Reviving a Grover-based Quantum Secret Sharing Scheme

Debajyoti Bera[1] and Santanu Majhi[2]

[1] Indraprastha Institute of Information Technology, New Delhi, 110020, India
dbera@iiitd.ac.in
[2] Indian Statistical Institute, Kolkata, 700108, India
santanum_r@isical.ac.in

Abstract. Secret-sharing schemes allow a dealer to split a secret into multiple "shares" and distribute them individually among many parties while mandating certain constraints on its reconstruction. Such protocols are usually executed over a secure communication channel since an eavesdropper, after intercepting all the shares, is expected to be able to reconstruct the secret. Leveraging the unique properties of quantum channels, several quantum protocols have been designed for secret sharing. However, almost all of them detect the presence of an eavesdropper by statistical analysis of the outcome of multiple rounds, or simply require a secure channel of communication.

We mathematically analyse the correctness and security properties of a quantum-search based secret-sharing framework proposed by Hsu (2003) (and attacked by Hao et al. (2010)) that was proposed as an alternative that works over public channels and does not require multiple rounds. We show how to improve the original protocol to be more resistant towards eavesdropping and other attacks; however, we also prove that complete security against an eavesdropper is not possible in this framework.

Our tight characterization will be helpful towards the construction of more quantum secret sharing schemes based on the same framework.

Keywords: quantum · secret-sharing · Grover

1 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 further desirable for such schemes to be robust against other attacks, e.g., those arising from internal and external eavesdropping. The adversary can be one of the parties who has gone rogue or an third-party, but she will always go by the name of Eve. 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-destructive 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 protection 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. [7], to analyse quantum secret sharing protocols. This 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 — someone who has the ability to capture the qubits en route and even replace them with her own qubits. Thus, it is common for many quantum secret sharing protocols to include additional heuristic steps to explicitly prohibit various kinds of attacks [2].

The heuristics mostly involve sending decoy states. Decoy states are common in many quantum protocols; these protocols have multiple additional rounds some of which are used for checking the presence of an eavesdropper and the rest are used for the desired task [9]. 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 [5], 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.

There are two specific concerns an eavesdropper carries with her. First, any attacker who can intercept all messages between the dealer and the parties can always determine the secret on her own. The best approach, therefore, is to find a way to detect the occurrence of an attack. 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 scenario in which the eavesdropper knows the correct secret, the honest parties know some secret but not necessarily the correct one, but none (the dealer and the honest parties) have spotted any anomaly.

Second, many QSS schemes are proposed without an adequate proof of security. 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. Take for instance the HBB-QSS scheme mentioned earlier [5]. 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 [8].

Guaranteed detection of eavesdropping using only public channels and that too using few iterations of a protocol appears to be a difficult challenge.

1.1 Related Work

Hillery et al. [5] 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. [3].

It can be shown that none of the individual parties in the those schemes can recreate the secret state by itself. However, any eavesdropper can launch a man-in-the-middle attack by intercepting both the shares and sending to the parties shares of a fake secret. With both shares the eavesdropper can recreate the secret and this would largely go undetected since the original parties would reconstruct some secret (not necessarily the one sent by the dealer). This is a general weakness common to most QSS schemes.

Hsu [6] proposed a 2-stage (2,2)-QSS scheme to address this limitation; we denote it H03-QSS. In the first stage of a 2-stage QSS, the dealer commits to a randomly chosen nonce, say c. Then, The scheme constructs a state $|\psi_{c,s}\rangle$ using the secret s and nonce c, and shares it with the parties. Ideally, $|\psi_{c,s}\rangle$ reveals nothing about s. Later, the dealer discloses c, allowing authorized parties to recover s. Such schemes are appealing since no direct encoding of s is transmitted, reducing the risk of eavesdropping The nonces recommended for H03-QSS are inspired by the reflection operators employed by the Grover's search algorithm.

The strength of this protocol was the quick detection of eavesdropping. 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." Hsu demonstrated the resilience of his scheme against many types of attacks by considering a large set of possibilities. However, he did not provide any mathematical guarantee about the resilience.

Sure enough, Hsu missed out on certain states and operators that Eve could have employed to know the secret without anyone else knowing about the incident. This was later pointed out by Hao et al. [4]. Hao et al. further proposed that decoy states can be used to prevent the above eavesdropping attack.

Several works have explored extensions and improvements of Hsu's protocol. Tseng et al. [13, 14] 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.

1.2 Overview of Results

The main motivation behind this work was to understand the security requirements of quantum secret sharing schemes in the presence of eavesdroppers. Technically, we wanted to understand if the decoy states and additional rounds are necessary for the security of the H03-QSS protocol.

The choice of nonces appear to be central to this scheme. Thus, could one choose a different set of nonces that retains the one-shot nature of the original protocol and yet retains the security claimed in the original protocol.

Our main results are the following:

1. We characterizing the correctness and security requirements of the scheme in terms of various properties of the nonces.
2. We are able to explain why the nonces in the original scheme are unable to prevent eavesdropping. In fact, we show how to generate such attacks for any set of weak nonces.
3. We show how to design nonces that satisfy two basic criteria: the secret should be perfectly recoverable and Eve cannot guess the nonce to construct the secret on her own.
4. We design a set of nonces that makes the scheme resistant towards eavesdropping with a non-negligible probability.
5. Quite disappointingly, we prove that Eve always has a reasonable chance of remaining undetected after an attack no matter what nonces are used.

Thus, to improve H03-QSS to meet our expectations, we have to make some fundamental changes to the protocol beyond changing the nonces.

Our characterization brought to our notice one interesting extension. The original scheme was developed only for classical 2-bit secrets, or 1-bit secret along with cheat-detection. However, we are able to show that the scheme can be used to send arbitrary quantum states as secret.

