$$|\psi_1\rangle_{10} = -ia_1|00\rangle|+\rangle_y + a_2|01\rangle|-\rangle_y - a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x$$
$$\text{iff} \quad f_{10}(00) = 1, f_{10}(01) = 0, f_{10}(10) = 1, f_{10}(11) = 0, \tag{53}$$

$$|\psi_1\rangle_{11} = -ia_1|00\rangle|+\rangle_y + a_2|01\rangle|-\rangle_y - a_3|10\rangle|-\rangle_x - a_4|11\rangle|-\rangle_x$$
$$\text{iff} \quad f_{11}(00) = 1, f_{11}(01) = 0, f_{11}(10) = 1, f_{11}(11) = 1, \tag{54}$$

$$|\psi_1\rangle_{12} = -ia_1|00\rangle|+\rangle_y - ia_2|01\rangle|+\rangle_y + a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x$$
$$\text{iff} \quad f_{12}(00) = 1, f_{12}(01) = 1, f_{12}(10) = 0, f_{12}(11) = 0, \tag{55}$$

$$|\psi_1\rangle_{13} = -ia_1|00\rangle|+\rangle_y - ia_2|01\rangle|+\rangle_y + a_3|10\rangle|-\rangle_x - a_4|11\rangle|-\rangle_x$$
$$\text{iff} \quad f_{13}(00) = 1, f_{13}(01) = 1, f_{13}(10) = 0, f_{13}(11) = 1, \tag{56}$$

$$|\psi_1\rangle_{14} = -ia_1|00\rangle|+\rangle_y - ia_2|01\rangle|+\rangle_y - a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x$$
$$\text{iff} \quad f_{14}(00) = 1, f_{14}(01) = 1, f_{14}(10) = 1, f_{14}(11) = 0, \tag{57}$$

$$|\psi_1\rangle_{15} = -ia_1|00\rangle|+\rangle_y - ia_2|01\rangle|+\rangle_y - a_3|10\rangle|-\rangle_x - a_4|11\rangle|-\rangle_x$$
$$\text{iff} \quad f_{15}(00) = 1, f_{15}(01) = 1, f_{15}(10) = 1, f_{15}(11) = 1. \tag{58}$$

Let us consider for distinguishing between the sixteen states. Unfortunately, they are not orthogonal each other. Thus we might consider we cannot distinguish between the sixteen states. In (43)-(58) the operations on the mapping look fine to us because the process here is based upon the phase obtained from the kickback formation. So, the issue of orthogonality is not so essential because we consider the phase of each state to be guaranteed here.

By measuring $|\psi_1\rangle_i$ we can determine simultaneously all the 2^2 mappings of $f_i(x, y)$ for all x and y. Interestingly, the quantum algorithm gives us the ability to determine a perfect property of $f_i(x, y)$, namely, $f_i(x, y)$ itself. This determination is faster than with a classical apparatus, which would require at least 2^2 evaluations.

Our cryptography is as follows:

- Alice randomly selects a function f_i.
- She applies U_{f_i} to $|\psi_0\rangle$ and obtains an entangled state $|\psi_1\rangle_i$.
- She sends the entangled state $|\psi_1\rangle_i$ to Bob.
- Bob compares (by measurement) the result state $|\psi_1\rangle_i$ with the input state and obtains all the 4 mappings with the values concerning the function f_i.
- Bob learns what function Alice selected.
- Alice and Bob compare their functions (a subset of the results).
- If Eve eavesdropped, Alice and Bob will each have a different function.
- If Eve did not eavesdrop, Alice and Bob will each have the same function.

Alice and Bob perform the protocol described above many times in order to obtain enough secret keys (functions).

A. Concrete Example

Let us consider the case where Alice selects a function f_1. Bob wants to know all the following mappings:

$$f(0,0) =?, f(0,1) =?, f(1,0) =?, f(1,1) =?. \tag{59}$$

In the classical case, Bob requires 4 evaluations. In the quantum case, Bob requires just one query.

