Security of a secret sharing protocol on the Qline

Alex B. Grilo[1], Lucas Hanouz[1,2,*] and Anne Marin[2]

[1] Sorbonne Université, CNRS, LIP6, Paris, France
[2] VeriQloud, Paris, France
[*] Corresponding author: lucas.hanouz@lip6.fr

Abstract. Secret sharing is a fundamental primitive in cryptography, and it can be achieved even with perfect security. However, the distribution of shares requires computational assumptions, which can compromise the overall security of the protocol. While traditional Quantum Key Distribution (QKD) can maintain security, its widespread deployment in general networks would incur prohibitive costs.
In this work, we present a quantum protocol for distributing additive secret sharing of 0, which we prove to be composably secure within the Abstract Cryptography framework. Moreover, our protocol targets the Qline, a recently proposed quantum network architecture designed to simplify and reduce the cost of quantum communication. Once the shares are distributed, they can be used to securely perform a wide range of cryptographic tasks, including standard additive secret sharing, anonymous veto, and symmetric key establishment.

Keywords: quantum cryptography · secret sharing

1 Introduction

Secret sharing is a fundamental cryptographic primitive that enables the sharing of a secret among multiple parties, such that only specific predefined sets of shares allow to recover the original secret, while any other sets give no information about it.

While classical secret sharing protocols, such as those introduced by Shamir and Blakley [1, 2], achieve perfect (information-theoretic) security, the effective deployment of secret sharing protocols faces a critical challenge: the shares must be securely distributed to the participants, ensuring their privacy and integrity.

In most cases, the share distribution is secured using standard cryptographic approaches such as public-key encryption, which lowers the overall security of the scheme. More concretely, using classical cryptography to distribute the shares, the security of data transmission holds under structured computational assumptions and cannot achieve the information-theoretic guarantees that secret sharing schemes provide.

This limitation, however, can be circumvented if we consider quantum cryptography. It is now well known that Quantum Key Distribution (QKD) protocols enable the establishment of a secure communication channel from an authenticated classical channel by leveraging the fundamental principles of quantum mechanics [3, 4, 5, 6]. However, while QKD enhances security, its practical implementation introduces significant challenges. Establishing secure channels using QKD requires expensive quantum hardware and suffers from low efficiency. Moreover, scaling such systems to securely distribute the shares of a secret sharing scheme would be prohibitively inefficient, as both the infrastructure needed to support QKD and the required amount of secure communication grows rapidly with the number of participants and communication links.

Recently, a quantum network architecture called *Qline* has been introduced [7] as an attempt to increase the connectivity of QKD networks, reduce their costs and improve their accessibility to end-users. The Qline consists of a standard QKD setup where a single

qubit source and detector are linked, but with intermediate nodes added in between, which only have the ability to perform single-qubit rotations—a task that can be implemented with much cheaper devices. We will call the nodes of the Qline *players* in this work.

Despite having a simpler setup, it has been recently shown that Qline enables several interesting cryptographic protocols. Clementi *et al.* demonstrated a Quantum-enhanced Classical multiparty computation protocol on the Qline [8]. Later, Doosti et al. [7] showed that any pair of player can establish symmetric keys with the same level of security as QKD with the help of trusted end nodes, and Polacchi et al. [9] introduced a protocol for secure multi-client delegated quantum computing for a Qline connected to a quantum computer. In all of these protocols, the main idea is to use Qline to allow a pair of nodes to perform a secure operation (such as communication or computation). We notice that while this can be used to distribute shares of a secret sharing scheme with information-theoretic security more cost-effectively compared to pairwise QKD, it still suffers from a linear overhead on the number of shares for it.

Our main result is to show that additive secret sharing can directly and securely be performed on the Qline without scaling overhead on the shares. The main novelty is to exploit the *global* correlations that Qline provides us to achieve additive secret sharing of 0 (i.e. the message is fixed). We notice that previous works have introduced propositions exploiting this idea[10, 11], but they lack a security proof against general attacks, composable, and under the most general dishonest participant scenarios. On the other hand, we achieve a protocol that we prove to be secure in the composable framework of Abstract Cryptography[12], while preserving the benefits of the Qline architecture regarding simplicity and cost of implementation.

In short, our protocol works as follows. The first player of the Qline sends a random BB84 states[1], each intermediate player re-randomizes the states, and the final player chooses to measure the received qubits in the Hadamard or computational basis uniformly at random. Then, the players perform a classical protocol to check the integrity of the shares and to correct any error incurred by the noise of quantum devices. In order to prove the security of our protocol, we require that at least 2 players are honest (which is natural for additive secret sharing of 0), and that the players share a classical authenticated channel with random subset broadcast (see Section 3.2 for a formal definition and a discussion on how to implement it). The core of the technical contribution is to show that our protocol is secure in a composable way.

This work was primarily motivated by the recent implementation of a Qline at VeriQloud, Paris, France. Our protocol is specifically designed to be compatible with their architecture, and simulations indicate that the sharing between four participants of a 2 Mbit secret can be expected to be achieved in less than 5 minutes on their setup.

To illustrate the protocol's performance, we compare it in Table 1 with the following alternatives of using classical secret sharing, along with either QKD or Qline's key establishment to distribute the shares. In the following table, for each of these alternatives and depending on the number J of players, we show the *cost* (hardware requirement) of an architecture allowing any player to share a secret, and the *efficiency*, measured in the number of required qubits to transmit to share one secret. We use realistic and identical parameters and targeted metrics.

Applications. We describe now some of the applications of the primitive that we implement, i.e. secret sharing of the bit 0, when used along with classical authenticated communication. First, we notice that we can implement standard additive secret sharing where the dealer chooses a secret bit string to share instead of having this value fixed to 0. To achieve such a primitive from shares of 0, the dealer can publish the one-time-pad

[1]In fact, we use the Hadamard Basis and the circular basis, but we prefer to continue the rough exposition with more well-known states.

Table 1: Comparison of solutions with 1.7 Mbits share size and 10^{-11} distinguishing advantage

	QKD + classical secret sharing	**Qline + classical secret sharing**	**Our protocol**
Cost Number of quantum channels	J^2	1	1
Efficiency Number of qubits to receive	$J \times 10^7$	$J \times 10^7$	10^7

encryption of his secret with his share as the key.

Another application is anonymous veto, also known as the Dining Cryptographers Problem [13], which is also the secure multi-party computation of the multiple-input boolean OR function. To achieve anonymous veto from n sharings of 0, the players perform n rounds of announcement with different announcement orders such that each player is last in one round. for all rounds, following the corresponding announcement order, the players broadcast either their share, or a random string instead if they wish to veto. For each round, the sum of the announcements is then compared to the all 0 string: inequality shows that at least one player vetoed. See [14] for a similar construction.

Finally, symmetric key establishment can be achieved by asking all players but two to reveal their share and having one of the two remaining players XOR it's share with all the thereby-revealed ones. Previous works[7] already introduced the corresponding protocol, but their security proof requires the honest collaboration of the end nodes of the network. We discuss in Section 3.2 how, for this particular application, our proof amounts to the same result, *without* this trust assumption.

Remarkably, for these applications, our protocol can be run in an offline phase, to then only in a later online phase, decide the cryptographic task to perform along with the set of involved players and use the shares together with classical authenticated communications to securely produce the desired resources at a high bit rate. This opportunity is all the more meaningful when considering the slow rates imposed by current quantum hardware.

The remainder of the manuscript proceeds as follows. We introduce preliminary information in Section 2. We then present our assumptions in Section 3.1, our protocol in Section 4, and it's security proof in Section 5.

Acknowledgments

We would like to thank Georg Harder and Anthony Leverrier for their valuable assistance regarding the question of syndrome leakage. We thank Céline Chevalier for her guiding insights on technical parts of the proof.

ABG is supported by the European Union's Horizon Europe Framework Program under the Marie Sklodowska Curie Grant No. 101072637, Project Quantum-Safe Internet (QSI). This work is part of HQI initiative (www.hqi.fr) and is supported by France 2030 under the French National Research Agency award number ANR-22-PNCQ-0002. This work was funded by the European Union's Horizon Europe research and innovation program under grant agreement No. 101102140 – QIA Phase 1.

2 Preliminaries

We recall the notation of basic concepts of quantum information theory in Section 2.1. For a more detailed introduction to the topic, we refer to [15]. In Section 2.2, we present the

abstract cryptography framework. Finally, in Section 2.3, we review the Qline architecture.

We defer to Appendix A for a summary of the notation used throughout this paper.

2.1 Quantum information theory

We assume basic knowledge about the theory of quantum communication and computing.

We denote the eigenstates of the Hadamard basis by $|+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)$ and $|-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$. The classical outcome of a measurement in the Hadamard basis yields 0 if $|+\rangle$ is measured and 1 if $|-\rangle$ is measured.

We denote the eigenstates of the circular basis by $|+_i\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + i\,|1\rangle\Big)$ and $|-_i\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - i\,|1\rangle\Big)$ with $i^2 = -1$. By convention in this paper, we consider that the classical outcome of a measurement in the circular basis yields 0 if $|-_i\rangle$ is measured and 1 if $|+_i\rangle$ is measured. This mismatch in the notation between Hadamard and circular basis will improve the clarity of later equations.

We denote the Pauli $\mathbf{Z}$ gate $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$, $\mathbf{Z}^{\frac{1}{2}}$ being the phase gate $\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$.

For a state σ_R on registers R and S, $Tr_R(\sigma_S)$ denotes the state obtained by tracing out the register R.

The trace distance $Tr|\sigma - \gamma|$ is a measure of the distinguishability between two states σ and γ. We write $\sigma \approx_\epsilon \gamma$ when $Tr|\sigma - \gamma| \leq \epsilon$

Throughout this article, we use the term single-qubit state to denote a two-dimensional, potentially mixed, state.

2.2 The abstract cryptography framework

We prove the security of our protocol using the *Abstract Cryptography* framework [12]. This framework is designed to guarantee the composability of the security of cryptographic constructions while remaining as general as possible concerning security notions.

In this framework, cryptographic protocols are defined as systems: abstract objects with *interfaces* that define all possible inputs and outputs of the said system. Each interface represents an entity's access to the system. A cryptographic construction typically includes *player* interfaces, where the interactions between the honest players and the system occur, as well as an adversarial interface, called the *outer* interface, which encapsulates the attacker's capabilities.

Systems can be composed, either in parallel or sequentially. The parallel composition of two systems $\mathcal{R}$ and $\mathcal{S}$, denoted $R||S$, is a system with the interfaces of both sub-systems. It simply describes the fact that these systems are put side by side and seen as a whole, unique system. The behavior of the composed system is naturally defined from the independent behaviors of the sub-systems (c.f Figure 1).

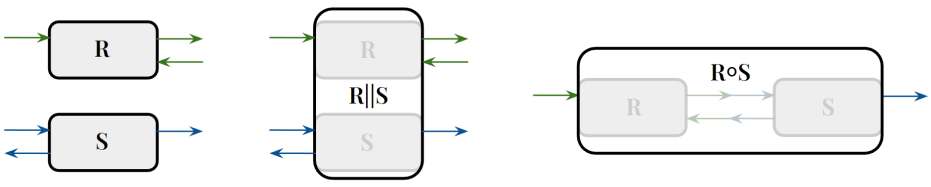

Figure 1: Composition of abstract systems

The sequential composition describes the fact that the output of a system can be used as input by other systems. For instance, two systems $\mathcal{R}$ and $\mathcal{S}$ can be sequentially composed *at the interfaces* $i_{\mathcal{R}}$ *of* $\mathcal{R}$ *and* $j_{\mathcal{S}}$ *of* $\mathcal{S}$ if each input (respectively output) of these interfaces can be associated with a unique output (respectively input) of the other interface. When it is clear at which interfaces a sequential composition occurs, we denote it $R \circ S$ or simply RS without specifying the interfaces i_R and j_S. The resulting system has all the interfaces of both sub-systems except from i_R and j_S.