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 [6, 4]). Instead, we derive mathematical characterisations that are tight to the extent possible. 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. Further, our framework would be useful to implement secure variations of the H03-QSS and design its extensions, e.g., to more parties [3].

2 Background

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

Table 1. States used to construct nonces

2.1 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 $U^{\dagger}_{|\alpha\rangle} = U_{|\alpha\rangle}$. If s is a bitstring, U_s may be written instead of $U_{|s\rangle}$.

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

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

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

$$-U_c U_s\,|c\rangle = |s\rangle\,, \tag{1}$$

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 1 for description of the states).

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

[3] Rathi et al. [11] designed an extension of H03-QSS to four parties; however, their work is only available as a pre-print to the best of our knowledge.

2.2 Grover-based H03-QSS by Hsu

In this subsection, we will give a quick overview of the H03-QSS proposed by Hsu [4]. Let $\mathfrak{Sec} \in \{0, 1\}$ denote the secret a dealer has to share among two parties named as Eve and Bob [5]. A schematic of the protocol is illustrated in Figure 1.

1. **Stage-I:**
2. Dealer choose a mode $m \in \{\texttt{SECRET}, \texttt{DETECT}\}$ uniformly at random.
3. If $m = \texttt{SECRET}$, s is chosen as 01 if $\mathfrak{Sec} = 0$ and as 10 if $\mathfrak{Sec} = 1$.
4. Else, if $m = \texttt{DETECT}$, s is chosen among $\{00, 11\}$ uniformly at random.
5. 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. 2.1.
6. 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).
7. After both the parties acknowledge receiving their shares (over a public channel), the dealer moves to Stage-II.

8. **Stage-II:**
9. Dealer announces (over a public channel) the choice of nonce $|\psi_i\rangle$.

10. **Stage-III:**
11. When the parties want to regenerate the secret, they get together and apply $U_{|\psi_i\rangle}$ to their joint-state.
12. Then they perform a measurement in the standard-basis; suppose, the outcome is $|b\rangle = |b_E\rangle |b_B\rangle$, where $b_E, b_B \in \{0, 1\}$.

13. **Stage-IV:**
14. If b_E and b_B are different, i.e., $b \in \{01, 10\}$, consider b as the regenerated secret, and b_E as $\mathfrak{Sec}$. All the (good) folks happily retire.
15. If $b_E = b_B$, i.e., $b \in \{00, 11\}$, parties publicly announce b to the dealer.
    - If $m = \texttt{DETECT}$, and $s = b$, announce over classical channel to drop this round (eavesdropper presence is not detected).
    - If $m = \texttt{DETECT}$, and $s \neq b$, announce over classical channel the presence of an eavesdropper.
    - If $m = \texttt{SECRET}$, announce over classical channel the presence of an eavesdropper.
16. If $m = \texttt{DETECT}$ but the parties did not announce their generated secrets, dealer announces over classical channel the presence of an eavesdropper.

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

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

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

[5] As is the norm, Bob is always honest.

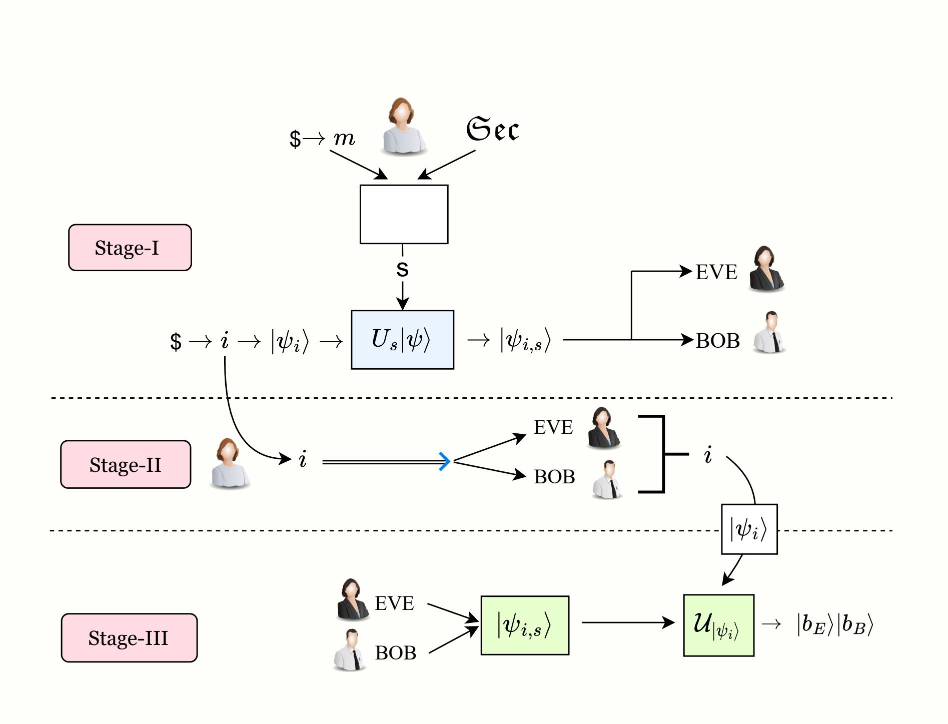


Fig. 1. The first three stages of the H03-QSS protocol. $ indicates drawing from a uniform random distribution. $\Longrightarrow$ indicates communication over a public channel.

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".

