



Article

# A Symmetric Extensible Protocol for Quantum Secret Sharing

Michael Ampatzis <sup>†</sup>  and Theodore Andronikos <sup>\*,†</sup> 

Department of Informatics, Ionian University, 7 Tsirigoti Square, 49100 Corfu, Greece

\* Correspondence: andronikos@ionio.gr

† These authors contributed equally to this work.

**Abstract:** This paper introduces the Symmetric Extensible Quantum Secret Sharing protocol, a novel quantum protocol for secret sharing. At its heart, it is an entanglement-based protocol that relies on the use of maximally entangled GHZ tuples, evenly distributed among the players, endowing the spymaster with the ability to securely share a secret message with the agents. Its security stems from the fact that it is highly improbable for a malicious eavesdropper or a rogue double agent to disrupt its successful execution. It is characterized by symmetry, since all agents are treated indiscriminately, utilizing identical quantum circuits. Furthermore, it can be seamlessly extended to an arbitrary number of agents. Finally, after the completion of the quantum part of the protocol, the spymaster will have to publicly transmit some information, in order to allow the agents to unlock the secret message. This part of the protocol can be considered as an additional advantage, due to the fact that it gives the spymaster the privilege of deciding if, or when, it is the right time for the agents to unlock the secret message, after the completion of the quantum part of the protocol.

**Keywords:** quantum secret sharing; quantum cryptography; quantum entanglement; GHZ states



**Citation:** Ampatzis, M.; Andronikos, T. A Symmetric Extensible Protocol for Quantum Secret Sharing. *Symmetry* **2022**, *14*, 1692. <https://doi.org/10.3390/sym14081692>

Academic Editor: Kuo-Hui Yeh

Received: 4 July 2022

Accepted: 11 August 2022

Published: 15 August 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

After the landmark announcement of IBM's new quantum computer, which managed to successfully break the 100-qubit barrier [1], it appears that we have moved closer than originally anticipated to the realization of practical quantum computation and the definitive transition from the digital era to the quantum era. However, such rapid technological advancements also herald some rather serious issues with our current infrastructure—issues that can pose significant threats to our information security. After the publication of one of the most famous papers in the field of quantum computing by Peter Shor in 1994 [2], which proposed an algorithm that can solve the integer factorization problem in polynomial time, and is thus theoretically able to break any cryptosystem based on the aforementioned problem, it was made apparent that, if quantum computers become a reality, then the existing digital security protocols must be replaced with ones that can withstand attacks from a quantum computer.

Fortunately, after recognizing the potential vulnerability of the current infrastructure, the scientific community came up with an explosion of proposals in the field of quantum cryptography, which resulted in a profound increase of the maturity of the field. Quantum cryptography in its present state can be broken down into two main branches. The first branch is referred to as post-quantum cryptography or quantum-resistant cryptography, and it relies on the development of cryptographic protocols that are based on the complexity of certain mathematical problems. It is believed, but not yet proven, that the aforementioned problems can not be solved in polynomial time even with a quantum computer. The second branch of the field, known as quantum cryptography, strives to create secure cryptosystems based on the clever implementation of certain properties of quantum mechanics, such as entanglement and superposition of quantum states, the non-locality principle, the no-cloning theorem, etc. This branch of quantum cryptography, which this paper is part of, was originally created by proposing two novel solutions to the fundamental problem of

key distribution. The historic works of Bennett and Brassard for the BB84 QKD protocol [3], and Ekert for the E91 QKD protocol [4], were instrumental, as they established the two main methods of sharing information between two or more players utilizing the power of quantum mechanics, known as the prepare-and-measure and the entanglement-based methods, upon which every quantum cryptographic protocol is based on.

After these two protocols, a rapid expansion of the sub-field of quantum key distribution ensued that resulted in multiple attempts on transitioning other sub-fields of cryptography into their quantum counterparts. One of the numerous sub-fields of cryptography which can be improved with the use of quantum mechanics, in order to enhance its security and efficiency against a quantum computer, is the field of secret sharing, which can be described as a clandestine game between three or more individual players that are located in two different geographical locations and are unable to communicate in person. For the sake of simplicity, we shall initially describe the simplest version of the game, involving only three players. However, the game can be scaled up to as many players as we want. Therefore, we start by dividing the three players into two groups. The first group consists of the dealer or spymaster, which is a single person, and, for this game, we shall give this honor to Alice, who is located in Athens. The second group consists of her secret agents, the rest of the players—in this case Bob and Charlie, who are located in Corfu. In this game, the spymaster Alice wants to send a set of secret instructions to her agents for them to act upon. However, Alice is not certain that she can trust both of her agents because she suspects that one of them, but not both, is a double agent and is working for the enemy, with the goal of foiling her plans. However, she knows that, if both of her agents partake in the mission together, the agent who is loyal to Alice will prevent the double agent from causing any damage. Furthermore, aside from the possible double agent who wants to sabotage the mission, Alice must also take precautions to assure the confidentiality of the mission from possible eavesdroppers, which for the sake of the game will be referred to as Eve. Therefore, Alice must somehow find a way to make both her agents act on her behalf, and, at the same time, prevent both the dishonest agent and Eve from tempering with the mission.

This elaborate game may at first sight seem a little redundant or even superfluous, yet the field of secret sharing has been proven vital for a certain type of problems with multiple real world uses, as for example, to guarantee that a single individual or a small group of the involved party can not access a valuable shared resource, such as a shared bank account. This means that, in order to take any action, all involved members must act in concert. As a consequence, this requirement makes it considerably more difficult for any individual who wants to have unauthorized access to secret information or to perform an unauthorized action, to achieve her purpose. Practically, this implies that the only way for a malicious player to perform any action is to convince every single member to go along.

The pioneering works of Hillery et al. [5] and Cleve et al. [6], which proved that secret sharing can be achieved with the use of quantum mechanics, paved the way for the creation of a new field with the name of Quantum Secret Sharing (QSS for short). Since then, there has been extensive progress in this field, with a plethora of proposals actively continuing the research to this day [7–14]. Multiple research groups have devised protocols demonstrating the viability of QSS (see, for instance, [15–17]). More recently, elaborate proof-of-concept experimental demonstrations of novel and effective protocols applicable to real world scenarios have been introduced by the researchers in [18–21]. Another line of research attempted to extend the capabilities of the field by proposing non-binary protocols that rely on the use of qudits rather than qubits [22,23].

With this rapid advancement of the field, one may also observe some notable efforts towards the application of Grover's algorithm [24], which is one of the most famous algorithms of all time, as a QSS protocol [25–27]. In the same vein, it has also been shown by multiple proposals that well-known quantum algorithms, such as the Deutsch-Josza, the Bernstein-Vazirani and Simon's algorithms can be utilized in implementing viable QKD protocols [28–31]. This decade promises to be the Quantum Decade that will, hopefully,

transform every aspect of the industry and the society for the better. Technologically, we are fast approaching the era of the quantum-centric supercomputer [32]. The quantum-centric supercomputer will combine quantum and classical processors, quantum and classical communication networks into a harmonious quantum ecosystem that will elevate our computing capabilities to new undreamed-of heights. Every quantum practitioner knows that building a quantum computer capable of practical impact involves millions of qubits. Hence, the problem of scaling the current, modest in terms of qubits, quantum processors is of paramount importance. One way to cleverly bypassing the problem of scaling the number of qubits of a single quantum processor is by linking multiple such processors together into a modular quantum system capable of scaling without limitations. In view of this current trend, we advocate the utility and efficiency of using quantum algorithms as cryptographic protocols, either by modifying established quantum algorithms, or by building new ones based on some fundamental concepts of other algorithms. We believe that this approach will prove beneficial for achieving effective security between multiple quantum computers, by simply exchanging information and processing it using gates, without the need of extra equipment [33].

In this paper, we propose a new QSS protocol in the form of a quantum game, which we hope will make its presentation simple and pedagogical, thanks to the inherent ability of game theory to present complex and challenging problems in a more innate and comprehensive way. As a consequence, quantum games have gained prominence as a useful paradigm of the quantum world and have been used to tackle important problems. A typical example in this area is the quantum game of coin tossing and its application to cryptographic protocols (see [3] and the more recent [34]). The beginning of this field can be traced back to two landmark papers from 1999: Meyer's PQ penny flip game [35] and the Eisert–Wilkens–Lewenstein scheme [36]. Numerous works that were inspired from the PQ penny flip game have appeared in the literature and some recent results are given in [37–39]. The Eisert–Wilkens–Lewenstein scheme was successfully employed in the study of quantum versions of well-known classical games, such as the famous Prisoners' Dilemma, where the quantum strategies outperformed the classical strategy [36], and to quantum extensions of the classical repeated Prisoners' Dilemma strategies [40]. Winning strategies for abstract quantum games can also be encoded as infinite words accepted by quantum automata, as demonstrated in [41]. Quantum games have even been used in [42] as a metaphor for the operation of a hypothetical quantum parliament.