In this framework, the security of a cryptographic scheme is defined as the "closeness" of that system to an ideal version of it. In this work, this closeness is measured using the *distinguishing* pseudo-metric (as in QKD security proofs [16]), which is defined as the maximum *distinguishing advantage* on two systems, over all computationally unbounded entities (called *distinguishers*). The distinguishing advantage of a distinguisher on two sets of signals (inputs and/or outputs) is the value ϵ such that when given either the first set or the second one with equal probability $\frac{1}{2}$, the distinguisher succeeds in guessing which one it is with probability $\frac{1}{2} + \epsilon$. The distinguishing advantage on two systems P and $\tilde{P}$ is the distinguishing advantage on their inputs and outputs.

We wright $P \approx_\epsilon \tilde{P}$ when the distance (measured by the distinguishing pseudo-metric) between the systems (or signals) P and $\tilde{P}$ is no more than ϵ.

Formally, A protocol P of ideal version $\tilde{P}$ is said to be ϵ-*secure* if there exists a system $\mathcal{SIM}$ called *simulator* such that $P \approx_\epsilon \tilde{P} \circ \mathcal{SIM}$.

The distinguishing pseudo-metric leads to a composable definition of security (Theorem 1 of [12]), meaning that the composition of an ϵ_1-secure and an ϵ_2-secure system is always $(\epsilon_1 + \epsilon_2)$-secure.

2.3 The Qline Architecture

A Qline consists in an initial node that can generate a given range of qubit states, an arbitrary number of intermediate nodes that can apply certain single qubit operations to these qubits, and a final node that can measure them in a chosen basis. An example of a Qline with four players is depicted in Section 2.3.

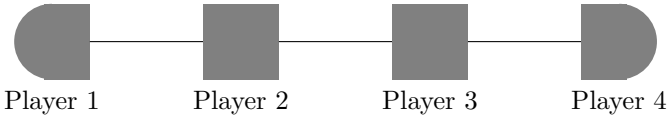

Figure 2: A Qline with four players

In this work, we consider a Qline with the following properties:

- The first node can generate and send the four following states: $|+\rangle$, $|-\rangle$, $|+_i\rangle$, $|-_i\rangle$.
- The intermediate nodes can apply the $\mathbf{Z}^x$ operation to single qubit states, with $x \in \{0, \frac{1}{2}, 1, \frac{3}{2}\}$.
- The last node can measure single qubit states in either the Hadamard or the circular basis.

3 Adversarial model

3.1 Assumptions

We study the security of the protocol under an *active*, *unbounded*, and *participant* adversarial model. This means that we consider that the adversary has access to noiseless, unbounded,

quantum and classical computational power and storage (*unbounded*), that they can attack the protocol during its execution (*active*), and most importantly that they can corrupt parties involved in the protocol, meaning that they take complete control over their knowledge and behavior (*participant*). An uncorrupted player is said to be *honest*.

In order to prove the security of the protocol, we require the following assumptions.

Assumption 1. *At least two players are honest.*

Note that this is a minimal assumption for our use case. Having only one honest player would not achieve any interesting result as the goal of the protocol is precisely that the secret of any player can be recovered using all the other's secrets.

Assumption 2. *Perfect randomness: Each player has access to an independent uniform random number generator.*

Assumption 3. *Sealed laboratories: No unwanted information transfer occurs at the frontier of the honest players laboratories.*

This is arguably the most challenging assumption to ensure in practice. It prevents side-channel attacks, which are inherently difficult to defend against. In particular, this assumption also encompasses that honest players receive and send only single qubit states, meaning that no higher-dimensional states arise when expecting two-dimensional ones.

Assumption 4. *Classical authenticated channel with random subset broadcast.*

We describe Assumption 4 in more details. The players are assumed to have access to a classical communication channel, which allows them to broadcast classical messages to all the other players, while ensuring the three following main features:

1. **Authentication:** The messages going through this channel cannot be tampered with, and come with the identity of the sender.
2. **Random subset broadcast:** Whenever required, the players can perform a *random subset broadcast* over the channel. In this procedure, each player first inputs an ordered list of values, and, in a second stage, the procedure randomly samples a subset of indices for which the corresponding values of all players are revealed and broadcast to everyone. See Section 3.2 for more details.
3. **Distributed coin-flipping:** Whenever required, the players can perform a *distributed coin-flipping* over the channel. This procedure allows the players to agree on a value that is uniformly random and independently sampled. The procedure can abort.

Such a channel is required to prevent potential malicious players to cheat by making choices that depend on the other player's announcements. We further discuss this assumption in Section 3.2 and provide constructions of such a channel using standard assumptions.

3.2 Discussion on Assumption 4

Assumption 4 and in particular the aspect of *random subset broadcast* is rather specific to our work and is unconventional in cryptography. While it could be replaced with other standard computational assumptions, we chose to retain Assumption 4 as we believe it best captures the purpose and significance of the assumption while highlighting the key protocol components that rely on it for security. In this section, we discuss different approaches to satisfy Assumption 4 based on more common assumptions.

Authenticated channel: Authenticated channels are well-studied resources that can be obtained from many different cryptographic solutions and for different paradigms [17, 18, 19, 20]. Remarkably, using pre-shared keys, authenticated channels can be obtained information-theoretically. It is a required assumption in Quantum Key Distribution protocols [2, 3].

Distributed coin-flipping: *distributed coin-flipping* is a protocol in which the participants agree on a random value with the guarantee that the probability distribution of the outcome is uniform, no matter what an adversary tries to do. We refer to [21] for a thorough study of distributed coin-flipping protocols and the required assumptions in our setup.

A particular situation that appears interesting enough to be mentioned is when one honest player is identified. This situation can arise when it has already been decided what the shares are going to be used for. If the goal is for instance to use the shares for the sharing of a document, the document holder is by definition honest. In this case, a simple implementation of the coin-flipping that does not involve any further assumption is to make the honest player sample the random value and simply announce it to the others.

Random subset broadcast: A random subset broadcast is a procedure that breaks down in two stages. In the first stage, each player chooses (and delivers to the procedure) a list of values indexed by a given set S and a unique size s is chosen. In the second stage, a subset of S of size s is randomly sampled and the procedure reveals to all players the values of each list that correspond to this subset, while the other values remain hidden.

A perhaps quite natural construction of such a procedure would be to use a commitment scheme and to ask each player to commit on each of his values in the first stage, to then in the second stage perform a distributed coin flip to randomly sample the subset, and finally to open their commitments of the required values. Commitment schemes rely on the assumption of the existence of a One-Way Function [22]. While this assumption is equivalent to the security of secret key encryption and most currently used implementations of One-way functions are widely believed to be secure even against quantum computers ([23]), relying on one-way functions bottlenecks the security. One must however notice that (if using statistically hiding commitments) the binding of the commitment scheme is only required during the time of the procedure for the final shares to be information-theoretic secure. This property is called *everlasting security* and is highly desirable when seeking long-term security.

A very particular, yet relevant situation is when all honest players are identified. For instance, this occurs when it has already been decided that the shares resulting from the protocol will be used to establish secret symmetric keys between two fixed players, as studied in [7]. In this specific case, a simple implementation of the random subset broadcast procedure that does not involve any computational assumption is as follows: First, all dishonest players broadcast all of their values. Then a honest player samples and announces the subset, and all honest players announce only their values that correspond to the subset.

4 The Protocol

In this section we present a quantum-assisted secret sharing protocol that is supported by the Qline architecture described in Section 2.3. This is the *prepare-and-measure* version of the protocol and we will introduce the entanglement-based version later.

The protocol involves J players, each having exclusive control of one device of the Qline architecture. The players are named according to Section 2.3.

The protocol can be decomposed into two major steps: the *State distribution* step involving quantum communication and the *Post-processing* step which only requires classical computation and communication.

Parameters

The protocol is parameterized by the following variables:

1. A security parameter N.
2. A correctness parameter η.
3. An integer τ' such that $\tau' = \omega(log(N))$ and $\tau' = o(N)$.

State distribution (prepare-and-measure version)

1. Each player $j \in [J]$ samples $2N$ random bits $(b_n^j)_{n\in[N]}$ and $(v_n^j)_{n\in[N]}$ and computes $x_n^j = \frac{b_n^j}{2} + v_n^j$, for all $n \in [N]$.
2. Player 1 generates the state $|\Phi^1\rangle = \bigotimes_{n\in[N]} \mathbf{Z}^{x_n^1} |+\rangle$ and sends it to player 2.
3. Players $j \in \{2, ...J-1\}$ receive a state $\tilde{\Phi}^{j-1}$ from player $j-1$, apply the operation $U^j = \bigotimes_{n\in[N]} \mathbf{Z}^{x_n^j}$ to it and send the resulting state $\Phi^j = U^j \tilde{\Phi}^{j-1} U^{j\dagger}$ to player $j+1$.
4. Player J receives $\tilde{\Phi}^{J-1}$ from player $J-1$, and measures each qubit $n \in [N]$ in either the Hadamard basis if $b_n^j = 0$ or in the circular basis if $b_n^j = 1$. The classical outcome of these measurements are denoted $(v_n^j)_{n\in[N]}$.

Post-processing (part 1)

At any point, if the classical channel fails, the protocol aborts.

1. **Announcements:**
   1.1. The players perform the first stage of two *random subset broadcast* procedures with respectively their basis choices b_n^j and values v_n^j for $n \in [N]$, and then the second stages so that all the values b_n^j for $n \in [N]$ are broadcast to all players, while a random subset $\mathcal{T}'$ of $[N]$ of size τ' is randomly sampled, and only v_n^j for $n \in \mathcal{T}'$ are broadcast.
2. **Sifting:**
   2.1. The players compute the indices of the inconclusive rounds $\mathcal{U} = \left\{ n \in [N] : \bigoplus_{j\in[J]} b_n^j \neq 0 \right\}$ and discard b_n^j and v_n^j where $n \in \mathcal{U}$. We define $L := N - |\mathcal{U}|$ We keep the same notation for the remaining values, but adjust the indices of the rounds:

$$(b_n^j)_{n\in[L],j\in[J]} := (b_n^j)_{n\in[N]\setminus\mathcal{U},j\in[J]}$$
$$(v_n^j)_{n\in[L],j\in[J]} := (v_n^j)_{n\in[N]\setminus\mathcal{U},j\in[J]}$$

   We equivalently adjust the indices of $\mathcal{T}$ such that $\mathcal{T} \subset [L]$ (the rounds in $\mathcal{T}$ are still the rounds previously in $\mathcal{T}' \setminus \mathcal{U}$)

Post-processing (part 2)

3. **Error estimation:**
   3.1. The players compute the *Qubit Error Rate*

$$q = \frac{1}{\tau}\left|\left\{n \in \mathcal{T} : \sum_{j\in[J]} (2v_n^j + b_n^j) = 2 \mod 4\right\}\right| \tag{1}$$

   If $q > \delta$, the parties abort.
   3.2. The players discard b_n^j and v_n^j for each index $n \in \mathcal{T}$. We define $M = L - \tau$ and again adjust the indices such that the remaining values are $(b_n^j)_{n\in[M],j\in[J]}$ and $(v_n^j)_{n\in[M],j\in[J]}$
4. **Error correction:**
   4.1. Player J updates his values $(v_n^j)_{n\in[M]}$ as

$$v_n^j := v_n^j \oplus \left(\frac{1}{2}\Big(\sum_{j\in[J]} b_n^j \mod 4\Big)\right)$$

   4.2. The players agree on an error correction margin $\nu \in [0, \frac{1}{2} - q]$, as well as a *linear* syndrome decoding protocol[2] of correction rate $(q + \nu)$ that they will apply on their respective shares $v_{[M]}^{[J]}$.
   4.3. According to this syndrome decoding protocol, each player $j \in [J-1]$ computes and announces the syndrome w^j of his share $v_{[M]}^J$.
   4.4. Player J corrects it's share $v_{[M]}^J$ through the syndrome decoding protocol using $\bigoplus_{j\in[J]} w^j$ as the correction syndrome.
   4.5. **Correctness check:** The players use the *distributed coin flipping* procedure to randomly sample f_{cc} from a 2-universal family of *linear* hash functions[3] from $\{0,1\}^M$ to $\{0,1\}^\eta$. Each player $j \in [J]$ computes and announces the hash $c^j = f_{cc}(v^j)$ and checks that

$$\bigoplus_{j\in[J]} c^j = 0 \tag{2}$$

   If the check fails, the protocol aborts.
5. **Privacy amplification:**
   5.1. The players agree on an integer $K < M$ and use the *distributed coin flipping* procedure to sample a function f_{pa} from a 2-universal family of *linear* hash functions from $\{0,1\}^M$ to $\{0,1\}^K$. They compute their final share as

$$s^j = f_{pa}(v^j) \tag{3}$$

4.1 Correctness

In this section, we prove the correctness of the protocol. For that, we prove in Proposition 1 that when the protocol succeeds, the produced shares are correct with high probability.

