

Tight Analysis of a One-Shot Quantum Secret Sharing Scheme

Santanu Majhi^{1,*} and Debajyoti Bera^{2,†}

¹*Indian Statistical Institute, Kolkata*

²*Indraprastha Institute of Information Technology Delhi*

(Dated: December 19, 2025)

Quantum communication protocols can be designed to detect eavesdropping attacks, something that classical technologies are unable to do since classical information can be replicated in a non-destructive manner. Eavesdropping detection is, therefore, a standard feature in all the proposed quantum secret sharing (QSS) protocols. However, detection is often done by a statistical analysis of the outcome of multiple decoy rounds, and this causes a significant communication overhead.

In our quest for a QSS protocol that works even in one round, we came across a one-shot secret-sharing framework proposed by Hsu (Phys. Rev. A 2003). The scheme was designed to work over public channels without requiring multiple rounds to detect eavesdropping but it lacked a thorough security analysis. In this work we present a complete characterisation of the correctness and security properties of this framework. Our characterisation allowed us to improve the original protocol to be more resistant towards eavesdropping. However, we prove a couple of impossibility results, including one that dictates that complete security against an eavesdropper is not possible in this framework. Thus, it is not possible to design a perfect QSS using this framework.

I. INTRODUCTION

Secret-sharing is one of the well-known and well-studied cryptographic tasks. In a very general sense, it involves a dealer who wants to entrust multiple parties, say N of them, with a common secret S but does not want to put all his eggs into one basket. The solution followed in secret sharing schemes is to “split” S into several parts (*aka.* shares) and share each part with a different party. The sharing should be done in a way such that any single individual, or even a set of individuals not pre-authorised by the dealer cannot gain any significant information about the secret; only an authorised group of parties will be able to reconstruct S by running some algorithm on their shares.

A common manner of defining authorised and unauthorised sets use the number of parties; e.g., in (k, N) -threshold schemes, any group containing k parties is authorised but any group with fewer parties is unauthorised. A $(2, 2)$ -scheme involves 2 parties and the shares of both are necessary to reconstruct S .

It is desirable for such schemes to be robust against eavesdropping attacks. The eavesdropper, whom we shall refer to as Eve, can be one of the parties who has gone rogue or a third-party. It is difficult for classical schemes to prevent Eve from learning the secret, specifically, if Eve can listen to every communication between the dealer and the parties. It is also unclear how to *detect* if an eavesdropping has happened due to the non-intrusive nature of classical observation. It is therefore common for classical secret sharing schemes to assume a secure channel for their communication.

However, a quantum communication channel has a few completely non-classical features that may allow protec-

tion against the above kind of vulnerabilities. First, quantum states destructively collapse upon measurement; thus, it is not possible for Eve to passively “read” the information sent by a dealer. Furthermore, Eve may not be able to retain a copy of a quantum state thanks to the no-cloning theorem; if Eve simply retains the transmitted qubits, the honest parties will raise a hue and cry! One of the most famous applications of this is the BB84 quantum key distribution scheme [1] that can detect the presence of an eavesdropper who merely tries to “read” information en passe.

Quantum secret sharing (QSS) extends the concept of classical secret sharing (SS) where either the secret is quantum or the protocol is quantum [2]. These schemes usually rely on features such as entanglement, superposition, interference, and no-cloning theorem to gain an extra mileage. The expectations are naturally higher for these. However, we are only aware of one theoretical model, proposed by Imai et al. [3], to analyse quantum secret sharing protocols. Their model focuses on the correctness of a quantum secret sharing protocol in which all parties are “curious-but-honest”; but it remains unclear whether that model holds in the presence of an active eavesdropper (*aka.* active participant) — someone who has the ability to capture the qubits en route and even replace them with her own qubits.

(Active) eavesdropper attacks are the worst-kinds in quantum schemes since the participants have access to additional information. If successful, such a participant can generate the secret with the involvement of fewer members than mandated; e.g., a participant who can intercept *all* messages between the dealer and the parties can always determine the secret on her own. A trivial approach for the honest party is to verify a reconstructed secret with the dealer. However, that either requires a private secure channel or multiple rounds (over a public channel) solely for detecting attacks. In the absence of these facilities, it may be possible to have an attack

* santanum_r@isical.ac.in

† dbera@iiitd.ac.in

scenario in which the eavesdropper knows the correct secret, but none (the dealer and the honest parties) have spotted any anomaly. Thus, it is common for many quantum secret sharing protocols to include additional steps to explicitly prohibit participant attacks and other kinds of attacks [2, 4].

The common safeguards involve sending decoy states. Decoy states are common in many quantum protocols; these protocols run in multiple rounds some of which are used for checking the presence of an eavesdropper and the rest are used for the desired task [5]. They naturally increase the cost of executing a protocol. For example, in one of the early and one of the most-cited HBB-QSS scheme [6], the dealer had to first share a GHZ state $\frac{1}{\sqrt{2}}[|000\rangle + |111\rangle]$ among two other parties, say Bob and Charlie, and then all three would independently measure their share in one of two non-commuting basis. Then they publicly would disclose their basis without revealing their measurement outcomes. Presence of an eavesdropper can be detected due to the disturbance an eavesdropping may cause to the outcomes. Thus, in the recommended implementation, a certain fraction of the rounds are used solely for detecting eavesdropping.

The current solutions beg an important question: *Is it possible to design a one-shot QSS scheme?* One that detects eavesdropping even in one round.

The motivation behind this work is an early QSS scheme proposed by Hsu [7], which we refer to as H03-QSS, that was designed to detect eavesdropping without using decoy rounds¹. Interestingly, the scheme could be used a framework, i.e., it allows variations in the form of choosing different sets of “nonce” states² Given that most of the proposed QSS schemes use multiple rounds to detect eavesdropping, the one-shot nature of H03-QSS appears to be an attractive blueprint for QSS schemes.

However, Hsu proposed the scheme without an adequate proof of security. Our primary objective was to tightly characterise the security of the H03-QSS scheme. Interestingly, we made a few surprising discoveries en route, including some negative results that fundamentally limit the security achievable within this framework.

	Original nonces	Our nonces
Recoverable	Yes	Yes
Secrecy attack	Resistant	Partial
Intercept-measure-resend	Resistant	Resistant
Intercept-fake-resend	Not	Partial

TABLE I. Comparison of the original nonces *vs.* our nonces with respect to their resistance towards different attacks.

¹ In the words of its author, “Detection is not based on the statistical violation of an outcome sequence, but on the correlation of the outcomes of a qubit pair.”.

² We use nonce to mean states chosen randomly but not kept secret, i.e., eventually disclosed. Similar to their role in secure protocols, they improve security by adding randomness.

A. Overview of Results

We will give a brief overview of H03-QSS here and explain it in detail in a later section. H03-QSS is executed in multiple stages. Apart from the secret s , the dealer commits to a random chosen nonce state, say c , in the first stage. Then the dealer constructs a state $|\psi_{c,s}\rangle$ using the secret s and nonce c , and shares it with the parties. $|\psi_{c,s}\rangle$ is constructed such that it reveals nothing about s . Later, the dealer discloses c , allowing authorized parties to recover s . The immediate observation is that no encoding of s is ever transmitted, reducing the risk of eavesdropping. A natural question, thus, arises: *Is it possible to prove that H03-QSS is indeed secure against an active rogue participant?*

The nonces recommended by Hsu are inspired by the reflection operators employed by the Grover’s search algorithm (see Table II). Our observation is that the role of the nonce states is central to the correctness and security guarantee of the scheme. Thus, even if the proposed nonces turn out to be vulnerable [8], could one choose a different set of nonces that retains both the one-shot nature of the original protocol and the security claimed about it?

Our overall discovery is that a one-shot QSS over public channels using Grover-type reflections is impossible without compromising on certain aspects of security. Following are the specific technical results that we show.

- (Section III) We tightly characterise the correctness and security requirements of H03-QSS in terms of various properties of the nonces. Our characterisation is information theoretic in nature and does not rely on complexity theoretic assumptions. The following results follow from our characterisation.
- We demonstrate that the original set of nonces in H03-QSS are vulnerable to eavesdropping (Section V); this generalizes an attack on H03-QSS demonstrated by Hao et al. [8]. In fact, we show how to generate an attack for any set of weak nonces.
- We prove two no-go results. The first one is that Eve always has a $\frac{1}{4}$ probability of remaining undetected after an intercept-fake-resend attack no matter what nonces are used (Section IV A).
- The second one is worse. If the scheme is designed to ensure secrecy, i.e., that the secret cannot be guessed by any individual party honestly running the protocol, then Eve can always launch an (intercept-fake-resend) attack to successfully learn the secret (Section IV B). Thus, to increase the chance of detecting this attack (which itself is bounded above by $3/4$), it is necessary to allow the honest parties a small chance to guess the secret.
- The negative results imply that secrecy must be compromised to prevent other attacks. But to what

extent? We present a set of nonces and prove that both secrecy and protection against intercept-fake-resend attack can be partially attained (Section VI). Table I presents a comparison of our nonces with the original ones.

6. The original scheme was developed only for classical 2-bit secrets, or 1-bit secret along with cheat-detection. On a positive note, we are able to show that H03-QSS can also be used to send arbitrary quantum states as secret (Observation 1).

The immediate advantage of our characterization is to do away with case-based analysis and hit-and-trial methods to demonstrate the correctness and security of H03-QSS (see, for example, the exhaustive tables in the related works [7, 8]). For example, we show that it is necessary and sufficient for the amplitudes of the basis states in any nonce to be $\frac{1}{2}$ for a secret to be recoverable by the honest parties, thus eliminating the need for exhaustive case analysis across all secrets and nonces.

B. Related Work

Hillery et al. [6] introduced the initial quantum secret sharing (HBB-QSS) scheme in 1999, utilizing the Greenberger-Horne-Zeilinger (GHZ) state. In that scheme, the dealer used ideas similar to the BB84-QKD protocol to create a shared secret quantum state with 2 other parties; however, it did not allow the dealer to send a secret of his choice.

The scheme that we will analyse and improve upon is a (2,2)-scheme that allows a dealer to send a classical 1-bit secret of his choice; the earliest (2,2) schemes to share a desired secret were designed by Cleve et al. [9].

Proving security of multiparty computation is in general difficult due to multiple points of vulnerability, and quantum schemes always bring in additional abilities of adversarial parties. Unfortunately, most quantum “secure” protocols are often proposed without a formal proof of security leading to later discoveries of vulnerabilities.

