entropy

MDPI

Article

QKD Based on Symmetric Entangled Bernstein-Vazirani

Michael Ampatzis † and Theodore Andronikos *,†

Department of Informatics, Ionian University, 7 Tsirigoti Square, 49100 Corfu, Greece; p16abat@ionio.gr
* Correspondence: andronikos@ionio.gr
† These authors contributed equally to this work.

Abstract: This paper introduces a novel entanglement-based QKD protocol, that makes use of a modified symmetric version of the Bernstein-Vazirani algorithm, in order to achieve secure and efficient key distribution. Two variants of the protocol, one fully symmetric and one semi-symmetric, are presented. In both cases, the spatially separated Alice and Bob share multiple EPR pairs, each one qubit of the pair. The fully symmetric version allows both parties to input their tentative secret key from their respective location and acquire in the end a totally new and original key, an idea which was inspired by the Diffie-Hellman key exchange protocol. In the semi-symmetric version, Alice sends her chosen secret key to Bob (or vice versa). The performance of both protocols against an eavesdroppers attack is analyzed. Finally, in order to illustrate the operation of the protocols in practice, two small scale but detailed examples are given.

Keywords: quantum cryptography; quantum key distribution; the Bernstein-Vazirani algorithm; EPR pairs; quantum entanglement; quantum information theory

Citation: Ampatzis, M.; Andronikos, T. QKD Based on Symmetric Entangled Bernstein-Vazirani. *Entropy* **2021**, *23*, 870. https://doi.org/10.3390/e23070870

Academic Editor: Ivan B. Djordjevic

Received: 9 June 2021
Accepted: 5 July 2021
Published: 7 July 2021

1. Introduction

In the course of the last century, the scientific community experimented with different ideas and forms of computation, trying to harness the power of nature and create machines that allowed us to process immeasurable amounts of information in mere seconds, thus radically changing the world around us in the span of a few decades. However, in the present era classical computers are reaching a point where it will be infeasible to substantially enhance their efficiency due to the physical limitations of transistors. This has started a new incentive to resurrect previous attempts concerning research of new types of computation. Out of all the different proposals for a viable substitute to classical computing, undoubtedly the most promising of them all is quantum computation, mainly due to the fact that it allows the exploitation of the most fundamental properties of physics.

1.1. Related Work

As technology comes closer to the realization of this goal, it appears that certain profound adaptations regarding different branches of computer science need to take place in order to achieve a smoother transition from the classical to the quantum era. One of the most important such branches is the field of cryptography, due to the vulnerability of the current security algorithms against quantum computers [1,2]. This inherent weakness in the modern security protocols and the race for building a resilient security infrastructure against quantum computers [3] before they become a reality, were the two catalysts that resulted in a schism of the field into two sub-fields, which are based on two different philosophies and ideologies. The first sub-field, known as post-quantum cryptography or quantum-resistant cryptography, relies on the complexity of mathematics as its security basis. It is an attempt to develop cryptographic systems that are secure against both quantum and classical computers and can also be interpreted within the already existing communications protocols and networks. The second sub-field, which is called quantum cryptography,

is being built upon the implementation of the properties of quantum mechanics and, thus, takes advantage of nature's own fundamental laws in order to achieve security.

The sub-field of quantum cryptography, on which the primary interest of the current paper lies upon, has seen enormous growth of both theoretical and practical nature. Two landmark papers, the BB84 protocol [4] and the E91 protocol [5], were the first papers that proved that key distribution between two parties relying on the properties of quantum mechanics was possible. These two protocols have established the two schemes that all quantum key distribution (QKD) protocols are based on, the *prepare-and-measure-based scheme* and the *entanglement-based scheme*. After the publications of these two protocols, a plethora of interesting proposals for different QKD protocols based on these two schemes were suggested, further expanding the field on a theoretical level. At the same time, some truly remarkable real life implementations of some protocols were demonstrated as in [6–11]. These implementations have demonstrated that quantum cryptography is not just a mere theoretical experiment, but a possible reality in the near future.

Over the last few years, there was a noticeable increase in the effort to find new viable applications for well-known quantum algorithms, such as the Deutsch-Jozsa algorithm [12], the Bernstein-Vazirani algorithm [13] and Simon's periodicity algorithm [14]. Many of these proposals have been made in the field of quantum cryptography, using these algorithms as viable QKD protocols [15–17]. Motivated from these attempts, this paper proposes two novel variants of an entanglement-based QKD protocol that makes use of the Bernstein-Vazirani algorithm. The novelty of this work lies on the fact that it uniquely combines some key ingredients. Starting with entanglement, which is an integral part of the protocol, the corresponding qubits in Alice and Bob's input registers are maximally entangled. Thus, the proposed protocols exhibit all the inherent advantages that an entanglement-based QKD protocol provides in terms of security against an eavesdropper, as first demonstrated in the E91 protocol [5]. Additionally, the Bernstein–Vazirani algorithm [13], a fast and useful quantum algorithm that guarantees the creation of the key using just one application of the appropriate function, is used in a critical manner. Furthermore, the fully symmetric variant is inspired by the Diffie-Hellman idea [18] of deriving the final key from a random combination of two separate keys. This idea is not just cosmetic, as the ability to obtain a key that neither Alice or Bob know from the start, adds an additional layer of security, further improving the strength of the protocol. Finally, the proposed protocol can be implemented in two versions: the fully symmetric version and the semi-symmetric one. In the fully symmetric variant, both Alice and Bob can input their tentative secret keys from their respective locations and acquire in the end a totally new and original key. In the semi-symmetric one, Alice (alternatively Bob) constructs the secret key that she (or he) communicates securely to the other party.

The protocol is described as a quantum game, which despite the rather playful name, it is another noteworthy field that has emerged due to the transition to the quantum era and is used to address difficult and interesting problems within the quantum realm. This approach was chosen in an effort to make the presentation more mnemonic and easier to follow, due to the close connection that both fields share and the fact that any cryptographic situation can be conceived as a game between the two fictional heroes Alice and Bob, who play the roles of two remote parties that are trying to communicate, and the enemy Eve who tries to eavesdrop the conversation, a case which becomes apparent with the quantum game of coin tossing and the BB84 protocol [4,19] and references therein. This situation has been generalized in [20] to quantum dice rolling. For the reader striving for a more rounded understanding of the connection of the two fields, one can start with the two important works in the field of quantum game theory dating back to 1999, which were instrumental for the creation of the field: Meyer's PQ penny flip game [21], which can be regarded as the quantum analogue of the classical penny flip game, and the introduction of the Eisert-Wilkens-Lewenstein scheme [22] that is widely used in the field. Regarding the PQ penny flip game, some recent results can be found in [23,24], were its connection to the dihedral groups was established. As for the Eisert-Wilkens-Lewenstein scheme, it proved

fruitful in providing many interesting results. For example, it led to quantum adaptations of the famous prisoners' dilemma in which the quantum strategies are better than any classical strategy ([22]), as well as extensions of the classical repeated prisoners' dilemma conditional strategies to a quantum setting ([25]).

1.2. Organization

The paper is structured as follows. Section 1 provides a brief introduction to the subject and gives the most relevant references. Section 2 introduces and explains the tools used for the formulation of the protocols in this article. Section 3 presents and thoroughly analyzes the fSEBV and sSEBV protocols, so that their functionality can be completely understood. Section 4 contains two detailed examples, one for each protocol, to demonstrate their operation. Finally, Section 5 summarizes the proposed protocols and discusses their potential applications in various situations.