[2]By syndrome decoding, we refer to a protocol allowing one to compute the syndrome of a message, such that the combined knowledge of this syndrome and a noisy version of the message allows (efficient) computation of the original message. Such a syndrome decoding protocol comes with a *correction rate* such that when the noise is less than or equal to that rate, the correction succeeds except with negligible probability in N. Linear syndrome decoding protocols can be derived from linear error correcting codes.

[3]Examples of such 2-universal families of linear hash functions can be found in [24].

Then, in Proposition 2 we show that when the parties are honest the protocol successfully terminates if the noise in the devices is low enough. The correctness highly depends on the correctness parameter η chosen by the players in the protocol during the correctness check step.

Proposition 1. *Let $\epsilon_{cor} = 2^{-\eta}$. Assuming that the protocol successfully terminates, then with probability at least $1 - \epsilon_{cor}$,*

$$\bigoplus_{j\in[J]} s^j = 0. \tag{4}$$

Proof. After the error correction step of a successful execution of the protocol, the correctness check verified that $\bigoplus_{j\in[J]} f_{cc}(v^j) = 0$. Since f_{cc} is sampled from a 2-universal *linear* hash family, the probability that $\bigoplus_{j\in[J]} v^j \neq 0$ is at most $2^{-\eta}$. □

Proposition 2. *If the parties are honest and the depolarizing noise is $\mu < \delta$, then the protocol successfully terminates except with a probability at most negligible in N.*

Proof. The protocol may abort at 3 stages, and we bound each of these probabilities below.

First, the parties would abort during sifting if $\tau < \frac{\tau'}{4}$. As the player's basis choices are uniformly random, the probability for each round $n \in [N]$ that $\bigoplus_{j\in[J]} b_n^j = 0$ is $\frac{1}{2}$. Hence, by Hoeffding's bound, except with probability at most $e^{-\frac{\tau'}{8}}$, $\tau \geq \frac{\tau'}{4}$. Similarly, except with independent probability at most $e^{-\frac{N-\tau'}{8}}$, $M \geq \frac{N-\tau'}{4}$. Both happen with probability at least $p_1 < e^{-\frac{\tau'}{8}} + e^{-\frac{N-\tau'}{8}}$.

Secondly, the parties abort during error estimation if $q > \delta$. During the state distribution step in an ideal noiseless case, for all $n \in [N]$, player J is expected to measure the state

$$\mathbf{Z}^{\left(\sum_{j\in[J-1]} v_n^j - \frac{1}{2} b_n^j\right)} |+\rangle = \mathbf{Z}^{\bigoplus_{j\in[J-1]} v_n^j} \mathbf{Z}^{-\frac{1}{2}\sum_{j\in[J-1]} b_n^j} |+\rangle$$
$$= \begin{cases} \mathbf{Z}^{\left(\bigoplus_{j\in[J-1]} v_n^j\right)\oplus\left(\frac{1}{2}\left(\sum_{j\in[J-1]} b_n^j \mod 4\right)\right)} |+\rangle & \text{if } \bigoplus_{j\in[J-1]} b_n^j = 0 \\ \mathbf{Z}^{\left(\bigoplus_{j\in[J-1]} v_n^j\right)\oplus\left(\frac{1}{2}\left(1+\sum_{j\in[J-1]} b_n^j \mod 4\right)\right)} |+_i\rangle & \text{if } \bigoplus_{j\in[J-1]} b_n^j = 1 \end{cases}$$

where the first equality comes from the facts that $\mathbf{Z}^2 = I$ and $Z^{a+b} = Z^a Z^b$.

As a consequence, for all $n \in [N]$ where player J chooses the basis $b_n^J = \bigoplus_{j\in[J-1]} b_n^j$ for his measurement, they should in principle obtain the following result deterministically:

$$v_n^J = \Big(\bigoplus_{j\in[J-1]} v_n^j\Big) \oplus \Big(\frac{1}{2}\big(b_n^J + \sum_{j\in[J-1]} b_n^j \mod 4\big)\Big) \tag{5}$$

Thus, because of the assumption on the noise and using Hoeffding's bound, the qubit

error rate

$$
\begin{aligned}
q &= \frac{1}{\tau}\left|\left\{n \in \mathcal{T} : \sum_{j\in[J]} (2v_n^j + b_n^j) = 2 \mod 4\right\}\right| \\
&= \frac{1}{\tau}\left|\left\{n \in \mathcal{T} : \bigoplus_{j\in[J]} b_n^j = 0 \text{ and } 2v_n^J = 2 - \sum_{j\in[J-1]} 2v_n^j - \sum_{j\in[J]} b_n^j \mod 4\right\}\right| \\
&= \frac{1}{\tau}\left|\left\{n \in \mathcal{T} : \bigoplus_{j\in[J]} b_n^j = 0 \text{ and } v_n^J = 1 - \left(\sum_{j\in[J-1]} v_n^j\right) - \frac{1}{2}\left(\sum_{j\in[J]} b_n^j \mod 4\right) \mod 2\right\}\right| \\
&= \frac{1}{\tau}\left|\left\{n \in \mathcal{T} : \bigoplus_{j\in[J]} b_n^j = 0 \text{ and } v_n^J \neq \left(\bigoplus_{j\in[J-1]} v_n^j\right) \oplus \frac{1}{2}\left(\sum_{j\in[J]} b_n^j \mod 4\right)\right\}\right| \\
&= \frac{1}{\tau}\left|\left\{n \in \mathcal{T} : b_n^J = \bigoplus_{j\in[J-1]} b_n^j \text{ and Equation 5 is invalidated}\right\}\right|
\end{aligned}
$$

is smaller than or equal to the threshold δ, except with probability at most $p_2 = e^{-2\tau(\delta-\mu)^2}$.

Finally, the parties may abort at the correctness check. Note that after error estimation, for all $n \in [M]$, $b_n^J = \bigoplus_{j\in[J-1]} b_n^j$ and thus Equation (5) is satisfied. After Player J updated their value at the beginning of the error correction step, Equation (5) gives

$$\bigoplus_{j\in[J]} v_n^j = 0. \tag{6}$$

Again by Hoeffding's bound and from the assumed bound on the noise, the Hamming weight of $\bigoplus_{j\in[J]} v_n^j$ will be smaller than or equal to $q + \nu$ except with probability at most $p_3 = e^{-2M(q+\nu-\mu)^2}$. In this event, after the error correction step, due to the properties of the error correcting code (see Footnote 2), except with a negligible probability in N that we denote p_{ec}, Equation (6) will strictly be satisfied for all rounds $n \in [M]$. Hence the correctness check will pass and the protocol will successfully terminate.

To conclude, by the union bound, the protocol successfully terminates except with probability at most $p_1+p_2+p_3+p_{ec}$ which, taking into account the different minimum values of τ, q and M under the assumed events, is lower than $e^{-\frac{1}{8}\tau'} + e^{-\frac{1}{8}(N-\tau')} + e^{-\frac{(\delta-\mu)^2}{2}\tau'} + e^{-\frac{(\nu-(\delta-\mu))^2}{2}(N-\tau')} + p_{ec}$ which is negligible in N since $\tau' = \omega(log(N))$. □

Proposition 2 and Proposition 1 together show the correctness of the protocol.

5 Security

This section is dedicated to the proof of security of the protocol described in Section 4. We first introduce an entanglement-based version of the protocol in Section 5.1 followed by formal definitions in Section 5.2. We establish the equivalence between the entanglement-based and the prepare-and-measure versions in Section 5.3, and then show the security of the entanglement-based version in Section 5.4. Finally, we bring together the results to conclude the security proof in Section 5.5.

5.1 Entanglement-based version of the protocol

The entanglement-based version of the protocol is identical to the prepare-and-measure version from Section 4, except for the state distribution step which is defined below. [4]

[4]The entanglement-based version requires the nodes of the Qline to have different capabilities compared to the prepare-and-measure version. As we only use the entanglement-based version as a tool to show the

State distribution (entanglement-based version)

1. The players agree on a integer N. Each player $j \in [J]$ samples N random bits $(b_n^j)_{n\in[N]}$
2. Player 1 generates N copies of the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends one qubit of each copy to player 2.
3. Each player $j \in \{2, ..., J-1\}$, obtains N qubits. For each qubit, player j applies a CNOT gate with the latter qubit as the control qubit of the operation, and a freshly prepared qubit in the $|0\rangle$ state as the target qubit. Player j then sends the first qubit to player $j+1$
4. Each player $j \in [J]$ measures each of their qubits $(\phi_n^j)_{n\in[N]}$ in either the Hadamard basis if $b_n^j = 0$ or in the circular basis if $b_n^j = 1$. The classical outcome of these measurements are denoted $(v_n^j)_{n\in[N]}$

5.2 Definitions

We hereafter define the systems that are later used to prove the security of the protocol. This includes the systems $\mathcal{QL}_{EB}$ and $\mathcal{QL}_{PM}$ respectively implementing the entanglement-based and the prepare-and-measure versions of the protocol. We first define individual components in Section 5.2.1, and then the complete systems in Section 5.2.2.

5.2.1 Component systems

- $\mathcal{C}_{auth}$ is a J-player classical authenticated broadcast channel with a random subset broadcast procedure implementing Assumption 4. It provides each player, honest or dishonest, with the ability to broadcast messages to all the others while authenticating the source of the messages. This is modeled by J player interfaces, each with an input t^j for $j \in [J]$ and an output t giving the transcript and the source of all the messages broadcast in the inputs of the other player interfaces. $\mathcal{C}_{auth}$ provides external entities with the ability to read the data or block the communications, but not to tamper with them. This is modeled by an outer interface providing as output no more than a copy of t, and receiving a binary input ℓ, called a blocking lever, which, if set to '1', prevents the messages to pass through. $\mathcal{C}_{auth}$ also provides the players with the ability to execute the *random subset broadcast* and *distributed coin-flip* procedures described Section 3.2.

- For each honest player $j \in \mathcal{H}$, $\mathcal{SD}_{PM}^j$ (respectively $\mathcal{SD}_{EB}^j$) is a system implementing the state distribution step for player j of the prepare-and-measure version (respectively the entanglement-based version) of the protocol. It has an outer interface with a N-qubit state input ρ_{in}^j and a N-qubits state output ρ_{out}^j, as well as an inner interface outputting the bits $b_{[N]}^j$ and $v_{[N]}^j$.

- The post-processing system $\mathcal{PP}$ implements the post-processing step of the protocol described in Section 4 (identical for any player $j \in \mathcal{H}$ and any version of the protocol). It has an inner interface with two N-bits inputs for $b_{[N]}^j$ and $v_{[N]}^j$, a player interface with a final share output s^j, as well as a side interface managing all the communications that occur on the classical authenticated channel. This side interface is designed to be plugged to a player interface of $\mathcal{C}_{auth}$ and thus has an output t^j for outgoing messages and an input t for incoming classical communication.

security of the prepare-and-measure version, this has no impact on the implementation requirements for the protocol.