Alice prepares the following input state:

$$|\psi_0\rangle = a_1|00\rangle|-\rangle_y + a_2|01\rangle|-\rangle_y + a_3|10\rangle|-\rangle_x + a_4|11\rangle|-\rangle_x. \tag{60}$$

Next, Alice applies U_{f_1} to $|\psi_0\rangle$ to obtain $U_{f_1}|\psi_0\rangle = |\psi_1\rangle_1$. She has the following output state:

$$|\psi_1\rangle_1 = a_1|00\rangle|-\rangle_y + a_2|01\rangle|-\rangle_y + a_3|10\rangle|-\rangle_x - a_4|11\rangle|-\rangle_x. \tag{61}$$

Bob enquires with Alice as to what phase factors of the quantum output state Alice has. In this example, the quantum phase factors of the output state are as follows:

$$1, 1, 1, -1. \tag{62}$$

Then, Bob obtains simultaneously all the mappings of f_1:

$$f(0,0) = 0, f(0,1) = 0, f(1,0) = 0, f(1,1) = 1. \tag{63}$$

Finally, Bob realizes that Alice selected f_1. Again, this quantum communication is faster than using a classical apparatus, which would require at least 4 evaluations. Likewise, Alice can select any of the 16 combinations of the mappings. That is, our argumentation holds for each fixed parameter i.

V. IMPLEMENTATION COST

The cost of implementing a realistic quantum key distribution system is relatively high at present. Quantum key distribution relies heavily on the availability and reliability of single-photon sources and single-photon detectors. The former is hard to realize practically and, as of now, there is no ideal on-demand single-photon emitter yet [21] that would produce a single photon in a known single mode each and every time it is used and do so at any given time. Due to the fact that single-photon sources are vital for quantum computing, quantum metrology as well as quantum cryptography, the field is under active research and progress has been reported using e.g. multiplexing ([22]), or new solid-state materials ([21]). The key in the security of the E91 and by extension of our protocol lies in the ability of producing pure photonic states as such states will not generate correlations with an eavesdropper.

Single-photon detectors constitute the most costly components in a cryptographic protocol. In a 2008 report by NIST [23] researchers have demonstrated a cost reduction by 50% for both the B92 and BB84 protocols by reducing the number of required photon detectors by half by using an improved detection-time-bin-shift (DTBS) scheme [24]. To the best of our knowledge, there is no such reduction implemented for the E91 protocol, which uses entangled pairs of photons. Such a reduction in implementation cost of the E91 would bear direct relevance to the present work.

In theory, quantum cryptography can transmit keys securely as is guaranteed by the fundamental physical principle that a measurement performed automatically by an eavesdropper in the act of eavesdropping will disturb the values of the keys and thereby make the fact of eavesdropping known to the communicating parties. In practice, single-photon detectors suffer from a phenomenon known as *dead time* where they are unable to record another photon within a certain time frame after detecting the previous photon [25]. This may cause data loss for sequences of data following narrowly.

VI. PROTOCOL SECURITY

It is believed in the field of quantum cryptography that all QKD protocols are unconditionally secure due to the fact that they are based on physical laws and physical laws cannot be violated (unconditional security) [6]. This is in contrast to classical cryptography, where the security of a protocol relies on the computational difficulty of certain mathematical functions, the evaluation of which can be done by analyzing their computational complexity. In quantum cryptography, no assumption is made on an eavesdropper's inability to compute hard mathematical problems [26]. Given this background, quantum cryptography's main purpose is to make it secure by detecting, and therefore preventing, eavesdropping during a communication. In his 1991 paper, Ekert introduced a cryptographic protocol

(E91) showing how entanglement in the Bell theorem can be used to test for eavesdropping to provide security in key distribution. It has since been discovered that Bell's inequality is not necessary for Ekert's protocol's security [27] as entanglement alone can provide for it.

The protocol proposed in this work is secure in the sense of the security type provided by the E91 for the reason that both E91 and our protocol are based on quantum entanglement, as opposed to the BB84 and B92 protocols, both of which utilize the Heisenberg uncertainly principle, or Biham et al. [28], which makes use of quantum nonlocality. Entanglement offers the possibility to detect eavesdropping, which makes both E91 and our protocol secure.

In general, there are two issues that affect a quantum key distribution protocol with regards to a third party eavesdropping. One stems from noisy channels used in communication and the other from imperfect equipment used to generate and detect photons.

In real cryptographic systems, if Alice and Bob discover that the information they measure is not perfectly correlated, they will find it hard to discern whether the discrepancy in the information was caused by an eavesdropper measuring the entangled photons or by noisy or imperfect equipment. It is very likely that some error will always be present in the process of distributing keys even if a third party has not disturbed the system by its measurement. In the case of eavesdropping, Eve will have successfully obtained some of the bits of the key. Against this, QKD protocols employ a defense mechanism called *privacy amplification*. It allows Alice and Bob to reduce to an arbitrary extent the amount of information that Eve might have learnt about the key and involves shrinking the originally transmitted key to form another key that is unknowable to the eavesdropper. One such shrinking scheme is presented in [29].