### 1.1. Contribution

As a result of our approach, in this paper, we propose the novel Symmetric Extensible Quantum Secret Sharing protocol, which we designate by SEQSS<sub>*n*</sub>, where *n* represents the number of participating players. The final result is an entanglement-based protocol that relies on the use of maximally entangled GHZ tuples, evenly distributed among the players, in order to allow our spymaster Alice to securely share the secret message with her agents, by implementing a unitary transform  $U_f$ . As the name suggests, it exhibits symmetry, since all agents are treated indiscriminately, utilizing identical quantum circuits. It offers uncompromising security, making it virtually impossible for a malicious eavesdropper or a rogue double agent to disrupt its successful execution, due to the fact that only the spymaster performs all the steps in the protocol, while the rest of the agents will only have to apply Hadamard gates and measure their registers, rendering them unable to tamper with the protocol. Additionally, we provide a rigorous mathematical analysis of what will happen, if Eve or a rogue agent decides to implement their own unitary function  $U'_f$ . After the completion of the quantum part of the protocol, it is mandatory for the spymaster to publicly communicate her final measurement to her agents, since without this information the agents will not be able to discover the secret message, even if they combine together all their individual data. However, this can be considered as an added advantage, which can be further illustrated as a clandestine mission with Alice as the spymaster and the rest of her agents acting on her behalf. In this mission, Alice has created a detailed

plan, outlining all possible scenarios of the mission, and she has broken down her plan into multiple secret messages, i.e.,  $s_1, s_2, \dots$ . At the beginning of the mission, Alice and her agents complete the quantum part of the protocol multiple times, in order for everyone to have a piece of every single secret message that might be used. At a later moment, Alice can decide if, or when she wants to broadcast some of her measurements based on the real-time feedback from her agents. For example, she will broadcast her piece of information  $s_1$  to start the mission, and then, based on how the mission progresses, she will only broadcast in real time only those secret messages that are relevant to unfolding scenario of the mission. This strategy provides her with the ability to hide from her agents and the enemy possible critical information. Furthermore, since she can broadcast her pieces of the secret message on a public channel, after the completion of the quantum part, Alice and her agents can use whatever communication method they deem suitable for the mission.

### 1.2. Organization

This paper is organized as follows: Section 1 gives an introduction to the subject along with some relevant references. Section 2 provides a brief introduction about the GHZ states and the principle of entanglement, a vital tool used in the formulation of the proposed protocol. Section 3 showcases the Symmetric Extensible QSS protocol twice, once in its simplest form, which is restricted to only three players and once in its general form, which is played by  $n$  players. Section 4 gives a brief security analysis on a certain number of known attack strategies that Eve can employ in order to compromise the security of the protocol and acquire confidential information about the secret message that Alice wants to share. Finally, Section 5 discusses the operation and advantages of the proposed protocol.

## 2. Background on GHZ States

Quantum entanglement can be described mathematically as the linear combination of two or more product states. This unique phenomenon is universally considered as one of the fundamental principles of quantum mechanics and is the basis of many fascinating proposals, one of which is the achievement of quantum teleportation. Moreover, entanglement-based techniques have been proven indispensable in the field of quantum secret sharing and quantum cryptography in general. In this paper, for the realization of our QSS protocol, we will heavily rely on the utilization of maximally entangled pairs of three or more qubits, which are commonly known as GHZ states. Therefore, we believe that the following subsection, in which we give a brief explanation on the nature of GHZ states, will facilitate the understanding of the proposed protocol.

From the perspective of quantum computing, a GHZ state can be produced by a circuit with three or more qubits, upon which a Hadamard gate is applied to the first qubit, then a CNOT gate is applied to the first and second qubits, and subsequently a CNOT to the second and third qubits, and so on until we reach the last qubit. A possible quantum circuit for preparing three qubits in the GHZ state is shown in Figure 1. Figure 2 gives the state vector description of the corresponding GHZ state. These figures were also obtained from the IBM Quantum Composer [43].

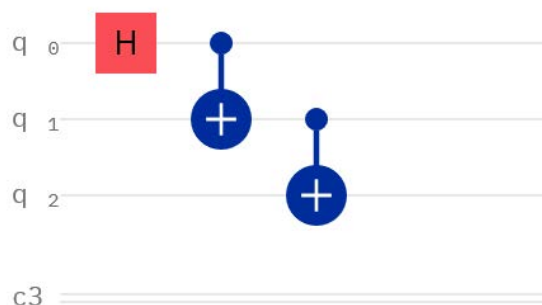
Generalizing the same reasoning as in the case of the 3 qubit GHZ state shown in Figure 1, the mathematical representation of a composite system consisting of  $n$  single qubit subsystems all entangled in the GHZ state, denoted by  $|GHZ_n\rangle$ , goes as follows:

$$|GHZ_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{n-1}|0\rangle_{n-2}\cdots|0\rangle_0 + |1\rangle_{n-1}|1\rangle_{n-2}\cdots|1\rangle_0). \quad (1)$$

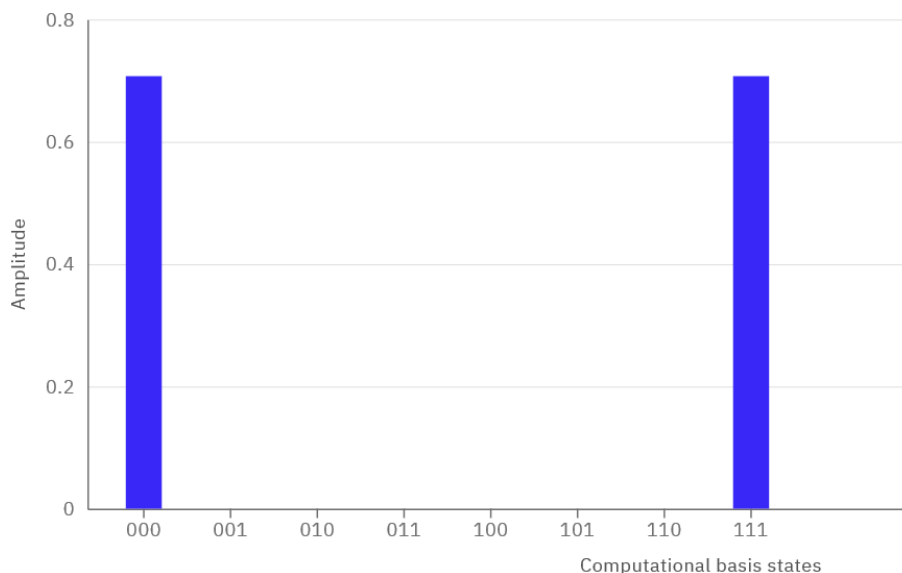
The above setting can be generalized to the case where a composite system consists of  $n$  subsystems, say  $n$  quantum registers  $r_0, r_1, \dots, r_{n-1}$ , each of them having  $m$  qubits, and the

corresponding qubits of all the  $n$  registers are entangled in the  $|GHZ_n\rangle$  state. The state of the composite system, denoted by  $|GHZ_n\rangle^{\otimes m}$ , is described by the formula below:

$$|GHZ_n\rangle^{\otimes m} = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} |\mathbf{x}\rangle_{n-1} \dots |\mathbf{x}\rangle_0 . \tag{2}$$



**Figure 1.** This quantum circuit can be used in Qiskit to entangle three qubits in the  $|GHZ_3\rangle = \frac{|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle}{\sqrt{2}}$  state.



**Figure 2.** The state vector description of three qubits entangled in the  $|GHZ_3\rangle$  state.

The proof for this formula is rather straightforward. If we take the entangled state  $|GHZ_n\rangle$ , as shown in (1) twice, the resulting tensor product can be portrayed as

$$\begin{aligned} |GHZ_n\rangle^{\otimes 2} &= \frac{1}{\sqrt{2}} (|0\rangle_{n-1} \dots |0\rangle_0 + |1\rangle_{n-1} \dots |1\rangle_0) \frac{1}{\sqrt{2}} (|0\rangle_{n-1} \dots |0\rangle_0 + |1\rangle_{n-1} \dots |1\rangle_0) \\ &= \frac{1}{2} (|00\rangle_{n-1} \dots |00\rangle_0 + |01\rangle_{n-1} \dots |01\rangle_0 + |10\rangle_{n-1} \dots |10\rangle_0 + |11\rangle_{n-1} \dots |11\rangle_0) . \end{aligned} \tag{3}$$

Following this pattern, we can successfully derive the general Formula (2) with induction and thus complete the proof.

### 3. The Symmetric Extensible QSS Protocol

In this section, we thoroughly analyze the proposed Symmetric Extensible QSS (for short SEQSS) protocol in great detail. All of Alice’s agents employ identical quantum circuits, hence the term *symmetric*. Due to the nature of the game, the least number of agents Alice can deploy is two, e.g., agents Bob and Charlie, but their number can seamlessly increase to accommodate as many as necessary, which explains the term *extensible*. We

begin our analysis with the simplest version, which is a demonstration of the protocol restricted to only three players, designated by SEQSS<sub>3</sub>, while later on we transition to the general version that consists of  $n$  agents and is aptly designated as SEQSS <sub>$n$</sub> .