- The systems $\mathcal{P}^j_{PM}$ (resp. $\mathcal{P}^j_{EB}$) implement the full prepare-and-measure (resp. entanglement-based) protocol described in Sections 4 and 5.1 for a given honest player $j \in \mathcal{H}$. $\mathcal{P}^j_{PM}$ ($\mathcal{P}^j_{EB}$) is the sequential composition of the state distribution and the post-processing systems at their respective inner interfaces. It thus has the outer interface of $\mathcal{SD}^j_{PM}$ ($\mathcal{SD}^j_{EB}$) as well as the player and side interfaces of $\mathcal{PP}$.

$$\mathcal{P}^j_{PM} = \mathcal{PP} \circ \mathcal{SD}^j_{PM} \tag{7}$$

$$\mathcal{P}^j_{EB} = \mathcal{PP} \circ \mathcal{SD}^j_{EB} \tag{8}$$

5.2.2 Complete systems

We define here the main systems that describe the protocol and its security. These systems are represented Figure 3

- The system $\mathcal{QL}_{PM}$ (resp. $\mathcal{QL}_{EB}$) is a theoretical model of the Qline for the prepare-and-measure version (resp. entanglement-based version) of the protocol. It is composed of the systems $\mathcal{P}^{\mathcal{H}}_{PM}$ ($\mathcal{P}^{\mathcal{H}}_{EB}$) modeling the H honest players, all composed sequentially to the classical channel $\mathcal{C}_{auth}$. $\mathcal{QL}_{PM}$ ($\mathcal{QL}_{EB}$) has an outer interface composed of $\rho^{\mathcal{H}}_{in}$ and $\rho^{\mathcal{H}}_{out}$ the outer inputs and outputs of all honest players, as well as the unused signals of $\mathcal{C}_{auth}$, namely the dishonest players inputs and outputs $((t^j)_{j\in[J]\setminus\mathcal{H}}$ and $J-H$ copies of t) and the blocking lever ℓ. $\mathcal{QL}_{PM}$ ($\mathcal{QL}_{EB}$) also has a share interface with $s^{\mathcal{H}}$ the share outputs of the player interfaces of the honest player systems $\mathcal{P}^{\mathcal{H}}_{PM}$ ($\mathcal{P}^{\mathcal{H}}_{EB}$).

  The dishonest players are fully controlled by the outside environment and thus are not part of the system. Instead, all their inputs and outputs are exposed to the outer interface of $\mathcal{QL}_{PM}$ ($\mathcal{QL}_{EB}$), modeling the fact that the outside world has complete control over the inputs and absolute knowledge of the outputs.

  According to these definitions, the systems $\mathcal{QL}_{PM}$ and $\mathcal{QL}_{EB}$ can equivalently be viewed as

$$\mathcal{QL}_{EB} = \mathcal{C}_{auth} \circ (\big|\big|_{j\in\mathcal{H}} P^j_{EB}) \tag{9}$$

$$\mathcal{QL}_{PM} = \mathcal{C}_{auth} \circ (\big|\big|_{j\in\mathcal{H}} P^j_{PM}) \tag{10}$$

- The ideal secret sharing system $\mathcal{I}$ has a *share* interface and an *outer* interface. The share interface has share outputs $(s^j)_{j\in\mathcal{H}}$, which are either binary strings of equal sizes, or the abort symbol $\perp$. The ideal property of $\mathcal{I}$ is captured by the fact that the only inputs and outputs of the outer interface, namely those exposed to the external entities, are the following:
  - A binary input ℓ called a a *blocking lever*, which, if set to 1, forces the system to abort regardless of any other input (enforcing $s^j = \perp$ for all $j \in [J]$).
  - An output $|s|$ giving the size of the honest shares outputs.
  - A "compromised" share s^{compr} which is a binary string *input* of size $|s|$. This models the fact that $\mathcal{I}$ handles dishonest entities: they are allowed to choose their share, and their sum (bit-wise xor $\oplus$), called s^{compr}, is taken into account in the honest shares' generation.

  $\mathcal{I}$ guarantees that if ℓ is set to 0, the shares are all uniformly random and independent of anything else, except for the last share s^{j_H} which is given by

$$s^{j_H} = \Big(\bigoplus_{j\in\mathcal{H}\setminus\{j_H\}} s^j \Big) \oplus s^{compr} \tag{11}$$

- The system $\mathcal{SIM}$ is a simulator. It has an inner interface meant to connect to the outer interface of $\mathcal{I}$, involving the blocking lever ℓ, the size $|s|$ of the honest shares, as well as the compromised share input s^{compr}. $\mathcal{SIM}$ also has an outer interface that matches the one of the $\mathcal{QL}_{EB}$ system. This interface consists of the following inputs and outputs: $\rho^{\mathcal{H}}_{in}, \rho^{\mathcal{H}}_{out}, t^{[J]\setminus\mathcal{H}}, t, \ell$.

  The simulator is represented in Figure 3. In order to produce inputs and outputs of the outer interface, the simulator internally runs a copy of the $\mathcal{QL}_{EB}$ system and directly maps every input and output of it's outer interface to the one of $\mathcal{SIM}$. The share outputs of $\mathcal{QL}_{EB}$ however, labeled $s^{\mathcal{H}}_{\mathcal{SIM}}$, are used to compute the compromised share output of $\mathcal{SIM}$ as

$$s^{compr} = \bigoplus_{j\in\mathcal{H}} s^j_{\mathcal{SIM}} \tag{12}$$

  Furthermore, in the event where $\mathcal{QL}_{EB}$ aborts (indicated by the output shares being set to $\perp$), the simulator will trigger the blocking lever ℓ of $\mathcal{I}$.

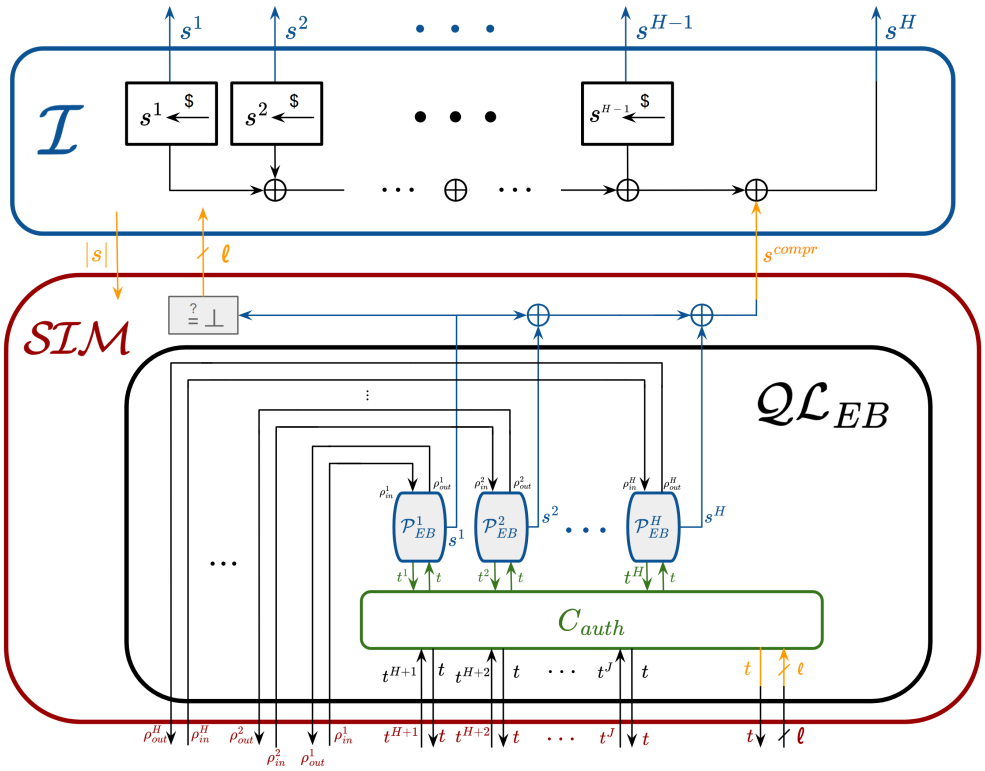

Figure 3: The simulator $\mathcal{SIM}$ plugged on $\mathcal{I}$.

5.3 Equivalence between $\mathcal{QL}_{EB}$ and $\mathcal{QL}_{PM}$

This section is dedicated to prove the equivalence of the entanglement-based version of the protocol implemented by the system $\mathcal{QL}_{EB}$ and the prepare-and-measure version of the protocol implemented by $\mathcal{QL}_{PM}$).

Theorem 1. *Under Assumptions 2 and 3,* $\mathcal{QL}_{PM} \approx_0 \mathcal{QL}_{EB}$.

Proof. Let us suppose that for any honest player $j \in \mathcal{H}$,

$$\mathcal{SD}^j_{PM} \approx_0 \mathcal{SD}^j_{EB}. \tag{13}$$

Due to the fact that the systems $\mathcal{QL}_{PM}$ and $\mathcal{QL}_{EB}$ are obtained by an identical construction, based on respectively $\mathcal{SD}^{\mathcal{H}}_{PM}$ and $\mathcal{SD}^{\mathcal{H}}_{EB}$ (see Equations (7) to (9)), the theorem follows from composing onto Equation (13) the systems $\mathcal{PP}$ and $\mathcal{C}_{auth}$. The remainder of the proof is devoted to prove Equation (13) for any given $j \in \mathcal{H}$.

For any $j \in \mathcal{H}$, $\mathcal{SD}^{j}_{PM}$ and $\mathcal{SD}^{j}_{EB}$ have the same interfaces, inputs and outputs. We first notice the following:

- The actions of $\mathcal{SD}^{J}_{PM}$ and $\mathcal{SD}^{J}_{EB}$ are the same.
- Both $\mathcal{SD}^{1}_{PM}$ and $\mathcal{SD}^{1}_{EB}$ output random bits $(b^1_n)_{n\in[N]}$ and the quantum state $\bigotimes_{n\in[N]} \frac{1}{\sqrt{2}}(|0\rangle + i^{b^1_n}|1\rangle)$

Hence, $\mathcal{SD}^{J}_{PM} \approx_0 \mathcal{SD}^{J}_{EB}$ and $\mathcal{SD}^{1}_{PM} \approx_0 \mathcal{SD}^{1}_{EB}$. We now deal with the case where $1 < j < J$.