Take for instance the HBB-QSS scheme mentioned earlier [6]. Soon after the scheme was proposed, Karlsson et al. explained how a dishonest player may evade detection by attacking the order in which the messages in that scheme were announced [10]. Unfortunately, most QSS schemes that have been proposed are based on the framework used in HBB-QSS, and many of them, like HBB-QSS, are vulnerable to participant attacks [10–12].

Another framework for QSS has been entanglement-swapping followed by measurements in a carefully-chosen basis [13]. However, such schemes are also known to suffer from participant attacks [14].

The H03-QSS scheme proposed by Hsu [7], that we analyse in this work, is also known to be vulnerable to participant attack. This was later pointed out by Hao et al. [8] whose attack crucially used the properties of the

$ +\rangle$	$ -\rangle$	$ +i\rangle$	$ -i\rangle$
$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$	$\frac{1}{\sqrt{2}}(0\rangle + i 1\rangle)$	$\frac{1}{\sqrt{2}}(0\rangle - i 1\rangle)$

TABLE II. States used to construct nonces.

$ +\rangle +\rangle$	$ +\rangle -\rangle$	$ +\rangle +i\rangle$	$ +\rangle -i\rangle$
$ -\rangle +\rangle$	$ -\rangle -\rangle$	$ -\rangle +i\rangle$	$ -\rangle -i\rangle$
$ +i\rangle +\rangle$	$ +i\rangle -\rangle$	$ +i\rangle +i\rangle$	$ +i\rangle -i\rangle$
$ -i\rangle +\rangle$	$ -i\rangle -\rangle$	$ -i\rangle +i\rangle$	$ -i\rangle -i\rangle$

TABLE III. Nonces used in the original H03-QSS protocol.

nonces proposed by Hsu. To fix the scheme they proposed that decoy states can be used. Our intention in this work is to explore the possibility of designing better nonces such that eavesdropping can be detected as originally envisioned, without decoy states.

Several works have explored extensions and improvements of Hsu’s protocol. Tseng et al. [15, 16] observed that H03-QSS, like many quantum schemes for secret sharing, requires the parties to store quantum states for a long time and apply quantum operations on their share. Thus, they proposed a variation that combined the HBB-QSS style of generating a classical secret by measuring states in superpositions and involving the Grover reflection operators employed by Hsu. Similar to HBB-QSS, they also use decoy states to detect eavesdropping.

There has been several interesting directions that research on QSS is leading into. Several research groups are investing into efficient hardware implementations of QSS schemes [17] while some others are studying the performance in a noisy environment [18]. However, Our work is of a theoretical nature and

If H03-QSS was to be implemented and deployed on the currently available hardware, it would be important to analyse its correctness and security guarantees in a NISQ environment, similar to how Basak et al. [18] analyse the HBB-QSS and two other QSS schemes. We left out such error analysis in this work, partly due to the theoretical limitations of H03-QSS that we discovered.

II. BACKGROUND

A. Grover-search Operator

The design of H03-QSS is based on an interesting observation made by its author about the “reflection” operators used in the Grover’s algorithm.

Suppose $|\alpha\rangle$ is some 2-qubit state. The reflection operator is defined below.

$$U_{|\alpha\rangle} = I - 2|\alpha\rangle\langle\alpha|$$

Observe that $U_{|\alpha\rangle}^\dagger = U_{|\alpha\rangle}$. If s is a bit string, U_s may be written instead of $U_{|s\rangle}$.

Notn.	Description	Notn.	Description
m	mode	J	proposed nonce set
$ \alpha\rangle$	fake state shared by Eve	\mathfrak{Scc}	secret bit to be sent
$ \psi_i\rangle$	nonces in J	ρ	$ \alpha\rangle\langle\alpha $
s	2-bit secret	U_x	$I - 2 x\rangle\langle x $
ρ^B	$Tr_E(\rho)$	\mathcal{I}	original nonce set
$ \psi_{i,s}\rangle$	$U_s \psi_i\rangle$ (sent by dealer)	$\sigma_{i,s}$	$ \psi_{i,s}\rangle\langle\psi_{i,s} $
b	regenerated secret	$\sigma_{i,s}^B$	$Tr_E(\sigma_{i,s})$
V_i	Eve's local unitary		

TABLE IV. List of notations used in this work.

The behaviour of this operator can be understood by its action on any (orthonormal) basis that contains $|\alpha\rangle$:

$$U_{|\alpha\rangle}|\beta\rangle = \begin{cases} -|\alpha\rangle & \beta = \alpha \\ |\beta\rangle & \langle\beta|\alpha\rangle = 0 \end{cases}$$

The Grover's algorithm for unordered search in an array of 4 elements with 1 solution essentially uses the identity:

$$-U_c U_s |c\rangle = |s\rangle, \quad (1)$$

where $|c\rangle = \frac{1}{2}[|0\rangle + |1\rangle]^{\otimes 2} = |++\rangle$, and s is a any 2-bit string. The author observed that the identity extends to other initial states (up to some global phase) chosen from the set $\mathcal{I} = \{|x\rangle \otimes |y\rangle : x, y \in \{+, -, +i, -i\}\}$ (refer to Table II for description of the states).

This operator is an integral part of the H03-QSS scheme that we describe in the next section.

B. Grover-based H03-QSS by Hsu

In this subsection, we will give a quick overview of the H03-QSS scheme³. Let $\mathfrak{Scc} \in \{0, 1\}$ denote the secret a dealer has to share among two parties named as Eve and Bob⁴. A schematic of the protocol is illustrated in Figure 1.

Stage-I: (Distribution of Shares)

1. Dealer choose a mode $m \in \{\text{SECRET}, \text{DETECT}\}$ uniformly at random.
2. Dealer maps \mathfrak{S} and m to a 2-bit string s according to a known mapping

$$\mathcal{M} : \{0, 1\} \times \{\text{SECRET}, \text{DETECT}\} \rightarrow \{0, 1\}^2.$$

In the original protocol, the following mapping was used which we will continue to use.

³ Hsu denoted the nonce by s for which we use $|\psi\rangle$, and he denoted the secret by w for which we use s .

⁴ As is the norm, Bob is always curious-but-honest.

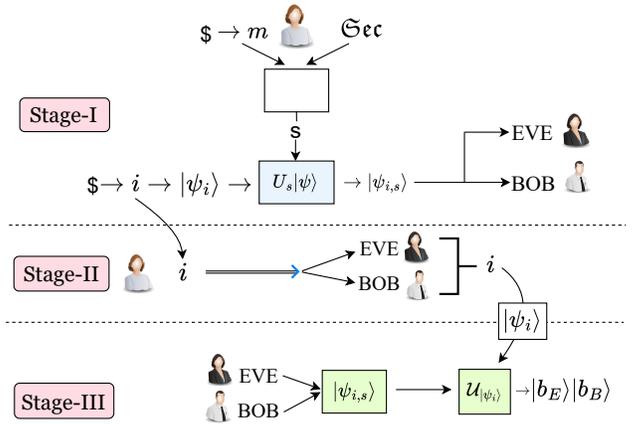


FIG. 1. The first three stages of the protocol when Eve is acting honestly. The symbol $\$$ indicates drawing from a uniform random distribution, and \Rightarrow indicates communication over a public channel.

- $\mathcal{M}(\mathfrak{S}, \text{SECRET}) \mapsto \mathfrak{S}\bar{\mathfrak{S}}$.
- $\mathcal{M}(\mathfrak{S}, \text{DETECT}) \mapsto \{00, 11\}$ uniformly at random.
- Thus, $s = \mathfrak{S}\bar{\mathfrak{S}}$ with probability $\frac{1}{2}$, 00 with probability $\frac{1}{4}$, and 11 with probability $\frac{1}{4}$.

3. A two-qubit nonce $|\psi_i\rangle$ is chosen from a known set of nonces. In the H03-QSS proposed by Hsu, the nonces are chosen from \mathcal{I} defined in Sec. II A.
4. Dealer generates the two-qubit state $|\psi_{i,s}\rangle = U_s|\psi_i\rangle$ and sends one qubit to Eve and another to Bob (both the qubits are symmetrical in nature).
5. After both the parties acknowledge receiving their shares (over a public channel), the dealer moves to Stage-II.

Stage-II: (Nonce Announcement)

6. Dealer announces (over a public channel) the choice of nonce $|\psi_i\rangle$.

Stage-III: (Secret Recovery)

7. When the parties want to regenerate the secret, they get together and apply $U_{|\psi_i\rangle}$ to their joint-state.
8. Then they perform a measurement in the standard-basis; suppose, the outcome is $|b\rangle$ for $b \in \{00, 01, 10, 11\}$.

Stage-IV: (Reconciliation)

9. A cheat-detection strategy is executed based on s . The strategy followed in the original protocol is described next. Let b_E and b_B denote the first and second bits of b , respectively.
10. If $b_E \neq b_B$, i.e., $b \in \{01, 10\}$, consider b as the regenerated secret, and b_E as \mathfrak{Sec} . All the (good) folks happily retire.
11. If $b_E = b_B$, i.e., $b \in \{00, 11\}$, parties publicly announce b to the dealer, who follows the next steps.
 - If $m = \text{DETECT}$, and $s = b$, announce over classical channel to drop this round (eavesdropper presence is not detected, but \mathfrak{Sec} was not shared either).
 - If $m = \text{DETECT}$, and $s \neq b$, announce over classical channel the presence of an eavesdropper.
 - If $m = \text{SECRET}$, announce over classical channel the presence of an eavesdropper.
12. If $m = \text{DETECT}$ but the parties did not announce their generated secrets, dealer announces over classical channel the presence of an eavesdropper.
13. The above steps are applicable to the mapping \mathcal{M} defined in the original protocol; they can be easily adapted for any other mapping without impacting security guarantees in any manner.

If both parties are honest, they will generate $b = s$ in Stage-3 since

$$U_{|\psi_i\rangle} |\psi_{i,s}\rangle = U_{|\psi_i\rangle} U_s |\psi_i\rangle = |s\rangle \quad \text{as per Eq. 1.}$$

s can be used to derive the actual secret bit \mathfrak{Sec} , so we will focus only on generating s and call it the “secret”.

The cheat-detection steps detect the presence of an eavesdropper by following this rule-of-thumb.

