electronics

MDPI

Article

An Entanglement-Based Protocol for Simultaneous Reciprocal Information Exchange between 2 Players

Theodore Andronikos [1,*,†] and Alla Sirokofskich [2,†]

[1] Department of Informatics, Ionian University, 7 Tsirigoti Square, 49100 Corfu, Greece
[2] Department of History and Philosophy of Sciences, National and Kapodistrian University of Athens, 15771 Athens, Greece; asirokof@math.uoa.gr
* Correspondence: andronikos@ionio.gr
† These authors contributed equally to this work.

Abstract: Let us consider a situation where two information brokers, whose currency is, of course, information, need to reciprocally exchange information. The two brokers, being somewhat distrustful, would like a third, mutually trusted entity to be involved in the exchange process so as to guarantee the successful completion of the transaction and also verify that it indeed took place. Can this be completed in such a way that both brokers receive their information simultaneously and securely, without the trusted intermediary knowing the exchanged information? This work presents and rigorously analyzes a new quantum entanglement-based protocol that provides a solution to the above problem. The proposed protocol is aptly named the entanglement-based reciprocal simultaneous information exchange protocol. Its security is ultimately based on the assumption of the existence of a third, trusted party. Although the reciprocal information flow is between our two information brokers, the third entity plays a crucial role in mediating this process by being a guarantor and a verifier. The phenomenon of quantum entanglement is the cornerstone of this protocol, as it makes its implementation possible even when all entities are spatially separated and ensures that, upon completion, the trusted third party remains oblivious to the actual information that was exchanged.

Keywords: quantum cryptography; quantum entanglement; bell states; GHZ states; secure information exchange

Citation: Andronikos, T.; Sirokofskich, A. An Entanglement-Based Protocol for Simultaneous Reciprocal Information Exchange between 2 Players. *Electronics* **2023**, *12*, 2506. https://doi.org/10.3390/electronics12112506

Academic Editors: Tuan-Vinh Le and Cheng-Chi Lee

Received: 18 April 2023
Revised: 29 May 2023
Accepted: 31 May 2023
Published: 1 June 2023

1. Introduction

Living in an era where privacy and security are fundamental and inherent rights in everyone's professional and social lives has undoubtedly motivated an enormous research effort to design and implement robust security algorithms, techniques, and protocols. It would seem that there are at least two major research directions aspiring to achieve this goal.

The first, known by the umbrella term post-quantum cryptography [1–4], could be perceived as the natural evolution of our present situation, where security relies on carefully chosen computationally hard problems. The efficiency and reliability of this approach have been practically confirmed thus far, and it offers the additional advantage that, implementation-wise, it is compatible with the existing infrastructure.

There is, however, reason for concern, as the computational difficulty of the underlying problems has not actually been mathematically proven but is rather empirically accepted because of the absence of efficient algorithms. Probably even more worrying is the fact that, upon stepping out of the confines of conventional, or classical, computation, one discovers that quantum algorithms have been developed by Peter Shor and Lov Grover [5,6], which may compromise the security afforded by conventional means. Thus, the emergence of the second direction, quantum cryptography, advocates the embrace of the unconventional, in particular the quantum realm, and relies on the laws of nature, at least as we understand them today, to achieve uncompromising security.

On the quantum front, there are many reasons to be optimistic lately, with clear signs of accelerated progress. The impressive breakthrough of the 100-qubit barrier by IBM's 127-qubit processor Eagle [7] has been followed almost immediately, by the more recent 433 qubit quantum processor named Osprey [8]. Therefore, it is now more important than ever before to address the problem of secure communication [9], and quantum cryptography seems the most promising approach for the job. Clever use of the fundamental properties of quantum mechanics offers undisputed advantages in that they not only guarantee the adequate protection of critical information, but also ensure the efficient and secure transmission of information, e.g., via the use of entanglement, as first suggested by Ekert [10]. In his 1991 influential paper, Ekert proved that key distribution is possible with the use of EPR pairs. Immediately afterwards, research in this field produced a plethora of entanglement-based protocols for quantum key distribution [11–17]. Quantum cryptographic protocols have the potential to enhance the security not only of established applications but also of new and emerging technologies, such as cloud computing, cloud storage [18,19], or blockchain [20]. Considerable progress has been recorded in the development of algorithms and protocols [21–26], accompanied by experimental demonstrations in real-life situations [27–30].

This work studies the ubiquitous problem of information exchange between two parties within the broader context of quantum information and cryptography. We envision a setting where the real currency is information, and in such a setting, two information brokers want to reciprocally exchange information. In their profession, trust cannot be taken for granted. Hence, they would like a third party that is mutually trusted by both to mediate the whole process and guarantee the honest implementation of the agreed upon protocol. This third party must have a pivotal role, in the sense that without its participation, it will be impossible to complete the exchange. Another important benefit of the presence of the trusted intermediary is that it can serve as a referee to verify that this transaction took place if such a need arises in the future, e.g., if one or both of the information brokers ever need such a "proof." This scheme should work even when all parties involved are spatially separated and, most importantly, be designed so carefully that the trusted intermediary does not end up in possession of the exchanged information.

The problem of information exchange has been studied in numerous works, especially from the point of view of classical, that is, non-quantum, protocols and algorithms. A recent work, which, similar to the present paper, deals with distributed environments and systems, is ref. [31], where the interested reader can find an extensive list of references. Therein, a comprehensive analysis of privacy and security issues for classical distributed systems in the presence of an adversary is given, along with algorithmic solutions to alleviate the risks. Another related line of research, dealing with quantum computation under strict requirements for privacy and security, was pursued in [32]. The authors in [32] presented a sophisticated protocol that achieves universal blind quantum computation by enabling the client player to complete privately and securely the required quantum computation, even when the server player cheats.

In the rest of this paper, we present, in the form of a game, a quantum protocol that provides a solution to this problem, satisfying all the previously set requirements. It is almost some kind of tradition to use games in quantum cryptography, from the very beginning [33] to the more recent [16,17]. The pedagogical aspect of games often makes expositions of difficult and technical concepts much more accessible, even entertaining. Quantum games, ever since their initial inception in 1999 [34,35], have offered motivation and additional insight because quite often quantum strategies seem to achieve better results than classical ones [36–38]. The famous prisoners' dilemma game provides the most prominent example [35,39], which also applies to other abstract quantum games [40]. The quantization of many classical systems can even apply to political structures, as was shown in [41].

To motivate the forthcoming presentation of the protocol, we give a real-life example where the ability to have such an efficient and secure three-party information exchange protocol, complying with the specifications previously outlined, is beneficial or even necessary.

Example 1 (The undercover agents)**.** *This example should be seen as a proof of concept for more intricate real-life situations. Let us suppose that Bob and Charlie are two undercover agents working for a law enforcement agency. Information is critical for the success of their mission. Bob is desperately in need of some piece of information that knows Charlie has. He also knows that in their line of work the only real currency is information. So, he is ready to offer Charlie another piece of information that he believes will prove useful to Charlie. Bob and Charlie are not friends, just colleagues, and they do not fully trust each other, but they both trust their boss, Alice. Alice would be the ideal intermediary because she trusted by both agents, so she should be involved in the process of information exchange. Moreover, based on her involvement, Alice would be able to remember this secret transaction and vouch for her agents in case one, or both, of them would need in the future to prove that this particular information exchange took place, e.g., if their missions failed. At the end of the exchange process, Alice, should not have become aware of the contents of the information that was exchanged because both agents want to protect their informants. Finally, Alice stays at the headquarters, whereas Bob and Charlie work undercover in different parts of town, so it would be safer and more prudent if they did not meet in person at all. How can they complete this task?* ◁

Contribution. This paper presents a quantum protocol that efficiently and securely solves the problem of reciprocal information exchange between two information brokers. Being quantum, the proposed protocol is information-theoretically secure because it is based on the laws of quantum mechanics, at least as we understand them today. In contrast, an analogous classical protocol can only offer security based on conjectured computationally hard problems, with the potential risks that it may entail.

Its novelty lies in the integral use of entanglement. Entanglement, one of the exclusive hallmarks of the quantum world, offers multiple benefits in this setting. It enables the two players to embed their secret information simultaneously and stealthily in the state of the composite system. Upon completion of the quantum part of the protocol, the combined secret information will be encoded in the correlated contents of the quantum registers, but it will only be revealed after the proper classical information is exchanged. Moreover, entanglement enhances the security of the protocol, as shown in Section 4, and, at the same time, provides for the spatially distributed execution of the protocol. Despite the fact that the three players are situated in different geographical locations and apply their local quantum circuits, the correlations due to entanglement ensure that we are still dealing with one composite system.

Finally, the inclusion of a third party to supervise and facilitate the exchange process can be beneficial. There are many practical situations, as briefly sketched in the preceding example, where the presence of an intermediary would be required. The most important observation here is that a trusted intermediary does not compromise the security of the protocol in any way. Particularly so, after taking into account that upon the completion of the protocol, the third party remains oblivious to the actual information that was exchanged between the two players, i.e., there is no information leak whatsoever. We note that, as briefly sketched in Section 5, it is possible to modify the protocol so as to enable the exchange of information without the presence of a trusted intermediary.

Organization

The structure of this paper is the following. Section 1 contains an introduction to the subject and related references. Section 2 gives a succinct reminder on entangled GHZ states. Section 3 provides a formal and detailed exposition of the quantum protocol. Section 4 is devoted to the security and efficiency analysis of the protocol, and, finally, Section 5 contains a summary and a brief discussion on some of the finer points of this protocol.