Consider a distinguisher which is given black-box access to a system $\mathcal{S} \in \{\mathcal{SD}^{j}_{PM}, \mathcal{SD}^{j}_{EB}\}$ and whose goal is to distinguish the two cases. Let $n \in [N]$ be a fixed round and P be the register of the single-qubit system input of player j at round n (i.e $\rho^{j}_{n,in}$). Without loss of generality, we can consider that the distinguisher holds a register D that contains a purification of P. The state of the whole system can be written as

$$|\psi^{in}\rangle_{DP} = \alpha\,|\psi_0\rangle_D\,|0\rangle_P + \beta\,|\psi_1\rangle_D\,|1\rangle_P \tag{14}$$

with $\alpha, \beta \in \mathbb{C}$. If $\mathcal{S}$ is $\mathcal{SD}^{j}_{PM}$, then player j picks uniformly random b^j_n and v^j_n, and applies the unitary $Z^{v^j_n - \frac{b^j_n}{2}}$ to system P. The resulting state is described by

$$|\psi^{out}_{PM(b^j_n,v^j_n)}\rangle_{DP} = \alpha\,|\psi_0\rangle_D\,|0\rangle_P + i^{2v^j_n - b^j_n}\beta\,|\psi_1\rangle_D\,|1\rangle_P \tag{15}$$

We show that this state is indistinguishable from the one obtained when S is $\mathcal{SD}^{j}_{EB}$. In this case, a CNOT gate is applied using register P as control and the target register, call it Q, contains a fresh qubit in the state $|0\rangle_Q$. The overall state after this operation is described by:

$$\begin{aligned}
&|\psi^{out}_{EB}\rangle_{DPQ} \\
&= (\mathbb{I}_D \otimes CNOT_{PQ})(|\psi^{in}\rangle_{DP} \otimes |0\rangle_Q) \\
&= \alpha\,|\psi_0\rangle_D\,|0\rangle_P\,|0\rangle_Q + \beta\,|\psi_1\rangle_D\,|1\rangle_P\,|1\rangle_Q \\
&= \frac{1}{\sqrt{2}}\Big[\Big(\alpha\,|\psi_0\rangle_D\,|0\rangle_P + \beta\,|\psi_1\rangle_D\,|1\rangle_P\Big)|+\rangle_Q + \Big(\alpha\,|\psi_0\rangle_D\,|0\rangle_P - \beta\,|\psi_1\rangle_D\,|1\rangle_P\Big)|-\rangle_Q\Big] \qquad (16)\\
&= \frac{1}{\sqrt{2}}\Big[\Big(\alpha\,|\psi_0\rangle_D\,|0\rangle_P - i\beta\,|\psi_1\rangle_D\,|1\rangle_P\Big)|+_i\rangle_Q + \Big(\alpha\,|\psi_0\rangle_D\,|0\rangle_P + i\beta\,|\psi_1\rangle_D\,|1\rangle_P\Big)|-_i\rangle_Q\Big] \qquad (17)
\end{aligned}$$

The register Q is then measured in either the Hadamard or the circular basis, depending on the uniformly random bit b^j_n. From Equation (16) and Equation (17), one can see that for all b^j_n and $|\psi^{in}\rangle_{DP}$, the outcome of the measurement is an uniformly random bit v^j_n. Moreover, the post-measurement state on registers D and P is exactly $|\psi^{out}_{PM(b^j_n,v^j_n)}\rangle_{DP}$

In conclusion, the outputs of round n of $\mathcal{SD}^{j}_{PM}$ and $\mathcal{SD}^{j}_{EB}$ are exactly the same, and therefore indistinguishable, which proves Equation (13) for any $j \in \mathcal{H}$. □

5.4 Security of $\mathcal{QL}_{EB}$

In this section, we prove the security of the entanglement based version of the protocol described in Section 5.1.

Theorem 2. *Under Assumptions 1, 2, 3, and 4,*

$$\mathcal{QL}_{EB} \approx_{\epsilon} \mathcal{I} \circ \mathcal{SIM} \tag{18}$$

where $\epsilon = (H-1)\epsilon_{\mathcal{QKD}'} + \epsilon_{cor}$ *with* $\epsilon_{\mathcal{QKD}'}$ *the distinguishing advantage of a QKD protocol with the same assumptions, and* $\epsilon_{cor} = 2^{-\eta}$ *the correctness parameter defined in Section 4.1*

In order to prove Theorem 2, we consider an unbounded distinguisher $\mathcal{D}$ which is given a system $\mathcal{S}$, either equal to $\mathcal{QL}_{EB}$ or to $\mathcal{I} \circ \mathcal{SIM}$, uniformly at random. To avoid any ambiguities, we denote the input and outputs of $\mathcal{QL}_{EB}$ by $\rho_{in}^{\mathcal{H}}, t^{[J]\setminus\mathcal{H}}, \ell$ and $s^{\mathcal{H}}, \rho_{out}^{\mathcal{H}}, t$, the input and outputs of $\mathcal{I} \circ \mathcal{SIM}$ by $\tilde{\rho}_{in}^{\mathcal{H}}, \tilde{t}^{[J]\setminus\mathcal{H}}, \tilde{\ell}$ and $\tilde{s}^{\mathcal{H}}, \tilde{\rho}_{out}^{\mathcal{H}}, \tilde{t}$, and the input and outputs of $\mathcal{S}$ by $\rho_{\mathcal{S},in}^{\mathcal{H}}, t_{\mathcal{S}}^{[J]\setminus\mathcal{H}}, \ell_{\mathcal{S}}$ and $s_{\mathcal{S}}^{\mathcal{H}}, \rho_{\mathcal{S},out}^{\mathcal{H}}, t_{\mathcal{S}}$ [5].

Lemma 1. *The probability for* $\mathcal{S}$ *to abort is the same regardless of whether* $\mathcal{S}$ *is* $\mathcal{QL}_{EB}$ *or* $\mathcal{I} \circ \mathcal{SIM}$*. Moreover, conditioned on the event that* $\mathcal{S}$ *aborts, then* $\mathcal{QL}_{EB} \approx_0 \mathcal{I} \circ \mathcal{SIM}$

Proof. Note that in both $\mathcal{QL}_{EB}$ and $\mathcal{I} \circ \mathcal{SIM}$, all the inputs are given to a $\mathcal{QL}_{EB}$ system, either directly in the real experiment or forwarded by $\mathcal{SIM}$ in the simulated one. This $\mathcal{QL}_{EB}$ system thus produces outputs with the exact same distribution in both cases. This gives the following:

- Since $\mathcal{I} \circ \mathcal{SIM}$ aborts if and only if its simulation of $\mathcal{QL}_{EB}$ aborts, the first part of the lemma trivially holds.
- If the systems abort, all the outputs of $\mathcal{QL}_{EB}$ and $\mathcal{I} \circ \mathcal{SIM}$ follow the exact same distribution. The shares $s^{\mathcal{H}}$ and $\tilde{s}^{\mathcal{H}}$ are indeed all set to $\perp$, while the other outputs directly come from the $\mathcal{QL}_{EB}$ system. This gives the second part of the lemma

□

Lemma 1 allows us to focus on the case where the protocol does not abort.

Our goal is now to show that conditioned on $\mathcal{S}$ successfully terminating, the systems $\mathcal{QL}_{EB}$ and $\mathcal{I} \circ \mathcal{SIM}$ are indistinguishable. In order to prove this, we introduce an intermediate protocol that we call $\mathcal{QKD}'$. The objective here is that $\mathcal{QKD}'$ be close enough to standard entanglement-based QKD so that its security follows trivially from historical results, yet slightly modified so that we can reduce the security of our protocol to the security of $\mathcal{QKD}'$

In order to define $\mathcal{QKD}'$, we first briefly recall entanglement-based QKD (EB-QKD).[6] EB-QKD involves two players, Alice_{QKD} and Bob_{QKD} and works as follow:

1. **(State distribution)** Alice_{QKD} and Bob_{QKD} receive N qubits and measure each qubit either in the computational or in the Hadamard basis, uniformly at random.
2. **(sifting)** Alice_{QKD} and Bob_{QKD} announce their basis choices and discard the rounds where they did not agree.
3. **(Error estimation)** Alice_{QKD} and Bob_{QKD} agree on a random subset of the remaining qubits and announce their measurement outcomes for the positions in that subset. They count the outcomes for which they disagree among this subset and abort the protocol if the corresponding rate is above a given threshold.
4. **(Error correction)** Alice_{QKD} announces the syndrome (relative to a given syndrome decoding protocol) of her secret and Bob_{QKD} corrects his secret using this syndrome. They then compare hashes of the corrected secrets, aborting upon any mismatch.

[5] This notation consists simply of *labels* for the inputs and outputs of the abstract systems. They do not denote the underlying quantum states (that could be potentially entangled).

[6] We refer the reader to [4] (part I) for a detailed description of EB-QKD.

5. **(Privacy amplification)** Alice_{QKD} and Bob_{QKD} compute their final key as the image of their error-corrected measurement outcomes (the raw key) under a 2-universal hash function.

We define the $\mathcal{QKD}'$ protocol with the following modifications from EB-QKD.

(1) In the state distribution step, for each position $n \in [N]$, $\text{Bob}_{\mathcal{QKD}'}$ receives from the eavesdropper two bits $b_n^{(\mathcal{D})}$ and $v_n^{(\mathcal{D})}$. Instead of measuring in a basis given by b_n^{Bob}, he measures in basis $\hat{b}_n^{\text{Bob}}$ where

$$\hat{b}_n^{\text{Bob}} = b_n^{\text{Bob}} \oplus b_n^{(\mathcal{D})} \tag{19}$$

Additionally, $\text{Bob}_{\mathcal{QKD}'}$ computes $\hat{v}_n^{\text{Bob}}$ where

$$\hat{v}_n^{\text{Bob}} = v_n^{\text{Bob}} \oplus v_n^{(\mathcal{D})} \oplus (b_n^{\text{Bob}} \vee b_n^{(\mathcal{D})}) \tag{20}$$

For the rest of the protocol, $\text{Bob}_{\mathcal{QKD}'}$ uses $\hat{b}_n^{\text{Bob}}$ and $\hat{v}_n^{\text{Bob}}$ instead of b_n^{Bob} and v_n^{Bob}.

We notice that these two steps are equivalent to Bob applying $\mathbf{Z}^{(v_n^{(\mathcal{D})} + \frac{1}{2} b_n^{(\mathcal{D})})\pi}$ on his qubit before measuring in the b_n^{Bob} basis[7].

(2) Before sifting, $\text{Alice}_{\mathcal{QKD}'}$ and $\text{Bob}_{\mathcal{QKD}'}$ agree on a random subset of all the qubits received in the state distribution step. At the error estimation step, this subset, restricted to the rounds that were not discarded during sifting, is used for the error rate computation instead of a freshly generated one.

(3) In the error correction step, $\text{Bob}_{\mathcal{QKD}'}$ does not correct his secret and instead announces its syndrome like $\text{Alice}_{\mathcal{QKD}'}$ does.

We claim now that Alice's key is as secure in $\mathcal{QKD}'$ as in standard QKD. To formalize this statement, we define the following "mask" systems, that replace or simply remove access for a given distinguisher to a specific output:

- $\mathcal{M}^{\mathcal{I}}_{Alice}$ takes as input the key of $\text{Alice}_{\mathcal{QKD}'}$, and outputs instead a freshly generated, uniformly random bit string of the same length.
- $\mathcal{M}_{Bob}$ takes as input the key of $\text{Bob}_{\mathcal{QKD}'}$, and has no output.

Our claim amounts to the following Proposition 3, of which we defer the proof to Appendix B.1.

Proposition 3.

$$\mathcal{QKD}' \circ \mathcal{M}_{Bob} \approx_{\epsilon_{QKD}} \mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{M}^{\mathcal{I}}_{Alice} \tag{21}$$

where ϵ_{QKD} is the distinguishing advantage of a QKD protocol with the same parameters and under the same assumptions.

Similarly as above, we define the system $\mathcal{M}_H$ that takes as input the share s^{j_H} and has no output. Using Proposition 3, we now prove Lemma 2.

Lemma 2. *Let $\epsilon_{\mathcal{QKD}'}$ be the distinguishing advantage of $\mathcal{QKD}'$ when run with the same parameters as $\mathcal{S}$. Then, assuming $\mathcal{S}$ successfully terminates,*

$$\mathcal{QL}_{EB} \circ \mathcal{M}_H \approx_{(H-1)\epsilon_{\mathcal{QKD}'}} \mathcal{I} \circ \mathcal{SIM} \circ \mathcal{M}_H \tag{22}$$

[7] In the formula of $\hat{v}_n^{\text{Bob}}$ (Equation (20)), $v_n^{(\mathcal{D})}$ flips the results according to the $\mathbf{Z}^{v_n^{(\mathcal{D})}}$ component of the operation, and $(b_n^{j'} \vee b_n^{(\mathcal{D})})$ accounts for the effect of the $\mathbf{Z}^{\frac{1}{2} b_n^{(\mathcal{D})}}$ part.