- In the detection mode, the dealer expects that the parties will announce a generated secret b that exactly matches s .
- In the secret message mode, the dealer expects the parties *not to* announce anything at all, i.e., b is neither 01 or 10.

Earlier, Imai et al. [3] had proposed an information-theoretic model of QSS. A correct QSS protocol has to satisfy two conditions of correctness: (1) Recoverability – the players in any set of authorized players should be able to gain complete information about the secret; this was shown by Rietjens to be equivalent to the existence of a mapping that can regenerate S [19]. (2) Secrecy – the players of any unauthorized group should *not* be able to extract significant information about the secret. The H03-QSS scheme can be proved correct according to Imai’s characterization. Unfortunately, Imai et al.’s model is not applicable in the presence of an eavesdropper.

C. Attack against H03-QSS ([8])

In this section we discuss the idea of the attack discovered by Hao et al. [8]; a schematic of the attack is presented in Fig. 2.

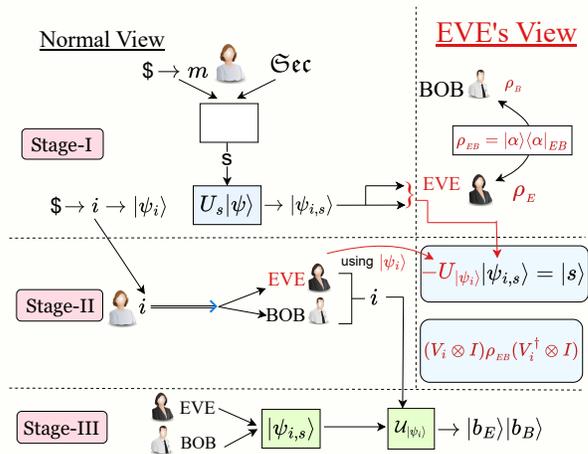


FIG. 2. Eavesdropping attack against H03-QSS. Observe that Eve has successfully generated $|s\rangle$ in Stage-II itself without Bob’s involvement.

As is common in active participant attacks, for this attack we assume that Eve has the ability to intercept the message from the dealer to Bob as well as send message to Bob pretending to be the dealer. To launch an attack, Eve first prepares the 2-qubit state $|\alpha\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$.

In Stage-I, when the dealer transmits the two qubits, say in state $|\psi_{i,s}\rangle$, Eve captures both and keeps them with her. She immediately sends Bob the second qubit of $|\alpha\rangle$ pretending to be the dealer. The state $|\alpha\rangle$ does not depend on $|\psi_{i,s}\rangle$.

In Stage-II, after the dealer announces the nonce $|\psi_i\rangle$, Eve applies $U_{|\psi_i\rangle}$ on $|\psi_{i,s}\rangle$ which is the secret-reconstruction procedure, and obtains $|s\rangle$. That’s it — Eve has found the secret.

However, if Bob and Eve were to come together in Stage-III to generate the secret, they would apply $U_{|\psi_i\rangle}$ to $|\alpha\rangle$ and the resultant state may not pass the cheat-detection steps of the protocol. Thus, to avoid detection, in Stage-II Eve applies some V_i , chosen according to $|\psi_i\rangle$ and s , on her share of $|\alpha\rangle$ such that

$$(V_i \otimes I) |\alpha\rangle = (V_i \otimes I) \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle] = U_s |\psi_i\rangle = |\psi_{i,s}\rangle.$$

The reader may refer to Hao et al. [8] for the exhaustive list of V_i for each $|\psi_i\rangle$ and s .

Thus, at the end of Stage-II, Eve has managed to create a joint state with Bob which is exactly the state the dealer wanted to share with both of them. So, when Bob and Eve want to reconstruct the secret, the reconstruction step works as expected and they are able to recreate the original secret. All the cheat-detection steps naturally fail to detect this tampering.

The attack leaves much to ponder upon. Is the state $|\alpha\rangle$ and the set of operators $\{V_i\}$ unique, or it is possibly to construct them from the nonces? Is it possible to launch the attack using some different $|\alpha\rangle$?

III. MATHEMATICAL CHARACTERIZATION

A desirable QSS scheme must satisfy three conditions: recoverability, secrecy and security.

Recoverability indicates the probability with which an authorised set (here, both the parties) can create the same secret used by the dealer. If the probability is 1, then the secret is perfectly recoverable.

In the absence of active participant attacks (Eve is only honest but curious), secrecy is defined as the protection against unauthorized parties (here Eve) knowing the secret (without Bob's help). Unfortunately, secrecy is fundamentally impossible to achieve in any active participant attack since Eve has to simply intercept both the shares, send any state to Bob, and then when the dealer announces the nonce, run the secret recovery operations on her intercepted qubits to reconstruct the dealer's secret. It is easy to see that recoverability and secrecy both cannot be satisfied at the same time.

A scheme is said to be secure if it holds its ground against different types of attacks. Since participant attacks are strictly more powerful compared to external attacks, we will only discuss the former.

In all active participant attacks, Eve, the active participant, is allowed the ability to intercept all the shares in Stage-I, i.e., she gets hold of the state $|\psi_{i,s}\rangle$. Next she create a 2-qubit state $|\alpha\rangle$; this state could either be created after measuring $|\psi_{i,s}\rangle$ in some basis or could be chosen from a fixed family of states. Eve sends one qubit of $|\alpha\rangle$ to Bob.

Attacks involving a measurement to create α are known as *intercept-measure-resend*, while those in which Eve creates $|\alpha\rangle$ without measurement (thus, retaining $|\psi_{i,s}\rangle$ as it is) are called as *intercept-fake-resend*.

After Bob and Eve informs the dealer about receiving their shares, the dealer announces the nonce $|\psi_i\rangle$ in Stage-II. This automatically prevents any possibility of timing attack. At this point, Eve can apply some unitary, possibly $U_{|\psi_i\rangle}$, to her qubits. She does it hoping to set the joint-state of her and Bob's qubits to some state.

Next, in the secret recovery phase (Stage-III), Eve and Bob get together and both present their qubits on which they apply $U_{|\psi_i\rangle}$. Eve hopes that the outcome will pass the cheat detection steps in Stage-IV.

Given that secrecy is not possible in a perfectly recoverable scheme, we can at best require that any form of eavesdropping be detected in a secure QSS scheme.

In the following subsections we derive mathematical conditions for the correctness and security of the H03-QSS scheme but with an arbitrary set of nonces denoted J ; the number of nonces will be denoted k . Earlier works by Hsu [7] and Hao et al. [8] did not provide a general

characterization, and that made it difficult to rigorously analyse their approaches and study their enhancements.

A. Recoverability

For H03-QSS, the secret recovery step involves applying $U_{|\psi\rangle}$ on the shared state $U_s|\psi\rangle$ for every nonce $|\psi\rangle \in J$. This gives us the following mathematical definition of recoverability.

Definition 1 (Recoverability). *An H03-QSS scheme is said to be recoverable if for every secret s and every nonce $|\psi\rangle \in J$, s can be recovered by both the parties following the steps of Stage-III, i.e.,*

$$\begin{aligned} U_{|\psi\rangle}U_s|\psi\rangle &= |s\rangle \text{ (up to some phase),} \\ \text{or equivalently, } U_{|\psi\rangle}|s\rangle &= U_s|\psi\rangle \text{ (up to some phase).} \end{aligned} \tag{2}$$

This unfortunately requires checking all combinations of secrets and nonces — an approach undertaken by Hsu (see Table I of [7]). We now present an equivalent but simpler condition that is easy to check.

Lemma 1. *An equivalent condition for Equation 2 is that*

$$|\langle s|\psi\rangle| = \frac{1}{2}$$

holds for all secret $|s\rangle$ and all nonce $|\psi\rangle \in J$.

The proof is available in Appendix A. An interesting aspect of the proof is that it holds for any 2-qubit state $|\psi\rangle$, unlike only the standard basis states ($|00\rangle, |01\rangle, |10\rangle, |11\rangle$) from which Hsu chose his secrets.

Observation 1. *An H03-QSS scheme remains recoverable for any 2-qubit state $|s\rangle$ satisfying Lemma 1.*

This allows us to extend H03-QSS to any 2-qubit state as secret. Of course, the secrets need to additionally meet the requirements of secrecy and security.

B. Secrecy

Another correctness condition of a QSS scheme is secrecy — how safe is a share with any curious but honest party. A secret QSS scheme should not allow such a party to know the secret without the involvement of the other party.

Definition 2 (Secrecy). *Secrecy of a party is defined as the probability with which that party, in a curious but honest scenario, cannot guess a randomly chosen \mathfrak{S} on its own.*

Observe that secrecy is at most $\frac{1}{2}$, since any party can always guess \mathfrak{S} by randomly tossing a coin, but this is

the best possible value. Secrecy of 0 indicates that the secret can be correctly inferred.

The characterization below uses Eve as the honest but curious party, but an equivalent characterization exists for Bob as well. An honest but curious Eve can neither intercept Bob's qubits nor send him fake qubits. Thus, to launch an attack, Eve has to construct the secret s based on her share of $|\psi_{i,s}\rangle$ and the nonce $|\psi_i\rangle$ announced in Stage-II.