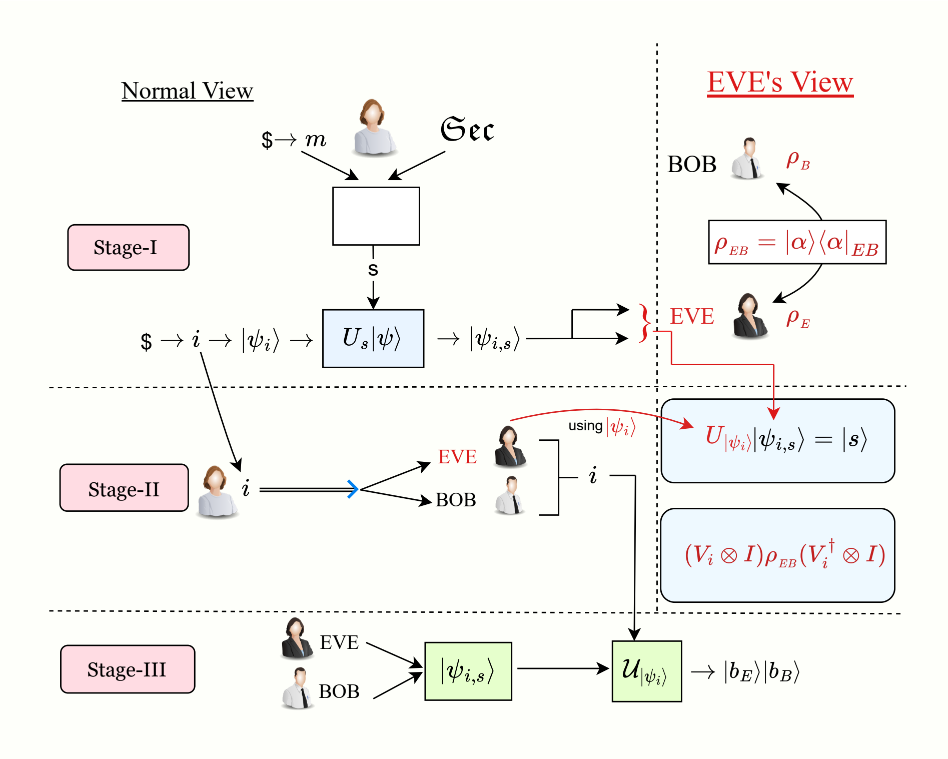
The cheat-detection steps detect the presence of an eavesdropper by following this rule-of-thumb.

- 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. [7] 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 [12]. (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.

2.3 Attack against H03-QSS ([4])

Let's discuss the idea of the attack discovered by Hao et al. [4]; a schematic of the attack is presented in Fig. 2.



Normal View
$\$ \to m$
$\mathfrak{Sec}$
Stage-I
s
$\$ \to i \to |\psi_i\rangle \to$
$U_s|\psi\rangle$
$\to |\psi_{i,s}\rangle$
EVE's View
BOB
ρ_B
$\rho_{EB} = |\alpha\rangle\langle\alpha|_{EB}$
EVE
ρ_E
Stage-II
i
EVE
BOB
i
using $|\psi_i\rangle$
$U_{|\psi_i\rangle}|\psi_{i,s}\rangle = |s\rangle$
$(V_i \otimes I)\rho_{EB}(V_i^\dagger \otimes I)$
Stage-III
EVE
BOB
$|\psi_{i,s}\rangle$
$\mathcal{U}_{|\psi_i\rangle}$
$\to |b_E\rangle|b_B\rangle$

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

Here, 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. First, she prepares a special 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, the 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. [4] 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 attach using some different $|\alpha\rangle$?

3 Mathematical Characterization

In this section, we derive mathematical conditions for the correctness and security of the QSS scheme. Earlier works by Hsu [6] and Hao et al. [4] did not provide such a characterization, and that made it difficult to rigorously analyse their approaches and study their enhancements. We will denote the set of nonces by J and k will denote the number of nonces.

Recoverability The recoverability of such a scheme 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.

Secrecy (*aka.* protection against intercept attack) Can a honest but curious player recreate the secret on her own? For H03-QSS scheme, this translates to Eve's ability to recreate the original secret even before the dealer sends the nonce, e.g., by guessing it.

(Internal) Tamperability (*aka.* protection against inject attack) Can a malicious player learn the secret on her own with a probability better than random guessing, and simultaneously also evade detection? For our H03-QSS, if Eve hijacks the share of Bob (and sends him a qubit in some other state), then Eve can learn the secret once the dealer announces the nonce. However, her act could be detected when Bob sits down with her to generate the secret. Tamperability is the probability with which Eve can evade detection in such a scenario.

External Tamperability Can a third-party who can intercept and inject messages learn the secret without getting noticed? Informally, this is weaker than internal tamperability since an internal player has a better chance of success with access to more information.

Intercept-measure-resend This is a variation of tamperability attack in which Eve intercepts the shares in Stage-I, *measures them*, and then sends the other parties qubits in some state. The difference from tamperability attacks is that the state Eve sends to the parties may depend on the measurement outcome.

We want the remind the reader two key operators with respect to the protocol. First, to reconstruct the key, the parties apply $U_{|\psi\rangle}$ on their share, and then perform measurement in the standard basis. Secondly, the joint-state representing both the shares, when Eve is honest, is $U_s \left|\psi\right\rangle$.

Notation	Description	Notation	Description	Notation	Description
m	mode	J	proposed set of nonces	$\left\|\alpha\right\rangle$	fake state shared by Eve
$\mathfrak{Sec}$	secret bit to be sent	$\left\|\psi_i\right\rangle$	Nonces in J	ρ	$\left\|\alpha\right\rangle \left\langle\alpha\right\|$
s	2-bit secret	U_x	$I - 2\left\|x\right\rangle \left\langle x\right\|$	ρ^B	$Tr_E(\rho)$
$\mathcal{I}$	original set of nonces	$\left\|\psi_{i,s}\right\rangle$	$U_s \left\|\psi_i\right\rangle$ Shared by dealer	$\sigma_{i,s}$	$\left\|\psi_{i,s}\right\rangle \left\langle\psi_{i,s}\right\|$
b	regenerated secret	$\sigma^B_{i,s}$	$Tr_E(\sigma_{i,s})$	V_i	Eve's local unitary

Table 2. Notations

3.1 Recoverability

The honest parties should be able to recover the secret with high probability, if not with certainty.