Proof. Without loss of generality, the output of the distinguisher (on whether S is $\mathcal{QL}_{EB}$ or $\mathcal{I} \circ \mathcal{SIM}$) is the outcome of a given measurement on the state $\sigma_{\mathcal{D}}$ containing all the outputs of $\mathcal{S}$ and the private register of the distinguisher. In particular, for all honest players $j \in \mathcal{H}$, we denote S^j the register corresponding to the share output s^j. We denote $\sigma_{D \setminus S^{j_H}} = Tr_{S^{j_H}}(\sigma_D)$.

In the remainder of the proof, we will aim to show that for any $h \in [H-1]$,

$$\left(\frac{1}{2^K} I\right)^{\otimes h-1} \otimes Tr_{S^{j_{[h-1]}}}(\sigma_{D \setminus S^{j_H}}) \approx_{\epsilon_{\mathcal{QKD}'}} \left(\frac{1}{2^K} I\right)^{\otimes h} \otimes Tr_{S^{j_{[h]}}}(\sigma_{D \setminus S^{j_H}}). \tag{23}$$

We notice that this finishes the proof, since chaining Equation (23) for each $h \in [H-1]$, we have

$$\sigma_{D \setminus S^{j_H}} \approx_{(H-1)\epsilon_{\mathcal{QKD}'}} \left(\frac{1}{2^K} I\right)^{\otimes H-1} \otimes Tr_{S^{\mathcal{H}}}(\sigma_D), \tag{24}$$

which exactly gives Equation (22).

To conclude the proof of Lemma 2, we prove Equation (23) by contradiction. Let us suppose that there exist $h \in [H-1]$ and a distinguisher $\mathcal{D}_{\mathcal{QL}}$ which distinguishes $(\frac{1}{2^K} I)^{\otimes h-1} \otimes Tr_{S^{j_{[h-1]}}}(\sigma_{D \setminus S^{j_H}})$ from $(\frac{1}{2^K} I)^{\otimes h} \otimes Tr_{S^{j_{[h]}}}(\sigma_{D \setminus S^{j_H}})$ with probability $\epsilon_{\mathcal{D}} > \epsilon_{\mathcal{QKD}'}$.

Using this assumption, we will design an attack on $\mathcal{QKD}'$ to contradict Proposition 3, thus proving Equation (23). The idea is to build a Qline around $\text{Alice}_{\mathcal{QKD}'}$ and $\text{Bob}_{\mathcal{QKD}'}$ such that when they perform $\mathcal{QKD}'$, they are in fact taking part (as players j_h and j_H respectively) in a $\mathcal{QL}_{EB}$ protocol that we can then attack with $\mathcal{D}_{\mathcal{QL}}$. Formally, we will define a system $\mathcal{A}$ represented in Figure 4 which interfaces between the $\mathcal{QKD}'$ protocol of $\text{Alice}_{\mathcal{QKD}'}$ and $\text{Bob}_{\mathcal{QKD}'}$ at an *inner* interface, and the distinguisher $\mathcal{D}_{\mathcal{QL}}$ at an *outer* interface. We define below the construction of $\mathcal{A}$ in details:

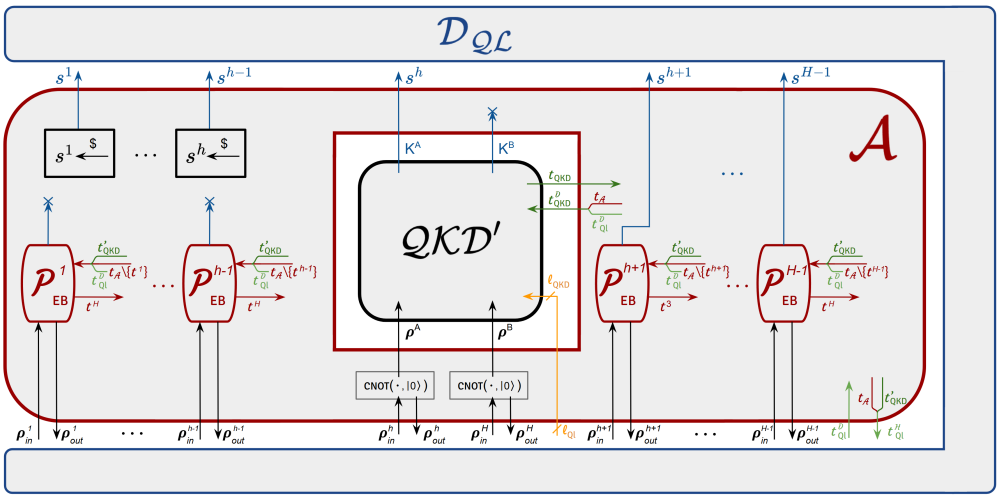

Figure 4: The system $\mathcal{A}$ interfacing between $\mathcal{QKD}'$ and $\mathcal{D}_{\mathcal{QL}}$.

$\mathcal{A}$ simulates the honest player systems $\mathcal{P}_{EB}^j$ of $\mathcal{QL}_{EB}$ for $j \in \mathcal{H} \setminus \{j_h, j_H\}$.

1. During the state distribution step:
   - $\mathcal{A}$ directly forwards the quantum inputs/outputs $\rho_{in}^j / \rho_{out}^j$ of $\mathcal{P}_{EB}^{\mathcal{H} \setminus \{j_h, j_H\}}$ from/to the distinguisher at the outer interface of $\mathcal{A}$.
   - $\mathcal{A}$ interfaces the quantum inputs of $\text{Alice}_{\mathcal{QKD}'}$ and $\text{Bob}_{\mathcal{QKD}'}$ with the quantum inputs *and outputs* of honest players j_h and j_H at its outer interface. Note

that when performing $\mathcal{QKD}'$, $\text{Alice}_{\mathcal{QKD}'}$ and $\text{Bob}_{\mathcal{QKD}'}$ exactly follow the state distribution step of $\mathcal{QL}_{EB}$ except for the step where the players propagate entanglement. $\mathcal{A}$ thus simulates this step by receiving at it's outer interface from the distinguisher $\mathcal{D}_{\mathcal{QL}}$ the qubits of input $\rho_{in}^{j_h}$, applying a CNOT gate on that qubit together with a freshly generated $|0\rangle$ and then sending one qubit to $\text{Alice}_{\mathcal{QKD}'}$ and the second one to $\mathcal{D}_{\mathcal{QL}}$ via the outer output $\rho_{out}^{j_h}$ of $\mathcal{A}$. $\mathcal{A}$ performs similar steps for j_H and $\text{Bob}_{\mathcal{QKD}'}$.

2. During the post-processing step:

   - $\mathcal{A}$ maps the blocking lever l of its outer interface to the corresponding input of the authenticated channel of $\mathcal{QKD}'$
   - The simulated honest player systems $\mathcal{P}_{EB}^{\mathcal{H}\setminus\{j_h,j_H\}}$ comply with $\text{Alice}_{\mathcal{QKD}'}$'s and $\text{Bob}_{\mathcal{QKD}'}$'s choices for $\mathcal{T}'$, ν, the syndrome decoding protocol, f_{cc}, K, and f_{pa}.
   - The inputs $b_{[N]}^{(\mathcal{D})}$ and $v_{[N]}^{(\mathcal{D})}$ of $\text{Bob}_{\mathcal{QKD}'}$, provided by the eavesdropper in $\mathcal{QKD}'$ protocol are defined by:

$$b_n^{(\mathcal{D})} = \bigoplus_{j\in[J]\setminus\{j_h,j_H\}} b_n^j$$
$$2v_n^{(\mathcal{D})} + b_n^{(\mathcal{D})} = \sum_{j\in[J]\setminus\{j_h,j_H\}} 2v_n^j + b_n^j \mod 4$$

     where the values $b_{[N]}^{[J]\setminus\{j_h,j_H\}}$ and $v_{[N]}^{[J]\setminus\{j_h,j_H\}}$ are defined either by the outputs of the simulated player systems $\mathcal{P}_{EB}^j$ for honest players $j \in \mathcal{H}\setminus\{j_h,j_H\}$, or by $\mathcal{D}_{\mathcal{QL}}$ in the announcements of the dishonest players for $j \in [J]\setminus\mathcal{H}$. Note that these dishonest announcements $v_{[N]}^{[J]\setminus\mathcal{H}}$ are all well defined and accessible to $\mathcal{A}$ at this moment because of the random subset broadcast of $\mathcal{QL}_{EB}$ (see Assumption 4) which guarantees that the distinguisher $\mathcal{D}_{\mathcal{QL}}$ does not use the honest players' announcements to produces the dishonest players' ones. In other words, as $\mathcal{A}$ simulates the whole Qline which contains the authenticated channel with random subset broadcast, it has control over that channel and can compute some announcements based on others.
   - The simulated honest player systems $\mathcal{P}_{EB}^{\mathcal{H}\setminus\{j_h,j_H\}}$ receive:
     - The announcements of the other simulated honest players.
     - The announcements of the dishonest players that come from the distinguisher at the outer interface of $\mathcal{A}$.
     - The announcements of $\text{Alice}_{\mathcal{QKD}'}$ labeled as coming from j_h.
     - The announcements of $\text{Bob}_{\mathcal{QKD}'}$, labeled as coming from j_H and slightly modified in order for the announcements that depend on $\hat{v}_n^{\text{Bob}}$ to instead match with what they would have been if Bob was using v_n^{Bob} all along. This amounts to computing the modification string

$$v_n^{\mathcal{A}} = \hat{v}_n^{\text{Bob}} \oplus v_n^{\text{Bob}} = v_n^{(\mathcal{D})} \oplus (b_n^{\text{Bob}} \vee b_n^{(\mathcal{D})}) \tag{25}$$

       for all $n \in [N]$ (see Equation (20)), and to XOR the corresponding check bits announcement $v_{\mathcal{T}}^{\mathcal{A}}$, syndrome $w^{\mathcal{A}}$, correctness check output $c^{\mathcal{A}}$ and final share $s^{\mathcal{A}}$ to the respective announcements of $\text{Bob}_{\mathcal{QKD}'}$.
   - $\mathcal{A}$ sends to $\mathcal{D}_{\mathcal{QL}}$ at it's outer interface the following announcements:
     - The announcements of the simulated honest player systems $\mathcal{P}_{EB}^{\mathcal{H}\setminus\{j_h,j_H\}}$.
     - The announcements of $\text{Alice}_{\mathcal{QKD}'}$ labeled as coming from j_h.

- The announcements of $\text{Bob}_{\mathcal{QKD}'}$, labeled as coming from j_H and modified the exact same way as described above.

- $\mathcal{A}$ exposes the following share outputs at it's outer interface:
  - The shares $s^{j_{[h-1]}}$ are all sampled uniformly at random.
  - The share s^{j_h} is directly the final key output of $\text{Alice}_{\mathcal{QKD}'}$.
  - The shares $s^{j_{\{h+1,\ldots,H-1\}}}$ are directly the output shares of the simulated honest players $\mathcal{P}_{EB}^{j_{\{h+1,\ldots,H-1\}}}$.

By connecting $\mathcal{A}$ onto $\mathcal{D}_{\mathcal{QL}}$ and $\mathcal{QKD}'$ as depicted in Figure 4, $\text{Alice}_{\mathcal{QKD}'}$ and $\text{Bob}_{\mathcal{QKD}'}$ are performing $\mathcal{QKD}'$, while in the same time $\mathcal{QKD}' \circ \mathcal{A}$ is undergoing the $\mathcal{QL}_{EB}$ secret sharing protocol. To obtain the contradiction, we use the following Proposition 4 which we prove in Appendix B.2.