According to the mapping \mathcal{M} used in the original protocol, s is chosen as:

$$\mathfrak{S}\bar{\mathfrak{S}} \text{ with prob. } \frac{1}{2}, 00 \ \& \ 11 \text{ with prob. } \frac{1}{4} \text{ each.}$$

Thus, the secret state $|\psi_{i,s}\rangle$ is chosen according to:

$$|\psi_{i,\mathfrak{S}\bar{\mathfrak{S}}}\rangle \text{ with prob. } \frac{1}{2}, |\psi_{i,00}\rangle \ \& \ |\psi_{i,11}\rangle \text{ with prob. } \frac{1}{4} \text{ each.}$$

Therefore, after the nonce $|\psi_i\rangle$ is announced, Eve's share, denoted $\lambda E_i^{\mathfrak{S}}$, is the partial trace of the above mixture. We use the notation $\sigma_{i,s}$ to denote $|\psi_{i,s}\rangle\langle\psi_{i,s}|$.

$$\lambda E_i^{\mathfrak{S}} = \text{Tr}_B \lambda_i^{\mathfrak{S}}, \quad \text{where,}$$

$$\begin{aligned} \lambda_i^{\mathfrak{S}} &= \frac{1}{2} |\psi_{i,\mathfrak{S}\bar{\mathfrak{S}}}\rangle\langle\psi_{i,\mathfrak{S}\bar{\mathfrak{S}}}| + \frac{1}{4} |\psi_{i,00}\rangle\langle\psi_{i,00}| + \frac{1}{4} |\psi_{i,11}\rangle\langle\psi_{i,11}| \\ &= \frac{1}{2} \sigma_{i,\mathfrak{S}\bar{\mathfrak{S}}} + \frac{1}{4} \sigma_{i,00} + \frac{1}{4} \sigma_{i,11}. \end{aligned}$$

To guess \mathfrak{S} , Eve can distinguish between λE_i^0 and λE_i^1 , and the probability of this is upper bounded by

$$\frac{1}{2} + \frac{1}{4} \|\lambda E_i^0 - \lambda E_i^1\|_1 = \frac{1}{2} + \frac{1}{8} \|\text{Tr}_B(\sigma_{i,01} - \sigma_{i,10})\|_1.$$

Lemma 2. *The probability of Eve's ability to guess \mathfrak{S} for any nonce $|\psi_i\rangle$ may be calculated as*

$$\frac{1}{2} + \frac{1}{8} \|\sigma_{i,01}^B - \sigma_{i,10}^B\|_1.$$

Thus, if $\sigma_{i,01}^B = \sigma_{i,10}^B$, then Eve cannot meaningfully guess \mathfrak{S} . The lemma allows us to characterise secrecy as the expected value of one minus the above quantity (since we are interested in the event of not being able to guess) where the expectation is taken over the choice of the nonce.

Lemma 3. *The secrecy with respect to Eve may be calculated as $\frac{1}{2} - \frac{1}{8|\mathcal{J}|} \sum_i \|\sigma_{i,01}^B - \sigma_{i,10}^B\|_1$.*

C. Intercept-Measure-Resend Attack

In this attack, Eve intercepts the qubit meant for Bob, giving her both qubits of $|\psi_{i,s}\rangle$, and these she then decides to measure in an attempt to get some information about s . Further, to avoid detection, she must ensure that the protocol plays according to the script, i.e., (i) she must send some qubit to Bob, say in state $\rho_B = \text{Tr}_E(\rho_{EAB})$ pretending it to come from the dealer, (ii) she must present a qubit in a suitable state, say in state $\rho_E = \text{Tr}_{AB}(\rho_{EAB})$, for the secret recovery step

jointly executed by her and Bob. Here, ρ_{EAB} denotes the joint-state of a register that Eve prepares for this purpose; the register may include additional qubits that we indicate using the subsystem A , apart from one (subsystem B) to send to Bob and another (subsystem E) to send during the secret recovery phase.

Hsu, in his paper, considered a common choice for the measurement basis based on a guess $|\psi_j\rangle$ of the nonce. Eve would then apply $U_{|\psi_j\rangle}$ to attempt recovery, yielding some secret s' (possibly incorrect). To avoid detection, she prepares $|\psi_{j,s}\rangle = U_{s'} |\psi_j\rangle$, keeps one qubit, and sends the other to Bob. The leftover qubit of $|\psi_{j,s}\rangle$ would be used for the secret recovery stage. If her guess j equals i , then, of course, the joint-state of Eve and Bob would be $|\psi_{i,s}\rangle$, and not only Eve would know the secret, no one will have any clue of her attack. Thus, the probability of success of this attack is the probability that Eve is able to generate the original secret s better than a random guessing. Hsu demonstrated that his scheme was secure by displaying an exhaustive case analysis for the original set of nonces (\mathcal{I}). However, we can characterize the probability that Eve will observe s in a much simpler manner using Eq. 2:

$$\begin{aligned} |\langle s | U_{|\psi_j\rangle} |\psi_{i,s}\rangle|^2 &= |\langle s | U_{|\psi_j\rangle} U_s |\psi_i\rangle|^2 \\ &= |\langle \psi_j | U_s U_s |\psi_i\rangle|^2 \\ &= |\langle \psi_j | \psi_i\rangle|^2. \end{aligned}$$

This allows us to compute the success probability of guessing using only the nonces in a more elegant manner.

Interestingly, the above analysis is applicable only when Eve follows the prescription described by Hsu, i.e., Eve first guessing the nonce. Other possibilities are left open? We observe if the state of the qubits intercepted by Eve is independent of the secret bit $\mathfrak{S}\mathfrak{e}\mathfrak{c}$, then Eve would not be able to extract any meaningful information about $\mathfrak{S}\mathfrak{e}\mathfrak{c}$ through a measurement. This allows us to derive a sufficient condition for protection against any form of intercept-measure-resend attack.

Lemma 4. *An H03-QSS scheme ensures protection against intercept-measure-resend attacks if*

$$\begin{aligned} \frac{1}{|\mathcal{J}|} \sum_i \lambda_i^0 &= \frac{1}{|\mathcal{J}|} \sum_i \lambda_i^1, \text{ or equivalently,} \\ \sum_i \sigma_{i,01} &= \sum_i \sigma_{i,10}. \end{aligned}$$

$\lambda_i^{\mathfrak{S}}$ was defined in Section IIIB as the state of the shares distributed by the dealer when secret bit is \mathfrak{S} and nonce is $|\psi_i\rangle$.

D. Intercept-fake-resend Attack

We discussed this attack in Section IIC earlier. This is the strongest of the attacks that we consider in this work in the sense that Eve is always able to determine

the secret. Thus, the best protection is to ensure that Eve's attack is detected in the Reconciliation Stage.

On the other hand, from Eve's perspective, if she is able to transform $|\alpha\rangle$ to exactly $|\psi_{i,s}\rangle$ then her tampering cannot be detected any further. Furthermore, even if $|\alpha\rangle$ is transformed to a state close to $|\psi_{i,s}\rangle$, the key recovery step will generate the original secret with a reasonable probability. Much to Eve's delight, the Reconciliation Stage will successfully pass.

Thus, we will be concerned only about "Eve's tampering leads to generation of s in Stage-III", an event that we will denote $\mathcal{E}(s)$ and that indicates a weakness of the scheme.

The next lemma derives the probability of $\mathcal{E}(s)$.

Lemma 5. *Fix any secret s . Let $\sigma_{s,i}$ denote the density operator $U_s |\psi_i\rangle \langle \psi_i| U_s$ where s is some secret and $|\psi_i\rangle$ is some nonce. Let ρ denote any two-qubit state $|\alpha\rangle \langle \alpha|$. Let $\{V_1, V_2, \dots, V_k\}$ denote the single-qubit unitary operators Eve applies corresponding the different nonces (V_i may depend on $\sigma_{s,i}$ and s).*

$$\text{Then, } \Pr_{|\psi\rangle}[\mathcal{E}(s)] = \sum_{i=1}^k \frac{1}{k} F(\sigma_{i,s}, (V_i \otimes I) \rho (V_i^\dagger \otimes I)) \quad (3)$$

Proof. The joint-state of Eve and Bob, after Eve has applied V_i on her qubit, can be written as $(V_i \otimes I) |\alpha\rangle$.

The probability that the the key-recovery step generates s from this state can be expressed as

$$\begin{aligned} & |\langle s | U_{|\psi_i\rangle} (V_i \otimes I) |\alpha\rangle|^2 \\ &= |\langle \psi_i | U_s (V_i \otimes I) |\alpha\rangle|^2 \\ &= F(U_s |\psi_i\rangle \langle \psi_i| U_s, (V_i \otimes I) |\alpha\rangle \langle \alpha| (V_i^\dagger \otimes I)) \\ &= F(\sigma_{i,s}, (V_i \otimes I) \rho (V_i^\dagger \otimes I)), \end{aligned}$$

using Eq. 2 and conditioned on the nonce being $|\psi\rangle$. The claim follows since the probability of each nonce is $\frac{1}{k}$. \square

The above lemma allows us to derive a sufficient condition for $\mathcal{E}(s)$ to not hold (i.e., for the scheme to be secure) that we state in the form of the next lemma. The lemma is obtained by tracing out Eve's state from Eq. 3 and using the fact that subsystem fidelity is no less than the fidelity of a larger system. Let $\sigma_{i,s}^B$ denote $\text{Tr}_E \sigma_{i,s}$ and ρ^B denote any single-qubit state; define the largest expected fidelity between them as $\mathbb{F}(s)$.

$$\mathbb{F}(s) = \max_{\rho^B} \sum_{i=1}^k \frac{1}{k} F(\sigma_{i,s}^B, \rho^B).$$

Lemma 6. *The probability that s is recovered is upper bounded as:*

$$\Pr_{\text{nonce}} [\mathcal{E}(s)] \leq \mathbb{F}(s) \quad (4)$$

For H03-QSS scheme with any set of nonces, $\mathbb{F}(s)$ can be computed by solving the corresponding optimization problem to find the best ρ^B that is independent of s .

If $s=00$ or 01 , then Eve's attack remains undetected if either 00 or 01 is recovered in Stage-III, and the probability of this happening is upper-bounded by $2\mathbb{F}(s)$. On the other hand, if $s=10$ or 11 , then Eve's attack remains undetected if exactly s is recovered in Stage-III whose probability is at most $\mathbb{F}(s)$. Thus, a low $\mathbb{F}(s)$ for every s ensures that Eve's attack can be detected almost always.

We actually show that the upper bound in Lemma 7 is tight, i.e., we show how Eve can launch an attack such that she manages to have s recovered in the Secret Recovery Stage with the highest possible probability.

Lemma 7. *Let s be some secret. Eve can select an $|\alpha\rangle$ and a set of operators $\{V_1, V_2, \dots, V_k\}$ such that*

$$\Pr_{|\psi\rangle}[\mathcal{E}(s)] = \mathbb{F}(s).$$

The proof of this lemma is based on Uhlmann's theorem and is constructive; i.e., the state $|\alpha\rangle$ and the operators $\{V_1, \dots, V_k\}$ can be explicitly constructed following the steps of the proof of Uhlmann's theorem.

Let us first state the version of Uhlmann's theorem that we use; it a slight variation of the version given by Nielsen and Chuang [20].

Theorem 1 (Uhlmann's theorem). *Let α and β be two states over some Hilbert space \mathcal{H}^B . Let \mathcal{H}_A be the Hilbert space of a reference system that is a copy of \mathcal{H}_B . Let $|b\rangle$ be any purification of β in $\mathcal{H}_A \otimes \mathcal{H}_B$. Then, one can construct a purification $|a\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ of α such that the following holds.*

$$F(\alpha, \beta) = F(|a\rangle \langle a|, |b\rangle \langle b|)$$

The proof of Lemma 7 is below.