Definition 1. *Let s be some secret chosen by the dealer. We will say that a scheme is recoverable if s is recovered after an honest execution of the protocol.*

$$\Pr_{\left|\psi\right\rangle}[s \textit{ is generated by the key-recovery step}] = 1$$

For H03-QSS, the key recovery step involves applying $U_{\left|\psi\right\rangle}$ on the shared state $U_s \left|\psi\right\rangle$. Thus, the condition for recoverability is

$$U_{\left|\psi\right\rangle} U_s \left|\psi\right\rangle = \left|s\right\rangle \text{ up to some phase, or equivalently } U_{\left|\psi\right\rangle} \left|s\right\rangle = U_s \left|\psi\right\rangle \qquad (2)$$

We now present an equivalent but simpler condition that is easy to check; in fact, our condition holds for more general forms of s that can be potentially used to extend the scheme to arbitrary quantum states.

Lemma 1. *Let $\left|s\right\rangle$ be some 2-qubit state. s is perfectly recoverable if and only if*

$$\left| \left\langle s \middle| \psi \right\rangle \right| = \tfrac{1}{2}$$

holds for all nonce $\left|\psi\right\rangle \in J$.

Proof. Let's first extend $\{\left|s\right\rangle\}$ to some basis $\{\left|b_1\right\rangle, \left|b_2\right\rangle, \ldots \left|b_n\right\rangle\}$. Now we can represent any nonce $\left|\psi\right\rangle$ in this basis. WLOG let $\left|b_1\right\rangle = \left|s\right\rangle$.

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

The shared secret in this case would be

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

Now,

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

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

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

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

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

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

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

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

as required.

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

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

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

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

implying that the scheme is perfectly recoverable.

3.2 Secrecy

In this section, we discuss the conditions for secrecy — resistance towards a curious Eve who tries to know the secret without the involvement of Bob.

In this attack, Eve intercepts the qubit meant for Bob, giving her both qubits of $|\psi_{i,s}\rangle$. She guesses a nonce $|\psi_j\rangle$ and applies $U_{|\psi_j\rangle}$ 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 protocol then proceeds from stage II as usual.

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.

Definition 2 (Secrecy). *Let s be any secret chosen by the dealer, and s' be the secret generated by Eve. The QSS scheme is said to ensure secrecy if*

$$\Pr_{|\psi_j\rangle \neq |\psi_i\rangle}[s = s'] \leq \tfrac{1}{4}.$$

The original H03-QSS scheme was shown to be secure by Hsu who presented an exhaustive case analysis for the set $\mathcal{I}$ of nonces. We present a mathematical characterization for any set J of nonces.

The probability that Eve will observe s when after she has intercepted the qubit of Bob and applied $U_{|\psi_j\rangle}$ on $|\psi_{i,s}\rangle$ is, using Eq. 2,

$$\left|\left\langle s \middle| U_{|\psi_j\rangle} \middle| \psi_{i,s} \right\rangle\right|^2 = \left|\left\langle s \middle| U_{|\psi_j\rangle} U_s \middle| \psi_i \right\rangle\right|^2 = \left|\langle \psi_j | U_s U_s | \psi_i \rangle\right|^2 = \left|\langle \psi_j | \psi_i \rangle\right|^2.$$

We can use this result to mathematically characterize secrecy.

Lemma 2. *Let s be any secret chosen by the dealer, and s' be the secret generated by Eve. The QSS scheme is said to ensure secrecy if and only if*

$$\sum_{\substack{|\psi\rangle \neq |\psi'\rangle \\ \text{nonces}}} \left|\langle \psi' | \psi \rangle\right|^2 \leq \tfrac{k(k-1)}{4}.$$

3.3 Internal Tamperability

Let's discuss how a scheme can resist attacks from a malicious Eve who tries to tamper with the protocol's execution as discussed in Sec. 2.3. $|\alpha\rangle$ will denote the joint-state of the qubits shared by Eve with Bob in Stage-I, and V_i will denote the unitary operator that Eve applies to her qubit in Stage-II.

We wish to re-emphasize that it is impossible to prevent Eve from knowing the secret.

Next, if Eve is able to transform $|\alpha\rangle$ to exactly $|\psi_{i,s}\rangle$ then her tampering cannot be detected any further. Even if $|\psi_{i,s}\rangle$ is not exactly generated, the state produced may be close to it which means that the key recovery step will generate the original secret with a reasonable probability, much to the happiness of Eve.

Thus, we will be concerned entirely about the parties recovering s in Stage-III, an event that we will denote $\mathcal{R}(s)$ — indicating a weakness of the scheme.

$$\mathcal{R}(s) = \text{Event : ``}s\text{ is generated by the key-recovery step in Stage-III''}$$

The next lemma characterizes the probability of this event in terms of fidelity.

Lemma 3. *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 $\{V_1, V_2, \ldots V_k\}$ denote the single-qubit unitary operators Eve applies corresponding the different nonces (V_i may depend on $\sigma_{s,i}$ and s).*

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

Proof. The proof is straightforward. The 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 the the key-recovery step generates s from this state is

$$\left|\left\langle s\middle|U_{|\psi_i\rangle}(V_i \otimes I)\middle|\alpha\right\rangle\right|^2 = \left|\langle\psi_i|U_s(V_i \otimes I)|\alpha\rangle\right|^2,$$

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

We derive a sufficient condition for $\mathcal{R}(s)$ to not hold (i.e., for the scheme to be secure) by tracing out Eve's state from Eq. 3 and using that subsystem fidelity is no less than the fidelity of a larger system.