2. Preliminaries

Many quantum protocols can be described as games between well-known fictional players, commonly referred to as Alice, Bob, Charlie, who, while being spatially separated, are attempting to send and/or receive information securely. Typically, secure communication can be established via a combination of classical pairwise authenticated channels and pairwise quantum channels. Usually, the process of transmitting secret information takes place through the quantum channel using a multitude of different techniques, and, subsequently, in order to complete the process, a message is exchanged through a classical public channel. During this phase, an adversary, mostly referred to as Eve, may appear and attempt to track this communication and steal any information possible. In such an eventuality, the major advantage of quantum cryptography over its classical counterpart is that during the transmission of information through the quantum channel, the communicating players are protected due to certain fundamental principles of quantum mechanics, such as the no-cloning theorem [42], entanglement monogamy, etc.

Entanglement constitutes the fundamental basis of most quantum protocols, including the one proposed in this work, and possibly the de facto future of quantum cryptography due to its numerous applications in the entire field. It 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. The entanglement of three or more qubits is referred to as a GHZ state. The fundamental idea of quantum entanglement in its simplest form is that it is possible for quantum particles to be entangled together, and when a property is measured in one particle, it can be observed in the other particles instantaneously.

Contemporary quantum computers based on the circuit model can readily produce general states involving n entangled qubits, which are denoted by $|GHZ_n\rangle$. Implementing such a circuit requires n qubits, one Hadamard gate that is applied to the first qubit, and $n-1$ CNOT gates. We refer the interested reader to [43] for a practical methodology that can be utilized to construct efficient GHZ circuits, in the sense that it just takes $\lg n$ steps to produce the $|GHZ_n\rangle$ state. For the proposed protocol, $|GHZ_3\rangle$ triplets suffice. A typical circuit capable of generating the $|GHZ_3\rangle$ state is given in Figure 1. The circuit was designed using the IBM Quantum Composer [44]. The dotted lines are not part of the circuit; they just serve to provide a visual aid in order to distinguish "time slices". Figure 2, also taken from the IBM Quantum Composer, depicts the state vector description of the $|GHZ_3\rangle$ state.

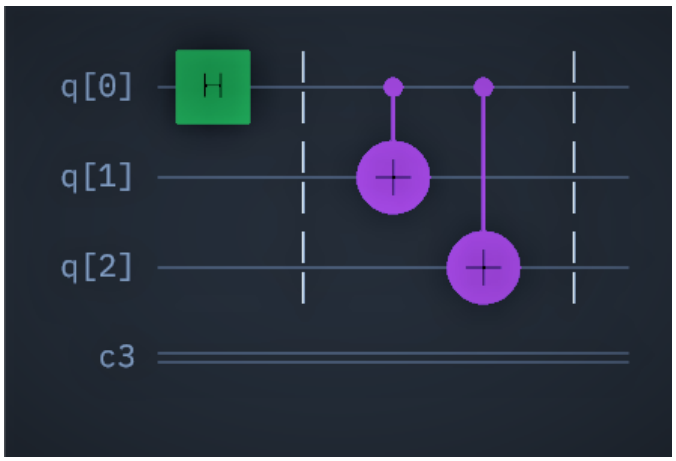

Figure 1. The above quantum circuit can entangle 3 qubits in the $|GHZ_3\rangle = \frac{|0\rangle|0\rangle|0\rangle+|1\rangle|1\rangle|1\rangle}{\sqrt{2}}$ state. Any $|GHZ_n\rangle$ state can be produced in an analogous manner.

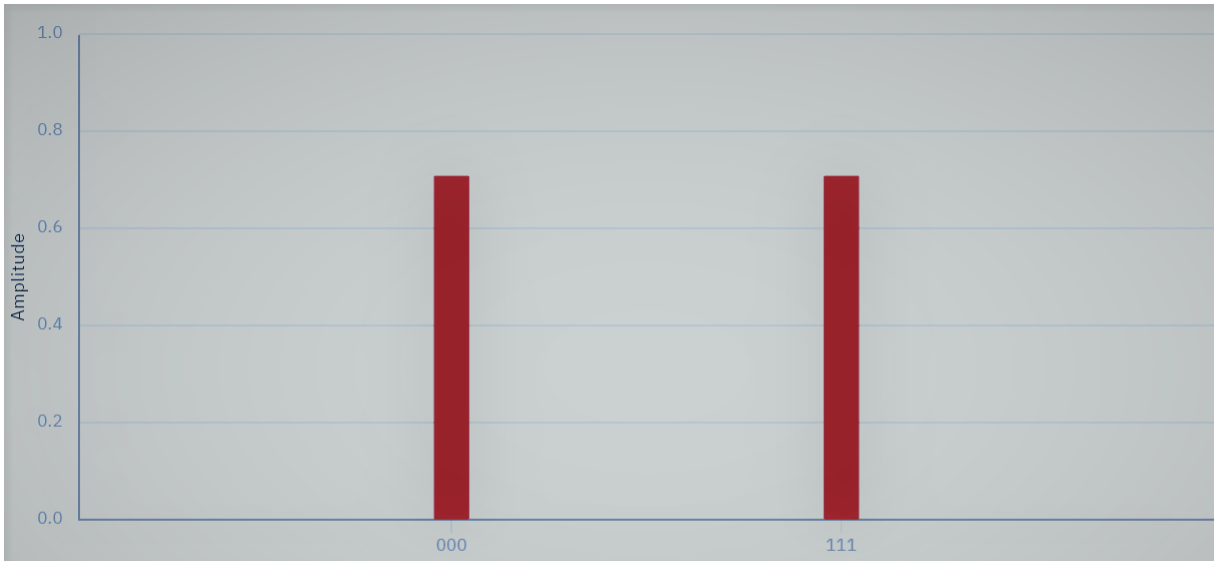

Figure 2. The above figure depicts the state vector description of the $|GHZ_3\rangle$ state.

The mathematical description of the $|GHZ_3\rangle$ state is given below.

$$|GHZ_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B|0\rangle_C + |1\rangle_A|1\rangle_B|1\rangle_C)\,. \tag{1}$$

Our protocol requires not just a single $|GHZ_3\rangle$ triplet, but n such triplets. The state of a composite system comprised of n $|GHZ_3\rangle$ triplets is given by the next formula (for details, refer to [17,45]).

$$|GHZ_3\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle_A|\mathbf{x}\rangle_B|\mathbf{x}\rangle_C\,. \tag{2}$$

In the above equation, $\mathbf{x} \in \{0,1\}^n$ ranges through all the 2^n basis kets, $|\mathbf{x}\rangle_A$, $|\mathbf{x}\rangle_B$, and $|\mathbf{x}\rangle_C$ correspond to the contents of Alice, Bob, and Charlie's input registers, respectively.

3. The Protocol for Simultaneous Reciprocal Information Exchange between 2 Players

In this section, we present the entanglement-based protocol for simultaneous reciprocal information exchange between two players, or ESR for short. The ESR protocol is designed so as to enable two players, named Bob, and Charlie, who are perceived as information brokers, to exchange information simultaneously and reciprocally. The process is mediated by Alice, who plays the mutually trusted intermediary. All three of our protagonists are assumed to be spatially separated. The main idea is to achieve this task by using an appropriate number (which we denote by n) of maximally entangled $|GHZ_3\rangle$ triplets. These are created by Alice, trusted by both Bob and Charlie, who evenly distributes all triplets among herself, Bob, and Charlie using two corresponding pairwise quantum channels. This results in each player having precisely one qubit in every triplet. Alice's role is crucial not only to the successful completion of the protocol but also as a possible witness to the fact that the information exchange really took place. It is very important to point out that, despite being an integral part of the exchange, Alice does not end up knowing anything.

To give a simplified overview of the ESR protocol, we first present the block diagram in Figure 3 that depicts the specific operations that are performed during the execution of the protocol. The protocol can be conceptually divided into two parts: a quantum and a classical part, taking place through the quantum and public classical channels, respectively. In each of the two parts, the specified actions are executed, as analyzed in the current section.