Proof. We can directly invoke Uhlmann's theorem to prove the above lemma. Let $\rho = |\alpha\rangle \langle \alpha|$ be any purification of ρ^B (thus, ρ is independent of i, s); for example, we can use the canonical purification of ρ^B .

We immediately get the following.

$$F(\sigma_{i,s}^B, \rho^B) = F(\sigma_{i,s}^*, \rho),$$

where $\sigma_{i,s}^*$ is some purification of $\sigma_{i,s}^B$.

Furthermore, since all purification are equivalent with respect to unitary operations on the reference system, and $\sigma_{i,s} = U_s |\psi_i\rangle \langle \psi_i| U_s$ is a purification of $\sigma_{i,s}^B$, there exists a unitary operator, say $U_{i,s}$, such that

$$\begin{aligned} \sigma_{i,s}^* &= (U_{i,s} \otimes I) \sigma_{i,s} (U_{i,s}^\dagger \otimes I), \\ F(\sigma_{i,s}^B, \rho^B) &= F((U_{i,s} \otimes I) \sigma_{i,s} (U_{i,s}^\dagger \otimes I), \rho) \\ &= F(\sigma_{i,s}, (U_{i,s}^\dagger \otimes I) \rho (U_{i,s} \otimes I)). \end{aligned}$$

$$\begin{aligned} \sum_{i=1}^k F(\sigma_{i,s}^B, \rho^B) &= \sum_{i=1}^k F(\sigma_{i,s}, (U_{i,s}^\dagger \otimes I)\rho(U_{i,s} \otimes I)) \\ \sum_{i=1}^k \frac{1}{k} F(\sigma_{i,s}^B, \rho^B) &= \sum_{i=1}^k \frac{1}{k} F(\sigma_{i,s}, (U_{i,s}^\dagger \otimes I)\rho(U_{i,s} \otimes I)) \\ &= \Pr[\mathcal{E}(s)] \quad (\text{from Eq. (3)}) \end{aligned}$$

Now ρ^B is any purification for Uhlmann's theorem, hence

$$\max_{\rho^B} \sum_{i=1}^k \frac{1}{k} F(\sigma_{i,s}^B, \rho^B) = \Pr_{|\psi\rangle}[\mathcal{E}(s)].$$

□

We now state the main theorem of this section that simply combines the main results proved earlier.

Theorem 2. *For any fixed s , Eve can always launch an intercept-fake-resend attack such that the parties generate s in the Secret Recovery stage with probability $\mathbb{F}(s)$, taken over the choice of the nonce, and this probability cannot be improved any further.*

Thus, a high-value of $\mathbb{F}(s)$, e.g., $\mathbb{F}(s) = 1$, implies that Eve can always evade detection if the secret chosen by the dealer is s .

IV. A LIMIT ON ONE-SHOT SECURITY

In this section we discuss a few results that highlight the underlying technical limitations of H03-QSS, even under the best possible choice of nonces.

A. Security against Intercept-fake-resend Attack

In this section we prove, contrary to our initial belief, that Eve always has a chance of avoiding detection after launching an intercept-fake-resend attack for any set of nonces.

First, we prove that average fidelity of a set of single-qubit (possibly mixed) states with an optimally chosen single-qubit (possibly mixed) state is at least $\frac{1}{2}$.

Lemma 8. *Let β_1, \dots, β_k denote any k single-qubit (possibly mixed) states. Then, there exists a single-qubit state γ (possibly mixed) such that the average fidelity of β_i from γ is at least $\frac{1}{2}$.*

$$\max_{\rho_\gamma} \sum_{i=1}^k \frac{1}{k} F(\rho_{\beta_i}, \rho_\gamma) \geq \frac{1}{2}$$

Proof. The fidelity between two single qubit states ρ_β and ρ_γ can be written as [21]

$$\begin{aligned} F(\rho_\beta, \rho_\gamma) &= \frac{1}{2} \left[1 + \vec{\beta} \cdot \vec{\gamma} + \sqrt{(1 - \|\vec{\beta}\|^2)(1 - \|\vec{\gamma}\|^2)} \right] \\ &\geq \frac{1}{2} [1 + \vec{\beta} \cdot \vec{\gamma}]. \end{aligned}$$

where, $\vec{\beta}$ and $\vec{\gamma}$ denote the Bloch vectors of ρ_β and ρ_γ , respectively. Expanding $\vec{\beta} \cdot \vec{\gamma} = \frac{1}{2} (\|\vec{\beta}\|^2 + \|\vec{\gamma}\|^2 - \|\vec{\beta} - \vec{\gamma}\|^2)$ allows us to lower bound the above fidelity as:

$$F(\rho_\beta, \rho_\gamma) \geq \frac{1}{2} + \frac{1}{4} [\|\vec{\beta}\|^2 + \|\vec{\gamma}\|^2 - \|\vec{\beta} - \vec{\gamma}\|^2].$$

We will use this bound on the sum of the fidelities in the statement of the lemma. Denote the Bloch vector of ρ_{β_i} by $\vec{\beta}_i$.

$$\begin{aligned} \max_{\rho_\gamma} \sum_{i=1}^k F(\rho_{\beta_i}, \rho_\gamma) &\geq \\ \frac{k}{2} + \frac{1}{4} \max_{\gamma} &\left[\sum_{i=1}^k \|\vec{\beta}_i\|^2 + k\|\vec{\gamma}\|^2 - \sum_{i=1}^k \|\vec{\beta}_i - \vec{\gamma}\|^2 \right]. \end{aligned}$$

Let's expand the last sum in the above expression.

$$\sum_{i=1}^k \|\vec{\beta}_i - \vec{\gamma}\|^2 = \sum_{i=1}^k \|\vec{\beta}_i\|^2 + k\|\vec{\gamma}\|^2 - 2 \left(\sum_{i=1}^k \vec{\beta}_i \right) \cdot \vec{\gamma}.$$

Substituting gives us

$$\max_{\rho_\gamma} \sum_{i=1}^k F(\rho_{\beta_i}, \rho_\gamma) \geq \frac{k}{2} + \frac{k}{2} \max_{\gamma} \vec{\beta} \cdot \vec{\gamma}, \quad (5)$$

where, $\vec{\beta} = \frac{1}{k} \sum_{i=1}^k \vec{\beta}_i$. The dot product is maximized when $\vec{\gamma}$ is parallel to $\vec{\beta}$, i.e., choose $\vec{\gamma}_{\max} = c\vec{\beta}$ for some positive c .

Since c and k are both constants, we can rewrite Eq. 5:

$$\max_{\rho_\gamma} \sum_{i=1}^k F(\rho_{\beta_i}, \rho_\gamma) \geq \frac{k}{2} + \frac{ck}{2} \|\vec{\beta}\|^2 \geq \frac{k}{2}$$

Hence, the average fidelity satisfies

$$\max_{\rho_\gamma} \frac{1}{k} \sum_{i=1}^k F(\rho_{\beta_i}, \rho_\gamma) \geq \frac{1}{2}.$$

□

Recall that Eve first generates the dealer's secret s in Stage-II using the knowledge of $|\psi_i\rangle$, and then manipulates the joint-state $|\alpha\rangle$ accordingly. The above lemma essentially lower bounds $\mathbb{F}(s) \geq \frac{1}{2}$, for any s Eve desires, leading to the following corollary.

Corollary 1. *Irrespective of the number of nonces, for any s , Eve can suitably tamper the protocol in Stage-I such that exactly $|s\rangle$ is generated in the key-recovery stage with probability at least $\frac{1}{2}$.*

The corollary does not quite imply that Eve can manipulate the protocol to have the s chosen by the dealer be generated in Stage-III. This is due to the reason that γ in the above lemma (whose purification would be the state $|\alpha\rangle$ shared by Eve) may be different for different sets of $\{\beta_i\}_{i=1}^k$.

Nevertheless, we show how to lower bound the success probability of Eve. As per Lemma 8, $\mathbb{F}(01) \geq \frac{1}{2}$. Further, using Lemma 7, Eve can determine $|\alpha\rangle$ and a set of operators $\{V_i\}_{i=1}^k$ such that the parties can recover 01 in Stage-III with probability at least $\frac{1}{2}$.

Now, here is one strategy that Eve can adopt: Eve selects $|\alpha\rangle$ and a set of operators $\{V_i\}_{i=1}^k$ such that the string “01” is generated in Stage-III, regardless of the announced nonce and the s she computes in Stage-II.

Recall that, in the SECRET mode, attack is not detected if 01 is generated in Stage-III. Since the probability of choosing this mode is exactly $\frac{1}{2}$, Eve can succeed with probability at least $(1/2) \cdot (1/2) = 1/4$. We summarise this as the following theorem.

Theorem 3. *For any set of nonces, Eve can always launch an intercept-fake-resend attack whose probability of detection is at most $\frac{3}{4}$.*

B. Secrecy Implies Intercept-fake-resend Attack

In Section IV A we analysed the security of the protocol against the *intercept-fake-resend* attack. In particular, Corollary 1 established that Eve can always ensure that a particular s is generated in Stage-III, thus leading to a successful attack with probability at least $\frac{1}{4}$. This begs the question whether the dealer can cap the probability of attack to $\frac{1}{4}$ and no more. We show that this is not possible unless the dealer wants to lower the expectation of secrecy.

We essentially prove a trade-off between secrecy and protection against intercept-fake-resend attack assuming that the dealer designs a perfectly recoverable scheme.

Consider a set of nonces such that the secret is perfectly recoverable (Lemma 1). We start by characterising the individual shares of Eve and Bob for this scenario.

Lemma 9. *Recoverability implies that then the reduced density operators of Eve and Bob must lie on the XY-plane of the Bloch sphere.*

Proof. Let $|\psi_i\rangle$ denote any nonce that satisfies recoverability. Then $\langle s|\psi_i\rangle = \frac{1}{2}$ for all $s \in \{00, 01, 10, 11\}$. Therefore, $|\psi_{i,s}\rangle = U_s|\psi\rangle$ can be written as

$$U_s|\psi\rangle = \frac{1}{2} [|00\rangle + e^{i\alpha_1} |01\rangle + e^{i\alpha_2} |10\rangle + e^{i\alpha_3} |11\rangle]. \quad (6)$$

Suppose the first qubit is sent to Eve and the second one to Bob. Let’s analyse $\sigma_{i,s}^B = \text{Tr}_E |\psi_{i,s}\rangle\langle\psi_{i,s}|$ that

represents the state of Bob’s share; that of Eve’s share has a similar analysis.