2. Preliminaries

2.1. Quantum Entanglement and Bell States

Quantum entanglement is one of the fundamental principles of quantum mechanics and can be described mathematically as the linear combination of two or more product states. The Bell states are specific quantum states of two qubits, sometimes called an EPR pair, that represent the simplest examples of quantum entanglement. From the perspective of quantum computation, an EPR pair can be produced by a circuit with two qubits, in which a Hadamard gate is applied to the first qubit and subsequently a CNOT gate is applied to both qubits. These states can be elegantly described by the following equation taken from [26].

$$|\beta_{x,y}\rangle = \frac{|0\rangle\,|y\rangle + (-1)^x\,|1\rangle\,|\bar{y}\rangle}{\sqrt{2}}\,, \tag{1}$$

where $|\bar{y}\rangle$ is the negation of $|y\rangle$.

In a more detailed manner, the Bell states can be described as follows.

$$|\Phi^+\rangle = |\beta_{00}\rangle = \frac{|0\rangle\,|0\rangle + |1\rangle\,|1\rangle}{\sqrt{2}} \tag{2}$$

$$|\Phi^-\rangle = |\beta_{10}\rangle = \frac{|0\rangle\,|0\rangle - |1\rangle\,|1\rangle}{\sqrt{2}} \tag{3}$$

$$|\Psi^+\rangle = |\beta_{01}\rangle = \frac{|0\rangle\,|1\rangle + |1\rangle\,|0\rangle}{\sqrt{2}} \tag{4}$$

$$|\Psi^-\rangle = |\beta_{11}\rangle = \frac{|0\rangle\,|1\rangle - |1\rangle\,|0\rangle}{\sqrt{2}} \tag{5}$$

The main advantage of quantum entanglement is that if one qubit of the pair is measured, then the other will collapse immediately despite the distance between the two. This unique characteristic of quantum entanglement can be used on quantum key distribution as first described by Ekert in the E91 protocol. Therefore, in order to achieve quantum key distribution, multiple EPR pairs will be needed. For this reason, the mathematical representation of multiple EPR pairs will be expedient. If one starts with the entangled Bell state $|\Phi^+\rangle$, which can be cast as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A\,|0\rangle_B + |1\rangle_A\,|1\rangle_B)\,, \tag{6}$$

some easy computations show that

$$|\Phi^+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle_A \, |\mathbf{x}\rangle_B \ , \tag{7}$$

which will be required in the presentation of Section 3.

2.2. A Brief Description of the Bernstein-Vazirani Algorithm

Regarded as one of the earliest quantum algorithms, along with the Deutsch-Josza algorithm and Simon's periodicity algorithm, the Bernstein-Vazirani algorithm, first introduced by Ethan Bernstein and Umesh Vazirani, can be considered to be a useful extension of the Deutsch-Josza algorithm, due to the fact that it was directly inspired by it and shared multiple common characteristics on both structure and implementation. Yet, despite the similarities, it has proved its value by demonstrating that the superiority of a quantum computer can be successfully used for more complex problems than the Deutsch-Josza problem.

The Bernstein-Vazirani problem can be described as the ensuing game between two players, namely Alice and Bob, who are spatially separated. Alice in Athens is corresponding with Bob in Corfu using letters. Alice starts the game by selecting a number x from 0 to $2^n - 1$ and mails its binary n-bit representation $\mathbf{x}$ to Bob. After Bob receives this message, he calculates the value of some function

$$f : \{0, 1, \ldots, 2^n - 1\} \to \{0, 1\} \ , \tag{8}$$

and replies with the result, which is either 0 or 1. The rules of the game dictate that Bob must use a function $f_{\mathbf{s}}(\mathbf{x})$, where $\mathbf{s} = s_{n-1} \ldots s_1 s_0$ and $\mathbf{x} = x_{n-1} \ldots x_1 x_0$ are n-bit binary numbers representing integers in the range $0, 1, \ldots, 2^n - 1$, such that

$$f_{\mathbf{s}}(\mathbf{x}) = \mathbf{s} \cdot \mathbf{x} \bmod 2 \ . \tag{9}$$

The inner product modulo 2 is defined as

$$\mathbf{s} \cdot \mathbf{x} \bmod 2 = s_{n-1} x_{n-1} \oplus \cdots \oplus s_0 x_0 \ , \tag{10}$$

where $\oplus$ is the exclusive-or operator. Therefore, the function is guaranteed to return the bitwise product of Alice's input $\mathbf{x}$ with a secret key $\mathbf{s}$ that Bob has chosen. Alice's goal in this game is to determine with certainty the secret key $\mathbf{s}$ that Bob has picked, corresponding with him as little as possible. How fast can she succeed?

In the *classical* version of this problem, Alice can find the secret key $\mathbf{s}$ by taking advantage of the nature of the function $f_{\mathbf{s}}(\mathbf{x})$ and, in particular, by sending Bob the inputs shown in Table 1.

Table 1. Alice must communicate with Bob n times in order find the secret key $\mathbf{s}$.

The Evolution of the Bernstein-Vazirani Game	
Alice's Input x	**Bob's Response**
$\mathbf{x} = 10 \ldots 00$	s_{n-1}
$\vdots$	$\vdots$
$\mathbf{x} = 00 \ldots 10$	s_1
$\mathbf{x} = 00 \ldots 01$	s_0

In that way, Alice will discover a bit of the string $\mathbf{s}$ (the bit s_i) with each query she sends. For example, with $\mathbf{x} = 10 \ldots 0$ she can obtain the most significant bit of $\mathbf{s}$, with $\mathbf{x} = 01 \ldots 0$ she will find the next most significant bit of $\mathbf{s}$, and by following the same procedure, when she reaches $\mathbf{x} = 00 \ldots 1$, she will have finally managed to reveal the entire

string **s**. Despite, the efficiency of this method, Alice is still limited by sending to Bob only one query at a time. Therefore, the best possible classical scenario requires from her to correspond with Bob at least n times, in order for her to succeed in her goal.

By observing the core attributes of the aforementioned game, we can divide it into the following three big steps, which are:

- Alice provides an input,
- Bob applies the function $f_{\mathbf{s}}(\mathbf{x})$, and
- after multiple repetitions of the previous two steps, Alice is finally able to reveal the secret key **s**.

It can be seen from the above steps that the game can easily become more efficient by implementing certain tools from quantum mechanics. If Alice and Bob were able to exchange information with the use of qubits instead of classical bits, then Alice could send the superposition of these qubits to Bob with only one message. Furthermore, if Bob was using a unitary transformation U_f instead of a function $f_{\mathbf{s}}(x)$, then Alice would be able to achieve her goal with only one communication.

The *quantum* version of the Bernstein-Vazirani algorithm, can be described by the following quantum game. The game initially starts with Alice preparing two quantum registers, one of size n to store her query in and one of size 1, in which Bob will store his answer in. We will refer to these registers as Alice's input and output registers, respectively. Next, she applies the Hadamard gate to every qubit, in order to acquire the even superposition state of each register and then she sends both registers to Bob. Right after Bob receives the contents of the registers, he applies the unitary transform U_f and sends them back to Alice. In the final stage of the game, Alice concludes the algorithm by measuring her input register and obtaining the secret key **s**. The whole process of the game, is summarized in Figure 1 below.

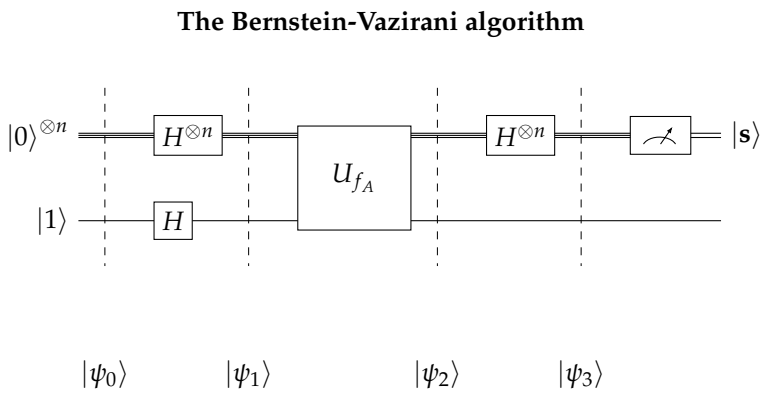

Figure 1. This figures gives a schematic representation of the Bernstein-Vazirani algorithm.