Proposition 4. *The system $\mathcal{A} \circ \mathcal{D}_{\mathcal{QL}}$ distinguishes $\mathcal{QKD}' \circ \mathcal{M}_{Bob}$ from $\mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{M}_{Alice}^{\mathcal{I}}$ with probability $\epsilon_{\mathcal{D}}$.*

As $\epsilon_{\mathcal{D}} > \epsilon_{\mathcal{QKD}'}$, this contradicts Proposition 3, hence proving Equation (23). □

Lemma 3. *If $\mathcal{S}$ successfully terminates, then*

$$\mathcal{QL}_{EB} \approx_{\epsilon} \mathcal{I} \circ \mathcal{SIM} \tag{26}$$

with $\epsilon = \epsilon_{cor} + (H-1)\epsilon_{\mathcal{QKD}'}$ where $\epsilon_{\mathcal{QKD}'}$ is the distinguishing advantage of Alice's key in a $\mathcal{QKD}'$ protocol with the same parameters and under the same assumptions.

Proof. We notice that following the description of the protocol, $s^{[J]}$ is a function of the values $v_{[N]}^{[J]}$ of the players along with publicly known data. As these values are all input in the random subset broadcast functionality of $\mathcal{S}$, they are all well defined in $\mathcal{S}$ and thus so are in particular the dishonest player's expected shares that we denote $s_{\mathcal{S}}^{[J]\setminus\mathcal{H}}$.

We assume that correctness (Equation (4)) holds for the $\mathcal{QL}_{EB}$ system of $\mathcal{S}$. From Proposition 1, this happens except with probability ϵ_{cor}.

If $\mathcal{S}$ is $\mathcal{I} \circ \mathcal{SIM}$, by definition of $\mathcal{I}$ and $\mathcal{SIM}$ (see Equations (11) and (12)), we have

$$\begin{aligned} s^{j_H} &= \Big(\bigoplus_{j \in \mathcal{H}\setminus\{j_H\}} \tilde{s}^j \Big) \oplus s^{compr} \\ &= \Big(\bigoplus_{j \in \mathcal{H}\setminus\{j_H\}} \tilde{s}^j \Big) \oplus \Big(\bigoplus_{j \in \mathcal{H}} s_{\mathcal{SIM}}^j \Big) \end{aligned}$$

which as we assume correctness gives

$$s^{j_H} = \Big(\bigoplus_{j \in \mathcal{H}\setminus\{j_H\}} \tilde{s}^j \Big) \oplus \Big(\bigoplus_{j \in [J]\setminus\mathcal{H}} s_{\mathcal{S}}^j \Big)$$

Similarly, if $\mathcal{S}$ is $\mathcal{QL}_{EB}$, by correctness,

$$\begin{aligned} s^{j_H} = &\bigoplus_{j \in [J]\setminus\{j_H\}} s^j \\ &\Big(\bigoplus_{j \in \mathcal{H}\setminus\{j_H\}} s^j \Big) \oplus \Big(\bigoplus_{j \in [J]\setminus\mathcal{H}} s_{\mathcal{S}}^j \Big) \end{aligned}$$

In conclusion, in both cases, s^{j_H} is identically defined from the other inputs and outputs of $\mathcal{S}$ as

$$s^{j_H} = \Big(\bigoplus_{j \in \mathcal{H}\setminus\{j_H\}} s_{\mathcal{S}}^j \Big) \oplus \Big(\bigoplus_{j \in [J]\setminus\mathcal{H}} s_{\mathcal{S}}^j \Big)$$

As a result, except with probability ϵ_{cor}, Lemma 2 holds even when giving the distinguisher access to s^{j_H}, meaning even when removing the $\mathcal{M}_H$ systems from Equation (22). This concludes the proof □

Theorem 2 then follows from Lemma 1 and Lemma 3.

5.5 Conclusion on the security

Combining the main results of the previous sections (Theorem 2 and Theorem 1) using the composability of the security definition, we obtain the following final statement.

Theorem 3. *Under Assumptions 1, 2, 3 and 4, the following holds.*

$$\mathcal{QL}_{PM} \approx_{\epsilon} \mathcal{I} \circ \mathcal{SIM} \tag{27}$$

with

$$\epsilon = \epsilon_{cor} + (H-1)\epsilon_{QKD} \tag{28}$$

An example for an expression of ϵ_{QKD} can be obtained from [4] (Theorem 3, Equations (57) and (58)), yielding the following, where χ is the size of the syndromes involved in the error correction step and $h(x) = -xlog(x) - (1-x)log(1-x)$ is the binary entropy function.

$$\epsilon_{QKD} = 2e^{-\frac{M\tau^2}{L(\tau+1)}\nu^2} + \frac{1}{2}\sqrt{2^{-M\left(1-h(\delta+\nu)\right)+\eta+\chi+K}} \tag{29}$$

For two honest players, our bound for ϵ matches known bounds for standard QKD. This is natural since the security proof follows from a reduction to QKD. However, the bound worsens when the number of honest players grows. This counter-intuitive behavior could be explained by the fact that more honest players imply more potential targets (shares) to distinguish from uniformly random ones. The composability of our security definition indeed imposes, in order for the whole scheme to be secure, that all shares are secure together, and not only individually.

References

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pp. 313–318, 1899.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[4] M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," *Quantum*, vol. 1, p. 14, 2017.

[5] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," 2014.

[6] N. J. Bouman and S. Fehr, "Sampling in a quantum population, and applications," in *Annual Cryptology Conference*, pp. 724–741, Springer, 2010.

[7] M. Doosti, L. Hanouz, A. Marin, E. Kashefi, and M. Kaplan, "Establishing shared secret keys on quantum line networks: protocol and security," 2023.

[8] M. Clementi, A. Pappa, A. Eckstein, I. A. Walmsley, E. Kashefi, and S. Barz, "Classical multiparty computation using quantum resources," *Phys. Rev. A*, vol. 96, no. 062317, 2017.

[9] B. Polacchi, D. Leichtle, L. Limongi, G. Carvacho, G. Milani, N. Spagnolo, M. Kaplan, F. Sciarrino, and E. Kashefi, "Multi-client distributed blind quantum computation with the qline architecture," *Nature Communications*, vol. 14, no. 1, p. 7743, 2023.

[10] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, "Experimental single qubit quantum secret sharing," *Phys. Rev. Lett.*, vol. 95, p. 230505, Dec 2005.

[11] K. Inoue, T. Ohashi, T. Kukita, K. Watanabe, S. Hayashi, T. Honjo, and H. Takesue, "Differential-phase-shift quantum secret sharing," *Opt. Express*, vol. 16, pp. 15469–15476, Sep 2008.

[12] U. Maurer and R. Renner, "Abstract cryptography," in *Proceedings of Innovations in Computer Science, ICS 2010, Tsinghua University Press*, pp. 1–21, 2011.

[13] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *J. Cryptology*, vol. 1, pp. 65–75, 1988.

[14] A. Broadbent and A. Tapp, "Information-theoretic security without an honest majority," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 410–426, Springer, 2007.

[15] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences, Cambridge University Press, 2000.

[16] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," Tech. Rep. arXiv:1409.3525, arXiv preprint, 2016.

[17] J. Rompel, "One-way functions are necessary and sufficient for secure signatures," in *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing*, STOC '90, (New York, NY, USA), p. 387–394, Association for Computing Machinery, 1990.

[18] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *Journal of computer and system sciences*, vol. 22, no. 3, pp. 265–279, 1981.

[19] D. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn, "Sphincs: Practical stateless hash-based signatures," vol. 9056, pp. 368–397, 04 2015.

[20] J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: A ring-based public key cryptosystem.," in *ANTS*, vol. 1423 of *Lecture Notes in Computer Science*, pp. 267–288, Springer, 1998.

[21] A. Beimel, E. Omri, and I. Orlov, "Protocols for multiparty coin toss with a dishonest majority," *Journal of Cryptology*, vol. 28, no. 3, pp. 551–600, 2015.

[22] M. Naor, "Bit commitment using pseudo-randomness," in *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, vol. 435 of *Lecture Notes in Computer Science*, pp. 128–136, Springer, 1989.

[23] J. Carolan and A. Poremba, "Quantum one-wayness of the single-round sponge with invertible permutations," 2024.

[24] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, pp. 143–154, 1979.

[25] D. Tupkary and N. Lütkenhaus, "Using cascade in quantum key distribution," *Phys. Rev. Appl.*, vol. 20, p. 064040, Dec 2023.

A Notation

Mathematical notation:

$\oplus$	Addition modulo 2.
$\vee$	Logical "or" between binary variables.
$[N]$	The set $\{1, ..., N\}$ of integers ranging from 1 to N.
$\|A\|$	Size of the set A.
log	Base 2 logarithm function of strictly positive real numbers.
$h(x)$	Binary entropy function of $x \in]0,1[$. $h(x) = -xlog(x) - (1-x)log(1-x)$
$\mathcal{R} \circ \mathcal{S}$	The sequential composition of two systems.
$\mathcal{R} \| \mathcal{S}$	The parallel composition of two systems.
$\approx_\epsilon$	Indistinguishability, except with probability ϵ. Between abstract systems, $R \approx_\epsilon S$ is relative to the distinguishing pseudo-metric, while between quantum states $\sigma \approx_\epsilon \gamma$ is relative to the trace distance.
$Tr(A)$	The trace of a matrix A.
$\|+\rangle$, $\|-\rangle$	Eigenstates of the Hadamard basis.
$\|+_i\rangle$, $\|-_i\rangle$	Eigenstates of the circular basis.
$\mathbf{Z}$	The Pauli $\mathbf{Z}$ single-qubit gate $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. $\mathbf{Z}^{\frac{1}{2}}$ is the phase gate $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

Abstract systems and protocols:

$\mathcal{C}_{auth}$	Classical authenticated channel with random subset broadcast subroutine representing Assumption 4.
$\mathcal{SD}^j_{PM}, \mathcal{SD}^j_{EB}$	State distribution system of player j for the prepare-and-measure and entanglement-based versions of the protocol respectively.
$\mathcal{PP}$	Post-processing system.
$\mathcal{P}^j_{PM}, \mathcal{P}^j_{EB}$	Player j's whole system for the prepare-and-measure and entanglement-based versions of the protocol respectively. $\mathcal{P}^j_{PM} = \mathcal{PP} \circ \mathcal{SD}^j_{PM}$ and $\mathcal{P}^j_{EB} = \mathcal{PP} \circ \mathcal{SD}^j_{EB}$
$\mathcal{QL}_{PM}, \mathcal{QL}_{EB}$	Whole system of an execution of the prepare-and-measure and entanglement-based versions of the protocol respectively.
$\mathcal{I}$	Ideal system for the secret sharing primitive.
$\mathcal{SIM}$	Simulator (see Figure 3).
$\mathcal{D}$	Distinguisher which is given $\mathcal{S}$ and tries to guess which of the two possible systems it is.
$\mathcal{S}$	Abstract system given to the Distinguisher.

For any variable x and any sets or families A and B, x^A_B denotes $(x^a_b)_{a \in A, b \in B}$.

Protocol parameters:

ϵ	Indistinguishability parameter (Security parameter).
τ', τ	Sizes of the sets $\mathcal{T}'$ and $\mathcal{T}$ respectively.
q	Qubit error rate.
δ	Threshold of the qubit error rate q for the protocol to proceed after error estimation.
ν	Error correction margin. It is to be chosen by the players to adjust the final share size K and security parameterϵ.
χ	Bit length of the syndromes $(w^j)_{j\in[J]}$.
η	Correctness parameter and binary size of the output of f_{cc}.
f_{cc}	Correctness check hash function mapping $\{0,1\}^M$ to $\{0,1\}^\eta$.
f_{pa}	Privacy amplification hash function mapping $\{0,1\}^M$ to $\{0,1\}^K$.