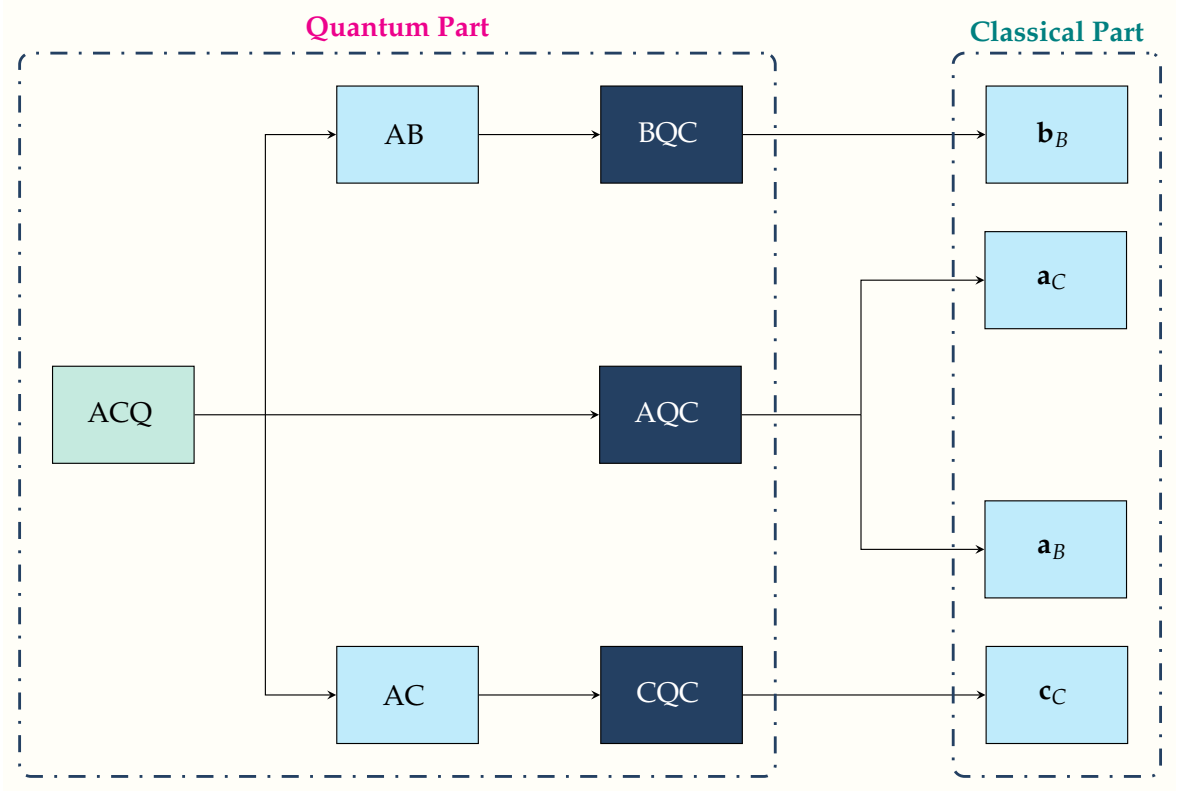

Figure 3. This figure gives the block diagram of the ESR protocol divided in a quantum and a classical part. The abbreviations for the operations taking place in each part are explained in Table 1.

Table 1 below contains the notations and abbreviations that appear in Figure 3.

Table 1. This table contains the notations and abbreviations shown in the block diagram of Figure 3.

Notations and Abbreviations	
Symbolism	Operation
ACQ	Alice creates n triplets of qubits in the $\|GHZ_3\rangle$ state
AB	Alice sends to Bob one qubit from each triplet through the quantum channel
AC	Alice sends to Charlie one qubit from each triplet via the quantum channel
BQC	Bob applies his quantum circuit and measures his input register
AQC	Alice applies her quantum circuit and measures her input register
CQC	Charlie applies his quantum circuit and measures his input register
$\mathbf{b}_B$	Bob sends to Charlie the bit vector $\mathbf{b}_B$
$\mathbf{a}_C$	Alice sends to Bob the bit vector $\mathbf{a}_C$
$\mathbf{a}_B$	Alice sends to Charlie the bit vector $\mathbf{a}_B$
$\mathbf{c}_C$	Charlie sends to Bob the bit vector $\mathbf{c}_C$

3.1. The Quantum Part of the Protocol

The game effectively begins after Alice, Bob and Charlie have populated their input registers, denoted by AIR, BIR, and CIR, respectively, with their n qubits. The whole setting is depicted in Figure 4. The protocol itself can be implemented with the distributed quantum circuit of Figure 5. Although this circuit is distributed, since the players' local circuits are spatially separated, it is in fact one composite system because their input registers are strongly correlated due to the presence of entanglement. The notation employed in the circuit of Figure 5 is explained in Table 2.

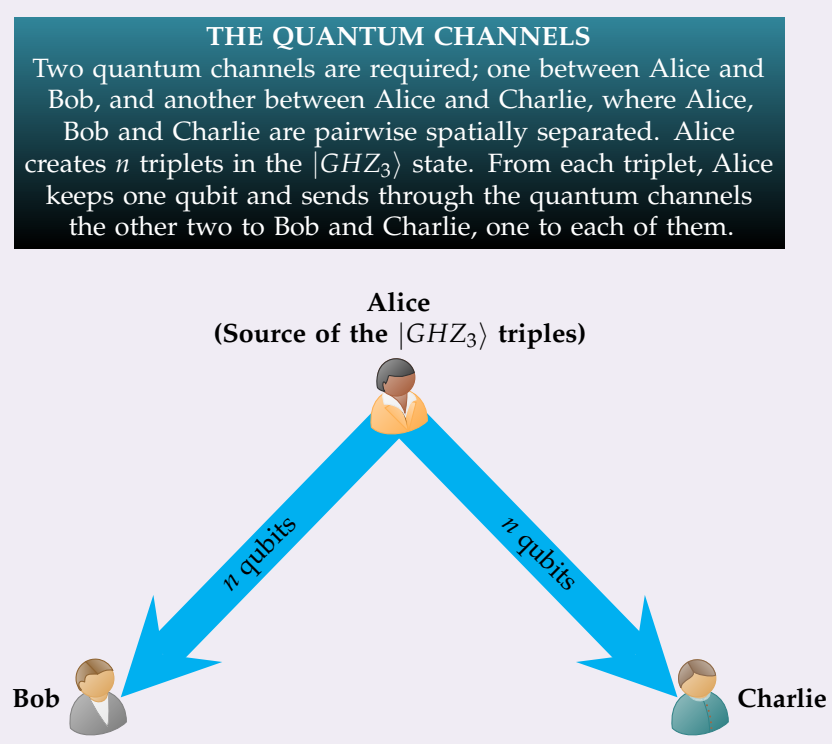

Figure 4. This figure shows Alice, Bob and Charlie, who are spatially separated, and the two quantum channels, one between Alice and Bob and the other between Alice and Charlie. Alice produces n triplets of photons entangled in the $|GHZ_3\rangle$ state. From each triplet Alice keeps one for herself, sends the second to Bob, and the third to Charlie through the corresponding quantum channels.

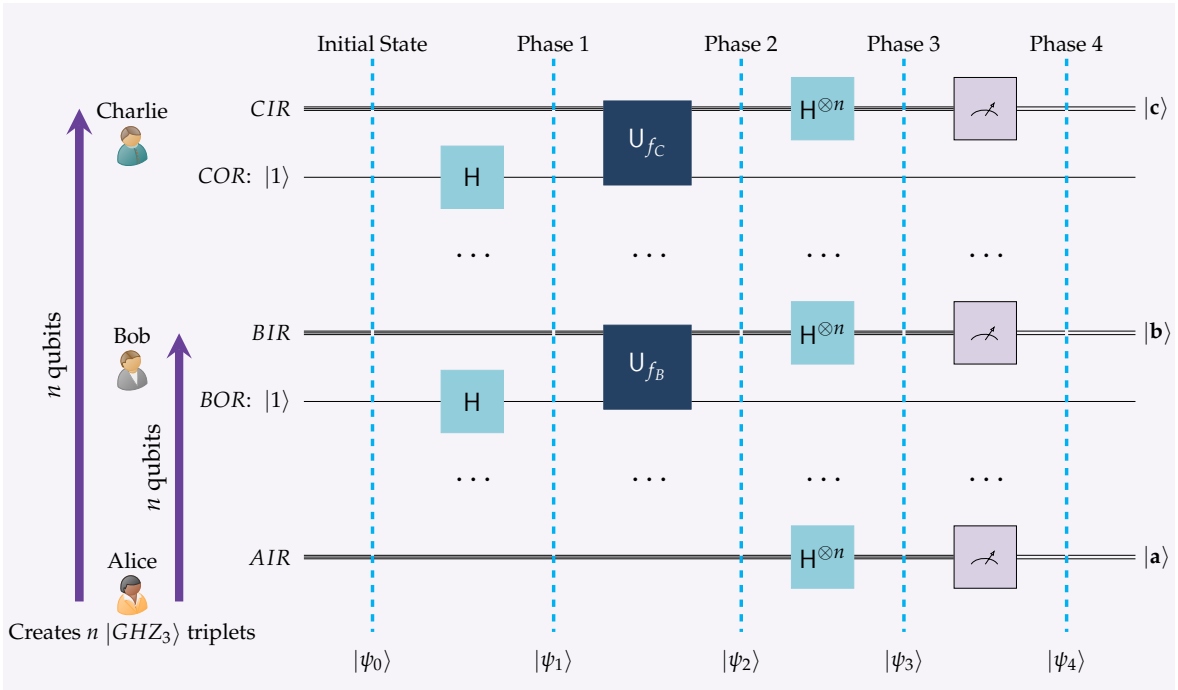

Figure 5. This figure is an abstract visualization of the quantum circuits employed by Alice, Bob and Charlie. Although they are spatially separated, they are correlated, due to the phenomenon of entanglement. Thus, they form a composite system, whose temporal evolution is given by the state vectors $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$ and $|\psi_4\rangle$.

Table 2. This table contains the notations and abbreviations that are used in Figure 5.