Now, in order to obtain a better understanding of the nature of the algorithm, let us examine the evolution of the quantum states more closely. First, Alice starts with the initial state

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle . \tag{11}$$

The n qubits of her input register are all prepared at state $|0\rangle$ and the qubit of the output register is prepared at state $|1\rangle$. Next, Alice applies the Hadamard transform to both registers and the state becomes

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \tag{12}$$

The derivation of the previous equation is based on the fact that

$$H^{\otimes n}\left|0\right\rangle^{\otimes n}=\frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\{0,1\}^n}\left|\mathbf{x}\right\rangle, \tag{13}$$

a standard result in the literature (for its derivation see [26,27]). At this point the input register is in an even superposition of all possible states and the output register is in an evenly weighted superposition of $|0\rangle$ and $|1\rangle$. Thus, Alice is now ready to send both registers to Bob so he may apply the function $f_{\mathbf{s}}(x)$ using

$$U_f:\left|\mathbf{x},y\right\rangle\rightarrow\left|\mathbf{x},y\oplus f(\mathbf{x})\right\rangle\ , \tag{14}$$

which results in the next state

$$\left|\psi_2\right\rangle=\frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}\left|\mathbf{x}\right\rangle\left(\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}\right). \tag{15}$$

The appearance of $(-1)^{f(\mathbf{x})}$ in Equation (15) is due to the fact that if $|y\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, then

$$\left|y\oplus f(\mathbf{x})\right\rangle=\begin{cases}\frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(\mathbf{x})=0\\ \frac{|1\rangle-|0\rangle}{\sqrt{2}} & \text{if } f(\mathbf{x})=1\end{cases}\Rightarrow\left|y\oplus f(\mathbf{x})\right\rangle=(-1)^{f(\mathbf{x})}\left(\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}\right). \tag{16}$$

In view of (9) and (15) becomes

$$\left|\psi_2\right\rangle=\frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{\mathbf{s}\cdot\mathbf{x}}\left|\mathbf{x}\right\rangle\left(\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}\right), \tag{17}$$

which is the state returned back to Alice.

Let us now recall the following well-known equation that gives in a succinct form the result of the application of the Hadamard transformation to an arbitrary n-qubit basis ket $|\mathbf{x}\rangle$ (see [26,27]).

$$H^{\otimes n}\left|\mathbf{x}\right\rangle=\frac{1}{\sqrt{2^n}}\sum_{\mathbf{z}\in\{0,1\}^n}(-1)^{\mathbf{z}\cdot\mathbf{x}}\left|\mathbf{z}\right\rangle\ . \tag{18}$$

Thus, after Alice receives the registers back, she applies the Hadamard transform to the input register for a second time. Via the use of Equation (18), the resulting state can be written as

$$\begin{aligned}\left|\psi_3\right\rangle &= \tfrac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{\mathbf{s}\cdot\mathbf{x}}H^{\otimes n}\left|\mathbf{x}\right\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\\ &= \tfrac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{\mathbf{s}\cdot\mathbf{x}}\left(\tfrac{1}{\sqrt{2^n}}\sum_{\mathbf{z}\in\{0,1\}^n}(-1)^{\mathbf{z}\cdot\mathbf{x}}\left|\mathbf{z}\right\rangle\right)\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\\ &= \tfrac{1}{2^n}\sum_{\mathbf{x}\in\{0,1\}^n}\sum_{\mathbf{z}\in\{0,1\}^n}(-1)^{\mathbf{s}\cdot\mathbf{x}\oplus\mathbf{z}\cdot\mathbf{x}}\left|\mathbf{z}\right\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\\ &= \tfrac{1}{2^n}\sum_{\mathbf{z}\in\{0,1\}^n}\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{(\mathbf{s}\oplus\mathbf{z})\cdot\mathbf{x}}\left|\mathbf{z}\right\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=\left|\mathbf{s}\right\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\end{aligned} \tag{19}$$

The last equation is due to the following fact: if $\mathbf{s}=\mathbf{z}$, then $\forall\,\mathbf{x}\in\{0,1\}^n\ (\mathbf{s}\oplus\mathbf{z})\cdot\mathbf{x}=0$, otherwise for exactly half of the inputs $\mathbf{x}$ the exponent will be 0 and for the remaining half the exponent will be 1. This is typically written in a more concise manner as follows:

$$\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{(\mathbf{s}\oplus\mathbf{z})\cdot\mathbf{x}}=2^n\delta_{\mathbf{s},\mathbf{z}}\ . \tag{20}$$

The algorithm terminates with the final measurement of the input register by Alice whereby she obtains the secret key **s** and concludes the whole process.

3. QKD Based on Symmetric Entangled B-V

In this section, the two versions of the proposed symmetric entangled QKD protocol based on the Bernstein-Vazirani algorithm are presented and described in great detail. These are the *fully symmetric* version of the protocol, or **fSEBV** for short, and the *semi-symmetric* version of the protocol, or **sSEBV** for short.

3.1. The fSEBV Protocol

Starting with the fSEBV protocol we consider a slight alteration of the aforementioned Bernstein-Vazirani game. As before, the game starts with the two players Alice and Bob who are spatially separated. This time, instead of using normal qubits in a separable state, they use maximally entangled EPR pairs, and they both share a qubit from each pair. An important rule of the game is that there are no limitations on which entity will actually create the EPR pairs in the first place. The pairs can be created and distributed accordingly by Alice or Bob, or they can be acquired from a third party source. This last situation is depicted in Figure 2. Exactly as in the previous game, the goal of the current game is to acquire a secret key **s**. However, in this specific protocol symmetry plays a crucial role, as Alice and Bod behave in a perfectly symmetrical way by both having their own secret keys, which they will attempt to input into the system, exactly as in the original algorithm. Alice's key is denoted by $\mathbf{s}_A$, Bob's key by $\mathbf{s}_B$ and they both take identical actions. Please note that neither Alice nor Bob need apply the Hadamard transform onto their input registers because they are already in the desired even superposition of all basis states, as they are populated by n pairs in the $|\Phi^+\rangle$ Bell state. In this respect the fSEBV protocol differs from the vanilla Bernstein-Vazirani algorithm.

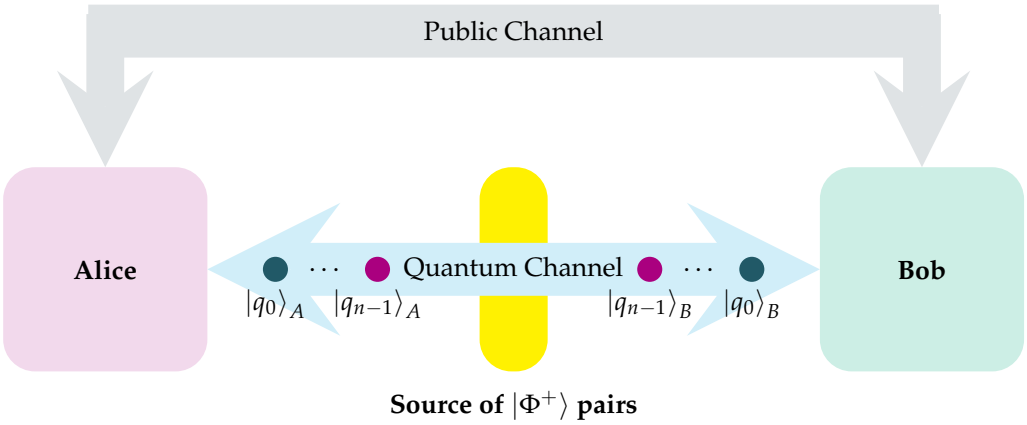

Figure 2. Alice and Bob are spatially separated. A third party, the source, creates n pairs of $|\Phi^+\rangle$ entangled photons and sends one qubit from every pair to Alice and the other qubit to Bob.