### 3.1. The 3-Player SEQSS<sub>3</sub> Protocol

Let us begin by showcasing the protocol as a game between three players divided into two groups, exactly as we outlined in Section 1. Thus, we will have Alice being the first group and playing the role of the spymaster, tasked with sharing the secret instructions denoted by  $s$  to her agents, and Bob and Charlie comprising the second group and playing the role of said secret agents, who are spatially separated from Alice, but they are both located in the same region of space. The game will start by having all three players share  $m$  triplets of maximally entangled qubits. Each triplet is in the  $|GHZ_3\rangle$  state and Alice, Bob and Charlie possess the qubit  $|q_2\rangle$ ,  $|q_1\rangle$  and  $|q_0\rangle$ , respectively, of the triplet. At this point, it is important to state that there are no limitations on which player will create the GHZ triplets in the first place. The states can be created and distributed accordingly by either Alice, her agents, or even by a third party source, e.g., a satellite [44]. The goal of the current game is for Alice to successfully share her secret message  $s$  with her agents Bob and Charlie. However, the secret message  $s$ , should not be readable by her agents individually. They must both combine their results in order to be able to read it. This task can be successfully accomplished by performing the steps shown below visually in Figure 3 in the form of a quantum circuit.

Furthermore, we point out that each of our three protagonists has a private quantum circuit and the three quantum circuits are similar, in the sense that they all contain an Input Register consisting of  $m$  qubits. Bob and Charlie’s circuits are virtually identical, whereas Alice’s circuit differs because it also contains an Output Register consisting of a single qubit, a Hadamard gate acting on the Output Register and the unitary transform  $U_{f_A}$ , which acts on both her Input and Output Registers. The corresponding qubits in Alice’s, Bob’s and Charlie’s Input Registers constitute a triplet entangled in the  $GHZ_3$  state. Table 1 explains the abbreviations that are used in the quantum circuit depicted in Figure 3.

**Table 1.** This table shows the abbreviations that are used in Figure 3.

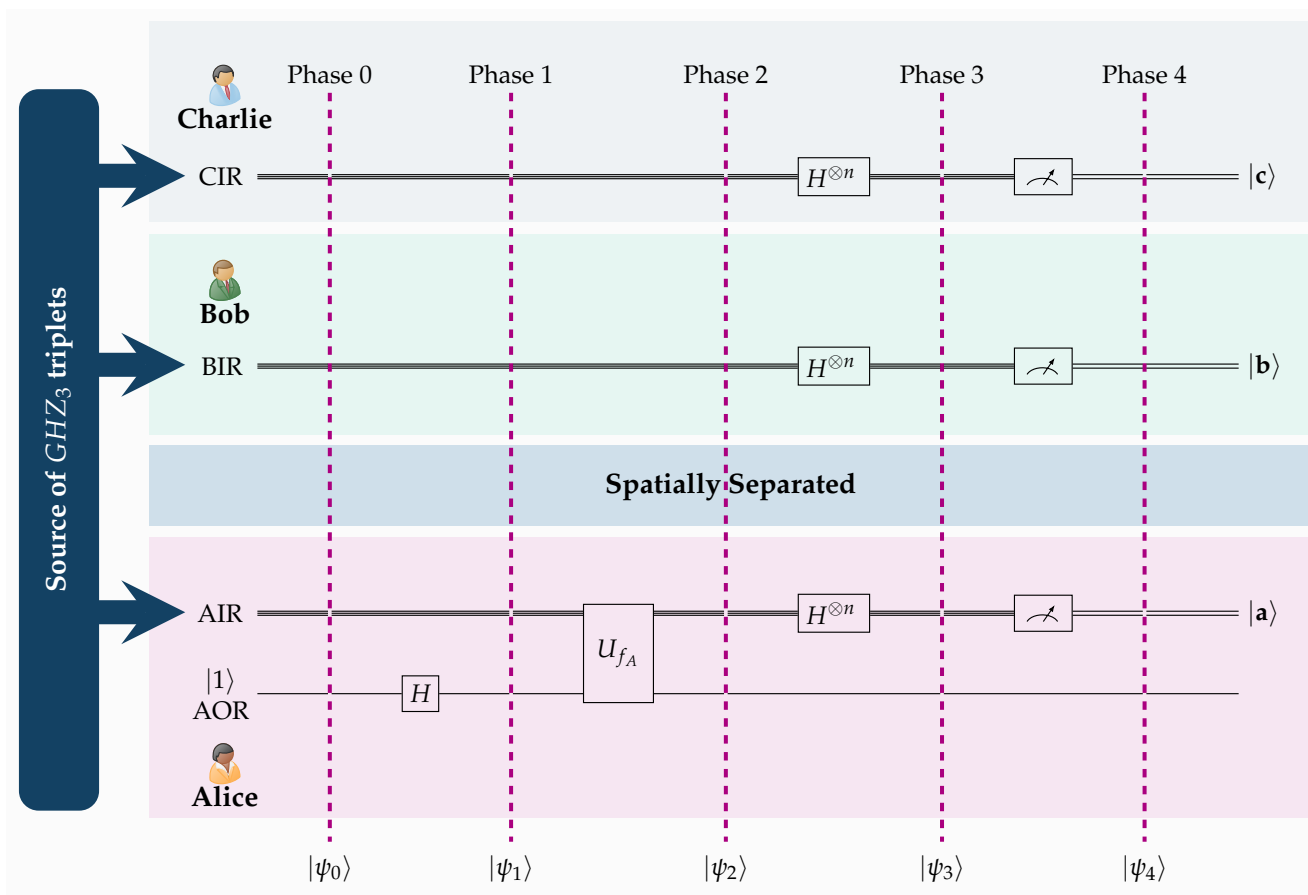
Abbreviations Used in Figure 3		
Abbreviations	Full Name	# of Qubits
AIR	Alice’s Input Register	$m$
AOR	Alice’s Output Register	1
BIR	Bob’s Input Register	$m$
CIR	Charlie’s Input Register	$m$

To describe the resulting composite system, we invoke Formula (2) setting  $n = 3$ . Following the steps of the circuit shown above, we can examine the phases of the algorithm more closely, starting with the initial state  $|\psi_0\rangle$  of the system:

$$|\psi_0\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} |1\rangle_A |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B |\mathbf{x}\rangle_C . \tag{4}$$

As expected,  $|\mathbf{x}\rangle_A$ ,  $|\mathbf{x}\rangle_B$  and  $|\mathbf{x}\rangle_C$  correspond to Alice’s, Bob’s and Charlie’s Input Registers, respectively, representing each player’s part of the GHZ states. Likewise,  $|1\rangle_A$  represents Alice’s Output Register. During our analysis, the subscripts  $A$ ,  $B$  and  $C$  will be consistently used to designate the registers belonging to Alice, Bob and Charlie, respectively. We also emphasize that for consistency we use the Qiskit [45] convention of ordering qubits, where the most significant qubit is the bottom qubit and the least significant qubit is the top qubit.





**Figure 3.** This figure visualizes the quantum circuit implementing the SEQSS<sub>3</sub> protocol.

Continuing to the next phase, Alice effectively initiates the protocol by applying the Hadamard transform to her Output Register. In view of the fact that  $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$ , this produces the ensuing state

$$|\psi_1\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} |-\rangle_A |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B |\mathbf{x}\rangle_C . \tag{5}$$

This will allow Alice to apply her function  $f_A$  on her registers by using the standard scheme:

$$U_{f_A} : |y, \mathbf{x}\rangle \rightarrow |y \oplus f_A(\mathbf{x}), \mathbf{x}\rangle . \tag{6}$$

Consequently, the next state becomes

$$|\psi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{f_A(\mathbf{x})} |-\rangle_A |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B |\mathbf{x}\rangle_C . \tag{7}$$

At this point, we emphasize that Alice’s function is

$$f_A(\mathbf{x}) = \mathbf{s} \cdot \mathbf{x} \text{ mod } 2 , \tag{8}$$

where  $\mathbf{s}$  is the secret message chosen by Alice. Refs. (7) and (8) can be written as

$$|\psi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{\mathbf{s} \cdot \mathbf{x}} |-\rangle_A |\mathbf{x}\rangle_A |\mathbf{x}\rangle_B |\mathbf{x}\rangle_C . \quad (9)$$

Subsequently, Alice, Bob and Charlie apply the  $m$ -fold Hadamard transform to their Input Registers, driving the system into the next state

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{\mathbf{s} \cdot \mathbf{x}} |-\rangle_A H^{\otimes m} |\mathbf{x}\rangle_A H^{\otimes m} |\mathbf{x}\rangle_B H^{\otimes m} |\mathbf{x}\rangle_C \\ &= \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{\mathbf{s} \cdot \mathbf{x}} |-\rangle_A \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{a} \in \{0,1\}^m} (-1)^{\mathbf{a} \cdot \mathbf{x}} |\mathbf{a}\rangle_A \right) \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{b} \in \{0,1\}^m} (-1)^{\mathbf{b} \cdot \mathbf{x}} |\mathbf{b}\rangle_B \right) \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{c} \in \{0,1\}^m} (-1)^{\mathbf{c} \cdot \mathbf{x}} |\mathbf{c}\rangle_C \right) \quad (10) \\ &= \frac{1}{(\sqrt{2^m})^4} \sum_{\mathbf{x} \in \{0,1\}^m} \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{b} \in \{0,1\}^m} \sum_{\mathbf{c} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c}) \cdot \mathbf{x}} |-\rangle_A |\mathbf{a}\rangle_A |\mathbf{b}\rangle_B |\mathbf{c}\rangle_C . \end{aligned}$$