Lemma 4. *Let $\sigma_{i,s}^B$ denote $\mathrm{Tr}_E\, \sigma_{i,s}$ and ρ^B denote any single-qubit state.*

$$\Pr_{|\psi\rangle}[\mathcal{R}(s)] \leq \max_{\rho^B} \sum_{i=1}^{k} \tfrac{1}{k} F(\sigma_{i,s}^B, \rho^B) \tag{4}$$

The condition in Lemma 4 is essentially an optimization problem to find the best ρ^B that is independent of s. One can use any metric related to fidelity and use triangle-inequality and other algebraic techniques to solve it; we will employ a more direct method in Sec. 4.2.

Finally, we show that an upper bound on the right-hand side of Eq. 4 is also a necessary condition for $\mathcal{R}(s)$ to not hold.

Lemma 5. *There exists some $|\alpha\rangle$ and a set of operators $\{V_1, V_2, \ldots, V_k\}$ such that*

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

We use a slight variation of a version given by Nielsen and Chuang [10].

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 5 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

$$\sigma_{i,s}^* = (U_{i,s} \otimes I)\sigma_{i,s}(U_{i,s}^\dagger \otimes I).$$

Thus,

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

$\therefore$ for all $i, s \quad F(\sigma_{i,s}^B, \rho^B) = F(\sigma_{i,s}, (U_{i,s}^\dagger \otimes I)\rho(U_{i,s} \otimes I))$

$$\begin{aligned}
\sum_{i=1}^{k} F(\sigma_{i,s}^B, \rho^B) &= \sum_{i=1}^{k} F(\sigma_{i,s}, (U_{i,s}^\dagger \otimes I)\rho(U_{i,s} \otimes I)) \\
\sum_{i=1}^{k} \frac{1}{k} F(\sigma_{i,s}^B, \rho^B) &= \sum_{i=1}^{k} \frac{1}{k} F(\sigma_{i,s}, (U_{i,s}^\dagger \otimes I)\rho(U_{i,s} \otimes I)) \\
&= \Pr_{|\psi\rangle}[\mathcal{R}(s)] \quad \text{(From equation 3)}
\end{aligned}$$

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

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

.

4 Fortifying the H03-QSS scheme

It is easy to prove that the nonces used in the original H03-QSS scheme are not strong enough to resist an internal tampering attack. The idea is to show that the do not satisfy the necessary condition as specified in Lemma 5.
In this section we prove that Hsu's H03-QSS scheme is vulnerable to a tampering attack by demonstrating that the original nonces violate the necessary condition as given in Lemma 5.

The original scheme uses 16 nonces formed by taking all possible combinations of two qubits from the set $\{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$.

It it straightforward to verify that the nonces chosen by Hsu coincidentally satisfy the following property:

$$\sigma_{i,s}^B = I/2 \quad \text{for all nonce } |\psi_i\rangle \text{ and all secret } s.$$

Now, let's choose any 2-qubit state $|\alpha\rangle$ that is a purification of $I/2$; Hao et al. [4] chose $|\alpha\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$ but we can chose any other state too. Let's set ρ^B in Lemma 5 to $|\alpha\rangle\langle\alpha|$. Clearly, $F(\sigma_{i,s}^B, \rho^B) = 1$.

Further recall that $\sigma_{i,s} = U_{\psi_i}|s\rangle$ is a purification of $\sigma_{i,s}^B$.

Now, by Uhlmann's theorem, there exists some V (that depends on s and $|\psi_i\rangle$ such that the fidelity of $\sigma_{i,s}$ and $(V \otimes I)\rho(V^\dagger \otimes I)$ is also 1.

$$F(\sigma_{i,s}, (V \otimes I)\rho(V^\dagger \otimes I) = |\langle\psi_{i,s}|(V \otimes I)|\alpha\rangle|^2 = 1,$$

and this exactly establishes a successful attack by Eve that avoids any chance of detection.

The proof of Uhlmann's theorem also allows us to construct a V for each i, s. It can be verified that the operators match exactly those proposed by Hao et al..

To strengthen the scheme, we propose the following set of nonces instead.

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

The nonces were actually created so that they evolve to certain states under the action of U_s for all possible s as shown in Table 3.

nonces in J	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_3\rangle$	$\|\psi_4\rangle$
$s = 00$	$-\|+\rangle\|-\rangle$	$-\|-\rangle\|+\rangle$	$-\|+i\rangle\|-i\rangle$	$-\|-i\rangle\|+i\rangle$
$s = 01$	$\|-\rangle\|-\rangle$	$\|+\rangle\|+\rangle$	$\|-i\rangle\|-i\rangle$	$\|+i\rangle\|+i\rangle$
$s = 10$	$\|+\rangle\|+\rangle$	$\|-\rangle\|-\rangle$	$\|+i\rangle\|+i\rangle$	$\|-i\rangle\|-i\rangle$
$s = 11$	$\|-\rangle\|+\rangle$	$\|+\rangle\|-\rangle$	$\|-i\rangle\|+i\rangle$	$\|+i\rangle\|-i\rangle$

Table 3. The table shows the states $U_s |\psi_i\rangle$ for every nonce $|\psi_i\rangle \in J$ and all secret s.

4.1 Recoverability and Secrecy

It is easy to verify from Table 3 that $|\langle s|\psi\rangle| = \frac{1}{2}$ for all s and $|\psi\rangle$. Thus, by Lemma 1, the QSS scheme using J for the nonces is perfectly recoverable.

Similarly, it can be verified that $|\langle\psi_i|\psi_j\rangle| \in \{0, \frac{1}{2}\}$ for all distinct i, j. Thus, according to Lemma 2, Eve cannot confidently determine the secret in Stage-I by incorrectly guessing the nonce.

4.2 Internal Tamperability

It can be shown from the above table that

$$\{\sigma^B_{i,s} \ : \ i \in \{1,2,3,4\}\} = \{|+\rangle\langle+|, |-\rangle\langle-|, |+i\rangle\langle+i|, |-i\rangle\langle-i|\}.$$

Let s be any secret chosen by the dealer. Let ρ^B be any single-qubit (possibly mixed) state. It is easy to prove that

$$\frac{1}{4} \sum_{i\in\{1,2,3,4\}} F(\sigma^B_{s,i}, \rho^B) = \frac{1}{2},$$

and thus according to Lemma 4, the parties recover s with probability at most $\frac{1}{2}$.