Currently available single-photon emitters and detectors may also introduce noise to communication. Due to unavailability of ideal on-demand photon sources, real-world systems often use lasers to generate a small amount of coherent light instead of single photons. This leads to the possibility of a type of attack known as *photon number splitting* (PNS) [30]. During such an attack, an eavesdropper can isolate a small amount of photons from each transmission while letting the remaining bits be transferred to Bob. The eavesdropper could then perform a measurement on the split-off bits without the bits received by Bob being ever affected by it. A way to counteract was developed in [31] and requires sending decoy pulses, on the basis of which Alice and Bob would be able to determine if a PNS attack took place during their communication.

After obtaining a final key, the relationship between the length of the final key and its security should be established. It was calculated for the Ekert protocol by Waks et al. [32] to be $I_E(K;GUZ) \leq 2^{-t}r + 2^{-s}/\ln 2$ with s and t being independent security parameters chosen by the two parties. This expression is exponentially small in s and t. The findings in [32] show that this relationship is the same for E91 as it is for BB84 with the significant difference though that BB84 must use an ideal single photon source while E91 could use any arbitrary photon source. As the authors point out, this indicates that the Ekert protocol is in effect resistant to the powerful photon splitting attacks that severely affect the security of BB84.

As pointed out in the introduction, it is not known whether QKD will be able to break the AES key. It appears however that there might be a potential in exploiting the structure of the AES to obtain the key. Murphy and Robshaw [33] proposed an alternative description of AES, which they call BES, that is mathematically much simpler than the original description of AES. The BES possesses a simple algebraic structure consisting of a componentwise inversion and a highly structured affine transformation over the same field $GF(2^8)$. A consequence of this would be that the security of the AES protocol is equivalent to the difficulty of solving certain very sparse multivariate quadratic systems over the field $GF(2^8)$.

VII. COMPARISON TO OTHER CRYPTOGRAPHIC PROTOCOLS

Entanglement-based protocols are more difficult to implement because entanglement gets destroyed by the quantum channel over long distances. Both BB84 and E91 have nonetheless been successfully implemented in large-scale studies in [34] and [35], respectively. A key measure of comparison among QKD protocols is that of a secure key rate, that is the ratio between the number of secret key bits and the number of sifted bits. Both experiments were tested between a low-Earth-orbit satellite equipped with a space borne photon source and a ground observatory. For the BB84 protocol, a sifted key rate of ca. 12 kbit/s was obtained at a distance of 645 km, and of ca. 1 kbit/s at a distance of 1200 km, where the QBERs (quantum bit error rate) were measured to be between $1-3\%$. A sifted key is obtained after basis reconciliation phase of a key distribution process. For the E91 protocol, a final key rate of ca. 3.5 bits/s on average was obtained at the distance range of 530–1000 km.

A variant of a decoy-state BB84 protocol was also tested over optical fiber channel in [36] albeit at a much lower distance of 25 km. The sifted and secure key rates and the QBER were measured to be ca. 42.21 Mb/s, 11.53 Mb/s, and 3.16%, respectively. Another test of viability of entanglement-based QKD has been reported in [37] over a 100 km long optical fiber. The 8-hour long experiment has successfully generated a 16 kbit sifted key with a quantum bit error rate of 6.9% at a rate of 0.59 bits/s, while the obtained secure key was 3.9 kbit long. A further experimental

result using entanglement-based key distribution over submarine optical telecommunicanions fibre of length 96 km between Malta and Sicily is presented in [38]. An estimated final key in this study is reported as ca. 57.5 bits/s after 60s. These results indicate that entanglement-based QKD still remains an outstanding challenge.

VIII. CONCLUSION

In conclusion, we have studied a quantum cryptography based on an algorithm for determining all the mappings of a Boolean function simultaneously using an entangled state. The security of our cryptography is based on the Ekert 1991 protocol, which uses an entangled state. Consequently, eavesdropping destroyed the entanglement. In the cryptography, Alice selected a secret function among the possible function types. Bob's aim was then to determine the selected function (a key) without an eavesdropper learning it. In order for both Alice and Bob to be able to select the same function classically, in the worst case Bob would require multiple queries to Alice. In the quantum case however, Bob required just a single query. By measuring the single entangled state, which was sent to him by Alice, Bob obtained the function that Alice had selected. This quantum key distribution method is faster than the multiple classical queries that would be required in the classical case.