We can observe now that, when

$$\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c} = \mathbf{s} , \quad (11)$$

then  $\forall \mathbf{x} \in \{0,1\}^m$ , the expression  $(-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c}) \cdot \mathbf{x}}$  becomes  $(-1)^0 = 1$ . As a result, the sum  $\sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c}) \cdot \mathbf{x}} = 2^m$ . Whenever  $\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c} \neq \mathbf{s}$ , 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

$$\sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c}) \cdot \mathbf{x}} = 2^m \delta_{\mathbf{s}, \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c}} . \quad (12)$$

Utilizing Equation (12), and ignoring for a moment Alice's Output Register, which is at state  $|-\rangle_A$ , the following three equivalent and symmetric forms can be derived:

$$\sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{b} \in \{0,1\}^m} \sum_{\mathbf{c} \in \{0,1\}^m} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c}) \cdot \mathbf{x}} |\mathbf{a}\rangle_A |\mathbf{b}\rangle_B |\mathbf{c}\rangle_C = 2^m \sum_{\mathbf{b} \in \{0,1\}^m} \sum_{\mathbf{c} \in \{0,1\}^m} |\mathbf{s} \oplus \mathbf{b} \oplus \mathbf{c}\rangle_A |\mathbf{b}\rangle_B |\mathbf{c}\rangle_C \quad (13)$$

$$= 2^m \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{c} \in \{0,1\}^m} |\mathbf{a}\rangle_A |\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{c}\rangle_B |\mathbf{c}\rangle_C \quad (14)$$

$$= 2^m \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{b} \in \{0,1\}^m} |\mathbf{a}\rangle_A |\mathbf{b}\rangle_B |\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{b}\rangle_C \quad (15)$$

By combining (10) with (13)–(15), state  $|\psi_3\rangle$  can be more succinctly written as:

$$|\psi_3\rangle = \frac{1}{2^m} \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{b} \in \{0,1\}^m} \sum_{\mathbf{c} \in \{0,1\}^m} |-\rangle_A |\mathbf{a}\rangle_A |\mathbf{b}\rangle_B |\mathbf{c}\rangle_C , \quad (16)$$

where the states of the three players' Input Registers are always correlated as expressed by the following fundamental property:

$$\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c} = \mathbf{s} \Leftrightarrow \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c} \oplus \mathbf{s} = \mathbf{0} . \quad (17)$$

Finally, Alice, Bob and Charlie measure their GHZ states in their Input Registers obtaining

$$|\psi_4\rangle = |\mathbf{a}\rangle_A |\mathbf{b}\rangle_B |\mathbf{c}\rangle_C , \quad \text{for some } \mathbf{a}, \mathbf{b}, \mathbf{c} \in \{0,1\}^m , \quad (18)$$

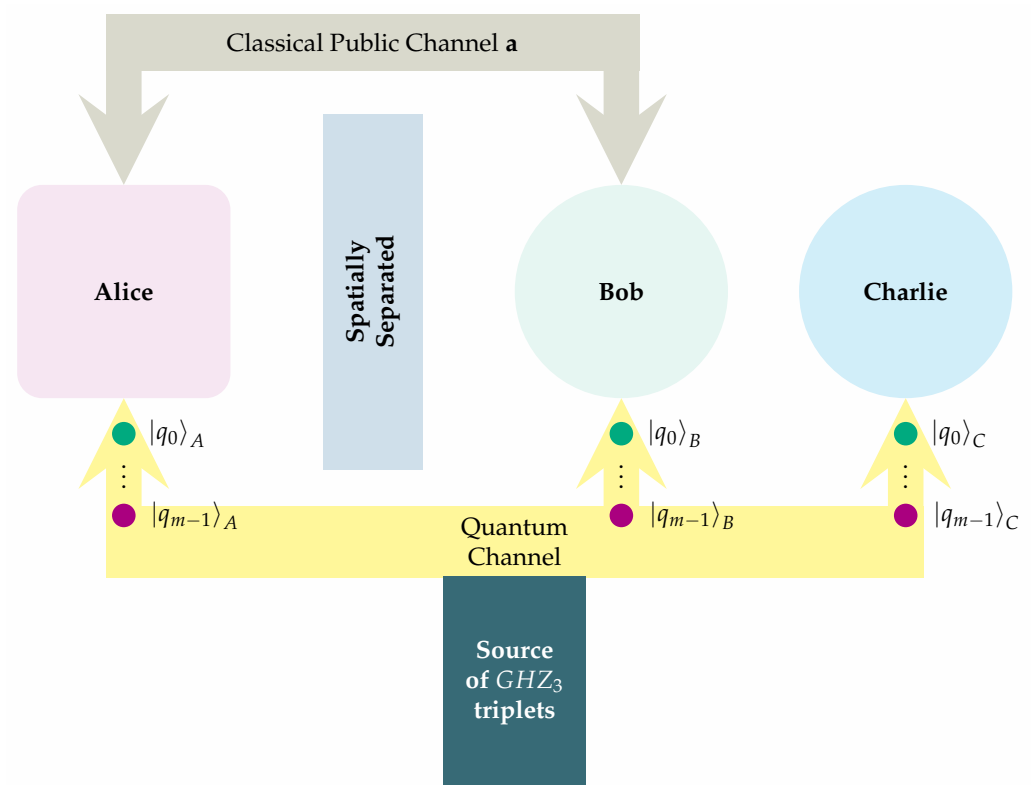
and thus successfully completing the quantum part of the protocol.



We may easily observe that the contents of each of the three Input Registers appear random to Alice, Bob and Charlie, but are, when viewed as a composite system, correlated by the fundamental property (17) of the SEQSS<sub>3</sub> protocol. We now recall that Bob and Charlie are in the same region of space. This implies that they can securely exchange information without using any classical or quantum communication channel. A critical remark is that, even if Bob and Charlie combine their measurements  $\mathbf{b}$  and  $\mathbf{c}$ , they still will not be able to retrieve Alice's secret  $\mathbf{s}$ , unless, of course, it happens that  $\mathbf{a} = \mathbf{0}$ . This last event can happen with probability  $\frac{1}{2^m}$ , which is virtually negligible for large values of  $m$ . Bob and Charlie still need a crucial ingredient from Alice, namely the contents  $\mathbf{a}$  of Alice's Input Register. Hence, we can conclude the protocol by having Alice share her measurement  $\mathbf{a}$  with *anyone* of her agents via a public channel. She can choose either Bob or Charlie without affecting the protocol. Finally, Bob and Charlie, being in possession of  $\mathbf{a}$ , can combine their measurements and obtain the secret message  $\mathbf{s}$ , according to (17).

The part where Alice must share her measurement with her agents after the quantum part of the protocol, can be seen as an advantage, due to the fact that Alice and her agents may perform the quantum part of the protocol at a given time and then have Alice, as the spymaster, determine when will be the right time for her agents to unlock the secret message, by deciding when to broadcast her measurement.

Figure 4 provides a mnemonic visualization of the spatial positions of Alice, Bob and Charlie in the SEQSS<sub>3</sub> protocol, as well as the operation of the quantum and the classical channel.



**Figure 4.** Alice is spatially separated from her agents Bob and Charlie, who are in the same region of space. A third party, the source, creates  $m$  triplets of  $GHZ_3$  entangled qubits and sends one qubit from every triplet to Alice and the remaining two to Bob and Charlie.

### 3.2. The $n$ -Player SEQSS <sub>$n$</sub> Protocol

Now that we have presented the simplest version of the protocol, we can move on to the general version, which can be described as an obvious extension of the SEQSS<sub>3</sub> game, where now Alice's agents are not only two but  $n - 1$ , namely Agent<sub>0</sub>, ..., Agent <sub>$n-2$</sub> . The quantum circuit implementing the SEQSS <sub>$n$</sub>  protocol is depicted in the next Figure 5.

As before, Alice is spatially separated from her  $n - 1$  agents, which are all located in the same region of space. Additionally, we point out that each of the  $n$  players has their own quantum circuit and that the  $n$  quantum circuits are similar, since they all contain an Input Register consisting of  $m$  qubits. All the  $n - 1$  Alice’s secret agents have identical circuits. Alice’s circuit differs because it also contains an Output Register, consisting of a single qubit, upon which a Hadamard gate acts, and the unitary transform  $U_{f_A}$  acting on both her Input and Output Registers. The corresponding qubits in the Input Registers used by Alice and her  $n - 1$  secret agents constitute an  $n$ -tuple entangled in the  $GHZ_n$  state. Table 2 explains the abbreviations that are used in the quantum circuit depicted in Figure 5.