We will explain how our nonces meet the sufficient conditions of non-tamperability as prescribed by Lemma 4. For this, first refer to the possible values of $\sigma^B_{i,s}$ as shown in Table 4.

We can see from the table that for any s, the set $\{\sigma^B_{i,s} \ : \ i \in \{1,2,3,4\}\}$ can be shown to be $\{|+\rangle\langle+|, |-\rangle\langle-|, |+i\rangle\langle+i|, |-i\rangle\langle-i|\}$.

nonces in J	$\lvert\psi_1\rangle$	$\lvert\psi_2\rangle$	$\lvert\psi_3\rangle$	$\lvert\psi_4\rangle$
$s = 00$	$\lvert-\rangle\langle-\rvert$	$\lvert+\rangle\langle+\rvert$	$\lvert-i\rangle\langle-i\rvert$	$\lvert+i\rangle\langle+i\rvert$
$s = 01$	$\lvert-\rangle\langle-\rvert$	$\lvert+\rangle\langle+\rvert$	$\lvert-i\rangle\langle-i\rvert$	$\lvert+i\rangle\langle+i\rvert$
$s = 10$	$\lvert+\rangle\langle+\rvert$	$\lvert-\rangle\langle-\rvert$	$\lvert+i\rangle\langle+i\rvert$	$\lvert-i\rangle\langle-i\rvert$
$s = 11$	$\lvert+\rangle\langle+\rvert$	$\lvert-\rangle\langle-\rvert$	$\lvert+i\rangle\langle+i\rvert$	$\lvert-i\rangle\langle-i\rvert$

Table 4. States $\sigma^B_{i,s}$ for every nonce $|\psi_i\rangle$ and every s.

Now, let ρ^B be any single-qubit (possibly mixed) state. Take any $\sigma^B_{i,s}$; since, it represents a pure state, $F(\sigma^B_{s,i}, \rho^B) = \mathrm{Tr}\{\sigma^B_{s,i}\rho^B\}$. Thus,

$$\begin{aligned}
&\sum_{i\in\{1,2,3,4\}} F(\sigma^B_{s,i}, \rho^B) \\
&= \sum_{i\in\{1,2,3,4\}} \mathrm{Tr}\{\sigma^B_{s,i}\rho^B\} \\
&= \mathrm{Tr}\{|+\rangle\langle+|\,\rho^B\} + \mathrm{Tr}\{|-\rangle\langle-|\,\rho^B\} + \mathrm{Tr}\{|+i\rangle\langle+i|\,\rho^B\} + \mathrm{Tr}\{|-i\rangle\langle-i|\,\rho^B\} \\
&= \mathrm{Tr}\{I\rho^B\} + \mathrm{Tr}\{I\rho^B\} \\
&= 2\,\mathrm{Tr}\{\rho^B\} \\
&= 2
\end{aligned}$$

So, we get that

$$\tfrac{1}{4} \sum_{i\in\{1,2,3,4\}} F(\sigma^B_{s,i}, \rho^B) = \tfrac{1}{2}$$

which satisfies the conditions of Lemma 4.

4.3 Complete Security Analysis

In this section we derive the probability of detecting an internal eavesdropper. Since the protocol can be run in two modes,

$$\Pr[\mathit{detection}] = \tfrac{1}{2}\Pr[\mathit{detection} \mid m = \mathit{SECRET}] + \tfrac{1}{2}\Pr[\mathit{detection} \mid m = \mathit{DETECT}].$$

In Sec. 4.2 we proved that any s can be generated by the parties after a tampering attack (thus, evading detection) with probability at most $\frac{1}{2}$. Now, in the detection mode, the attack is *not* detected if the s chosen by the dealer ($s \in \{00, 11\}$) is generated.

$$\Pr[\mathit{detection} \mid m = \mathit{DETECT}] \geq \tfrac{1}{2}$$

In the secret sending mode, the attack is *not* detected if any s other than 01 and 10 is generated (for this case, $s \in \{01, 10\}$). However, we do not get any meaningful lower bound for this case since

$$\Pr[\textit{not detection} \mid m = \textit{SECRET}] \leq \tfrac{1}{2} + \tfrac{1}{2} = 1.$$

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

Theorem 2. *The probability of detecting an eavesdropper is at least $\frac{1}{4}$.*

While this may not meet our general expectations, recall that the probability is zero in the original scheme. In the next section we discuss a lower bound on the same.

4.4 No Attack Ain't Possible

In this section we prove that Eve always has a chance of avoiding detection for any set of nonces. First, we prove that average fidelity of a set of single-qubit pure states with a fixed single-qubit (possibly mixed) state is at at least $\frac{1}{2}$.

Lemma 6. *Let $\beta_1, \ldots \beta_k$ and γ denote $k+1$ (possibly mixed) single-qubit states. Then, 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. We prove this by analysing their Euclidean distances in the Bloch sphere. Thee known relation between fidelity of two single-qubit mixed states to the Euclidean distance between their corresponding Bloch vectors.

$$F(\rho_{\lambda_1}, \rho_{\lambda_2}) = 1 - \frac{1}{4} \|\overrightarrow{\lambda_1} - \overrightarrow{\lambda_2}\|_2^2 \tag{5}$$

where $\overrightarrow{\lambda_1}$ and $\overrightarrow{\lambda_2}$ are two vectors in the Bloch sphere corresponding to the two states [6].