It is straightforward to show the following from Eq. 6:

$$\langle 0|\sigma_{i,s}^B|0\rangle = \langle 1|\sigma_{i,s}^B|1\rangle = \frac{1}{2}$$

This implies that $\sigma_{i,s}^B$, when represented in terms of its Bloch vectors as $\sigma_{i,s}^B = \frac{I}{2} + \frac{1}{2}[r_X\sigma_X + r_Y\sigma_Y + r_Z\sigma_Z]$, must have $r_Z = 0$, i.e., $\sigma_{i,s}^B$ must lie on the XY plane. \square

The next lemma characterises $\sigma_{i,s}$.

Lemma 10. *Recoverability implies that $|\psi_{i,s}\rangle$ has one of the following structures.*

- $|\psi_{i,s}\rangle$ is a bipartite state $|E_{i,s}\rangle|B_{i,s}\rangle$ in which both $|E_{i,s}\rangle$ and $|B_{i,s}\rangle$ lie on the XY-plane.
- $|\psi_{i,s}\rangle$ is an equal superposition of $|E_{i,s}\rangle|B_{i,s}\rangle$ and $|E_{i,s}^\perp\rangle|B_{i,s}^\perp\rangle$ in which $|E_{i,s}\rangle$ and $|E_{i,s}^\perp\rangle$ lie on the Z-axis but $|B_{i,s}\rangle$ and $|B_{i,s}^\perp\rangle$ lie on the XY-plane.

Proof. We will use the fact that $|\psi_{i,s}\rangle$ is a purification of $\sigma_{i,s}^B$ and $\sigma_{i,s}^E$ both of which must be on the XY-plane of the Bloch sphere.

Any mixed state on the on the XY-plane can be expressed as

$$c_1|e_1\rangle\langle e_1| + c_2|e_1^\perp\rangle\langle e_1^\perp|,$$

where c_1, c_2 are (real) positive constants adding up to 1, $|e_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_1}|1\rangle)$, and $|e_1^\perp\rangle$ is orthogonal to $|e_1\rangle$.

This allows us to represent $|\psi_{i,s}\rangle$ using Schmidt decomposition:

$$|\psi_{i,s}\rangle = \sqrt{c_1}|E_{i,s}\rangle|B_{i,s}\rangle + \sqrt{c_2}|E_{i,s}^\perp\rangle|B_{i,s}^\perp\rangle,$$

where,

$$|B_{i,s}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_i}|1\rangle) \text{ and } |E_{i,s}\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\mu_i}\sin\frac{\theta}{2}|1\rangle$$

are two single-qubit pure states (here, $\phi_i, \mu_i \in [0, 2\pi]$ and $\theta \in [0, \pi]$).

Let’s write amplitudes of $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ in $|\psi_{i,s}\rangle$.

$$\text{amplitude of } |00\rangle = \frac{1}{\sqrt{2}} \left[\sqrt{c_1} \cos\frac{\theta}{2} - \sqrt{c_2} \sin\frac{\theta}{2} \right]$$

$$\text{amplitude of } |01\rangle = \frac{1}{\sqrt{2}} \left[\sqrt{c_1} \cos\frac{\theta}{2} + \sqrt{c_2} \sin\frac{\theta}{2} \right] e^{i\phi_i^s}$$

$$\text{amplitude of } |10\rangle = \frac{1}{\sqrt{2}} \left[\sqrt{c_1} \sin\frac{\theta}{2} + \sqrt{c_2} \cos\frac{\theta}{2} \right] e^{i\mu_i^s}$$

$$\text{amplitude of } |11\rangle = \frac{1}{\sqrt{2}} \left[\sqrt{c_1} \sin\frac{\theta}{2} - \sqrt{c_2} \cos\frac{\theta}{2} \right] e^{i(\phi_i^s + \mu_i^s)}$$

We know from Eq. 6 that recoverability also implies that the above amplitudes have their real parts as $\frac{1}{2}$.

$$\left| \sqrt{c_1} \cos \frac{\theta}{2} - \sqrt{c_2} \sin \frac{\theta}{2} \right| = \frac{1}{\sqrt{2}} \quad (P_1)$$

$$\left| \sqrt{c_1} \cos \frac{\theta}{2} + \sqrt{c_2} \sin \frac{\theta}{2} \right| = \frac{1}{\sqrt{2}} \quad (P_2)$$

$$\left| \sqrt{c_1} \sin \frac{\theta}{2} + \sqrt{c_2} \cos \frac{\theta}{2} \right| = \frac{1}{\sqrt{2}} \quad (P_3)$$

$$\left| \sqrt{c_1} \sin \frac{\theta}{2} - \sqrt{c_2} \cos \frac{\theta}{2} \right| = \frac{1}{\sqrt{2}} \quad (P_4)$$

From P_3 and P_4 , we get these.

$$c_1 \sin^2 \frac{\theta}{2} + c_2 \cos^2 \frac{\theta}{2} = \frac{1}{2} \quad (P_5)$$

$$2\sqrt{c_1}\sqrt{c_2} \sin \theta = 0 \quad (P_6)$$

Similarly, from P_1 and P_2 , we get

$$c_1 \cos^2 \frac{\theta}{2} + c_2 \sin^2 \frac{\theta}{2} = \frac{1}{2} \quad (P_7)$$

Equations P_5 , P_6 and P_7 imply that one of these hold.

- $c_1 = 0$, implying that $c_2 = 1$ and $\theta = \frac{\pi}{2}$.
- $c_1 = 1$, implying that $c_2 = 0$ and $\theta = \frac{\pi}{2}$.
- $\theta = 0$ or π , implying that $c_1 = c_2 = \frac{1}{2}$.

For the first two scenarios, $|\psi_{i,s}\rangle$ is a bipartite state $|E_{i,s}\rangle|B_{i,s}\rangle$. By Lemma 9, both $|E_{i,s}\rangle$ and $|B_{i,s}\rangle$ lie on the XY -plane.

For the third, $|\psi_{i,s}\rangle$ is an equal superposition of $|E_{i,s}\rangle|B_{i,s}\rangle$ and $|E_{i,s}^\perp\rangle|B_{i,s}^\perp\rangle$. Since $\theta = 0$ or π , $|E_{i,s}\rangle$ lie on the Z -axis and $|B_{i,s}\rangle$ lie on the XY -plane. For any state on the XY -plane, its orthogonal state also lies on the XY -plane, and for any state on the Z -axis, its orthogonal state lies on the Z -axis. Thus, both $|E_{i,s}\rangle$ and $|E_{i,s}^\perp\rangle$ lie on the Z -axis and both $|B_{i,s}\rangle$ and $|B_{i,s}^\perp\rangle$ lie on the XY -plane.

The required claims about the Schmidt coefficients are obtained. \square

We are now ready to state and prove our theorem capturing the trade-off between secrecy and intercept-fake-resend protection.

Theorem 4. *Consider an H03-QSS scheme that is perfectly recoverable. At least one of the following is always possible.*

1. *Eve can mount an intercept-fake-resend attack that cannot be detected at all.*
2. *Secrecy is violated for one of the parties (among Eve and Bob), i.e., one of the parties can determine the secret with probability 1 without launching any interception attack.*

Proof. Consider an H03-QSS scheme with a set of nonces $\{|\psi_i\rangle\}_{i \in J}$.

Without loss of generality, we focus on the nonce $|\psi_1\rangle$, since the analysis for the other states $|\psi_i\rangle$ proceeds in an identical manner. In Lemma 10, we proved that $|\psi_{1,01}\rangle$ is either a bipartite state or an equal superposition. Next, we analyse these two possibilities separately.

Let's begin by assuming that $|\psi_{1,01}\rangle$ is a bipartite state $|E_{1,01}\rangle|B_{1,01}\rangle$ in which both states lie on the XY -plane. Thus, we can represent

$$\begin{aligned} |\psi_{1,01}\rangle &= |E_{1,01}\rangle \otimes |B_{1,01}\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_1}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{i\mu_1}|1\rangle) \\ &= \frac{1}{2}[|00\rangle + e^{i\mu_1}|01\rangle + e^{i\phi_1}|10\rangle + e^{i(\phi_1+\mu_1)}|11\rangle]. \end{aligned}$$

Observe that $|\psi_{1,10}\rangle = U_{10}|\psi_1\rangle = U_{10}U_{01}|\psi_{1,01}\rangle$.

$$\begin{aligned} |\psi_{1,10}\rangle &= \frac{1}{2}[|00\rangle - e^{i\mu_1}|01\rangle - e^{i\phi_1}|10\rangle + e^{i(\phi_1+\mu_1)}|11\rangle] \\ &= \frac{1}{\sqrt{2}}(|0\rangle - e^{i\phi_1}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - e^{i\mu_1}|1\rangle) \\ &= (\text{denoted}) |E_{1,01}^\perp\rangle \otimes |B_{1,01}^\perp\rangle \end{aligned}$$

So, the states Eve receives for $s = 01$ and $s = 10$ are pure and orthogonal to each other implying that $\|\sigma_{1,01}^E - \sigma_{1,10}^E\|_1 = 2$. Since Eve can distinguish between these states with probability 1, she violates the requirement of best possible secrecy at her end (see Lemma 2).

A similar attack on secrecy at Bob's end also exists. Thus, should we care for perfect secrecy, *all the nonces* should be chosen such that for all i , $|\psi_{i,01}\rangle$ is an equal superposition state of the form specified in Lemma 10, i.e.,

$$|\psi_{i,01}\rangle = \frac{1}{\sqrt{2}}|E_{i,01}\rangle|B_{i,01}\rangle + \frac{1}{\sqrt{2}}|E_{i,10}^\perp\rangle|B_{i,10}^\perp\rangle$$

in which $|E_{i,10}\rangle$ and $|E_{i,10}^\perp\rangle$ lie on the XY -axis and $|B_{i,10}\rangle$ and $|B_{i,10}^\perp\rangle$ lie on the Z -axis.