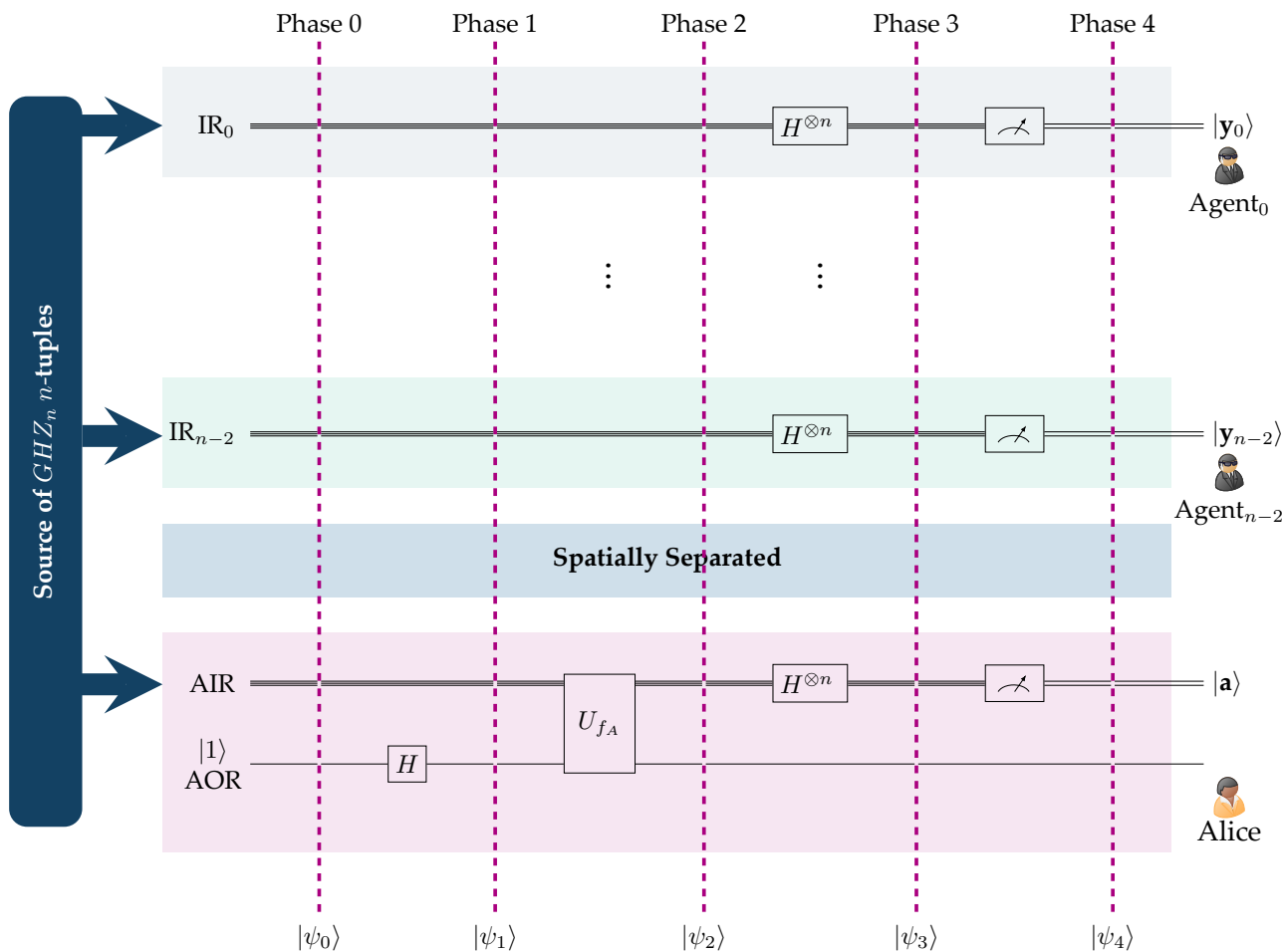


Figure 5. A schematic representation of the quantum circuit implementing the SEQSS<sub>n</sub> protocol.

Table 2. This table shows the abbreviations that are used in Figure 5.

Abbreviations Used in Figure 5		
Abbreviations	Full Name	# of Qubits
AIR	Alice’s Input Register	$m$
AOR	Alice’s Output Register	1
$IR_i, 0 \leq i \leq n - 2$	The Input Register of Agent <sub><math>i</math></sub>	$m$

Once again, following the steps of the circuit shown in Figure 5, we can examine the steps of the algorithm more closely, by starting with the initial state of the system

$$|\psi_0\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} |1\rangle_A |\mathbf{x}\rangle_A |\mathbf{x}\rangle_{n-2} \dots |\mathbf{x}\rangle_0 . \tag{19}$$

As before,  $|\mathbf{x}\rangle_A$  gives the state of Alice’s Input Register,  $|\mathbf{x}\rangle_i, 0 \leq i \leq n - 2$ , represent the states of the Input Registers of the  $n - 1$  agents, and  $|1\rangle_A$  is the state of Alice’s Output Register. In our subsequent analysis, the subscripts  $A, 0, 1, \dots, n - 2$  are consistently used to designate the registers belonging to Alice and Agent<sub>0</sub>, ..., Agent<sub>n-2</sub>, respectively. Thus, we may move on to the next phase, by having Alice initiate the protocol, via the application of the Hadamard transform to her Output Register, which produces the ensuing state

$$|\psi_1\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} |-\rangle_A |\mathbf{x}\rangle_A |\mathbf{x}\rangle_{n-2} \dots |\mathbf{x}\rangle_0 . \tag{20}$$

Akin to the previous version, this will allow Alice to apply her function given by (8) on her registers and lead to the next state, which is

$$|\psi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{\mathbf{s}\cdot\mathbf{x}} |-\rangle_A |\mathbf{x}\rangle_A |\mathbf{x}\rangle_{n-2} \dots |\mathbf{x}\rangle_0 . \tag{21}$$

Afterwards, Alice and all her secret agents apply the  $m$ -fold Hadamard transformation to their Input Registers, driving the system into the next state

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{\mathbf{s}\cdot\mathbf{x}} |-\rangle_A H^{\otimes m} |\mathbf{x}\rangle_A H^{\otimes m} |\mathbf{x}\rangle_{n-2} \dots H^{\otimes m} |\mathbf{x}\rangle_0 \\ &= \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{\mathbf{s}\cdot\mathbf{x}} |-\rangle_A \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{a} \in \{0,1\}^m} (-1)^{\mathbf{a}\cdot\mathbf{x}} |\mathbf{a}\rangle_A \right) \\ &\quad \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} (-1)^{\mathbf{y}_{n-2}\cdot\mathbf{x}} |\mathbf{y}_{n-2}\rangle_{n-2} \right) \dots \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}_0 \in \{0,1\}^m} (-1)^{\mathbf{y}_0\cdot\mathbf{x}} |\mathbf{y}_0\rangle_0 \right) \\ &= \frac{1}{(\sqrt{2^m})^{n+1}} \sum_{\mathbf{x} \in \{0,1\}^m} \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \dots \sum_{\mathbf{y}_0 \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0) \cdot \mathbf{x}} |-\rangle_A |\mathbf{a}\rangle_A |\mathbf{y}_{n-2}\rangle_{n-2} \dots |\mathbf{y}_0\rangle_0 . \end{aligned} \tag{22}$$

The crucial observation now is that, if

$$\mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0 = \mathbf{s} , \tag{23}$$

then  $\forall \mathbf{x} \in \{0,1\}^m$ , the expression  $(-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0) \cdot \mathbf{x}}$  becomes  $(-1)^0 = 1$ . As a result, the sum  $\sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0) \cdot \mathbf{x}} = 2^m$ . Whenever  $\mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0 \neq \mathbf{s}$ , 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, we derive that

$$\sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0) \cdot \mathbf{x}} = 2^m \delta_{\mathbf{s}, \mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0} . \tag{24}$$

Equation (24) leads to the following  $n$  equivalent and symmetric formulations:

$$\begin{aligned} & \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \cdots \sum_{\mathbf{y}_0 \in \{0,1\}^m} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \cdots \oplus \mathbf{y}_0) \cdot \mathbf{x}} |-\rangle_A |\mathbf{a}\rangle_A |\mathbf{y}_{n-2}\rangle_{n-2} \cdots |\mathbf{y}_0\rangle_0 \\ &= 2^m \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \cdots \sum_{\mathbf{y}_0 \in \{0,1\}^m} |-\rangle_A |\mathbf{s} \oplus \mathbf{y}_{n-2} \oplus \cdots \oplus \mathbf{y}_0\rangle_A |\mathbf{y}_{n-2}\rangle_{n-2} \cdots |\mathbf{y}_0\rangle_0 \end{aligned} \quad (25)$$

$$= 2^m \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-3} \in \{0,1\}^m} \cdots \sum_{\mathbf{y}_0 \in \{0,1\}^m} |-\rangle_A |\mathbf{a}\rangle_A |\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{y}_{n-3} \oplus \cdots \oplus \mathbf{y}_0\rangle_{n-2} |\mathbf{y}_{n-3}\rangle_{n-3} \cdots |\mathbf{y}_0\rangle_0 \quad (26)$$

$$\begin{aligned} & \cdots \\ &= 2^m \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \cdots \sum_{\mathbf{y}_1 \in \{0,1\}^m} |-\rangle_A |\mathbf{a}\rangle_A |\mathbf{y}_{n-2}\rangle_{n-2} \cdots |\mathbf{y}_1\rangle_1 |\mathbf{s} \oplus \mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \cdots \oplus \mathbf{y}_1\rangle_0 \end{aligned} \quad (27)$$