Notations and Abbreviations	
Symbolism	Explanation
n	The number of qubits in each input register
AIR	Alice's n-qubit Input Register
BIR	Bob's n-qubit Input Register
BOR	Bob's single qubit Output Register
CIR	Charlie's n-qubit Input Register
COR	Charlie's single qubit Output Register

The rigorous mathematical analysis of the ESR information exchange protocol invokes a couple of standard relations from the literature, typically found in most textbooks, such as refs. [46,47]):

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle\,, \quad \text{and} \tag{3}$$

$$H^{\otimes n}|\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{z}\in\{0,1\}^n} (-1)^{\mathbf{z}\cdot\mathbf{x}}|\mathbf{z}\rangle\,. \tag{4}$$

In Equation (4), we have adhered to the typical convention of writing the contents of quantum registers in boldface, e.g., $|\mathbf{x}\rangle = |x_{n-1}\rangle \ldots |x_0\rangle$, for some $n \geq 1$. Moreover, the notation $\mathbf{z}\cdot\mathbf{x}$ stands for the inner product modulo 2, which, assuming that $|\mathbf{z}\rangle = |z_{n-1}\rangle \ldots |z_0\rangle$, is defined as

$$\mathbf{z}\cdot\mathbf{x} = z_{n-1}x_{n-1} \oplus \cdots \oplus z_0 x_0\,. \tag{5}$$

Let us assume that $\mathbf{i}_B$ is the bit vector that represents the information that Bob possesses and intends to exchange with Charlie and, symmetrically, that $\mathbf{i}_C$ is the bit vector corresponding to the information that Charlie possesses and intends to exchange with Bob. We define the *auxiliary information bit vectors* $\widetilde{\mathbf{i}_B}$ and $\widetilde{\mathbf{i}_C}$ as follows, where the notation $|\cdot|$ denotes the length, i.e., number of bits, of the enclosed bit vector:

$$\widetilde{\mathbf{i}_B} = \mathbf{i}_B \underbrace{0 \cdots 0}_{|\mathbf{i}_C| \text{ times}}\,, \quad \text{and} \tag{6}$$

$$\widetilde{\mathbf{i}_C} = \underbrace{0 \cdots 0}_{|\mathbf{i}_B| \text{ times}} \mathbf{i}_C\,. \tag{7}$$

We define the *aggregated information bit vector* $\mathbf{i}$ as the concatenation of $\mathbf{i}_B$ and $\mathbf{i}_C$:

$$\mathbf{i} = \mathbf{i}_B\, \mathbf{i}_C\,, \tag{8}$$

and we set

$$n = |\mathbf{i}| = |\widetilde{\mathbf{i}_B}| = |\widetilde{\mathbf{i}_C}| = |\mathbf{i}_B| + |\mathbf{i}_C|\,. \tag{9}$$

We use the boldface $\mathbf{0}$ to abbreviate the zero-bit vector of length n. Of course, we assume that n is common knowledge among all three players. In effect, this can be easily achieved if Bob and Charlie share though the public channel the lengths $|\mathbf{i}_B|$ and $|\mathbf{i}_C|$ of their respective information bit vectors. This poses no danger whatsoever, as sharing the length does not reveal the contents of the secret information. The preceding discussion also implies that

$$\mathbf{i} = \widetilde{\mathbf{i}_B} \oplus \widetilde{\mathbf{i}_C} \,. \tag{10}$$

The next Figure 6 is intended to clarify pictorially the formation of the aggregated information bit vector $\mathbf{i}$ from Bob and Charlie's information bit vectors $\mathbf{i}_B$ and $\mathbf{i}_C$, via the use of the auxiliary information bit vectors $\widetilde{\mathbf{i}_B}$ and $\widetilde{\mathbf{i}_C}$.

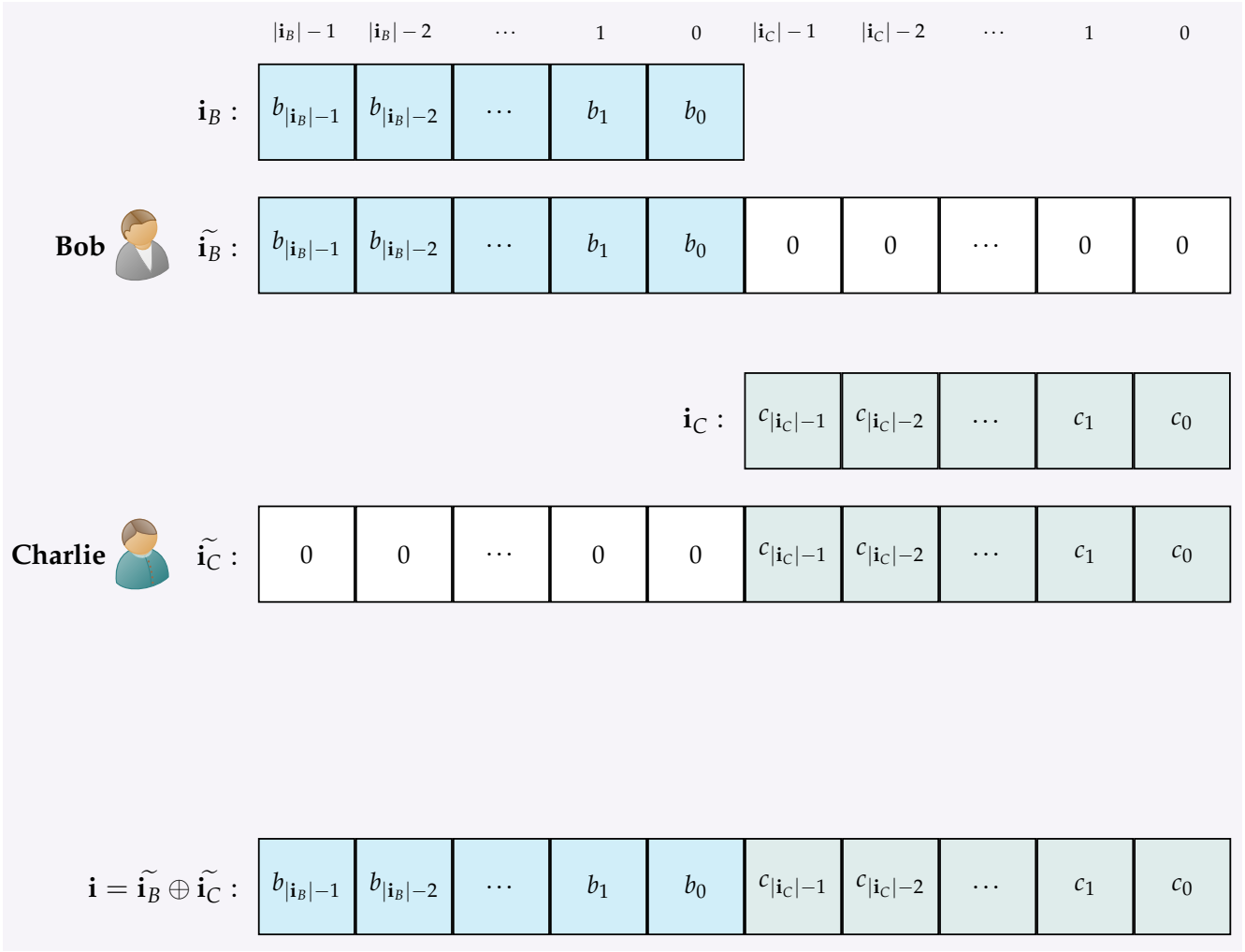

Figure 6. This figure gives a pictorial representation of Bob and Charlie's information bit vectors $\mathbf{i}_B$ and $\mathbf{i}_C$, the resulting auxiliary information bit vectors $\widetilde{\mathbf{i}_B}$ and $\widetilde{\mathbf{i}_C}$, and the aggregated information bit vector $\mathbf{i}$.

The initial state of the circuit of Figure 5 is denoted by $|\psi_0\rangle$. In view of (2), $|\psi_0\rangle$ is given by

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle_A |1\rangle_B |\mathbf{x}\rangle_B |1\rangle_C |\mathbf{x}\rangle_C \,. \tag{11}$$

As is the trend nowadays, we stick to the Qiskit [48] way of ordering the qubits, in which the most significant is the bottom qubit and the least significant is the top. Furthermore, we rely on the subscripts A, B, and C in order to designate Alice, Bob, and Charlie's registers, respectively.

At the end of the first phase, Bob and Charlie have applied the Hadamard transform to their output registers, and the resulting state has become $|\psi_1\rangle$:

$$|\psi_1\rangle \overset{(3)}{=} \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle_A |-\rangle_B |\mathbf{x}\rangle_B |-\rangle_C |\mathbf{x}\rangle_C \,. \tag{12}$$

It is during the second phase that Bob and Charlie simultaneously encode the information they intend to exchange within the state of the quantum circuit. They do so by acting with their unitary transforms U_{f_B} and U_{f_C} on both their output and input registers. The unitary transforms U_{f_A} and U_{f_B} are constructed using the functions $f_B(\mathbf{x})$ and $f_C(\mathbf{x})$, respectively, according to the usual scheme

$$U_{f_B} : |y\rangle_B |\mathbf{x}\rangle_B \to |y \oplus f_B(\mathbf{x})\rangle_B |\mathbf{x}\rangle_B \,, \quad \text{and} \tag{13}$$

$$U_{f_C} : |y\rangle_C |\mathbf{x}\rangle_C \to |y \oplus f_C(\mathbf{x})\rangle_C |\mathbf{x}\rangle_C \,. \tag{14}$$

The functions $f_B(\mathbf{x})$ and $f_C(\mathbf{x})$ are quite straightforward, relying on Bob and Charlie's auxiliary information bit vectors $\widetilde{\mathbf{i}_B}$ and $\widetilde{\mathbf{i}_C}$, respectively, according to the formulas (15) and (16) presented below.

$$f_B(\mathbf{x}) = \widetilde{\mathbf{i}_B} \cdot \mathbf{x} \,, \quad \text{and} \tag{15}$$

$$f_C(\mathbf{x}) = \widetilde{\mathbf{i}_C} \cdot \mathbf{x} \,. \tag{16}$$

Therefore, (13) and (14) can be explicitly written as

$$U_{f_B} : |-\rangle_B |\mathbf{x}\rangle_B \to (-1)^{\widetilde{\mathbf{i}_B}\cdot\mathbf{x}} |-\rangle_B |\mathbf{x}\rangle_B \,, \quad \text{and} \tag{17}$$

$$U_{f_C} : |-\rangle_C |\mathbf{x}\rangle_C \to (-1)^{\widetilde{\mathbf{i}_C}\cdot\mathbf{x}} |-\rangle_C |\mathbf{x}\rangle_C \,. \tag{18}$$