ACKNOWLEDGMENTS

The authors wish to thank Soliman Abdalla, Jaewook Ahn, Josep Batle, Mark Behzad Doost, Ahmed Farouk, Han Geurdes, Shahrokh Heidari, Wenliang Jin, Hamed Daei Kasmaei, Janusz Milek, Mosayeb Naseri, Santanu Kumar Patro, and Germano Resconi for their valuable support.

NOTE

On behalf of all authors, the corresponding author states that there is no conflict of interest.

[1] Boyer M, Liss R and Mor T, Theoret Comput Sci **801**, pp. 96-109 (2020).
[2] Geihs M et al., IEEE Trans Sustain Comput. **6(1)**, pp. 19-29 (2021).
[3] Samuel Jaques, Michael Naehrig, Martin Roetteler and Fernando Virdia, *Advances in Cryptology - EUROCRYPT*, (2020).
[4] Mayers D, J ACM **48(3)**, pp. 351-406 (2001).
[5] Biham E, Boyer M, Boykin PO, Mor T and Roychowdhury V., J Cryptol. **19(4)**, pp. 381-439 (2006).
[6] H. K. Lo and H. F. Chau, Science **283(5410)**, 2050-2056 (1999).
[7] E. Bernstein and U. Vazirani, Proceedings of 25th Annual ACM Symposium on Theory of Computing (STOC '93), p. 11 (1993).
[8] E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).
[9] D. Deutsch, Proc. R. Soc. Lond. A **400**, 97 (1985).
[10] D. Deutsch and R. Jozsa, Proc. R. Soc. Lond. A **439**, 553 (1992).
[11] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. Lond. A **454**, 339 (1998).
[12] D. R. Simon, Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science, p. 116 (1994).
[13] P. W. Shor, Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science, p. 124 (1994).
[14] L. K. Grover, Proceedings of 28th Annual ACM Symposium on Theory of Computing, p. 212 (1996).
[15] K. Nagata and T. Nakamura, Int. J. Theor. Phys. **59**, 611 (2020).
[16] T. Nakamura and K. Nagata, Int. J. Theor. Phys. **60**, 70 (2021).
[17] K. Nagata, D. N. Diep, and T. Nakamura, Int. J. Theor. Phys. **59**, 2875 (2020).
[18] D. N. Diep, K. Nagata, and R. Wong, Int. J. Theor. Phys. **59**, 3184 (2020).
[19] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[20] W. J. Gilbert and W. K. Nicholson, *Modern algebra with applications* (John Wiley and Sons, Inc. Second edition, 2004).
[21] Igor Aharonovich, Dirk Englund and Milos Toth, Nature Photonics **10**, 631-641 (2016).
[22] Evan Meyer-Scott, Christine Silberhorn and Alan Migdall, Review of Scientific Instruments **91**, 041101 (2020).
[23] L. Ma, T. Chang, A. Mink, O. Slattery, B. Hershman and X. Tang, IEEE Communications Letters **12(6)**, 459-461 (2008).
[24] J. Breguet, A. Muller, and N. Gisin, J. Modern Optics **41(12)**, 2405-2412 (1994).
[25] W. R. Leo, Springer, pp. 122-127 (1994).
[26] Bruss, D., Erdelyti, G., Meyer, T., Riege, T. and Rothe, J., ACM Computing Surveys **39(2)**, 6 (2007).
[27] C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68(5)**, pp. 557-559 (1992).

[28] E. Biham, B. Huttner and T. Mor, Phys. Rev. A **54(3)**, 2651-2658 (1996).
[29] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., Reviews of Modern Physics **74**, pp. 146-195 (2002).
[30] Brassard, G., Lutkenhaus, N., Mor, T., and Sanders, B., Phys. Rev. A **61**, 052304 (2000).
[31] Lo, H., Ma, X. and Chen, K., Phys. Rev. Lett. **94**, 230504 (2005).
[32] Edo Waks, Assaf Zeevi and Yoshihisa Yamamoto, Phys. Rev. A **65**, 052310 (2002).
[33] Sean Murphy and Matthew J.B. Robshaw, *Annual International Cryptology Conference - Advances in Cryptology - CRYPTO*, pp. 1-16 (2002).
[34] S. K. Liao et al, Nature **549**, pp. 43-47 (2017).
[35] J. Yin et al, Phys. Rev. Lett. **119**, 200501 (2017).
[36] Z. L. Yuan et al, Journal of Lightwave Technology **36(16)**, pp. 3427-3433 (2018).
[37] T. Honjo et al., Optics Express **16(23)**, pp. 19118-19126 (2008).
[38] S. Wengerowsky et al., PNAS **116(14)**, pp. 6684-6688 (2019).