Let's compute Bob's state for any nonce $|\psi_i\rangle$ and s .

$$\sigma_{i,s}^B = \text{Tr}_E |\psi_{i,s}\rangle \langle \psi_{i,s}| = \frac{1}{2}|B_{i,s}\rangle \langle B_{i,s}| + \frac{1}{2}|B_{i,s}^\perp\rangle \langle B_{i,s}^\perp| = I/2$$

When the reduced density operator of Bob equals $\frac{I}{2}$ for all i , it is known that Eve can launch an intercept-fake-resend attack that cannot be detected with non-zero probability; in fact, the details of such an attack has already been discussed in Section II C.

Thus, preventing both the scenarios in the statement of the theorem is not possible. \square

V. ANALYSING ORIGINAL H03-QSS SCHEME

In this section we analyse the vulnerabilities of the original H03-QSS scheme using our characterization.

$ \psi_1\rangle = +\rangle +\rangle = \frac{1}{2}[00\rangle + 01\rangle + 10\rangle + 11\rangle]$
$ \psi_2\rangle = -\rangle -\rangle = \frac{1}{2}[00\rangle - 01\rangle - 10\rangle + 11\rangle]$
$ \psi_3\rangle = \frac{1}{2}[00\rangle + 01\rangle - 10\rangle + 11\rangle]$
$ \psi_4\rangle = \frac{1}{2}[00\rangle - 01\rangle + 10\rangle + 11\rangle]$

TABLE V. Nonce states proposed by us.

The original scheme uses 16 nonces formed by taking all possible combinations of two qubits from the set $T = \{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$. These nonces can be shown to satisfy recoverability, has perfect secrecy, and ensures protection against the intercept-measure-resend attack.

It is straightforward to verify that for any nonce $|\psi\rangle$ and any $s \in \{00, 01, 10, 11\}$, $|\langle s|\psi\rangle| = \frac{1}{2}$ (see Table III), and thus, all its secrets are recoverable as per Lemma 1.

To show that secrecy is preserved, the following lemma will be useful. It can be directly verified from the nonces; the complete table of $\{\sigma_{i,s}\}_{i,s}$ is presented in Appendix B.

Lemma 11. *For any i and s , $\text{Tr}_E \sigma_{i,s} = \text{Tr}_B \sigma_{i,s} = I/2$.*

The above lemma immediately implies that the condition in Lemma 3 is met, i.e., the original protocol preserves perfect secrecy for both the parties.

To analyse the scheme's protection against an intercept-measure-resend attack, observe that

$$\begin{aligned} \sum_i \sigma_{i,01} &= \sum_i |\psi_{i,01}\rangle \langle \psi_{i,01}| \\ &= \sum_i U_{01} |\psi_i\rangle \langle \psi_i| U_{01} \\ &= U_{01} \left(\sum_{b \in T} \sum_{d \in T} |b\rangle \langle b| \otimes |d\rangle \langle d| \right) U_{01} \\ &= U_{01} \cdot 4I \cdot U_{10} = 4I. \end{aligned}$$

A similar analysis shows that $\sum_i \sigma_{i,10} = 4I$. Thus, according to Lemma 4, the nonces are able to prevent an intercept-measure-resend attack.

However, it completely fails to protect against the intercept-fake-resend attack. We will show this by computing $\mathbb{F}(s)$ for every s .

We showed in Lemma 11 that $\sigma_{i,s}^B = \text{Tr}_E \sigma_{i,s} = I/2$ for all nonce $|\psi_i\rangle$ and all secret s . Now, let's choose any 2-qubit state $|\alpha\rangle$ that is a purification of $I/2$; Hao et al. [8] chose $|\alpha\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$ but we can choose any other state too, e.g., $\frac{1}{\sqrt{2}}[|++\rangle - |--\rangle]$. Clearly, $F(\sigma_{i,s}^B, |\alpha\rangle \langle \alpha|) = 1$, and thus $\mathbb{F}(s) = 1$ for all s .

Using $|\alpha\rangle \langle \alpha|$ as ρ^B in lemma 7, we can conclude that Eve can always launch an attack by sharing a suitable $|\alpha\rangle$ between her and Bob and later tampering it remotely using an operator from a set $\{V_1, \dots, V_k\}$.

It can be further verified that if $|\alpha\rangle$ is chosen to be $\frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$, then the operators match exactly those proposed by Hao et al. [8, Table 2].

nonces in J	$ \psi_1\rangle$	$ \psi_2\rangle$	$ \psi_3\rangle$	$ \psi_4\rangle$
$s = 00$	$U_{00} ++\rangle$	$U_{00} --\rangle$	$- +\rangle -\rangle$	$- -\rangle +\rangle$
$s = 01$	$U_{01} ++\rangle$	$U_{01} --\rangle$	$ -\rangle -\rangle$	$ +\rangle +\rangle$
$s = 10$	$U_{10} ++\rangle$	$U_{10} --\rangle$	$ +\rangle +\rangle$	$ -\rangle -\rangle$
$s = 11$	$U_{11} ++\rangle$	$U_{11} --\rangle$	$ -\rangle +\rangle$	$ +\rangle -\rangle$

TABLE VI. The table shows the states $|\psi_{i,s}\rangle = U_s |\psi_i\rangle$ for every nonce $|\psi_i\rangle \in J$ and all secret s .

The following theorem summarises the appropriateness of the original nonces.

Theorem 5. *H03-QSS using the nonces shown in Table III is recoverable, ensures secrecy for both the parties, prevents an intercept-measure-resend attack but fails against an intercept-fake-resend attack, i.e., a Eve can learn the secret after intercepting the qubits en route without anyone noticing the attack anytime ever after.*

VI. FORTIFYING THE H03-QSS SCHEME

In this section we propose a new set of nonces that improves the security of H03-QSS with respect to the intercept-fake-resend attack by slightly compromising on the secrecy of the secrets. To strengthen the scheme, we propose a set of four nonces, denoted J , and listed in Table V. We retained two of the original nonces and added two of our own.

A. Recoverability

It is easy to verify from Table V that $|\langle s|\psi\rangle| = \frac{1}{2}$ for all $s \in \{00, 01, 10, 11\}$ and $|\psi\rangle$. Thus, by Lemma 1, the QSS scheme using J as nonces is perfectly recoverable.

B. Secrecy

Let's discuss the secrecy of Bob first.

We can use Table VII to calculate that

$$\sum_{i=1}^4 \|\sigma_{i,01}^B - \sigma_{i,10}^B\|_1 = 2\| |+\rangle\langle +| - |-\rangle\langle -| \|_1 = 4.$$

Based on this and by Lemma 3, secrecy of Bob is $\frac{3}{8}$ which is quite close to the optimal value of $\frac{1}{2}$. Thus, Bob can independently guess the secret with expected probability at most $\frac{5}{8}$ where the expectation is taken over the randomly chosen nonce.

A similar analysis for Eve also shows that Eve too can guess the secret with expected probability at most $\frac{5}{8}$.

nonces in J	$ \psi_1\rangle$	$ \psi_2\rangle$	$ \psi_3\rangle$	$ \psi_4\rangle$
$s = 00$	$I/2$	$I/2$	$ -\rangle\langle- $	$ +\rangle\langle+ $
$s = 01$	$I/2$	$I/2$	$ -\rangle\langle- $	$ +\rangle\langle+ $
$s = 10$	$I/2$	$I/2$	$ +\rangle\langle+ $	$ -\rangle\langle- $
$s = 11$	$I/2$	$I/2$	$ +\rangle\langle+ $	$ -\rangle\langle- $

TABLE VII. States $\sigma_{i,s}^B$ for every nonce $|\psi_i\rangle$ and every s .

nonces in J	$ \psi_1\rangle$	$ \psi_2\rangle$	$ \psi_3\rangle$	$ \psi_4\rangle$
$s = 00$	$I/2$	$I/2$	$ +\rangle\langle+ $	$ -\rangle\langle- $
$s = 01$	$I/2$	$I/2$	$ -\rangle\langle- $	$ +\rangle\langle+ $
$s = 10$	$I/2$	$I/2$	$ +\rangle\langle+ $	$ -\rangle\langle- $
$s = 11$	$I/2$	$I/2$	$ -\rangle\langle- $	$ +\rangle\langle+ $

TABLE VIII. States $\sigma_{i,s}^E$ for every nonce $|\psi_i\rangle$ and every s .

C. Intercept-measure-resend

Next we will show that the new nonces satisfy the conditions of Lemma 4. First, observe in Table VI that

$$U_{01} |--\rangle = U_{10} |++\rangle \quad \text{and} \quad U_{10} |--\rangle = U_{01} |++\rangle.$$

Thus, both $\sum_{i=1}^4 \sigma_{i,01}$ and $\sum_{i=1}^4 \sigma_{i,10}$ are equal mixtures of these four states:

$$U_{01} |++\rangle, U_{01} |--\rangle, |--\rangle, |++\rangle.$$

This implies that the condition in Lemma 4 holds, and thus, the new nonces provide protection against any intercept-measure-resend attack.

D. Intercept-fake-resend Prevention

We will start by computing $\mathbb{F}(s)$ as we did in Section V. Fix any s , and let ρ^B be any single-qubit (possibly mixed) state. From Table VII we can observe that the multiset $\{\sigma_{i,s}^B : i \in \{1, 2, 3, 4\}\}$ is exactly $\{I/2, I/2, |+\rangle\langle+|, |-\rangle\langle-|\}$ two of which are pure states. We will use the fact that for pure $\sigma_{i,s}^B$, $F(\sigma_{s,i}^B, \rho^B) = \text{Tr}\{\sigma_{s,i}^B \rho^B\}$.

$$\begin{aligned} & \sum_{i \in \{1, 2, 3, 4\}} F(\sigma_{s,i}^B, \rho^B) \\ &= 2F(I/2, \rho^B) + \text{Tr}\{|+\rangle\langle+| \rho^B\} + \text{Tr}\{|-\rangle\langle-| \rho^B\} \\ &\leq 2 + \text{Tr}\{I \cdot \rho^B\} = 3. \end{aligned}$$

So, we get that

$$\mathbb{F}(s) = \frac{1}{4} \sum_{i \in \{1, 2, 3, 4\}} F(\sigma_{s,i}^B, \rho^B) \leq \frac{3}{4}.$$

Therefore, Eve won't be able to force generation of a *particular* s in Stage-III with probability more than $1/4$.