In view of the above calculations, at the end of the second phase the state of the quantum circuit has become $|\psi_2\rangle$:

$$\begin{aligned} |\psi_2\rangle &= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle_A (-1)^{\widetilde{\mathbf{i}_B}\cdot\mathbf{x}} |-\rangle_B |\mathbf{x}\rangle_B (-1)^{\widetilde{\mathbf{i}_C}\cdot\mathbf{x}} |-\rangle_C |\mathbf{x}\rangle_C \\ &= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\widetilde{\mathbf{i}_B}\oplus\widetilde{\mathbf{i}_C})\cdot\mathbf{x}} |\mathbf{x}\rangle_A |-\rangle_B |\mathbf{x}\rangle_B |-\rangle_C |\mathbf{x}\rangle_C \\ &\overset{(10)}{=} \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{\mathbf{i}\cdot\mathbf{x}} |\mathbf{x}\rangle_A |-\rangle_B |\mathbf{x}\rangle_B |-\rangle_C |\mathbf{x}\rangle_C \,. \end{aligned} \tag{19}$$

As the third phase unfolds, Alice, Bob and Charlie apply their n-fold Hadamard transform to their input registers, driving the quantum circuit to the next state $|\psi_3\rangle$.

$$\begin{aligned} |\psi_3\rangle &= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{\mathbf{i}\cdot\mathbf{x}} H^{\otimes n} |\mathbf{x}\rangle_A |-\rangle_B H^{\otimes n} |\mathbf{x}\rangle_B |-\rangle_C H^{\otimes n} |\mathbf{x}\rangle_C \\ &\overset{(4)}{=} \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{\mathbf{i}\cdot\mathbf{x}} \Big(\tfrac{1}{\sqrt{2^n}} \sum_{\mathbf{a}\in\{0,1\}^n} (-1)^{\mathbf{a}\cdot\mathbf{x}} |\mathbf{a}\rangle_A \Big) \\ &\qquad |-\rangle_B \Big(\tfrac{1}{\sqrt{2^n}} \textstyle\sum_{\mathbf{b}\in\{0,1\}^n} (-1)^{\mathbf{b}\cdot\mathbf{x}} |\mathbf{b}\rangle_B \Big) \\ &\qquad |-\rangle_C \Big(\tfrac{1}{\sqrt{2^n}} \textstyle\sum_{\mathbf{c}\in\{0,1\}^n} (-1)^{\mathbf{c}\cdot\mathbf{x}} |\mathbf{c}\rangle_C \Big) \\ &= \tfrac{1}{2^{2n}} \textstyle\sum_{\mathbf{x}\in\{0,1\}^n} \sum_{\mathbf{a}\in\{0,1\}^n} \sum_{\mathbf{b}\in\{0,1\}^n} \sum_{\mathbf{c}\in\{0,1\}^n} (-1)^{(\mathbf{i}\oplus\mathbf{a}\oplus\mathbf{b}\oplus\mathbf{c})\cdot\mathbf{x}} |\mathbf{a}\rangle_A |-\rangle_B |\mathbf{b}\rangle_B |-\rangle_C |\mathbf{b}\rangle_C \\ &= \tfrac{1}{2^{2n}} \textstyle\sum_{\mathbf{a}\in\{0,1\}^n} \sum_{\mathbf{b}\in\{0,1\}^n} \sum_{\mathbf{c}\in\{0,1\}^n} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{(\mathbf{i}\oplus\mathbf{a}\oplus\mathbf{b}\oplus\mathbf{c})\cdot\mathbf{x}} |\mathbf{a}\rangle_A |-\rangle_B |\mathbf{b}\rangle_B |-\rangle_C |\mathbf{b}\rangle_C \,. \end{aligned} \tag{20}$$

We can express (20) in a more intelligible form by invoking a useful property of the inner product modulo 2. Whenever $\mathbf{c}$ is a fixed element of $\{0,1\}^n$, but different from $\mathbf{0}$, then for half of the elements $\mathbf{x} \in \{0,1\}^n$, $\mathbf{c}\cdot\mathbf{x}$ is 0 and for the other half, $\mathbf{c}\cdot\mathbf{x}$ is 1. However, when $\mathbf{c} = \mathbf{0}$, then for all $\mathbf{x} \in \{0,1\}^n$, $\mathbf{c}\cdot\mathbf{x} = 0$. For a more detailed analysis of this point, refer to ref. [45]. Therefore, if

$$\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c} = \mathbf{i}\,, \tag{21}$$

the sum $\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{(\mathbf{i}\oplus\mathbf{a}\oplus\mathbf{b}\oplus\mathbf{c})\cdot\mathbf{x}}|\mathbf{a}\rangle_A|-\rangle_B|\mathbf{b}\rangle_B|-\rangle_C|\mathbf{b}\rangle_C$ is equal to $2^n\ |\mathbf{a}\rangle_A\ |-\rangle_B|\mathbf{b}\rangle_B\ |-\rangle_C$ $|\mathbf{b}\rangle_C$, whereas if $\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c} \neq \mathbf{i}$, the sum reduces to 0. Ergo, $|\psi_3\rangle$ can be written simpler as

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{\mathbf{a}\in\{0,1\}^n} \sum_{\mathbf{b}\in\{0,1\}^n} \sum_{\mathbf{c}\in\{0,1\}^n} |\mathbf{a}\rangle_A|-\rangle_B|\mathbf{b}\rangle_B|-\rangle_C|\mathbf{b}\rangle_C\,, \quad \text{where} \quad \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c} = \mathbf{i}\,. \tag{22}$$

We call relation (21) the Fundamental Correlation Property that intertwines the contents of Alice, Bob, and Charlie's input registers. The intuition behind this property is that the entanglement between their input registers in the initialization of the quantum circuit, has caused this specific dependency that disallows the contents of the input registers from varying independently of its other.

The final measurement of their input registers by Alice, Bob, and Charlie drives the quantum circuit into its final state $|\psi_4\rangle$.

$$|\psi_4\rangle = |\mathbf{a}\rangle_A|-\rangle_B|\mathbf{b}\rangle_B|-\rangle_C|\mathbf{b}\rangle_C\,, \quad \text{for some} \quad \mathbf{a}, \mathbf{b}, \mathbf{c} \in \{0,1\}^n\,, \tag{23}$$

where **a**, **b**, and **c** are correlated via (21). One may regard the final contents **a** and **b** of Alice and Bob's input registers as random, but in that case, the final contents **c** of Charlie's input register are completely determined. Symmetrically, one may regard the final contents **b** and **c** of Bob and Charlie's input register as random, in which case the final contents **a** of Alice's input register are completely determined, and so on.

3.2. The Classical Part of the Protocol

To complete the ESR information exchange protocol, one final step remains, and this step takes place in the classical public channels. We may write the contents of the players' input registers as follows:

$$\mathbf{a} = \mathbf{a}_B\ \mathbf{a}_C, \qquad \text{where } |\mathbf{a}_B| = |\mathbf{i}_B| \text{ and } |\mathbf{a}_C| = |\mathbf{i}_C| \tag{24}$$

$$\mathbf{b} = \mathbf{b}_B\ \mathbf{b}_C, \qquad \text{where } |\mathbf{b}_B| = |\mathbf{i}_B| \text{ and } |\mathbf{b}_C| = |\mathbf{i}_C|\,, \quad \text{and} \tag{25}$$

$$\mathbf{c} = \mathbf{c}_B\ \mathbf{c}_C, \qquad \text{where } |\mathbf{c}_B| = |\mathbf{i}_B| \text{ and } |\mathbf{c}_C| = |\mathbf{i}_C|\,. \tag{26}$$

The previous formulas allow us to refine Equation (21) into two independent parts: the first regarding the information bit vector $\mathbf{i}_B$ that Bob intends to communicate to Charlie, and the second regarding the information bit vector $\mathbf{i}_C$, that Charlie intends to communicate to Bob.

$$\mathbf{a}_B \oplus \mathbf{b}_B \oplus \mathbf{c}_B = \mathbf{i}_B\,, \quad \text{and} \tag{27}$$

$$\mathbf{a}_C \oplus \mathbf{b}_C \oplus \mathbf{c}_C = \mathbf{i}_C\,. \tag{28}$$

The following Figure 7 visualizes the situation regarding the contents of Alice, Bob, and Charlie's input registers.