Following the aforementioned steps of the fSEBV protocol, a valid question may arise regarding what will Alice and Bob acquire after they both apply their starting secret keys $\mathbf{s}_A$ and $\mathbf{s}_B$ into their own pieces of the EPR pairs? To provide the answer, let us examine the algorithm more closely. With the help of Equation (7), the initial state of the protocol can be written as

$$|\psi_0\rangle = |\Phi^+\rangle^{\otimes n} |1\rangle_A |1\rangle_B = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B |1\rangle_A |1\rangle_B \ . \tag{21}$$

Subscripts A and B are consistently used to designate Alice's and Bob's registers respectively. Alice and Bob initiate the protocol by applying the Hadamard transform to their output registers, which produces the ensuing state

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B . \tag{22}$$

Now, both Alice and Bob can apply their functions on their registers using the standard scheme

$$U_f : |\mathbf{x}, y\rangle \to |\mathbf{x}, y \oplus f(\mathbf{x})\rangle \ . \tag{23}$$

Consequently, the next state becomes

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f_A(\mathbf{x})} |\mathbf{x}\rangle_A (-1)^{f_B(\mathbf{x})} |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B . \tag{24}$$

At this stage, let us recall that Alice's and Bob's functions are

$$f_A(\mathbf{x}) = \mathbf{s}_A \cdot \mathbf{x} \bmod 2 \tag{25}$$

$$f_B(\mathbf{x}) = \mathbf{s}_B \cdot \mathbf{x} \bmod 2 \, , \tag{26}$$

where $\mathbf{s}_A$ and $\mathbf{s}_B$ are the keys chosen by Alice and Bob, respectively. Based on (24)–(26) can be written as

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{\mathbf{s}_A\cdot\mathbf{x}} |\mathbf{x}\rangle_A (-1)^{\mathbf{s}_B\cdot\mathbf{x}} |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{\mathbf{s}_A\cdot\mathbf{x}\oplus\mathbf{s}_B\cdot\mathbf{x}} |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B)\cdot\mathbf{x}} |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B . \end{aligned} \tag{27}$$

Subsequently, both Alice and Bob apply the Hadamard transformation to their input registers. This drives the system into the next state, which, by utilizing Equation (18) twice, can be written as

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B)\cdot\mathbf{x}} H^{\otimes n} |\mathbf{x}\rangle_A H^{\otimes n} |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B)\cdot\mathbf{x}} \left(\frac{1}{\sqrt{2^n}} \sum_{\mathbf{z}\in\{0,1\}^n} (-1)^{\mathbf{z}\cdot\mathbf{x}} |\mathbf{z}\rangle_A\right) \left(\frac{1}{\sqrt{2^n}} \sum_{\mathbf{w}\in\{0,1\}^n} (-1)^{\mathbf{w}\cdot\mathbf{x}} |\mathbf{w}\rangle_B\right) \\ &\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{(\sqrt{2^n})^3} \sum_{\mathbf{x}\in\{0,1\}^n} \sum_{\mathbf{z}\in\{0,1\}^n} \sum_{\mathbf{w}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} |\mathbf{z}\rangle_A |\mathbf{w}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{(\sqrt{2^n})^3} \sum_{\mathbf{z}\in\{0,1\}^n} \sum_{\mathbf{w}\in\{0,1\}^n} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} |\mathbf{z}\rangle_A |\mathbf{w}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B . \end{aligned} \tag{28}$$

When $\mathbf{z} \oplus \mathbf{w} = \mathbf{s}_A \oplus \mathbf{s}_B$, then $\forall \mathbf{x} \in \{0,1\}^n$, the expression $(-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}}$ becomes $(-1)^0 = 1$ and the sum $\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} = 2^n$.

Whenever $\mathbf{z} \oplus \mathbf{w} \neq \mathbf{s}_A \oplus \mathbf{s}_B$, the sum is just 0 because for exactly half of the inputs $\mathbf{x}$ the exponent will be 0 and for the remaining half the exponent will be 1. Hence, one may write that

$$\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} = 2^n \delta_{\mathbf{s}_A\oplus\mathbf{s}_B,\mathbf{z}\oplus\mathbf{w}} \,. \tag{29}$$

Using Equation (29), and ignoring for the moment the two factors $\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_A$ and $\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_B$, the following two equivalent and symmetric forms can be derived

$$\sum_{\mathbf{z}\in\{0,1\}^n}\sum_{\mathbf{w}\in\{0,1\}^n}\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} |\mathbf{z}\rangle_A |\mathbf{w}\rangle_B = 2^n \sum_{\mathbf{z}\in\{0,1\}^n} |\mathbf{z}\rangle_A |\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\rangle_B \,, \tag{30}$$

and

$$\sum_{\mathbf{w}\in\{0,1\}^n}\sum_{\mathbf{z}\in\{0,1\}^n}\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} |\mathbf{z}\rangle_A |\mathbf{w}\rangle_B = 2^n \sum_{\mathbf{w}\in\{0,1\}^n} |\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{w}\rangle_A |\mathbf{w}\rangle_B \,. \tag{31}$$

By combining (28) with (30) and (31), state $|\psi_3\rangle$ can be written in two different ways:

$$\begin{aligned} |\psi_3\rangle &= \tfrac{1}{\sqrt{2^n}} \sum_{\mathbf{z}\in\{0,1\}^n} |\mathbf{z}\rangle_A |\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\rangle_B \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_A \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_B \\ &= \tfrac{1}{\sqrt{2^n}} \sum_{\mathbf{w}\in\{0,1\}^n} |\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{w}\rangle_A |\mathbf{w}\rangle_B \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_A \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_B . \end{aligned} \tag{32}$$

Finally, Alice and Bob measure their EPR pairs in the input registers, obtaining

$$|\psi_4\rangle = |\mathbf{z}_0\rangle_A |\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}_0\rangle_B = |\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{w}_0\rangle_A |\mathbf{w}_0\rangle_B \,, \quad \text{for some} \quad \mathbf{z}_0, \mathbf{w}_0 \in \{0,1\}^n \,. \tag{33}$$

Please note that in general $\mathbf{z}_0 \neq \mathbf{w}_0$. The quantum part of the protocol is now complete. The final secret key is the string $\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0$ that Bob measured in his input register. In the highly unlikely event that $|\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0\rangle = |0\rangle^{\otimes n}$, Bob should inform Alice through the use of the public channel that the whole procedure must be repeated once again, since such a key is clearly unacceptable. However, for a n-bit key the probability of this happening is negligible, specifically $\frac{1}{2^n}$, which rapidly tends to 0 as $n \to \infty$. Hence, it may be safely assumed that Bob possesses a viable secret key, namely $\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0$. Now the final step is for Alice to obtain the secret key too. This is easily achieved by simply having Bob publicly announce his tentative secret key $\mathbf{s}_B$ to Alice via the use of the public channel. Alice, who has measured the binary string $\mathbf{z}_0$ and she is already aware of her initial secret key $\mathbf{s}_A$, can easily obtain the final key, by simply calculating the XOR of $\mathbf{s}_A$, her measurement $\mathbf{z}_0$ and Bob's initial key $\mathbf{s}_B$, which she learns from the public channel. This concludes the fSEBV protocol.

The symmetry inherent in this protocol, enables the seamless reversal of roles. The protocol, as stated above, grants the initiative to Bob: it is his measurement $\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0$ that produces the secret key and it is his task to send his initial key $\mathbf{s}_B$ to Alice, in order to successfully complete the procedure. It is equally feasible to have Alice instead of Bob drive the whole process by taking her measurement $\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{w}_0$ to be the secret key, as shown in (33). In such an implementation of the fSEBV protocol, Alice must reveal her initial key $\mathbf{s}_A$ to Bob via the public channel.