Using Eq. 5, we can restate the statement of the lemma in terms of Euclidean distance.

$$\min_{\gamma} \sum_{i=1}^{k} ||\overrightarrow{\beta_i} - \overrightarrow{\gamma}||^2 \leq 2k$$

[6] A quick way to see this are two identities: $1 - \frac{1}{4}||\overrightarrow{\lambda_1} - \overrightarrow{\lambda_2}||_2^2 = \frac{1}{2} + 2\overrightarrow{\lambda_1} \cdot \overrightarrow{\lambda_2}$ and the Bloch sphere representation of any single-qubit mixed state $\rho_\lambda = \frac{1}{2}(I + \overrightarrow{\lambda} \cdot \overrightarrow{P})$, where $\overrightarrow{P} = (X, Y, Z)$ is the vector Pauli operators.

It is well know that the center-of-mass or mean of a set of a vectors has the closest sum of distances from vectors in the set. Let's represent the mean as:

$$\overline{\beta} = \frac{1}{k}\sum_{i=1}^{k}\overrightarrow{\beta}_i$$

$$\overline{\beta} = \frac{1}{k}\sum_{i=1}^{k}\overrightarrow{\beta}_i$$

Now we are ready to prove the required claim.

$$\min_{\gamma}\sum_{i=1}^{k}||\overrightarrow{\beta}_i - \overrightarrow{\gamma}||^2 = \sum_{i=1}^{k}||\overrightarrow{\beta}_i - \overline{\beta}||^2 \leq \sum_{i=1}^{k} 2 = 2k$$

Hence, from this we have

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

.

Lemma 7. *For any set of nonces, Eve can design $|\alpha\rangle$ and her local unitaries such that the probability, over the random nonce by the dealer, that the parties generate $b = 10$ or $b = 11$ as secret is at least $\frac{1}{2}$ each.*

Recall that Eve first generates the dealer's secret s in Stage-II using the knowledge of i, and then manipulates the joint-state $|\alpha\rangle$ accordingly. One strategy that Eve can adopt is the following: if $s = 10$ (or if $s = 11$), apply some unitary V_i on her qubit to convert $\alpha \mapsto |\psi_{i,10}\rangle$ (or to $|\psi_{i,11}\rangle$, respectively); she can achieve that with probability at least $\frac{1}{2}$ according to the above lemma.

Eve can now evade detection in Stage-IV if the dealer had chosen $s = 10, 01$ or 11. For no one to be suspicious, it suffices if the parties generate 11 if $s = 11$, and 10 if s is either 01 or 10. We, thus, arrive at the following theorem.

Theorem 3. *The probability of detecting an eavesdropper is at most $\frac{5}{8}$.*

Proof. Since the protocol operates in two distinct modes and there are four possible values of b $(00, 01, 10, 11)$ we have,

$$\begin{aligned} &\Pr[\textbf{detect mode}] = \Pr[\textbf{secret mode}] = \frac{1}{2} \\ &\Pr[\mathbf{s = 11}] = \frac{1}{4}, \quad \Pr[\mathbf{s = 10 \text{ or } s = 01}] = \frac{1}{2}. \end{aligned}$$

Now from Lemma 7, we get

$$\begin{aligned} \Pr[\textbf{not detect if } s = 11] &\geq \frac{1}{2} \\ \text{also,} \quad \Pr[\textbf{not detect if } s = 01 \text{ or } s = 10] &\geq \frac{1}{2} \end{aligned}$$

Finally, Pr[**not detect**] is

$$\begin{aligned}\Pr[\textbf{not detect}] =& \Pr[\mathbf{s = 11}] * \Pr[\textbf{not detect if } s = 11] + \\ & \Pr[\mathbf{s = 10 \text{ or } s = 01}] * \Pr[\textbf{not detect if } s = 01 \text{ or } s = 10] \\ \implies \Pr[\textbf{not detect}] \geq& \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{8}\end{aligned}$$

$$\therefore \Pr[\textbf{Detect}] \leq 1 - \frac{3}{8} = \frac{5}{8}$$

Hence, the probability of detecting an eavesdropper is at most $\frac{5}{8}$.

4.5 Other Security Attacks

We explained earlier that the success of third-party eavesdropping is weaker than that of internal eavesdropping; we show how our nonces resist the latter, and thus, should be effective for the former too. Nevertheless, a mathematical model of an external eavesdropper and a proof of the resistance of our nonces towards such an attack is discussed below.

Let's discuss how our nonces can prevent a third-party (again, named Eve) from launching an eavesdropping attack. For this, we will name the two honest parties Bob and Charlie. The attack is similar to the internal tamperability attack discussed in Sec. 3.3.

The sequence of events starts by Eve intercepting the qubits headed towards Bob and Charlie in Stage-I and sending them 2 qubits of a tripartite entangled state denoted $|\alpha\rangle$.

In Stage-II when the nonce $|\psi_i\rangle$ is revealed, Eve's intention is to modify $|\alpha\rangle$ such that the key-recovery steps to be undertaken by Bob and Charlie in Stage-III would be mostly successful. Similar to the internal tampering attack, here too Eve will always be able to generate the secret s on her own given the $|\psi_{i,s}\rangle$ in her possession and her knowledge of the nonce. Thus, the goal of the dealer and the honest parties is only to detect the tampering.

Now, we will derive a sufficient condition for such an attack to be detected. As before, denote $|\alpha\rangle \langle\alpha|$ by ρ, and denote $\mathrm{Tr}_E\, \rho$ by ρ^{BC} – state of Bob and Charlie's share that is surreptitiously sent by Eve. Now, the probability that those two parties can successfully regenerate some secret $|s\rangle$ after the key-recovery step is

$$\mathrm{Tr}\big(|s\rangle \langle s| \, U_{|\psi_i\rangle} \rho^{BC} U_{|\psi_i\rangle}\big) = F(|s\rangle \langle s| \, , U_{|\psi_i\rangle} \rho^{BC} U_{|\psi_i\rangle}).$$

Thus, the expected probability of generating $|s\rangle$, taking expectation over the random choice of nonce, is

$$\tfrac{1}{k} \sum_{i=1}^{k} F(|s\rangle \langle s| \, , U_{|\psi_i\rangle} \rho^{BC} U_{|\psi_i\rangle}) = \tfrac{1}{k} \sum_{i=1}^{k} F(\sigma_{i,s}, \rho^{BC}).$$

Thus, a sufficient condition to thwart the attack is to choose nonces such that the above quantity is small.