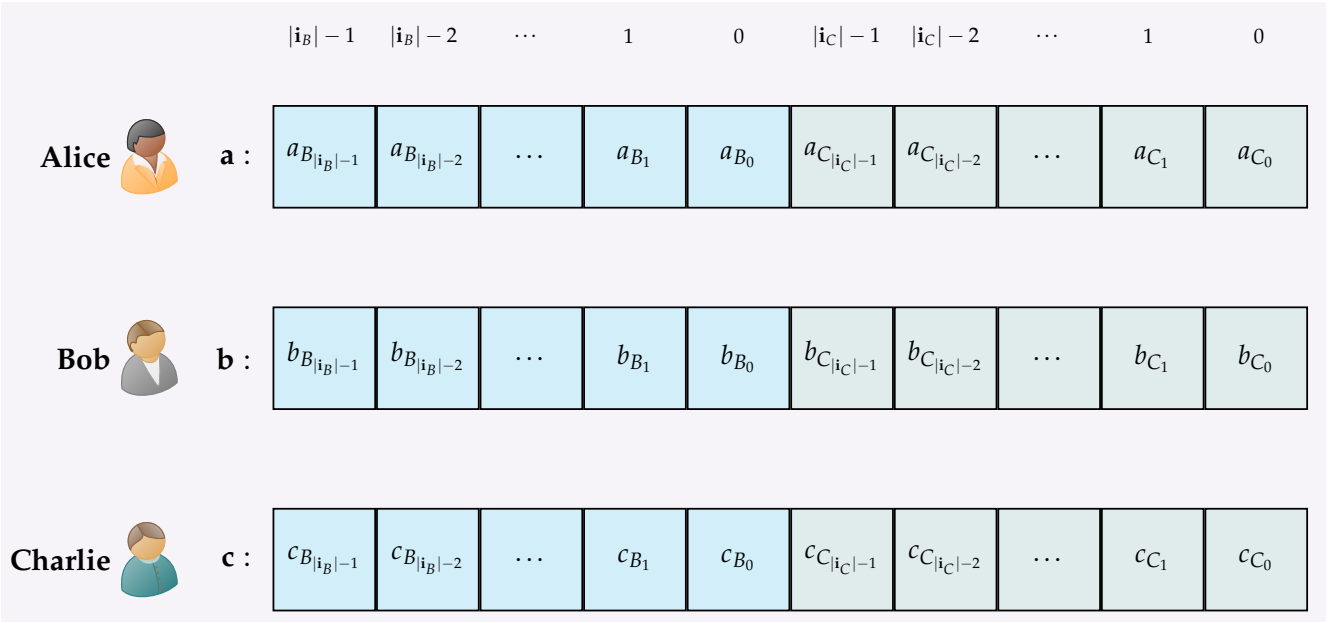

Figure 7. This figure gives indicates the contents of Alice, of Bob and Charlie's input registers after the measurement. The information bit vector $\mathbf{i}_B$ is revealed by adding (modulo 2) $\mathbf{a}_B \oplus \mathbf{b}_B \oplus \mathbf{c}_B$, according to (27). Symmetrically, $\mathbf{i}_C$ is constructed as $\mathbf{a}_C \oplus \mathbf{b}_C \oplus \mathbf{c}_C$, according to (28).

The above relations (27) and (28) dictate what remains to be completed in the final classical part of the ESR information exchange protocol so that Bob and Charlie receive the intended information.

- Alice must use two classical public channels to communicate with Bob and Charlie. Specifically, she must send through these channels the information bit vectors $\mathbf{a}_C$ and $\mathbf{a}_B$ to Bob and Charlie, respectively.
- Bob and Charlie must use a third classical channel to communicate with each other. This communication must take place with caution. They must not reveal the entire contents of their input registers because then Alice, and any other adversary for that matter, will be able to piece together the secret information in $\mathbf{i}_B$ and $\mathbf{i}_C$. They must transmit only the absolutely necessary information for the successful completion of the exchange. This means that Bob must send to Charlie only the information vector $\mathbf{b}_B$ and not the whole contents $\mathbf{b}$ of his input register. Reciprocally, Charlie must send to Bob only the information vector $\mathbf{c}_C$ and not the whole contents $\mathbf{c}$ of his input register.

Figure 8 depicts graphically the classical communications between the players that must take place through the public classical channel in order to successfully complete the protocol. After these communications have taken place, the ESR protocol is concluded. Bob knows $\mathbf{a}_C$, $\mathbf{c}_C$, and, of course, the contents of his input register, and can discover the secret information $\mathbf{i}_C$, according to Equation (28). Symmetrically, Charlie, being in possession of $\mathbf{a}_B$, $\mathbf{b}_B$, can reconstruct $\mathbf{i}_B$, as Equation (27) asserts. Alice, despite her critical contribution to the implementation of the protocol, lacks the necessary information, namely $\mathbf{b}_C$ and $\mathbf{c}_B$, which has not been made public. Thus, she is in no position to uncover either $\mathbf{i}_B$, or $\mathbf{i}_C$.

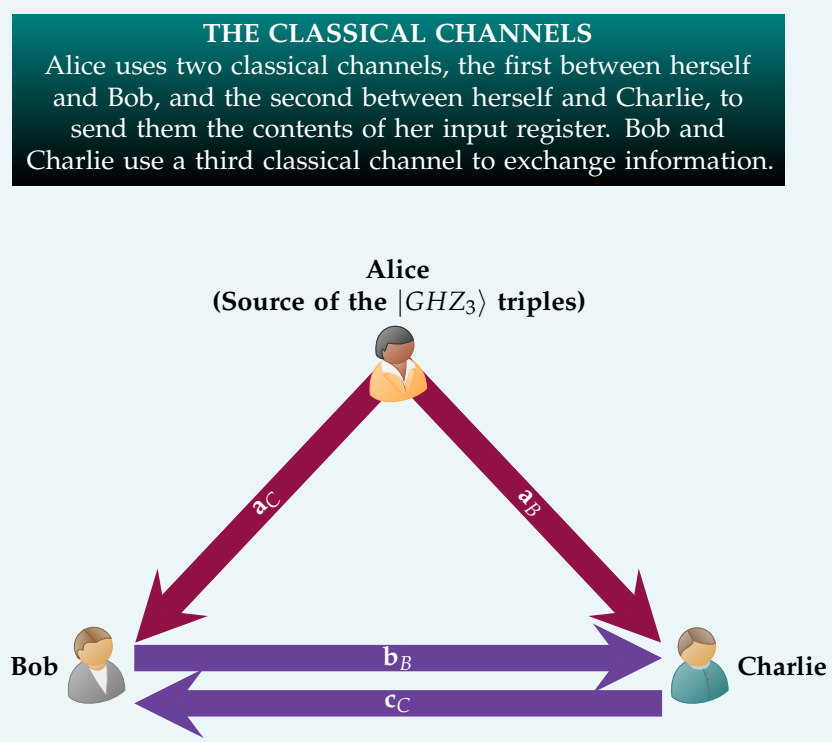

Figure 8. This figure shows Alice, Bob and Charlie, who are spatially separated, and their three classical channels, the first between Alice and Bob, the second between Alice and Charlie, and the third between Bob and Charlie.

4. Security and Efficiency Considerations

The current section is devoted to the security and efficiency analysis of the ESR protocol. We begin by first considering security. For a recent comprehensive text analyzing the security issues of quantum protocols, we refer to ref. [49] and the more recent ref. [50].

4.1. Security

The setting of the subsequent security analysis involves, in addition to our three protagonists, Alice, Bob, and Charlie, a forth notorious entity, traditionally named Eve, whose sole purpose is to devise and implement attacks against our protocol, aiming to acquire a piece of the secret information or even, the complete secret information.

Ultimately, the security analysis of any quantum protocol, including, of course, our ESR protocol, depends on certain well-understood assumptions. For the sake of completeness, we briefly mention them at this point. First, we assume that quantum theory is correct, which in turn means that it allows accurate predictions regarding measurement outcomes and that hallmark features such as the no-cloning theorem [42], the monogamy of entanglement [51], and nonlocality [52] are valid. Clearly, if quantum protocols did not exhibit these properties, they would be useless. Secondly, we assume that quantum theory is complete, which implies that Eve is constrained by the laws of physics and cannot derive more information beyond what is predicted by quantum mechanics.

We now begin our formal analysis of the most well-known attacks that Eve can employ, in order to compromise the ESR protocol and gain secret information.

(**Attack**$_1$) Measure and Resend. In this type of attack, Eve's strategy is to intercept the $|GHZ_3\rangle$ triplets during their transmission from Alice to Bob and Charlie, measure them, and then resend them back to Bob and Charlie. By doing so, Eve will fail to discover any information because, at this phase, the $|GHZ_3\rangle$ triplets do not carry any information. Consequently, the ESR protocol is completely impervious to this strategy.

(**Attack**$_2$) Intercept and Resend. In such an attack, Eve's strategy is to intercept $|GHZ_3\rangle$ triplets during their transmission from Alice to Bob and Charlie. Then, since cloning is prohibited by the no-cloning theorem, in her effort to get information, Eve measures them on a predefined basis. Afterwards, Eve prepares new qubits and sends them to the intended recipient. As we have pointed out above, during the transmission phase of the ESR protocol, the $|GHZ_3\rangle$ triplets carry no information whatsoever. Thus, Eve fails again to discover any information.

(**Attack**$_3$) Entangle and Measure. In this type of attack, Eve's strategy is to intercept the $|GHZ_3\rangle$ triplets during their transmission from Alice to Bob and Charlie. However, now Eve does not measure them, but entangles them with her ancilla state and then sends the corresponding GHZ qubits to Bob and Charlie. Furthermore, Eve waits until the protocol is complete before measuring her qubits, hoping to gain useful information. However, the result of Eve's actions is that instead of having n $|GHZ_3\rangle$ triplets evenly distributed among Alice, Bob, and Charlie, we end up with n $|GHZ_4\rangle$ quadruples evenly distributed among Alice, Bob, Charlie, and Eve. Accordingly, during the classical part of the ESR protocol, when Alice, Bob, and Charlie send their (partial) measurements through the public channel, hoping to unlock the secret information, they will realize that they are not able to reveal the secret information vectors $\mathbf{i}_B$ and $\mathbf{i}_C$ because they will require Eve's measurement. Eve will also fail to compute $\mathbf{i}_B$ and $\mathbf{i}_C$ because, in order to achieve this, she needs the bit vectors $\mathbf{b}_C$ and $\mathbf{c}_B$ that Bob and Charlie possess, respectively, but never transmit through the public channel. Therefore, in this case, Eve will also fail, whereas Bob and Charlie will be able to infer that Eve tempered with the protocol.