By combining (22) with (25)–(27), we can write state  $|\psi_3\rangle$  in a compact way as

$$|\psi_3\rangle = \frac{1}{(\sqrt{2^m})^{n-1}} \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \cdots \sum_{\mathbf{y}_0 \in \{0,1\}^m} |-\rangle_A |\mathbf{a}\rangle_A |\mathbf{y}_{n-2}\rangle_{n-2} \cdots |\mathbf{y}_0\rangle_0, \quad (28)$$

where the states of all the  $n$  players' Input Registers are always correlated as dictated by the fundamental property

$$\mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \cdots \oplus \mathbf{y}_0 = \mathbf{s} \quad \Leftrightarrow \quad \mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \cdots \oplus \mathbf{y}_0 \oplus \mathbf{s} = \mathbf{0}. \quad (29)$$

Finally, Alice and her secret agents Agent<sub>0</sub>, ..., Agent<sub>n-2</sub> measure their GHZ states in their Input Registers obtaining

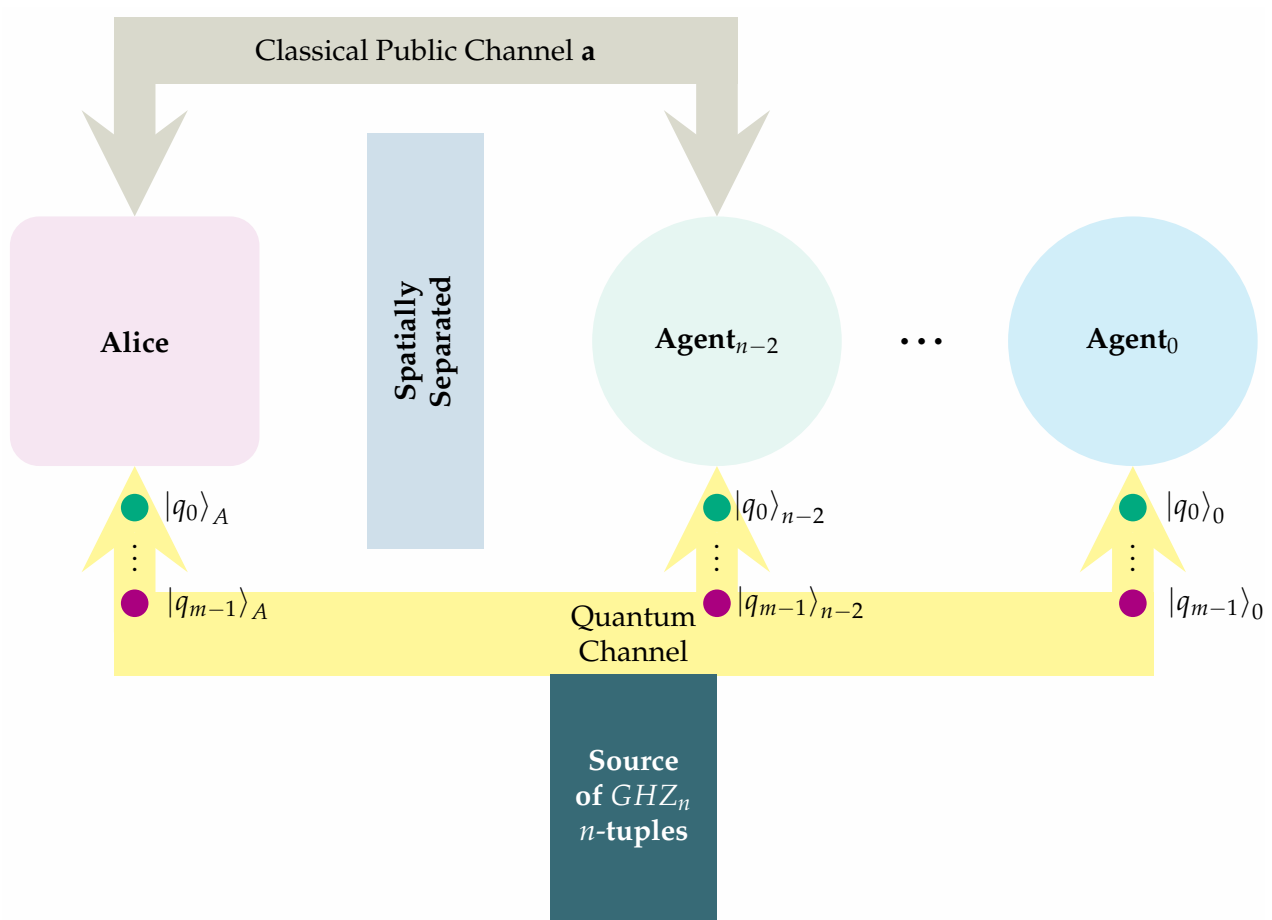
$$|\psi_4\rangle = |\mathbf{a}\rangle_A |\mathbf{y}_{n-2}\rangle_{n-2} \cdots |\mathbf{y}_0\rangle_0, \quad \text{for some } \mathbf{a}, \mathbf{y}_0, \dots, \mathbf{y}_{n-2} \in \{0,1\}^m, \quad (30)$$

which completes the quantum part of the SEQSS<sub>n</sub> protocol.

In this most general case, we encounter the same motif we saw in the case of the three players. In particular, although the contents of each of the  $n$  Input Registers appear random to Alice and her secret agents, when viewed as a composite system, they are correlated by the fundamental property (29) of the SEQSS<sub>n</sub> protocol. The fact that all of Alice's agents are in the same geographical region implies that they can securely exchange information without using any classical or quantum communication channel. However, even if all the  $n - 1$  secret agents combine their measurements  $\mathbf{y}_0, \dots, \mathbf{y}_{n-2}$ , they will still not be able to retrieve Alice's secret  $\mathbf{s}$ , unless, of course, it happens that  $\mathbf{a} = \mathbf{0}$ . This last event can happen with probability  $\frac{1}{2^m}$ , which tends to zero as  $m$  increases. Alice's agents lack a crucial ingredient from Alice, namely the contents  $\mathbf{a}$  of Alice's Input Register. Hence, we can conclude the protocol by having Alice share her measurement  $\mathbf{a}$  with *anyone* of her  $n - 1$  agents via a public channel. She can choose either one of them without affecting the protocol. Finally, the  $n - 1$  secret agents, being in possession of  $\mathbf{a}$ , can combine their measurements and obtain the secret message  $\mathbf{s}$ , according to (29).

Let us again stress that Alice may share her measurement with *anyone* of her agents. This is undoubtedly an important advantage of the protocol, due to the fact that Alice and her agents may perform the quantum part of the protocol at a given time and then have Alice, as the spymaster, determine when will be the right time for her agents to unlock the secret message, by deciding when to broadcast her measurement. Furthermore, the broadcast of Alice's measurement via a public channel, will not hinder the security of the protocol because, even if Eve is present, she will still need the rest of the measurements, in order to retrieve the secret message  $\mathbf{s}$ .

Figure 6 presents a mnemonic representation of the SEQSS<sub>n</sub> protocol, together with the operation of the quantum and classical channels.



**Figure 6.** Alice is spatially separated from her  $n - 1$  agents, who are in the same region of space. A possibly different entity, the source, creates  $m$   $n$ -tuples of  $GHZ_n$  entangled qubits and sends one qubit from every  $n$ -tuple to Alice and her  $n - 1$  secret agents.

#### 4. Security Analysis of the Protocol

In this section, we provide a brief security analysis of the SEQSS protocol, against certain known types of attacks that Eve can employ, in an attempt to acquire vital information and break the confidentiality of the protocol. The SEQSS protocol is an entanglement-based protocol, which allows Alice to secretly transmit information to her agents with the use of entangled GHZ qubits. Therefore, the security of our protocol can be assured by a plethora of well-established phenomena, namely, the monogamy of entangled particles, the no cloning theorem and non-locality. Furthermore, it is important to state that Eve's goal here is only to acquire the measurements of the secret agents. This is because, during the final stage of the protocol, Alice will publicly share her measurement with her secret agents, in order for them to unlock the secret message. Now, in order to further establish the security of the protocol, we will consider the following attack strategies.

##### 4.1. Measure and Resend Attack

In this attack, Eve's strategy is to intercept the GHZ tuples during their transmission from the source to the players, measure them and then resend them back to the players. In this attack, Eve will not acquire any information, due to the fact that the GHZ tuples during the transmission phase will not be carrying any information—thus rendering this strategy ineffective against the protocol.

#### 4.2. Intercept and Resend Attack

This is one of the oldest strategies for Eve to gain any valuable information from the protocol and the way this strategy works is by having Eve intercept the transmitted GHZ tuples, then measure them in the computational basis with the goal of gaining valuable information and, finally, send the new cloned GHZ qubits to the players. As we mentioned above, Eve will not gain any information, simply because the GHZ tuples at the transmission phase do not contain any information about the secret message. Additionally, the no cloning theorem prohibits the ability to create clones of the intercepted qubits without destroying them.