During the transmission of Bob's key $\mathbf{s}_B$ using a public channel, any potential eavesdropper, namely Eve, does not gain any advantage by listening to the public channel. Due to the fact that she is oblivious of $\mathbf{z}_0$ and $\mathbf{s}_A$, she has no way of knowing or computing the final secret key. Hence, the fSEBV protocol ensures that if Alice and Bob can create their keys using a random number generator, in order to avoid possible patterns in the keys, Eve will be left with 2^n different combinations to test in order to find the secret key.

The steps of the protocol from Alice's and Bob's side are shown below in an algorithmic manner. Figure 3 depicts the protocol graphically in the form of a quantum circuit.

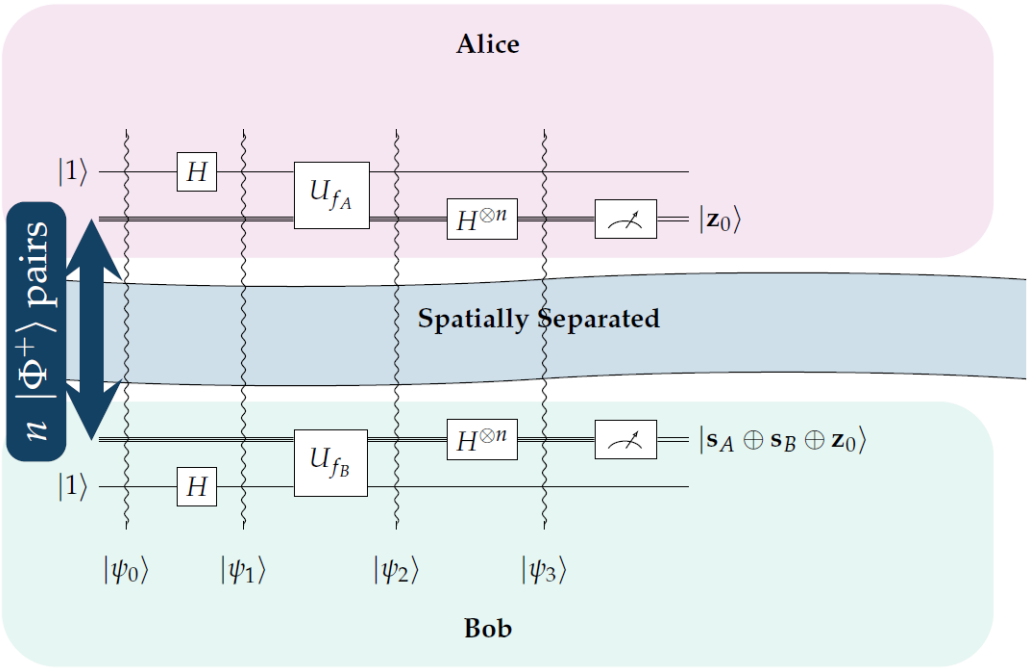

Figure 3. This figures gives a schematic representation of the proposed protocol.

Protocol fSEBV: Alice's actions

Alice's input register is populated with entangled qubits
- Alice's output register is set to $|1\rangle$
- Alice applies the Hadamard transform to her output register
- Alice applies her tentative key $\mathbf{s}_A$
- Alice applies the Hadamard transform to her input register
- Alice measures her input register to find the random binary string $\mathbf{z}_0$
- Alice receives information from Bob whether the process was a success or must be repeated
- If the procedure was successful, Alice receives from Bob his key $\mathbf{s}_B$ and, by already knowing $\mathbf{s}_A$ and $\mathbf{z}_0$, she computes the final key $\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0$

Protocol fSEBV: Bob's actions
- Bob's input register is populated with entangled qubits
- Bob's output register is set to $|1\rangle$
- Bob applies the Hadamard transform to his output register
- Bob applies his tentative key $\mathbf{s}_B$
- Bob applies the Hadamard transform to his input register
- Bob measures his input register to find the final secret key $\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0$
- In the unlikely event that $|\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0\rangle = |0\rangle^{\otimes n}$, Bob informs Alice that the process must be repeated from the start
- Otherwise Bob communicates his tentative key $\mathbf{s}_B$ to Alice via the public channel

3.2. The sSEBV Protocol

The sSEBV protocol explores a special but important case of the fSEBV protocol, which differs from the latter in one important aspect. Alice possesses her random initial key $\mathbf{s}_A$, but Bob's key $\mathbf{s}_B$ is not a random binary string anymore; it is specifically taken to be $\mathbf{0} = 0 \ldots 0$. Essentially, sSEBV protocol answers the question of what will happen, if one of the players, either Alice or Bob, decides not to send a key. As before Alice and Bob are

spatially separated and they both share n EPR pairs. In this variant, Alice and Bod behave in a semi-symmetrical way. Alice still uses her random initial key $\mathbf{s}_A$, but Bob is obliged to use $\mathbf{0}$ as his initial key.

In this case, by using Equation (7), it can seen that the initial state of the system is the following

$$|\psi_0\rangle = |\Phi^+\rangle^{\otimes n} |1\rangle_A |1\rangle_B = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B |1\rangle_A |1\rangle_B \ . \tag{34}$$

Similarly, Alice and Bob initiate the protocol by applying the Hadamard transform to their output registers, which produces the ensuing state

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B . \tag{35}$$

Next Alice and Bob apply their corresponding functions on their registers via the standard scheme

$$U_f : |\mathbf{x}, y\rangle \to |\mathbf{x}, y \oplus f(\mathbf{x})\rangle \ , \tag{36}$$

only now the situation is quite different because Bob must necessarily use $\mathbf{0}$:

$$f_A(\mathbf{x}) = \mathbf{s}_A \cdot \mathbf{x} \bmod 2 \tag{37}$$

$$f_B(\mathbf{x}) = \mathbf{0} \cdot \mathbf{x} \bmod 2 = 0 \, . \tag{38}$$

In view of Equations (37) and (38), the next state becomes

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f_A(\mathbf{x})} |\mathbf{x}\rangle_A (-1)^0 |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{\mathbf{s}_A\cdot\mathbf{x}} |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B . \end{aligned} \tag{39}$$

Subsequently, both Alice and Bob apply the Hadamard transformation to their input registers. Taking into account Equation (18), one can see that their combined actions drive the system into the next state

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{\mathbf{s}_A\cdot\mathbf{x}} H^{\otimes n} |\mathbf{x}\rangle_A H^{\otimes n} |\mathbf{x}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{\mathbf{s}_A\cdot\mathbf{x}} \left(\frac{1}{\sqrt{2^n}} \sum_{\mathbf{z}\in\{0,1\}^n} (-1)^{\mathbf{z}\cdot\mathbf{x}} |\mathbf{z}\rangle_A\right) \left(\frac{1}{\sqrt{2^n}} \sum_{\mathbf{w}\in\{0,1\}^n} (-1)^{\mathbf{w}\cdot\mathbf{x}} |\mathbf{w}\rangle_B\right) \\ &\quad \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{(\sqrt{2^n})^3} \sum_{\mathbf{x}\in\{0,1\}^n} \sum_{\mathbf{z}\in\{0,1\}^n} \sum_{\mathbf{w}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} |\mathbf{z}\rangle_A |\mathbf{w}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{(\sqrt{2^n})^3} \sum_{\mathbf{z}\in\{0,1\}^n} \sum_{\mathbf{w}\in\{0,1\}^n} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} |\mathbf{z}\rangle_A |\mathbf{w}\rangle_B \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)_B . \end{aligned} \tag{40}$$