(**Attack**$_4$) PNS. The photon number splitting attack (PNS), first introduced in [53] and later analyzed in [54,55], is currently regarded as one of the most effective attack strategies that Eve can employ against any quantum protocol. As it happens with our current technology, photon sources occasionally do not emit single-photon signals, which practically means that a photon source may produce multiple identical photons instead of just one. This opens up for Eve the possibility of intercepting pulses emanating from Alice for the distribution of the $|GHZ_3\rangle$ triplets, keeping one photon from the multi-photon pulse for herself, and sending the remaining photons to Bob and Charlie without being detected during the transmission phase. Nonetheless, as the execution of the ESR protocol shows, the situation in this case resembles the Entangle and Measure attack analyzed above. Again, instead of $|GHZ_3\rangle$ triplets evenly distributed among Alice, Bob, and Charlie, there are $|GHZ_4\rangle$ quadruples evenly distributed among Alice, Bob, Charlie, and Eve. Eve becomes effectively the fourth player and is unable to gain any information about the other players' measurements.

The above succinct security analysis demonstrates that the ESR is information-theoretically secure.

4.2. Efficiency

A typical measure of the qubit efficiency of quantum protocols (see, for instance, ref. [56,57]) is the ratio η of the total number of transmitted "useful" classical bits to the total number of utilized qubits. In the case of the ESR protocol, the former refers to the length of the aggregated information bit vector $\mathbf{i}$ that contains the total information exchanged by Bob and Charlie, and which, according to (9), is n. The latter refers to the total number of qubits employed by the local quantum circuits of Alice, Bob, and Charlie, which is $3n$, since n maximally entangled $|GHZ_3\rangle$ triplets are used. To be very precise and account for every detail in the quantum protocol, we may take into account the single qubit output registers used by Bob and Charlie and say that the total number of qubits is $3n + 2$,

but for large n the difference would be negligible. Therefore, the η qubit efficiency of the ESR protocol is

$$\eta = \frac{n}{3n+2} \approx \frac{n}{3n} = \frac{1}{3} = 33.33\% \tag{29}$$

Another, stricter measure of the qubit efficiency was introduced in ref. [58], as the ratio η' of the total number of classical bits of information to the sum of the total number of utilized qubits plus the total number of classical bits necessary to reveal the information. In the final classical phase of the ESR protocol, Alice sends the bit vectors $\mathbf{a}_C$ and $\mathbf{a}_B$ through the public channels to Bob and Charlie, respectively. Their combined length, given by (24), is n. Additionally, Bob sends to Charlie the bit vector $\mathbf{b}_B$ and Charlie sends to Bob the bit vector $\mathbf{c}_C$. Their combined length, according to (25) and (26), is also n. Hence, the η' qubit efficiency of the ESR protocol is

$$\eta' = \frac{n}{3n+2+2n} \approx \frac{n}{5n} = \frac{1}{5} = 20\% \tag{30}$$

These efficiency results are the norm in quantum protocols that utilize GHZ states. For an extensive and detailed comparative analysis of the efficiency of many quantum protocols, where this fact can be immediately corroborated, we refer to [59,60].

5. Discussion and Conclusions

This paper introduced a novel quantum protocol, called ESR, for the simultaneous reciprocal exchange of secret information between Bob and Charlie. The whole process is mediated by Alice, who is assumed to be a trusted intermediary.

The proposed protocol, being quantum, was shown in Section 4 to be information-theoretically secure against the attacks of the malicious eavesdropper Eve. The underlying reason for its security rests with the laws of quantum mechanics, as currently understood. In contrast, an analogous classical protocol can only offer security based on conjectured computationally hard problems, with the potential risks that it may entail. Moreover, the efficiency analysis of the ESR protocol conducted in Section 4 demonstrated that its efficiency is comparable to that of most other entanglement-based protocols.

The protocol is based on the uniquely quantum phenomenon of entanglement, which offers multiple advantages. It enables the two players to embed their secret information simultaneously and stealthily in the state of the composite system. Upon completion of the quantum part of the protocol, the combined secret information will be encoded in the correlated contents of the quantum registers, but it will only be revealed after the proper classical information is exchanged. Moreover, entanglement guarantees the security of the protocol, as shown in Section 4, and, at the same time, provides for the spatially distributed execution of the protocol. Despite the fact that the three players are situated in different locations and utilize localized quantum circuits, the correlations present due to entanglement ensure that we are still dealing with one composite system.

The inclusion of a third party to supervise and facilitate the exchange process can be beneficial. There are a plethora of situations, as briefly sketched in Example 1, where the presence of an intermediary would be necessary. The most important observation here is that a trusted intermediary does not compromise the security of the protocol in any way. Particularly so, after taking into account that upon the completion of the protocol, the third party remains oblivious to the actual information that was exchanged between the two players, i.e., there is no information leak whatsoever. Alice is essential for the completion of the ESR protocol because, without the contents of her input register, the information can't be reconstructed. Although her contribution is crucial, proper execution of the last classical part of the protocol ensures that she gains no insight whatsoever about the information that was exchanged. Moreover, since Alice is assumed to be a player who is mutually trusted by both Bob and Charlie, her involvement does not compromise the security of the protocol.

Of course, one can easily envision a protocol for information exchange between Bob and Charlie that does not involve Alice at all. The ESR protocol can be easily simplified to function without the presence of Alice, using, for instance, the quantum circuit shown in Figure 9. In such a case, instead of entangled triplets, it would be necessary to employ entangled pairs, e.g., EPR pairs in the Bell $|\Phi^+\rangle$ state:

$$|\Phi^+\rangle = \frac{|0\rangle_B|0\rangle_C + |1\rangle_B|1\rangle_C}{\sqrt{2}} \,. \tag{31}$$

Such an approach would certainly require a somewhat simpler quantum circuit for the production of the EPR pairs. Furthermore, the whole mathematical description of the protocol would be considerably easier. Nonetheless, one would still have to address the requirement for a trusted source to produce and distribute those n $|\Phi^+\rangle$ pairs to Bob and Charlie. However, it is our belief that, as we have advocated in the Introduction, there are many real-life situations where having a third party witness and verify that such a transaction has indeed occurred can be beneficial or even necessary. Ergo, it seems prudent to be able to account for this eventuality, particularly in view of the fact that the third party is not only trusted but does not gain knowledge of the secret information that was exchanged.

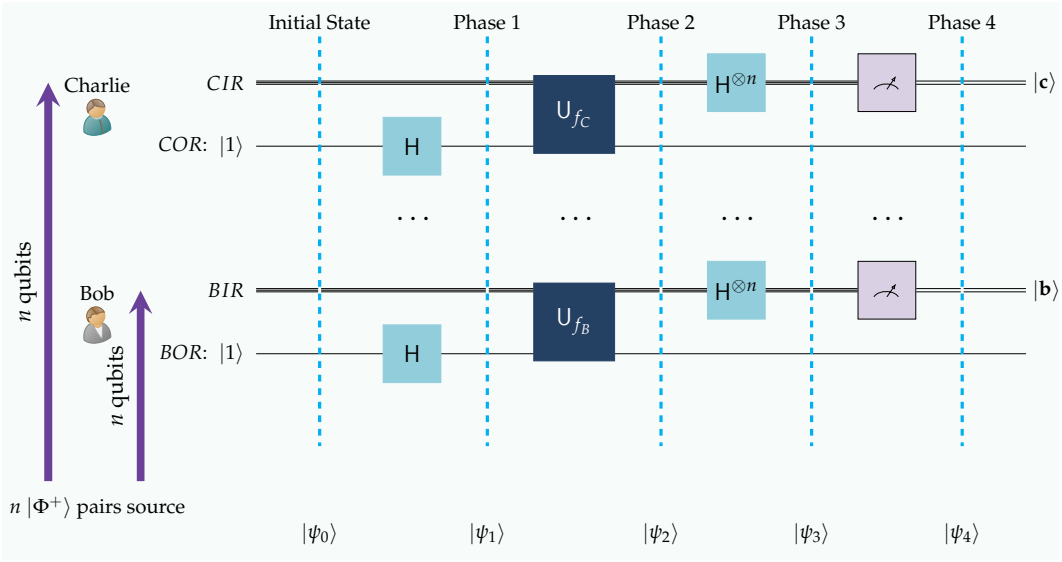

Figure 9. This figure outlines a distributed quantum circuit, where only Bob and Charlie are present. Again both are correlated, due to the phenomenon of entanglement. Thus, they form a composite system, whose temporal evolution is given by the state vectors $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$ and $|\psi_4\rangle$.

In closing, we clarify that although the ESR protocol was shown in Section 4 to be information-theoretically secure against the attacks of the external adversary Eve, it assumes that the three protagonists, Alice, Bob, and Charlie, are honest. Its security is based on the assumption that Alice is a trusted intermediary and that both Bob and Charlie, the internal parties to this game, are honest and do not attempt to compromise the protocol. It would be an interesting and challenging direction for future work to extend the ESR protocol so as to take into account the possibility that one, but not both, of Bob or Charlie are dishonest.