For our nonce, we showed that

$$\tfrac{1}{4}\sum_{i=1}^{4} F(\sigma_{i,s}^{B}, \rho^{B}) = \tfrac{1}{2}$$

for any ρ^B that is independent of i.

Since, fidelity does not decrease with partial trace,

$$\tfrac{1}{4}\sum_{i=1}^{4} F(\sigma_{i,s}, \rho^{BC}) \leq \tfrac{1}{2}$$

for any ρ^{BC} that is independent of i. Thus, the parties would not generate the desired secret s with probability at least $\mathbf{\frac{1}{2}}$, and this clips Eve's chance of success.

We discuss the intercept-measure-resend attack next.

Define the mixed state representing the shares generated by the dealer.

$$\tilde{\sigma} = \tfrac{1}{4} \sum_{s \in \{0,1\}^2} \tfrac{1}{k} \sum_{i=1}^{k} |\psi_{i,s}\rangle \langle\psi_{i,s}|$$

If $\tilde{\sigma} \equiv I$, then the state of the shares intercepted by Eve carries no information about s or nonce. Thus, it is a sufficient condition for the attack to be not successful (better than a random guess of s).

The intercept-resend attack is completely useless for our nonces since it can be easily verified that

$$\tilde{\sigma} = \tfrac{1}{4} \sum_{s \in \{0,1\}^2} \tfrac{1}{4} \sum_{i=i}^{4} |\psi_{i,s}\rangle \langle\psi_{i,s}| = \frac{1}{16} I.$$

Thus, the shares intercepted by Eve are equivalent to the completely mixed state, and hence, Eve cannot manipulate the honest parties to generate $|s\rangle$ with a probability better than a random guess, even with the knowledge of the nonce announced by the dealer in Stage-II.

5 Conclusion

In this work we have analysed the conditions of correctness and security against different types of attacks of a (2,2) Grover-search-based quantum secret sharing scheme [6] 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, all his analysis was done by considering typical operations that he thought were all an adversary could do. A subsequent work by Hao et al. [4] proved him wrong. Unfortunately, this has been the trend in secure protocol design, both classical and quantum. 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.

Finally, H03-QSS was designed for classical 1-bit secrets (or, 2-bit secrets without eavesdropping detection). We show that it is possible to send arbitrary quantum secret states too with suitably designed nonces that satisfy the requirements of Lemma 1.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science **560**, 7–11 (2014). https://doi.org/https://doi.org/10.1016/j.tcs.2014.05.025, https://www.sciencedirect.com/science/article/pii/S0304397514004241, theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84
2. Chattopadhyay, A.K., Saha, S., Nag, A., Nandi, S.: Secret sharing: A comprehensive survey, taxonomy and applications. Computer Science Review **51**, 100608 (2024). https://doi.org/https://doi.org/10.1016/j.cosrev.2023.100608, https://www.sciencedirect.com/science/article/pii/S1574013723000758
3. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. **83**, 648–651 (Jul 1999). https://doi.org/10.1103/PhysRevLett.83.648, https://link.aps.org/doi/10.1103/PhysRevLett.83.648
4. Hao, L., Li, J., Long, G.L.: Eavesdropping in a quantum secret sharing protocol based on grover algorithm and its solution. Science China Physics, Mechanics & Astronomy **53**, 491–495 (2010). https://doi.org/10.1007/s11433-010-0145-7
5. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (Mar 1999). https://doi.org/10.1103/PhysRevA.59.1829, https://link.aps.org/doi/10.1103/PhysRevA.59.1829
6. Hsu, L.Y.: Quantum secret-sharing protocol based on grover's algorithm. Phys. Rev. A **68**, 022306 (Aug 2003). https://doi.org/10.1103/PhysRevA.68.022306, https://link.aps.org/doi/10.1103/PhysRevA.68.022306
7. Imai, H., Mueller-Quade, J., Nascimento, A.C.A., Tuyls, P., Winter, A.: A quantum information theoretical model for quantum secret sharing schemes (2003)
8. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (Jan 1999). https://doi.org/10.1103/PhysRevA.59.162, https://link.aps.org/doi/10.1103/PhysRevA.59.162
9. Lo, H.K., Ma, X., Chen, K.: Decoy state quantum key distribution. Physical Review Letters **94**(23) (Jun 2005). https://doi.org/10.1103/physrevlett.94.230504, http://dx.doi.org/10.1103/PhysRevLett.94.230504
10. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press (2010)
11. Rathi, D., Musanna, F., Kumar, S.: A four-party quantum secret-sharing scheme based on grover's search algorithm (2021), arXiv:2111.08932
12. Rietjens, K., Schoenmakers, I.L., Tuyls, P.: Quantum secret sharing schemes. Ph.D. thesis, Citeseer (2004)

13. Tseng, H.Y., Tsai, C.W., Hwang, T., Kuo, S.Y.: Quantum secret sharing based on quantum search algorithm. International Journal of Theoretical Physics **51**(10), 3101–3108 (2012). https://doi.org/10.1007/s10773-012-1191-x
14. Yu, Z.: The improved quantum secret sharing protocol based on grover algorithm. Journal of Physics: Conference Series **2209**(1), 012031 (feb 2022). https://doi.org/10.1088/1742-6596/2209/1/012031, https://dx.doi.org/10.1088/1742-6596/2209/1/012031