Recall that, in the DETECT mode, the attack is detected if the exact s chosen by the dealer ($s \in \{00, 11\}$) is not generated; we show above that this happens with probability at least $1/4$. On the other hand, in the SECRET mode, the attack is *not* detected if either 01 or 10 is generated, and Eve may be succeed in that with a very high probability.

Since the dealer choses each mode with equal probabilities, the overall probability that Eve's attack can be detected is at least $\frac{1}{8}$.

We state the overall behaviour of our nonces in the following lemma.

Lemma 12. *The probability of detecting an intercept-fake-resend attack using our nonces is at least $\frac{1}{8}$.*

While this may not meet our general expectations, recall that the probability is zero in the original scheme.

E. Discussion

The overall behaviour of our nonces with respect to security and correctness is given below.

Theorem 6. *H03-QSS using the nonces shown in Table V is recoverable, and it prevents any intercept-measure-resend attack. Further, no honest party can guess the secret on its own with probability more than $\frac{5}{8}$ and any attempt by the dishonest party to learn the secret using an intercept-fake-resend attack will be detected with probability at least $\frac{1}{8}$.*

It is important to contrast this with Theorem 5 and observe that while the latter does not allow an honest party to guess the secret, it allows a dishonest party to learn the secret in a completely covert manner. An additional consideration is the fact that in this framework the dishonest party *always* has a reasonable chance ($\frac{1}{4}$) of remaining undetected after mounting an attack (Theorem 3), no matter what nonces are used.

VII. CONCLUSION

In this work we have analysed the conditions of correctness and security (against different types of attacks) on a one-shot supposedly-perfect quantum secret sharing scheme [7] denoted H03-QSS. Even though the author of the scheme included various heuristics to prevent the attacks and explained how various attacks can be prevented, his analysis was done by considering a few typical operations an adversary could launch. A subsequent work by Hao et al. [8] proved him wrong.

The benefit and importance of mathematical models of attacks and provable claims of security is, thus, super-critical for security protocols. Riding on the above sentiments, we present a formal model of eavesdropping attack for H03-QSS and explain how its security against this attack can be improved as compared to the original version. We analysed two-types of eavesdropping attacks, one in which Eve measures the intercepted state (and thus destroys it), and in another, retains it until

the dealer announces a nonce. However, we show that it is impossible to design a perfectly one-shot secret sharing scheme in this framework. Thus, the quest of such a scheme, of-course in a different framework, continues.

It is easy to workaroud the vulnerability arising from the original nonces by running the protocol for multiple rounds, involving a few decoy ones, and running statistical tests [8]. This of course destroys the one-shot nature.

In our opinion, all the limitations of the H03-QSS framework arises from the requirement of recoverability (see Section III A). Recoverability imposes that the nonces have equiprobable amplitudes, and this forces the states of the shares obtained by the individual parties to take specific symmetric forms. The lower bound proofs in Section IV heavily rely on the symmetries. The conditions for recoverability, in turn, are derived from the reflection operations in the Grover's iterator (Eq. 1). Thus, a natural direction towards designing a more resilient one-shot framework is to explore reconstruction mechanisms beyond these operations.

-
- [1] C. H. Bennett and G. Brassard, Theoretical Computer Science **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.
 - [2] A. K. Chattopadhyay, S. Saha, A. Nag, and S. Nandi, Computer Science Review **51**, 100608 (2024).
 - [3] H. Imai, J. Mueller-Quade, A. C. A. Nascimento, P. Tuijls, and A. Winter, A quantum information theoretical model for quantum secret sharing schemes (2003), arXiv:quant-ph/0311136 [quant-ph].
 - [4] S.-Y. Kuo, K.-C. Tseng, C.-C. Yang, and Y.-H. Chou, EPJ Quantum Technol. **10** (2023).
 - [5] H.-K. Lo, X. Ma, and K. Chen, Physical Review Letters **94**, 10.1103/physrevlett.94.230504 (2005).
 - [6] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
 - [7] L.-Y. Hsu, Phys. Rev. A **68**, 022306 (2003).
 - [8] L. Hao, J. Li, and G.-L. Long, Science China Physics, Mechanics & Astronomy **53**, 491 (2010).
 - [9] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
 - [10] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
 - [11] Q.-X. Bai, Int. J. Theor. Phys. **60**, 1705 (2021).
 - [12] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, Phys. Rev. A **76**, 062324 (2007).
 - [13] Z. Ying-Qiao, J. Xing-Ri, and Z. Shou, Chinese Physics **15**, 2252 (2006).
 - [14] S. Ting-Ting, Z. Jie, G. Fei, W. Qiao-Yan, and Z. Fu-Chen, Chinese Physics B **18**, 1333 (2009).
 - [15] H. Y. Tseng, C. W. Tsai, T. Hwang, and S. Y. Kuo, International Journal of Theoretical Physics **51**, 3101 (2012).
 - [16] Z. Yu, Journal of Physics: Conference Series **2209**, 012031 (2022).
 - [17] Y. Qin, J. Cheng, J. Ma, D. Zhao, Z. Yan, X. Jia, C. Xie, and K. Peng, Phys. Rev. Res. **6**, 033036 (2024).
 - [18] N. Basak, N. Das, G. Paul, K. Nandi, and N. Patel, Quantum Inf. Process. **22** (2023).
 - [19] K. Rietjens, I. L. Schoenmakers, and P. Tuijls, *Quantum secret sharing schemes*, Ph.D. thesis, Citeseer (2004).
 - [20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).
 - [21] R. Jozsa, Journal of Modern Optics **41**, 2315 (1994), <https://doi.org/10.1080/09500349414552171>.

Appendix A: Appendix: Proof of Lemma 1

Proof. Let's first extend $\{|s\rangle\}$ to some basis $\{|b_1\rangle, |b_2\rangle, \dots, |b_n\rangle\}$. Without loss of generality, let $|b_1\rangle = |s\rangle$. Now we can represent any nonce $|\psi\rangle$ in this basis.

$$|\psi\rangle = \sum_{i=1}^N \alpha_i |b_i\rangle$$

Now,

$$\begin{aligned} U_{|\psi\rangle} U_{|s\rangle} |\psi\rangle &= -(2|\psi\rangle\langle\psi| - I) \left[\sum_{i=2}^N \alpha_i |b_i\rangle - \alpha_1 |b_1\rangle \right] \\ &= -2|\psi\rangle \left\langle \psi \left| \sum_i \alpha_i |b_i\rangle - \alpha_1 |b_1\rangle \right. \right\rangle + \left[\sum_{i=2}^N \alpha_i |b_i\rangle - \alpha_1 |b_1\rangle \right] \\ &= -2|\psi\rangle \left[\sum_{i=2}^N |\alpha_i|^2 - |\alpha_1|^2 \right] + \left[\sum_{i=2}^N \alpha_i |b_i\rangle - \alpha_1 |b_1\rangle \right] \\ &= -2|\psi\rangle \left[\sum_{i=2}^N |\alpha_i|^2 - |\alpha_1|^2 \right] + \left[\sum_{i=2}^N \alpha_i |b_i\rangle - \alpha_1 |b_1\rangle \right] \\ &= -2|\psi\rangle [1 - 2|\alpha_1|^2] + \left[\sum_{i=2}^N \alpha_i |b_i\rangle - \alpha_1 |b_1\rangle \right] \\ &= -[2 - 4|\alpha_1|^2] |\psi\rangle + \sum_{i=2}^N \alpha_i |b_i\rangle - \alpha_1 |b_1\rangle \\ &= -[2 - 4|\alpha_1|^2 - 1] \sum_{i=2}^N \alpha_i |b_i\rangle - [2 - 4|\alpha_1|^2 + 1] \alpha_1 |b_1\rangle \end{aligned}$$

As we assume $|b_1\rangle$ is the secret, therefore

$$|\langle b_1 | U_{|\psi\rangle} U_{|s\rangle} |\psi\rangle|^2 = |\alpha_1|^2 (3 - 4|\alpha_1|^2)^2$$

For the forward direction, suppose that the scheme is perfectly recoverable. Then,

$$|\langle b_1 | U_{|\psi\rangle} U_{|s\rangle} |\psi\rangle|^2 = 1.$$

$$\therefore |\alpha_1|^2 (3 - 4|\alpha_1|^2)^2 = 1 \equiv |\alpha_1| (3 - 4|\alpha_1|^2) = \pm 1$$

Hence, the possible values for $|\alpha_1|$ are $\frac{1}{2}$ and 1. However, we discard $|\alpha_1| = 1$ since it results in the state $|b_1\rangle$ only. The only possibility is

$$|\langle b_1 | \psi \rangle|^2 = \frac{1}{4}, \quad \text{or,} \quad |\langle b_1 | \psi \rangle| = \frac{1}{2},$$

as required.

The shared secret in this case would be

$$|\psi_{i,s}\rangle = U_{|s\rangle} |\psi\rangle = \sum_{i=2}^N \alpha_i |b_i\rangle - \alpha_1 |b_1\rangle$$

Conversely, let $|\langle b_1 | \psi \rangle|^2 = |\alpha_1|^2 = \frac{1}{4}$, where $|b_1\rangle$ is the secret state. Now,

$$|\langle b_1 | U_{|\psi\rangle} U_{|s\rangle} |\psi\rangle|^2 = |\alpha_1|^2 (3 - 4|\alpha_1|^2)^2$$

Putting $|\alpha_1|^2 = \frac{1}{4}$ gives us

$$|\langle b_1 | U_{|\psi\rangle} U_{|s\rangle} |\psi\rangle|^2 = 1,$$

implying that the scheme is perfectly recoverable. \square

Appendix B: Appendix: Hsu's Nonces

Hsu introduced the use of nonces [7] by selecting $|A\rangle \otimes |B\rangle \in \{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}^{\otimes 2}$. Below, we list the states $U_s |\psi_i\rangle$ for all i . For clarity, we classify the possible choices into four cases:

- (i) $|A\rangle \in \{|+\rangle, |-\rangle\}$ and $|B\rangle \in \{|+\rangle, |-\rangle\}$;
- (ii) $|A\rangle \in \{|+\rangle, |-\rangle\}$ and $|B\rangle \in \{|+i\rangle, |-i\rangle\}$;
- (iii) $|A\rangle \in \{|+i\rangle, |-i\rangle\}$ and $|B\rangle \in \{|+\rangle, |-\rangle\}$; and
- (iv) $|A\rangle \in \{|+i\rangle, |-i\rangle\}$ and $|B\rangle \in \{|+i\rangle, |-i\rangle\}$.