Author Contributions: Conceptualization, T.A. and A.S.; methodology, T.A.; validation, A.S.; formal analysis, A.S.; investigation, T.A.; writing original draft preparation, T.A. and A.S.; writing review and editing, T.A. and A.S.; visualization, A.S.; supervision, T.A.; project administration, T.A. and A.S. 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: Not applicable, the study does not report any data.

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

References

1. 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.
2. Alagic, G.; Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Liu, Y.K.; Miller, C.; Moody, D.; Peralta, R.; et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019.
3. Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Kelsey, J.; Liu, Y.K.; Miller, C.; Moody, D.; Peralta, R.; et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*; US Department of Commerce, NIST: Gaithersburg, MD, USA, 2020.
4. Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Miller, C.; Moody, D.; Peralta, R.; et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
5. Shor, P. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994. [CrossRef]
6. 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]
7. Chow, J.; Dial, O.; Gambetta, J. IBM Quantum Breaks the 100-Qubit Processor Barrier. 2021. Available online: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle (accessed on 3 April 2022).
8. Newsroom, I. IBM Unveils 400 Qubit-Plus Quantum Processor. 2022. Available online: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two (accessed on 3 April 2022).
9. Chamola, V.; Jolfaei, A.; Chanana, V.; Parashari, P.; Hassija, V. Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. *Comput. Commun.* **2021**, *176*, 99–118. [CrossRef]
10. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
11. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557–559. [CrossRef] [PubMed]
12. Gisin, N.; Ribordy, G.; Zbinden, H.; Stucki, D.; Brunner, N.; Scarani, V. Towards practical and fast quantum cryptography. *arXiv* **2004**, arXiv:quant-ph/0411022.
13. Inoue, K.; Waks, E.; Yamamoto, Y. Differential phase shift quantum key distribution. *Phys. Rev. Lett.* **2002**, *89*, 037902. [CrossRef]
14. Guan, J.Y.; Cao, Z.; Liu, Y.; Shen-Tu, G.L.; Pelc, J.S.; Fejer, M.; Peng, C.Z.; Ma, X.; Zhang, Q.; Pan, J.W. Experimental passive round-robin differential phase-shift quantum key distribution. *Phys. Rev. Lett.* **2015**, *114*, 180502. [CrossRef]
15. Waks, E.; Takesue, H.; Yamamoto, Y. Security of differential-phase-shift quantum key distribution against individual attacks. *Phys. Rev. A* **2006**, *73*, 012344. [CrossRef]
16. Ampatzis, M.; Andronikos, T. QKD Based on Symmetric Entangled Bernstein-Vazirani. *Entropy* **2021**, *23*, 870. [CrossRef]
17. Ampatzis, M.; Andronikos, T. A Symmetric Extensible Protocol for Quantum Secret Sharing. *Symmetry* **2022**, *14*, 1692. [CrossRef]
18. Attasena, V.; Darmont, J.; Harbi, N. Secret sharing for cloud data security: A survey. *VLDB J.* **2017**, *26*, 657–681. [CrossRef]
19. Ermakova, T.; Fabian, B. Secret sharing for health data in multi-provider clouds. In Proceedings of the 2013 IEEE 15th Conference on Business Informatics, Vienna, Austria, 15–18 July 2013; pp. 93–100.
20. Cha, J.; Singh, S.K.; Kim, T.W.; Park, J.H. Blockchain-empowered cloud architecture based on secret sharing for smart city. *J. Inf. Secur. Appl.* **2021**, *57*, 102686. [CrossRef]
21. Karlsson, A.; Koashi, M.; Imoto, N. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **1999**, *59*, 162. [CrossRef]
22. Smith, A.D. Quantum secret sharing for general access structures. *arXiv* **2000**, arXiv:quant-ph/0001087.
23. Gottesman, D. Theory of quantum secret sharing. *Phys. Rev. A* **2000**, *61*, 042311. [CrossRef]
24. Fortescue, B.; Gour, G. Reducing the quantum communication cost of quantum secret sharing. *IEEE Trans. Inf. Theory* **2012**, *58*, 6659–6666. [CrossRef]
25. Qin, H.; Tang, W.K.; Tso, R. Hierarchical quantum secret sharing based on special high-dimensional entangled state. *IEEE J. Sel. Top. Quantum Electron.* **2020**, *26*, 1–6. [CrossRef]
26. Senthoor, K.; Sarvepalli, P.K. Theory of communication efficient quantum secret sharing. *IEEE Trans. Inf. Theory* **2022**, *68*, 3164–3186. [CrossRef]
27. Fu, Y.; Yin, H.L.; Chen, T.Y.; Chen, Z.B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **2015**, *114*, 090501. [CrossRef]

28. Wu, X.; Wang, Y.; Huang, D. Passive continuous-variable quantum secret sharing using a thermal source. *Phys. Rev. A* **2020**, *101*, 022301. [CrossRef]
29. Grice, W.P.; Qi, B. Quantum secret sharing using weak coherent states. *Phys. Rev. A* **2019**, *100*, 022339. [CrossRef]
30. Gu, J.; Xie, Y.M.; Liu, W.B.; Fu, Y.; Yin, H.L.; Chen, Z.B. Secure quantum secret sharing without signal disturbance monitoring. *Opt. Express* **2021**, *29*, 32244–32255. [CrossRef]
31. An, L.; Yang, G.H. Enhancement of opacity for distributed state estimation in cyber–physical systems. *Automatica* **2021**, *136*, 110087. [CrossRef]
32. Broadbent, A.; Fitzsimons, J.; Kashefi, E. Universal Blind Quantum Computation. In Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science, Atlanta, GA, USA, 25–27 October 2009. [CrossRef]
33. 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, 9–12 December 1984; pp. 175–179.
34. Meyer, D.A. Quantum strategies. *Phys. Rev. Lett.* **1999**, *82*, 1052. [CrossRef]
35. Eisert, J.; Wilkens, M.; Lewenstein, M. Quantum games and quantum strategies. *Phys. Rev. Lett.* **1999**, *83*, 3077. [CrossRef]
36. 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]
37. Andronikos, T.; Sirokofskich, A. The Connection between the PQ Penny Flip Game and the Dihedral Groups. *Mathematics* **2021**, *9*, 1115. [CrossRef]
38. Andronikos, T. Conditions that enable a player to surely win in sequential quantum games. *Quantum Inf. Process.* **2022**, *21*, 268. [CrossRef]
39. 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]
40. Giannakis, K.; Papalitsas, C.; Kastampolidou, K.; Singh, A.; Andronikos, T. Dominant Strategies of Quantum Games on Quantum Periodic Automata. *Computation* **2015**, *3*, 586–599. [CrossRef]
41. Andronikos, T.; Stefanidakis, M. A Two-Party Quantum Parliament. *Algorithms* **2022**, *15*, 62. [CrossRef]
42. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
43. Cruz, D.; Fournier, R.; Gremion, F.; Jeannerot, A.; Komagata, K.; Tosic, T.; Thiesbrummel, J.; Chan, C.L.; Macris, N.; Dupertuis, M.A.; et al. Efficient Quantum Algorithms for GHZ and W States, and Implementation on the IBM Quantum Computer. *Adv. Quantum Technol.* **2019**, *2*, 1900015. [CrossRef]
44. IBM. IBM Quantum Composer. Available online: https://quantum-computing.ibm.com/composer (accessed on 3 April 2022).
45. Ampatzis, M.; Andronikos, T. Quantum Secret Aggregation Utilizing a Network of Agents. *Cryptography* **2023**, *7*, 5. [CrossRef]
46. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2010.
47. Mermin, N. *Quantum Computer Science: An Introduction*; Cambridge University Press: Cambridge, UK, 2007. [CrossRef]
48. Qiskit. Qiskit Open-Source Quantum Development. Available online: https://qiskit.org (accessed on 3 April 2022).
49. Wolf, R. *Quantum Key Distribution*; Springer International Publishing: Berlin/Heidelberg, Germany, 2021. [CrossRef]
50. Renner, R.; Wolf, R. Quantum Advantage in Cryptography. *AIAA J.* **2023**, *61*, 1895–1910. [CrossRef]
51. Coffman, V.; Kundu, J.; Wootters, W.K. Distributed entanglement. *Phys. Rev. A* **2000**, *61*, 052306. [CrossRef]
52. Brunner, N.; Cavalcanti, D.; Pironio, S.; Scarani, V.; Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **2014**, *86*, 419. [CrossRef]
53. Huttner, B.; Imoto, N.; Gisin, N.; Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **1995**, *51*, 1863. [CrossRef]
54. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]
55. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330. [CrossRef]
56. Tsai, C.W.; Hsieh, C.R.; Hwang, T. Dense coding using cluster states and its application on deterministic secure quantum communication. *Eur. Phys. J. D* **2011**, *61*, 779–783. [CrossRef]
57. Hwang, T.; Hwang, C.C.; Tsai, C.W. Quantum key distribution protocol using dense coding of three-qubit W state. *Eur. Phys. J. D* **2011**, *61*, 785–790. [CrossRef]
58. Cabello, A. Quantum Key Distribution in the Holevo Limit. *Phys. Rev. Lett.* **2000**, *85*, 5635–5638. [CrossRef]
59. Banerjee, A.; Pathak, A. Maximally efficient protocols for direct secure quantum communication. *Phys. Lett. A* **2012**, *376*, 2944–2950. [CrossRef]
60. Joy, D.; Surendran, S.P.; Sabir, M. Efficient deterministic secure quantum communication protocols using multipartite entangled states. *Quantum Inf. Process.* **2017**, *16*, 157. [CrossRef]