When $\mathbf{z} \oplus \mathbf{w} = \mathbf{s}_A$, then $\forall \mathbf{x} \in \{0,1\}^n$, the expression $(-1)^{(\mathbf{s}_A\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}}$ becomes $(-1)^0 = 1$ and the sum $\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} = 2^n$. Whenever $\mathbf{z} \oplus \mathbf{w} \neq \mathbf{s}_A$, the sum is

just 0 because for exactly half of the inputs $\mathbf{x}$ the exponent will be 0 and for the remaining half the exponent will be 1. Therefore, again one may write that

$$\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} = 2^n \delta_{\mathbf{s}_A,\mathbf{z}\oplus\mathbf{w}} \,. \tag{41}$$

Using Equation (41), and ignoring for the moment the two factors $\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_A$ and $\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_B$, the following two equivalent and symmetric forms can be derived

$$\sum_{\mathbf{z}\in\{0,1\}^n}\sum_{\mathbf{w}\in\{0,1\}^n}\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{s}_B\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} |\mathbf{z}\rangle_A |\mathbf{w}\rangle_B = 2^n \sum_{\mathbf{z}\in\{0,1\}^n} |\mathbf{z}\rangle_A |\mathbf{s}_A\oplus\mathbf{z}\rangle_B \,, \tag{42}$$

and

$$\sum_{\mathbf{w}\in\{0,1\}^n}\sum_{\mathbf{z}\in\{0,1\}^n}\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{s}_A\oplus\mathbf{z}\oplus\mathbf{w})\cdot\mathbf{x}} |\mathbf{z}\rangle_A |\mathbf{w}\rangle_B = 2^n \sum_{\mathbf{w}\in\{0,1\}^n} |\mathbf{s}_A\oplus\mathbf{w}\rangle_A |\mathbf{w}\rangle_B \,. \tag{43}$$

By combining (40) with (42) and (43), state $|\psi_3\rangle$ can be written in two different ways:

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{z}\in\{0,1\}^n} |\mathbf{z}\rangle_A |\mathbf{s}_A\oplus\mathbf{z}\rangle_B \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_B \\ &= \frac{1}{\sqrt{2^n}} \sum_{\mathbf{w}\in\{0,1\}^n} |\mathbf{s}_A\oplus\mathbf{w}\rangle_A |\mathbf{w}\rangle_B \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_A \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)_B . \end{aligned} \tag{44}$$

Now, when Alice and Bob measure their input registers, they will obtain

$$|\psi_4\rangle = |\mathbf{z}_0\rangle_A |\mathbf{s}_A\oplus\mathbf{z}_0\rangle_B = |\mathbf{s}_A\oplus\mathbf{w}_0\rangle_A |\mathbf{w}_0\rangle_B \,, \quad \text{for some} \quad \mathbf{z}_0, \mathbf{w}_0 \in \{0,1\}^n \,. \tag{45}$$

As in the fSEBV protocol, here also holds that $\mathbf{z}_0 \neq \mathbf{w}_0$ in general. This time, there are two ways in which the final part of the protocol can unfold. One way, exactly like before, is to take Bob's measurement as the new secret key. The other, equally viable choice, is to take Alice's initial key $\mathbf{s}_A$ as the final secret key. In that case Alice must publicly announce $\mathbf{z}_0$ to Bob via a public channel, so that he can compute $\mathbf{s}_A$. This is a suitable choice in cases where, for whatever reason, Alice must set the secret key herself, not wanting to leave anything to chance. In that way she may securely communicate her chosen key to Bob. As before, during the transmission of Alice's measurement $\mathbf{z}_0$ using a public channel, Eve does not gain any advantage by eavesdropping on their communication. Due to the fact that she is oblivious to $\mathbf{s}_A$, she has no way of knowing or computing the final secret key. Hence, the sSEBV protocol also ensures that if Alice devises her key using a random number generator, in order to avoid possible patterns in the keys, Eve will be left with 2^n different combinations to test in order to find the secret key.

The detailed actions for the implementation of the sSEBV protocol from Alice's and Bob's side are given below. Although the sSEBV protocol is not perfectly symmetric, reversal of Alice's and Bob's roles is still trivially easy. As can be seen from the following description, not only is Alice the one to choose the secret key, but it is also she that sends the final measurement $\mathbf{z}_0$ to Bob so that he can successfully derive the secret key. It is equally feasible to have Bob instead of Alice choose the secret key and have Alice use $\mathbf{0}$ in the first stage. In such a realization of the sSEBV protocol, Bob must also reveal his final measurement $\mathbf{w}_0$ to Alice via the public channel.

4. Examples Illustrating the Operation of the Protocols

This section presents and analyzes two small scale but detailed examples in order to illustrate the operation of the fSEBV and sSEBV protocols in practice. The fSEBV and sSEBV protocols were simulated using IBM's *Qiskit* open source SDK ([28]). Specifically, the Aer provider using the high performance *qasm* simulator for simulating quantum circuits [29]

in its default settings was used. Please note that during our tests it was not possible to simulate in Qiskit Alice and Bob being spatially separated or a third party source providing the entangled EPR pairs. So these important assumptions cannot be accurately reflected in the simulation and for that reason the examples do not represent a real life environment. As a result Alice and Bob appear in the same circuit. Specifically, Alice's input register consists of the qubits $|q_2q_1q_0\rangle$ and her output register is $|q_3\rangle$. Symmetrically, Bob's input register consists of the qubits $|q_6q_5q_4\rangle$ and his output register is $|q_7\rangle$. Moreover, the entangled EPR pairs are created by the circuit itself. This is depicted in Figures 4, where in the initial stage of the corresponding circuits Hadamard and CNOT gates are used to populate Alice's and Bob's input registers with entangled EPR pairs, exactly as explained in Section 2.

Protocol sSEBV: Alice's actions

- Alice's input register is populated with entangled qubits
- Alice's output register is set to $|1\rangle$
- Alice applies the Hadamard transform to her output register
- Alice applies her chosen key $\mathbf{s}_A$
- Alice applies the Hadamard transform to her input register
- Alice measures her input register to find the random binary string $\mathbf{z}_0$
- Alice announces the binary string $\mathbf{z}_0$ to Bob via the public channel

Protocol sSEBV: Bob's actions

- Bob's input register is populated with entangled qubits
- Bob's output register is set to $|1\rangle$
- Bob applies the Hadamard transform to his output register
- Bob applies his key $\mathbf{0}$
- Bob applies the Hadamard transform to his input register
- Bob measures his input register to find the binary string $\mathbf{s}_A \oplus \mathbf{z}_0$
- Bob receives $\mathbf{z}_0$ and computes the key $\mathbf{s}_A$

4.1. Example for the fSEBV Protocol

In this example it is assumed that $\mathbf{s}_A = 101$ and $\mathbf{s}_B = 110$. The resulting circuit in displayed in Figure 4.

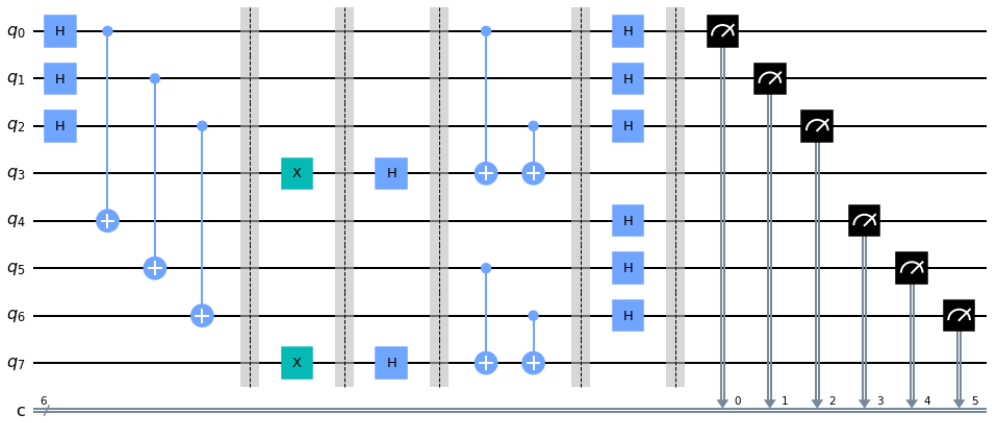

Figure 4. The circuit for the fSEBV protocol.