Indices and Sets:

J	Total number of players ($j \in [J]$).
$\mathcal{H}$	The set of honest players ($j \in \mathcal{H}$). The elements of $\mathcal{H}$ are denoted $j_1, ..., j_H$.
H	Number of honest players. $H = \lvert\mathcal{H}\rvert$
N	Number of rounds of the protocol ($n \in [N]$).
L	Number of remaining data bits after sifting. $L = N - \lvert\mathcal{U}\rvert$
M	Number of remaining data bits after error estimation. $M = L - \tau$
K	Bit size of the final shares.
$\mathcal{T}', \mathcal{T}$	Set of indices of the check bits, before and after sifting respectively.
$\mathcal{U}$	Set of indices of the rounds discarded for uncorrelated basis choices. $\mathcal{U} \subset [N]$

Other notation:

QKD	Quantum Key distribution protocol.
$\mathcal{QKD}'$	A slightly modified QKD protocol introduced Section 5.4 and used as a tool for the security proof
$j_1, ..., j_H$	The elements of $\mathcal{H}$ in their corresponding order on the Qline (meaning $j_1 < ... < j_H$)
b_n^j, b^j	b_n^j: Basis bit of player j for round n in $\mathcal{QL}_{EB}$. $b^j = (b_n^j)_{n\in[N]}$.
v_n^j, v^j	v_n^j: Value bit of player j for round n in $\mathcal{QL}_{EB}$. $v^j = (v_n^j)_{n\in[N]}$
w^j	Syndrome of the raw key $(v_n^j)_{n\in[M]}$ of player j announced during the error correction step
s^j	Final share of player j. Share output for player j in systems performing secret sharing.
$\rho_{n,in}^j$	Single-qubit quantum state input of player j for round n. $\rho_{in}^j = (\rho_{n,in}^j)_{n\in[N]}$
$\rho_{n,out}^j$	Single-qubit quantum state output of player j for round n. $\rho_{out}^j = (\rho_{n,out}^j)_{n\in[N]}$
t	Whole transcript of all the classical authenticated communications that occur during the protocol.
ℓ	Blocking lever.
$\rho_{in}^{\mathcal{H}}, \rho_{out}^{\mathcal{H}}, t^{[J]\setminus\mathcal{H}}, \ell, s^{\mathcal{H}}$	inputs and outputs of $\mathcal{QL}_{EB}$.
$\tilde{\rho}_{in}^{\mathcal{H}}, \tilde{\rho}_{out}^{\mathcal{H}}, \tilde{t}^{[J]\setminus\mathcal{H}}, \tilde{\ell}, \tilde{s}^{\mathcal{H}}$	inputs and outputs of $\mathcal{I} \circ \mathcal{SIM}$.
$\rho_{\mathcal{S},in}^{\mathcal{H}}, \rho_{\mathcal{S},out}^{\mathcal{H}}, t_{\mathcal{S}}^{[J]\setminus\mathcal{H}}, \ell_{\mathcal{S}}, s_{\mathcal{S}}^{\mathcal{H}}$	inputs and outputs of $\mathcal{S}$ (in Section 5.4).

B Proofs

B.1 Proof of Proposition 3

The security of entanglement-based QKD has been shown by several different works ([4, 5, 6]). More concretely, under Assumptions 2, 3 and 4, there exists ϵ_{QKD} negligible in N such that the key obtained by Alice through this protocol is indistinguishable to a uniformly random bit string of the same length except with probability ϵ_{QKD}.

We discuss here why the three differences of $\mathcal{QKD}'$ preserve this indistinguishability.

1. First, we notice that difference (1) does not impact the security because the quantum communication channel in QKD is assumed to be controlled by the adversary. Any attack on a QKD protocol with such modification can be turned into an attack on QKD by simply applying $\text{Bob}_{\mathcal{QKD}'}$'s rotation to the input states of Bob_{QKD}.

2. Difference (2) preserves the main properties of the subset for the error rate computation, which are that it is uniformly random (among all subsets of the same size) and independent of the secrets of the players. These are indeed sufficient properties to prove that the error estimation gives a good estimate of the amount of errors outside that subset [8].

3. For the case of difference (3) we introduce some notation. Let K_A and K_B be the respective raw keys (after sifting and before error correction) of Alice and Bob in QKD. These keys are linked by the relation $K_A = K_B \oplus e$ where e is the error string that Bob ought to identify during error correction. By the linearity of the syndrome function $w(\cdot)$ of the error correcting code, we have that $w(K_A) = w(K_B) \oplus w(e)$. Hence, During the error correction step, as the eavesdropper learns $w(K_A)$, difference (3), which leaks $w(K_B)$ to the eavesdropper, is equivalent to leaking $w(e)$. The impact of the leakage of $w(e)$ (or equivalently of e) in QKD protocols has been studied in [25]. Under our assumptions, and because the protocol does not make use of more statistics than the qubit error rate during the parameter estimation step, this leak does not reveal any additional information on K_A to the eavesdropper. As a consequence, difference (3) does not influence the security of K_A.

In conclusion, none of the differences between standard QKD and $\mathcal{QKD}'$ influences the indistinguishability of Alice's final key to a random bit string. This concludes the proof.

B.2 Proof of Proposition 4

Let $\mathcal{M}^{\mathcal{I}}_{[h-1]}$ and $\mathcal{M}^{\mathcal{I}}_{[h]}$ be systems that respectively take as input the shares $s^{j_{[h-1]}}$ and $s^{j_{[h]}}$ and outputs instead the same amount of random bit strings of the same size. With this notation, our assumption on the distinguisher amounts to the fact that $\mathcal{D}_{\mathcal{QL}}$ distinguishes $\mathcal{QL}_{EB} \circ (\mathcal{M}_H || \mathcal{M}^{\mathcal{I}}_{[h-1]})$ from $\mathcal{QL}_{EB} \circ (\mathcal{M}_H || \mathcal{M}^{\mathcal{I}}_{[h]})$ with probability $\epsilon_{\mathcal{D}}$.

We wish to show that

$$\mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{A} \approx_0 \mathcal{QL}_{EB} \circ (\mathcal{M}_H || \mathcal{M}^{\mathcal{I}}_{[h-1]}), \tag{30}$$

and

$$(\mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{M}^{\mathcal{I}}_{Alice}) \circ \mathcal{A} \approx_0 \mathcal{QL}_{EB} \circ (\mathcal{M}_H || \mathcal{M}^{\mathcal{I}}_{[h]}). \tag{31}$$

We first focus on Equation (30). Note that in the two systems $\mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{A}$ and $\mathcal{QL}_{EB} \circ (\mathcal{M}_H || \mathcal{M}^{\mathcal{I}}_{[h-1]})$, the behavior of all players $j \in \mathcal{H} \setminus \{j_h, j_H\}$ is the same.

Furthermore, one can see that in both systems:

[8] Such a proof can be found in [4], Proposition 8.

- At the state distribution step, the input state of players j_h and j_H undergoes identical CNOT gates with freshly generated qubits and is output back. The remaining qubits are then measured in random basis (for Bob, the basis are $b^{j_H}_{[N]}$ in $\mathcal{QL}_{EB}$ and $\hat{b}^{Bob}_{[N]}$ in $\mathcal{QKD}'$).

- At the sifting step, in $\mathcal{QL}_{EB}$, a round n is discarded if (see Equation (19))

$$\begin{aligned} & b_n^{j_h} \oplus b_n^{j_H} \oplus \big[\bigoplus_{j \in [J] \setminus \{j_h, j_H\}} b_n^j \big] \neq 0 \\ \Leftrightarrow \quad & b_n^{j_h} \oplus b_n^{j_H} \oplus b_n^{(\mathcal{D})} \neq 0 \\ \Leftrightarrow \quad & b_n^{j_h} \neq \hat{b}_n^{Bob} \end{aligned} \tag{32}$$

  which is the exact discarding condition of the sifting step of $\mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{A}$.

- At the error estimation step in $\mathcal{QL}_{EB}$, a round n is considered as erroneous if

$$\begin{aligned} & (2v_n^{j_h} + b_n^{j_h}) + (2v_n^{j_H} + b_n^{j_H}) + \big(\sum_{j \in [J] \setminus \{j_h, j_H\}} (2v_n^j + b_n^j) \big) && = 2 \mod 4 \\ \Leftrightarrow \quad & 2(v_n^{j_h} + v_n^{j_H} + v_n^{(\mathcal{D})}) + b_n^{j_h} + b_n^{j_H} + b_n^{(\mathcal{D})} && = 2 \mod 4. \end{aligned} \tag{33}$$

  Note that because of the sifting step, all rounds satisfying Equation (32) have been discarded. As a consequence, for all $n \in [\mathcal{T}]$, $b_n^{j_h} = b_n^{j_H} \oplus b_n^{(\mathcal{D})}$ and thus $b_n^{j_h} + b_n^{j_H} + b_n^{(\mathcal{D})} = 2(b_n^{j_H} \vee b_n^{(\mathcal{D})})$[9]. Condition (33) is then equivalent to (see Equation (20))

$$\begin{aligned} & 2\big(v_n^{j_h} + v_n^{j_H} + v_n^{(\mathcal{D})} + (b_n^{j_H} \vee b_n^{(\mathcal{D})})\big) = 2 \mod 4 \\ \Leftrightarrow \quad & v_n^{j_h} + v_n^{j_H} + v_n^{(\mathcal{D})} + (b_n^{j_H} \vee b_n^{(\mathcal{D})}) = 1 \mod 2 \\ \Leftrightarrow \quad & v_n^{j_H} \oplus v_n^{(\mathcal{D})} \oplus (b_n^{j_H} \vee b_n^{(\mathcal{D})}) \neq v_n^{j_h} \\ \Leftrightarrow \quad & \hat{v}_n^{Bob} \neq v_n^{j_h} \end{aligned}$$

  which is exactly the condition under which rounds are considered erroneous in $\mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{A}$.

- Since the sifting and error estimation are similar, the announcements are made following the same process. Moreover, in both systems, they are based on the basis used to measure the state and the outcome of that measurement. This is indeed directly the case for $\mathcal{QL}_{EB}$. In $\mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{A}$, the announcements are those of $\text{Bob}_{\mathcal{QKD}'}$ based on $\hat{v}^{Bob}_{[N]}$, later XOR-ed by $\mathcal{A}$ with announcements corresponding to $v^{\mathcal{A}}_{[N]} = \hat{v}^{Bob}_{[N]} \oplus v^{Bob}_{[N]}$ (see Equation (25)). By linearity of the error correction and correctness check, the modified announcements exactly match the ones corresponding to the actual outcomes $v^{Bob}_{[N]}$ of the measurements of $\text{Bob}_{\mathcal{QKD}'}$.

As a consequence, $\mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{A}$ and $\mathcal{QL}_{EB} \circ (\mathcal{M}_H || \mathcal{M}^{\mathcal{I}}_{[h-1]})$ are indistinguishable, which gives Equation (30).

The same reasoning applies for Equation (31), the only difference being the share outputs of players $j_{[h]}$ that are replaced by randomly sampled bit strings in both systems.

Composing $\mathcal{D}_{\mathcal{QL}}$ onto Equations (30) and (31), and using the property that $\mathcal{D}_{\mathcal{QL}}$ distinguishes $\mathcal{QL}_{EB} \circ (\mathcal{M}_H || \mathcal{M}^{\mathcal{I}}_{[h-1]})$ from $\mathcal{QL}_{EB} \circ (\mathcal{M}_H || \mathcal{M}^{\mathcal{I}}_{[h]})$ with probability $\epsilon_{\mathcal{D}}$, we get that the system $\mathcal{A} \circ \mathcal{D}_{\mathcal{QL}}$ distinguishes $\mathcal{QKD}' \circ \mathcal{M}_{Bob}$ from $\mathcal{QKD}' \circ \mathcal{M}_{Bob} \circ \mathcal{M}^{\mathcal{I}}_{Alice}$ with that same probability $\epsilon_{\mathcal{D}}$. This concludes the proof.

[9] This is true for any binary a, b, c: $a = b \oplus c \Rightarrow a + b + c = 2(b \vee c)$.