#### 4.3. Entangle and Measure Attack

In this attack, Eve’s strategy is to intercept the transmitted GHZ qubits that are heading to the secret agents. Only now, instead of measuring them, as we saw above, she will entangle them with her ancilla state, prepared in some state  $|E\rangle$  determined by Eve, by performing a unitary operation  $U$  on the composite system and then send the GHZ qubits to the secret agents. Finally, Eve will wait for the protocol to complete and then measure her qubits in order to acquire useful information about the secret message. In order to analyze this attack, we consider the worst case scenario, wherein Eve is already in an advantageous position, by assuming that, instead of intercepting the GHZ states, she will be the one who will create them, along with an extra tuple for herself and distribute them to the rest of the players. Therefore, rather than having  $|GHZ_n\rangle^{\otimes m}$  states for the  $n$  players, we will have  $|GHZ_{n+1}\rangle^{\otimes m}$  states for the  $n$  players plus Eve. Furthermore, we will assume that, in this scenario, Eve can also perform her own unitary transform  $U'_f$  just like Alice. Thus, we begin our scenario in the initial state  $\psi_0$  of the system:

$$|\psi_0\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} |1\rangle_A |1\rangle_E |\mathbf{x}\rangle_A |\mathbf{x}\rangle_E |\mathbf{x}\rangle_{n-2} \dots |\mathbf{x}\rangle_0 . \tag{31}$$

Starting in a similar fashion as the  $SEQSS_n$  protocol presented in the previous section,  $|\mathbf{x}\rangle_A$  and  $|1\rangle_A$  represent Alice’s Input and Output Registers, respectively,  $|\mathbf{x}\rangle_i, 0 \leq i \leq n - 2$ , represent the states of the Input Registers of the  $n - 1$  agents, and  $|\mathbf{x}\rangle_E$  and  $|1\rangle_E$  represent Eve’s Input and Output Registers respectively. As before, the subscripts  $A, 0, 1, \dots, n - 2, E$  will consistently be used to designate the registers belonging to Alice, her Agents, and Eve respectively. Thus, we proceed to the next phase, by having Alice and Eve initiate the protocol by having both apply the Hadamard transform to their Output Registers, which will produce the following state:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} |-\rangle_A |-\rangle_E |\mathbf{x}\rangle_A |\mathbf{x}\rangle_E |\mathbf{x}\rangle_{n-2} \dots |\mathbf{x}\rangle_0 . \tag{32}$$

Next, Alice and Eve will have the ability to apply their functions given by (8) on their registers. In this scenario,  $\mathbf{s}$  and  $\mathbf{s}_E$  represent Alice’s secret message and Eve’s input string, respectively, that leads to the next state, which is

$$|\psi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{\mathbf{s} \cdot \mathbf{x}} (-1)^{\mathbf{s}_E \cdot \mathbf{x}} |-\rangle_A |-\rangle_E |\mathbf{x}\rangle_A |\mathbf{x}\rangle_E |\mathbf{x}\rangle_{n-2} \dots |\mathbf{x}\rangle_0 . \tag{33}$$

Afterwards, everyone can apply the  $m$ -fold Hadamard transformation to their Input Registers, driving the system into the next state



$$\begin{aligned}
 |\psi_3\rangle &= \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{\mathbf{s} \cdot \mathbf{x}} (-1)^{\mathbf{s}_E \cdot \mathbf{x}} |-\rangle_A |-\rangle_E H^{\otimes m} |\mathbf{x}\rangle_A H^{\otimes m} |\mathbf{x}\rangle_E H^{\otimes m} |\mathbf{x}\rangle_{n-2} \dots H^{\otimes m} |\mathbf{x}\rangle_0 \\
 &= \frac{1}{\sqrt{2^m}} \sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{s}_E) \cdot \mathbf{x}} |-\rangle_A |-\rangle_E \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{a} \in \{0,1\}^m} (-1)^{\mathbf{a} \cdot \mathbf{x}} |\mathbf{a}\rangle_A \right) \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{e} \in \{0,1\}^m} (-1)^{\mathbf{e} \cdot \mathbf{x}} |\mathbf{e}\rangle_E \right) \\
 &\quad \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} (-1)^{\mathbf{y}_{n-2} \cdot \mathbf{x}} |\mathbf{y}_{n-2}\rangle_{n-2} \right) \dots \left( \frac{1}{\sqrt{2^m}} \sum_{\mathbf{y}_0 \in \{0,1\}^m} (-1)^{\mathbf{y}_0 \cdot \mathbf{x}} |\mathbf{y}_0\rangle_0 \right) \\
 &= \frac{1}{(\sqrt{2^m})^{n+1}} \sum_{\mathbf{x} \in \{0,1\}^m} \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{e} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \dots \sum_{\mathbf{y}_0 \in \{0,1\}^m} \\
 &\quad (-1)^{(\mathbf{s} \oplus \mathbf{s}_E \oplus \mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0) \cdot \mathbf{x}} |-\rangle_A |-\rangle_E |\mathbf{a}\rangle_A |\mathbf{e}\rangle_E |\mathbf{y}_{n-2}\rangle_{n-2} \dots |\mathbf{y}_0\rangle_0 .
 \end{aligned} \tag{34}$$

Again, the crucial observation now is that, if

$$\mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0 = \mathbf{s} \oplus \mathbf{s}_E , \tag{35}$$

then  $\forall \mathbf{x} \in \{0,1\}^m$ , the expression  $(-1)^{(\mathbf{s} \oplus \mathbf{s}_E \oplus \mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0) \cdot \mathbf{x}}$  becomes  $(-1)^0 = 1$ . As a result, the sum  $\sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{s}_E \oplus \mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0) \cdot \mathbf{x}} = 2^m$ . Whenever  $\mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0 \neq \mathbf{s} \oplus \mathbf{s}_E$ , 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, we derive that

$$\sum_{\mathbf{x} \in \{0,1\}^m} (-1)^{(\mathbf{s} \oplus \mathbf{s}_E \oplus \mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0) \cdot \mathbf{x}} = 2^m \delta_{\mathbf{s} \oplus \mathbf{s}_E, \mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0} . \tag{36}$$

Equation (36) leads to the following  $n$  equivalent and symmetric formulations.

$$\begin{aligned}
 &\sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{e} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \dots \sum_{\mathbf{y}_0 \in \{0,1\}^m} \sum_{\mathbf{x} \in \{0,1\}^m} \\
 &\quad (-1)^{(\mathbf{s} \oplus \mathbf{s}_E \oplus \mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0) \cdot \mathbf{x}} |-\rangle_A |-\rangle_E |\mathbf{a}\rangle_A |\mathbf{e}\rangle_E |\mathbf{y}_{n-2}\rangle_{n-2} \dots |\mathbf{y}_0\rangle_0 \\
 &= 2^m \sum_{\mathbf{e} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \dots \sum_{\mathbf{y}_0 \in \{0,1\}^m} |-\rangle_A |-\rangle_E \\
 &\quad |\mathbf{s} \oplus \mathbf{s}_E \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0\rangle_A |\mathbf{e}\rangle_E |\mathbf{y}_{n-2}\rangle_{n-2} \dots |\mathbf{y}_0\rangle_0
 \end{aligned} \tag{37}$$

$$\begin{aligned}
 &= 2^m \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-3} \in \{0,1\}^m} \dots \sum_{\mathbf{y}_0 \in \{0,1\}^m} |-\rangle_A |-\rangle_E \\
 &\quad |\mathbf{a}\rangle_A |\mathbf{s} \oplus \mathbf{s}_E \oplus \mathbf{a} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0\rangle_E |\mathbf{y}_{n-2}\rangle_{n-2} \dots |\mathbf{y}_0\rangle_0
 \end{aligned} \tag{38}$$

$$\begin{aligned}
 &= 2^m \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{e} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \dots \sum_{\mathbf{y}_1 \in \{0,1\}^m} |-\rangle_A |-\rangle_E \\
 &\quad |\mathbf{a}\rangle_A |\mathbf{e}\rangle_E |\mathbf{y}_{n-2}\rangle_{n-2} \dots |\mathbf{y}_1\rangle_1 |\mathbf{s} \oplus \mathbf{s}_E \oplus \mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_1\rangle_0
 \end{aligned} \tag{39}$$

By combining (34) with (37)–(39), we can write state  $|\psi_3\rangle$  in a compact way as

$$|\psi_3\rangle = \frac{1}{(\sqrt{2^m})^n} \sum_{\mathbf{a} \in \{0,1\}^m} \sum_{\mathbf{e} \in \{0,1\}^m} \sum_{\mathbf{y}_{n-2} \in \{0,1\}^m} \dots \sum_{\mathbf{y}_0 \in \{0,1\}^m} |-\rangle_A |-\rangle_E |\mathbf{a}\rangle_A |\mathbf{e}\rangle_E |\mathbf{y}_{n-2}\rangle_{n-2} \dots |\mathbf{y}_0\rangle_0 , \tag{40}$$

where the states of all the  $n$  players' plus Eve's Input Registers are always correlated as dictated by the fundamental property

$$\mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0 = \mathbf{s} \oplus \mathbf{s}_E \iff \mathbf{a} \oplus \mathbf{e} \oplus \mathbf{y}_{n-2} \oplus \dots \oplus \mathbf{y}_0 \oplus \mathbf{s} \oplus \mathbf{s}_E = \mathbf{0} . \tag{41}$$

Finally, Alice, her secret agents  $\text{Agent}_0, \dots, \text{Agent}_{n-2}$  and Eve can measure their GHZ states in their Input Registers obtaining

$$|\psi_4\rangle = |\mathbf{a}\rangle_A |\mathbf{e}\rangle_E |y_{n-2}\rangle_{n-2} \dots |y_0\rangle_0, \quad \text{for some } \mathbf{a}, \mathbf{e}, y_0, \dots, y_{n-2} \in \{0, 1\}^m. \quad (42)$$

From the above procedure, we can make several important observations about Eve's measurement. Starting with (37)–(39), from which it is easy to see that Eve will measure  $\mathbf{e}$ , which in fact is Alice's message XORed with Eve's input string and the random variables measured by the  $n - 1$  agents. Therefore, even if Eve manages to take part in the procedure, she will not be able to acquire any useful information about the secret message  $\mathbf{s}$ . Additionally, after the completion of the quantum part of the protocol, when the players will try to combine their measurements, in order to unlock the secret message, they will realize that they are not able to unlock the secret message  $\mathbf{s}$  because they will still need Eve's measurement. Hence, in that case, they will be alerted about the fact that Eve tampered with the procedure.