The final measurement by Alice and Bob will produce one of the 8 outcomes shown in Figure 5 along with their corresponding probabilities as given by running the qasm simulator for 2048 shots. A simple inspection of the possible outcomes confirms Equation (33). This is because every possible outcome can be written either as $|\mathbf{z}_0\rangle_A |\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0\rangle_B$ or as $|\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{w}_0\rangle_A |\mathbf{w}_0\rangle_B$, for some, generally different, $\mathbf{z}_0, \mathbf{w}_0 \in \{0,1\}^n$. Hence, Bob, after

measuring (and accepting) the secret key $\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0$, just needs to send his secret key $\mathbf{s}_B = 110$ to Alice so that she too can derive the secret key.

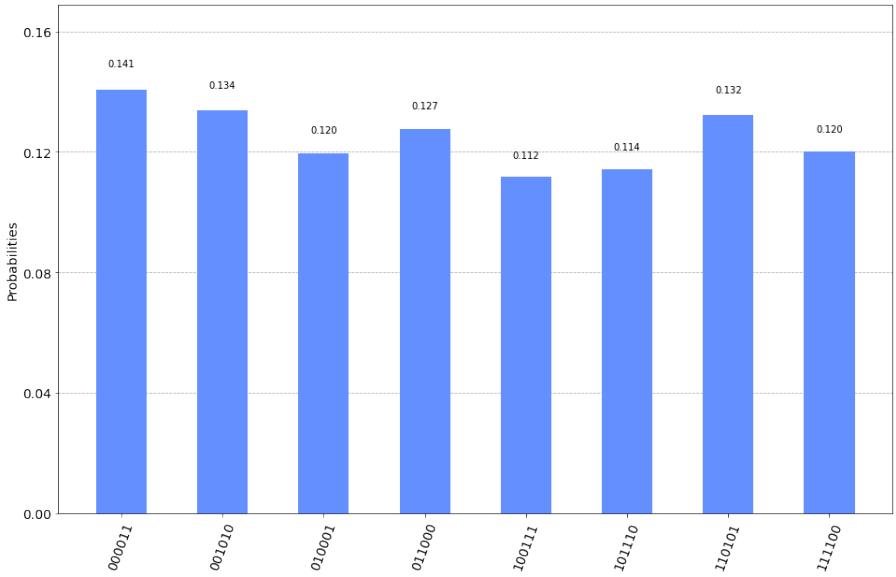

Figure 5. The possible outcomes of the measurement and their corresponding probabilities for the circuit in Figure 4.

To avoid any confusion, we clarify that the measurements shown in Figure 5 depict both Alice's and Bob's input registers as $|q_6q_5q_4q_2q_1q_0\rangle$. In particular, every one of the eight possible outcomes is shown along with the probability of measuring this outcome, as computed by the qasm simulator. The three most significant bits represent Bob's measurement or $|\mathbf{s}_A \oplus \mathbf{s}_B \oplus \mathbf{z}_0\rangle_B$ and the three least significant bits represent Alice's measurement or $|\mathbf{z}_0\rangle_A$. Thus, for this specific example, if Bob announces his initial key $\mathbf{s}_B = 110$ to Alice, and Alice performs a XOR operation upon her measurement with Bob's initial key and her own initial key $\mathbf{s}_A = 101$, then Alice will obtain Bob's final measurement, which is the secret key.

4.2. Example for the sSEBV Protocol

In this example too, the entangled EPR pairs are created by the circuit itself. In the initial stage of the corresponding circuits Hadamard and CNOT gates are used to populate Alice's and Bob's input registers with entangled EPR pairs, as explained in Section 2. Moreover, it is assumed that $\mathbf{s}_A = 101$ and $\mathbf{s}_B = 000$. The resulting circuit in displayed in Figure 6.

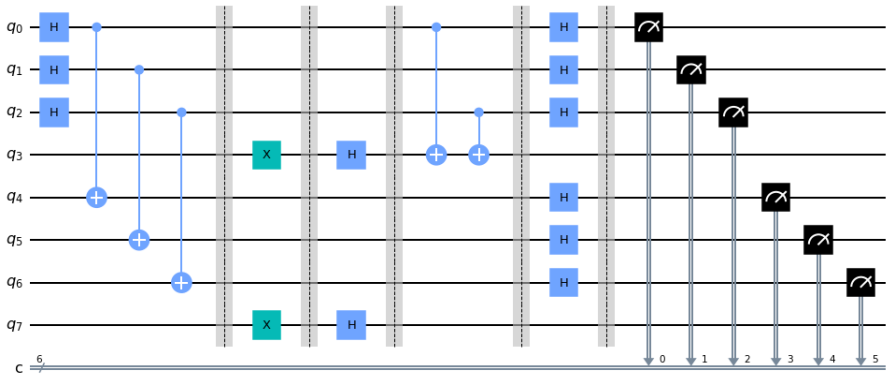

Figure 6. The circuit for the sSEBV protocol.

This time the final measurement by Alice and Bob will produce one of the 8 outcomes shown in Figure 7 along with their corresponding probabilities as given by running the qasm simulator for 2048 shots. As noted in the previous case, it suffices to inspect the possible outcomes in order to confirm Equation (45). Now the correct interpretation of the outcomes means viewing them either as $|\mathbf{z}_0\rangle_A |\mathbf{s}_A \oplus \mathbf{z}_0\rangle_B$ or as $|\mathbf{s}_A \oplus \mathbf{w}_0\rangle_A |\mathbf{w}_0\rangle_B$, for some, generally different, $\mathbf{z}_0, \mathbf{w}_0 \in \{0,1\}^n$. Hence, Alice, after making her final measurement and finding a random binary string $\mathbf{z}_0$, she just needs to send $\mathbf{z}_0$ to Bob. Then Bob will be able to derive Alice's chosen secret key $\mathbf{s}_A = 101$.

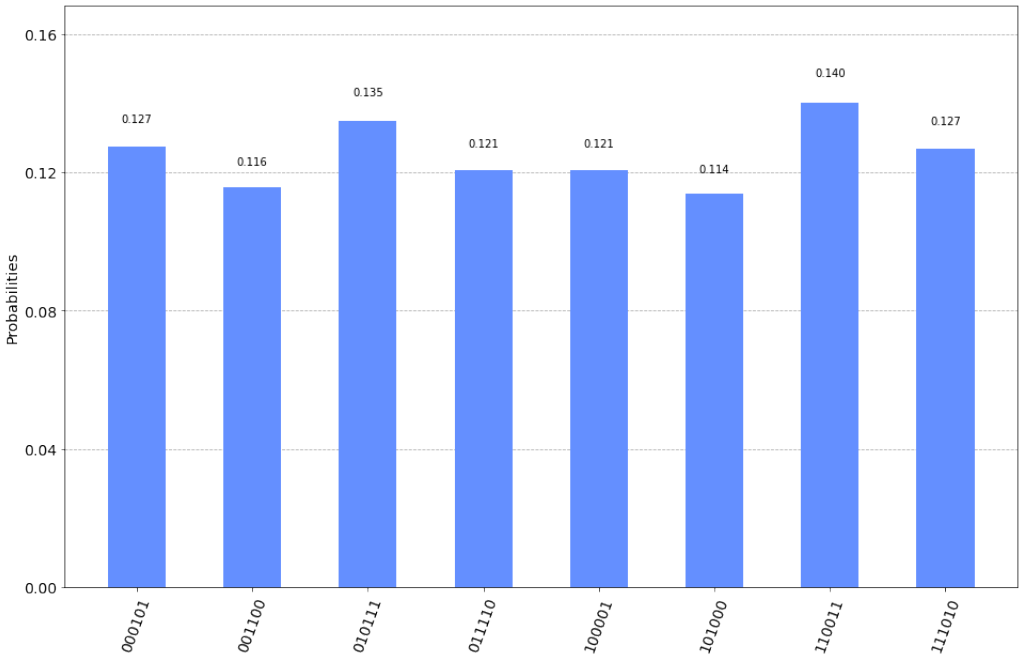

Figure 7. The possible outcomes of the measurement and their corresponding probabilities for the circuit in Figure 6.