#### 4.4. Blinding Attack

In this attack, Eve's strategy is not to intercept the transmitted GHZ qubits, but actually block them entirely from ever reaching the intended players and then create her own GHZ qubits and transmit these to the players. Of course, it is clear that this strategy only works if the players rely on a third party for the creating and distribution of the GHZ states. However, even if that is the case, Eve will not be able to acquire any information by having her own qubits entangled in the system, due to the fact that, in our protocol, she will be considered as an extra player and she will still need the measurements of the other players, in order to unlock the secret message.

## 5. Discussion and Conclusions

In this paper, we proposed a new entanglement-based QSS protocol, called SEQSS $_n$ , that relies on the use of maximally entangled GHZ tuples, evenly distributed among the players, giving the spymaster Alice the ability to securely share a secret message with her agents, in a simple and symmetric way, since all her agents are treated similarly, utilizing identical quantum circuits. We presented in great detail the simplest version of the protocol and afterwards we continued our analysis with the general version involving  $n$  players, thus proving its scalability to as many players as necessary. Moreover, we showed that our proposal can give a rather useful advantage to Alice that plays the role of the spymaster and is responsible for the transmission of the secret message  $\mathbf{s}$ , by giving her the ability to decide when the rest of the players will have access to the message, even at a time instant after the completion of the quantum part of the protocol. Next, we presented a brief security analysis against a number of known attack strategies, in order to further establish the reliability of our protocol. However, we believe that, as a future work, a more exhaustive and detailed security analysis of the protocol, along with its performance analysis, will prove beneficial to further test and guarantee its reliability.

**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.; writing—review and editing, T.A.; visualization, M.A.; supervision, T.A.; project administration, T.A. and M.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:** Not Applicable, the study does not report any data.

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

## References

1. 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).
2. 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]
3. 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.
4. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef]
5. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829. [CrossRef]
6. Cleve, R.; Gottesman, D.; Lo, H.K. How to share a quantum secret. *Phys. Rev. Lett.* **1999**, *83*, 648. [CrossRef]
7. Karlsson, A.; Koashi, M.; Imoto, N. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **1999**, *59*, 162. [CrossRef]
8. Smith, A.D. Quantum secret sharing for general access structures. *arXiv* **2000**, arXiv:quant-ph/0001087.
9. Gottesman, D. Theory of quantum secret sharing. *Phys. Rev. A* **2000**, *61*, 042311. [CrossRef]
10. Bandyopadhyay, S. Teleportation and secret sharing with pure entangled states. *Phys. Rev. A* **2000**, *62*, 012308. [CrossRef]
11. Xiao, L.; Long, G.L.; Deng, F.G.; Pan, J.W. Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A* **2004**, *69*, 052307. [CrossRef]
12. Fortescue, B.; Gour, G. Reducing the quantum communication cost of quantum secret sharing. *IEEE Trans. Inf. Theory* **2012**, *58*, 6659–6666. [CrossRef]
13. 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]
14. Senthoo, K.; Sarvepalli, P.K. Theory of communication efficient quantum secret sharing. *IEEE Trans. Inf. Theory* **2022**, *68*, 3164–3186. [CrossRef]
15. Tittel, W.; Zbinden, H.; Gisin, N. Experimental demonstration of quantum secret sharing. *Phys. Rev. A* **2001**, *63*, 042301. [CrossRef]
16. Bogdanski, J.; Rafiei, N.; Bourennane, M. Experimental quantum secret sharing using telecommunication fiber. *Phys. Rev. A* **2008**, *78*, 062307. [CrossRef]
17. Bell, B.; Markham, D.; Herrera-Martí, D.; Marin, A.; Wadsworth, W.; Rarity, J.; Tame, M. Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.* **2014**, *5*, 1–12. [CrossRef] [PubMed]
18. 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]
19. Wu, X.; Wang, Y.; Huang, D. Passive continuous-variable quantum secret sharing using a thermal source. *Phys. Rev. A* **2020**, *101*, 022301. [CrossRef]
20. Grice, W.P.; Qi, B. Quantum secret sharing using weak coherent states. *Phys. Rev. A* **2019**, *100*, 022339. [CrossRef]
21. 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]
22. Tavakoli, A.; Herbauts, I.; Żukowski, M.; Bourennane, M. Secret sharing with a single d-level quantum system. *Phys. Rev. A* **2015**, *92*, 030302. [CrossRef]
23. Pinnell, J.; Nape, I.; de Oliveira, M.; TabeBordbar, N.; Forbes, A. Experimental Demonstration of 11Dimensional 10-Party Quantum Secret Sharing. *Laser Photonics Rev.* **2020**, *14*, 2000012. [CrossRef]
24. 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]
25. Hsu, L.Y. Quantum secret-sharing protocol based on Grover's algorithm. *Phys. Rev. A* **2003**, *68*, 022306. [CrossRef]
26. Hao, L.; Wang, C.; Long, G.L. Quantum secret sharing protocol with four state Grover algorithm and its proof-of-principle experimental demonstration. *Opt. Commun.* **2011**, *284*, 3639–3642. [CrossRef]
27. Yu, Z. The Improved Quantum Secret Sharing Protocol Based on Grover Algorithm. *J. Phys. Conf. Ser.* **2022**, *2209*, 012031. [CrossRef]
28. Nagata, K.; Nakamura, T. The Deutsch-Jozsa Algorithm Can Be Used for Quantum Key Distribution. *OALib* **2015**, *2*, e1798. [CrossRef]
29. Nagata, K.; Nakamura, T.; Geurdes, H.; Batle, J.; Abdalla, S.; Farouk, A. Quantum Communication Based on Simon's Algorithm. *Int. J. Emerg. Eng. Res. Technol.* **2017**, *5*, 28–31.
30. Nagata, K.; Nakamura, T. Quantum Cryptography, Quantum Communication, and Quantum Computer in a Noisy Environment. *Int. J. Theor. Phys.* **2017**, *56*, 2086–2100. [CrossRef]
31. Nguyen, D.M.; Kim, S. Quantum Key Distribution Protocol Based on Modified Generalization of Deutsch-Jozsa Algorithm in d-level Quantum System. *Int. J. Theor. Phys.* **2019**, *58*, 71–82. [CrossRef]
32. IBM. IBM Quantum Roadmap. Available online: <https://research.ibm.com/blog/ibm-quantum-roadmap-2025> (accessed on 27 July 2022).
33. Curcic, T.; Filipkowski, M.E.; Chtchelkanova, A.; D'Ambrosio, P.A.; Wolf, S.A.; Foster, M.; Cochran, D. Quantum networks: From quantum cryptography to quantum architecture. *ACM SIGCOMM Comput. Commun. Rev.* **2004**, *34*, 3–8. [CrossRef]
34. Ampatzis, M.; Andronikos, T. QKD Based on Symmetric Entangled Bernstein-Vazirani. *Entropy* **2021**, *23*, 870. [CrossRef]

35. Meyer, D.A. Quantum strategies. *Phys. Rev. Lett.* **1999**, *82*, 1052. [[CrossRef](#)]
36. Eisert, J.; Wilkens, M.; Lewenstein, M. Quantum games and quantum strategies. *Phys. Rev. Lett.* **1999**, *83*, 3077. [[CrossRef](#)]
37. 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](#)]
38. Andronikos, T.; Sirokofskich, A. The Connection between the PQ Penny Flip Game and the Dihedral Groups. *Mathematics* **2021**, *9*, 1115. [[CrossRef](#)]
39. Andronikos, T. Conditions that enable a player to surely win in sequential quantum games. *Quantum Inf. Process.* **2022**, *21*, 268. [[CrossRef](#)]
40. 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](#)]
41. 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](#)]
42. Andronikos, T.; Stefanidakis, M. A Two-Party Quantum Parliament. *Algorithms* **2022**, *15*, 62. [[CrossRef](#)]
43. IBM. IBM Quantum Composer. Available online: <https://quantum-computing.ibm.com/composer> (accessed on 3 April 2022).
44. Aspelmeyer, M.; Jennewein, T.; Pfennigbauer, M.; Leeb, W.R.; Zeilinger, A. Long-distance quantum communication with entangled photons using satellites. *IEEE J. Sel. Top. Quantum Electron.* **2003**, *9*, 1541–1551. [[CrossRef](#)]
45. Qiskit. Qiskit Open-Source Quantum Development. Available online: <https://qiskit.org> (accessed on 3 April 2022).