Again, all of the eight possible outcomes are shown along with the probability of measuring each one of them, as computed by the qasm simulator. The measurements shown in Figure 7 depict both Alice's and Bob's input registers as $|q_6 q_5 q_4 q_2 q_1 q_0\rangle$, that is the three most significant bits represent Bob's measurement or $|\mathbf{s}_A \oplus \mathbf{z}_0\rangle_B$ and the three least significant bits represent Alice's measurement or $|\mathbf{z}_0\rangle_A$. In this specific example, if Alice announces her measurement $|\mathbf{z}_0\rangle_A$ to Bob, and Bob performs a XOR operation upon his measurement, with Alice's measurement, then Bob will obtain the secret key $\mathbf{s}_A = 101$ chosen by Alice.

5. Discussion and Conclusions

QKD protocols have surely proved by now that they are the future of key distribution. Their advantage stems from the fact that they allow us to harness the power of quantum-mechanics and nature's own laws, without having to rely on the complexity of certain mathematical problems. In this paper, we tried to further expand the field of quantum cryptography, by proposing a novel use for the Bernstein-Vazirani algorithm as a symmetrical entanglement-based QKD protocol, coming in two flavors.

These two flavors differ on the degree of symmetry employed by the protocol. In the fully symmetric variant, Alice and Bob take completely identical actions. This variant has the ability to create a totally new and original key, a key that both Alice and Bob were initially oblivious of. This can be useful in many situations as it ensures an additional advantage security wise. Furthermore, it provides a degree of fairness, by putting both parties on an equal footing, in the sense that neither Alice nor Bob can solely determine the secret key.

On the other hand, the semi-symmetric variant, which can technically be viewed as a special case of the first protocol, deviates from this symmetry. In effect, the semi-symmetric protocol answers the question of what will happen if one of the two players wants to specify the secret key. In the presentation given in Section 3 it was Alice that chose the secret key, but it is trivial to adjust the protocol so that Bob can be the party to decide the secret key. This protocol can be useful in situations where a specific key must be chosen by either Alice or Bob, and this key must be securely transmitted to the other party.

Additionally, we demonstrated two small scale but comprehensive examples, illustrating the operation of the two protocols in practice. Finally, we explained the protocols strength against an eavesdropping attack by Eve. Both variants exhibit the inherent robustness of entanglement-based protocols against Eve's attacks, as originally described by Ekert. Moreover, the use of extra inputs in order to acquire the final secret key, adds another layer of security.

In closing, we remark that we also believe that the rest of the old quantum algorithms, such as the Deutsch-Jozsa algorithm and Simon's periodicity algorithm, can all be implemented as a symmetrical entanglement-based QKD protocols, posing a viable suggestion for future work, along with the performance of these proposals against different quantum attacks.

Author Contributions: Conceptualization, T.A. and M.A.; methodology, T.A.; validation, M.A.; formal analysis, T.A.; investigation, M.A.; writing original draft preparation, M.A. and T.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
2. Grover, L. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; [CrossRef]
3. Chen, L.; Chen, L.; Jordan, S.; Liu, Y.K.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D. *Report on POST-Quantum Cryptography*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016; Volume 12.
4. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
5. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
6. Bennett, C.H.; Brassard, G. Experimental quantum cryptography: The dawn of a new era for quantum cryptography: the experimental prototype is working. *ACM Sigact News* **1989**, *20*, 78–80. [CrossRef]
7. Elliott, C.; Colvin, A.; Pearson, D.; Pikalo, O.; Schlafer, J.; Yeh, H. Current status of the DARPA quantum network. In *Quantum Information and Computation III*; International Society for Optics and Photonics: Bellingham, Washington, USA, 2005; Volume 5815, pp. 138–149.
8. Elliott, C. The DARPA quantum network. In *Quantum Communications and Cryptography*; CRC Press: Boca Raton, FL, USA, 2018; pp. 91–110.
9. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes, J.; et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **2009**, *11*, 075001. [CrossRef]
10. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409. [CrossRef] [PubMed]
11. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef] [PubMed]
12. Deutsch, D.; Jozsa, R. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. Ser. A Math. Phys. Sci.* **1992**, *439*, 553–558. [CrossRef]
13. Bernstein, E.; Vazirani, U. Quantum Complexity Theory. *SIAM J. Comput.* **1997**, *26*, 1411–1473. [CrossRef]
14. Simon, D.R. On the Power of Quantum Computation. *SIAM J. Comput.* **1997**, *26*, 1474–1483. [CrossRef]

15. Nagata, K.; Nakamura, T.; Farouk, A. Quantum Cryptography Based on the Deutsch-Jozsa Algorithm. *Int. J. Theor. Phys.* **2017**, *56*, 2887–2897. [CrossRef]
16. Nagata, K.; Nakamura, T. Quantum Cryptography, Quantum Communication, and Quantum Computer in a Noisy Environment. *Int. J. Theor. Phys.* **2017**, *56*, 2086–2100. [CrossRef]
17. Nagata, K.; Nakamura, T.; Geurdes, H.; Batle, J.; Abdalla, S.; Farouk, A. Secure quantum key distribution based on a special Deutsch-Jozsa algorithm. *Asian J. Math. Phys.* **2017**, *2*, 6–13.
18. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
19. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
20. Aharon, N.; Silman, J. Quantum dice rolling: A multi-outcome generalization of quantum coin flipping. *New J. Phys.* **2010**, *12*, 033027. [CrossRef]
21. Meyer, D.A. Quantum strategies. *Phys. Rev. Lett.* **1999**, *82*, 1052. [CrossRef]
22. Eisert, J.; Wilkens, M.; Lewenstein, M. Quantum games and quantum strategies. *Phys. Rev. Lett.* **1999**, *83*, 3077. [CrossRef]
23. Andronikos, T.; Sirokofskich, A.; Kastampolidou, K.; Varvouzou, M.; Giannakis, K.; Singh, A. Finite Automata Capturing Winning Sequences for All Possible Variants of the PQ Penny Flip Game. *Mathematics* **2018**, *6*, 20. [CrossRef]
24. Andronikos, T.; Sirokofskich, A. The Connection between the PQ Penny Flip Game and the Dihedral Groups. *Mathematics* **2021**, *9*, 1115. [CrossRef]
25. Giannakis, K.; Theocharopoulou, G.; Papalitsas, C.; Fanarioti, S.; Andronikos, T. Quantum Conditional Strategies and Automata for Prisoners' Dilemmata under the EWL Scheme. *Appl. Sci.* **2019**, *9*, 2635. [CrossRef]
26. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2010.
27. Mermin, N. *Quantum Computer Science: An Introduction*; Cambridge University Press: Cambridge, UK, 2007.10.1017/cbo9780511813870. [CrossRef]
28. Qiskit. Qiskit Open-Source Quantum Development. Available online: https://qiskit.org (accessed on 5 June 2021).
29. Qasm. The Qasm Simulator. Available online: https://qiskit.org/documentation/stubs/qiskit.providers.aer.QasmSimulator.html (accessed on 3 July 2021).