
Article:
Ouyang, Y., Goswami, K., Romero, J. et al. (2023) Approximate reconstructability of quantum states and noisy quantum secret sharing schemes. Physical Review A, 108 (1). 012425. ISSN: 2469-9926

https://doi.org/10.1103/physreva.108.012425

Approximate reconstructability of quantum states and noisy quantum secret sharing schemes

Yingkai Ouyang,[1,2,*] Kaumudibikash Goswami,[3,4] Jacquiline Romero,[3]
Barry C. Sanders,[5,4,†] Min-Hsiu Hsieh,[6,‡] and Marco Tomamichel[2,7]

[1] *Department of Physics & Astronomy, University of Sheffield, Sheffield, S3 7RH, United Kingdom*
[2] *Centre for Quantum Technologies, National University of Singapore, Singapore*
[3] *School of Mathematics and Physics, University of Queensland, Brisbane, Queensland 4072, Australia*
[4] *Raman Research Institute, Sadashivanagar, Bengaluru, Karnataka 560080, India*
[5] *Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*
[6] *Hon Hai (Foxconn) Research Institute, Taipei, Taiwan*
[7] *Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583, Singapore*

We introduce and analyse approximate quantum secret sharing in a formal cryptographic setting, wherein a dealer encodes and distributes a quantum secret to players such that authorized structures (sets of subsets of players) can approximately reconstruct the quantum secret and omnipotent adversarial agents controlling non-authorized subsets of players are approximately denied the quantum secret. In particular, viewing the map encoding the quantum secret to shares for players in an authorized structure as a quantum channel, we show that approximate reconstructability of the quantum secret by these players is possible if and only if the information leakage, given in terms of a certain entanglement-assisted capacity of the complementary quantum channel to the players outside the structure and the environment, is small.

I. INTRODUCTION

Quantum resources enable cryptographic tasks beyond what is classically possible. For instance, quantum key distribution [1, 2] provides an information-theoretic means for generating shared classical keys. Secret sharing (SS) is another fundamental cryptographic primitive, wherein a dealer D distributes a secret as shares to a set of players $\wp$ such that any group in the authorised structure $\Gamma \subseteq 2^{\wp}$ (sets of authorised subsets of the players) reconstructs the secret by combining shares and decoding, whereas groups in the complementary adversarial structure $\bar{\Gamma} = 2^{\wp} \setminus \Gamma$ cannot obtain any information about the secret. SS has been quantised in two ways: quantum-safe classical SS [3] and the version we employ here—quantum-secret sharing (QSS) [4] as a special case of quantum error correction [5]—which can be partially unified via quantum graph states for qubits [6] and subsequently for qudits [7]. Quantum secret sharing has applications in quantum Byzantine agreements [8] and distributed quantum computation [9], amongst others.

Ideal (t, n)-threshold QSS features perfect reconstructability and perfect secrecy as elucidated in Fig. 1(a); i.e., any t out of n players can reconstruct the secret perfectly, and perfect secrecy means that fewer than t players do not gain any information about the secret. From this foundation, generalised QSS can be constructed from threshold QSS by evenly or unevenly distributing shares to players [4, 10, 11]. In (t, n)-QSS [4, 10, 12], a dealer D employs an encoding map $\mathcal{E}$ to encode a quantum secret $\varrho \in \mathcal{D}(\mathscr{H})$ (trace-class positive density operator) into n q-dimensional qudits, i.e., onto Hilbert space $\mathscr{H}_q^{\otimes n}$ (n-fold tensor product of q-dimensional Hilbert spaces). Each share of one qudit is sent to one of n players, such that Γ comprises all groups of at least t players and $\bar{\Gamma}$ is the complement, namely, all groups of fewer than t players.

Here, we construct a theory of approximate secrecy and reconstructability by introducing an adversary model as shown in Fig. 1(b). In our model, the adversary structure comprises omnipotent adversaries who are denied control over Γ but can collaborate with players in $\bar{\Gamma}$. Imperfect SS has been considered, but strong assumptions on the adversary's capability are required [13]. In contrast, the dichotomy between reconstructability and secrecy is quite general and is inherently quantum due to the no-cloning principle [14, 15], devoid of any classical analogue: classically, the ability to copy a secret allows an authorised set to reconstruct the secret exactly but cannot provide a guarantee that an adversary who could have intercepted the communication cannot do the same. Approximate QSS relaxes the requirements of perfect reconstructability for Γ and perfect secrecy for $\bar{\Gamma}$. Approximate quantum secret sharing schemes derived from quantum Reed-Solomon codes were investigated in [16], but this leaves open the question of how more general approximate quantum secret sharing schemes perform. The dichotomy between approximate recoverability and approximate secrecy has also been investigated [17–20], but it remains unclear how these quantities relate to the maximum rate at which the secret is transmitted to the adversary.

* y.ouyang@sheffield.ac.uk
† sandersb@ucalgary.ca
‡ min-hsiu.hsieh@foxconn.com

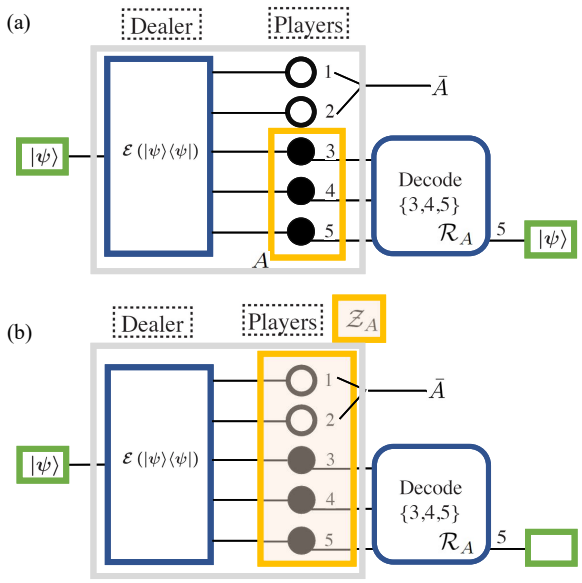

FIG. 1: **(a) Ideal threshold QSS scheme.** The dealer encodes the secret with channel $\mathcal{E}$, and distributes the shares to players 1,2,3,4 and 5. Players in the set $A = \{3, 4, 5\}$ collaborate in the decoding using the map $\mathcal{R}_A$ and reconstruct the secret. We label the players outside A as $\bar{A} = \{1, 2\}$. **(b) Adversarial attack on a threshold QSS scheme.** The adversary colludes with players 1 and 2. They apply the map $\mathcal{Z}_A$ on the players' qudits, potentially adding noise to the systems of any player. Depending on the attack, the legitimate players can still approximately recover the secret $|\psi\rangle$.

II. MAIN RESULT

Consider now a (t, n)-threshold QSS scheme where a q-dimensional secret is shared with players holding qudits (d-dimensional quantum systems). In our model, given any $A \in \Gamma$, the adversary can attack all qudits after the dealer applies the encoding map $\mathcal{E}$ and prior to reconstruction. The effect of the adversary's action amounts to applying an effective channel $\mathcal{Z}_A$. Thus, the quantum channel mapping the quantum secret to the quantum state on A just before reconstruction is

$$\mathcal{N}_A = \mathrm{tr}_{\bar{A}} \circ \mathcal{Z}_A \circ \mathcal{E}, \tag{1}$$

with $\mathrm{tr}_{\bar{A}}$ denoting the partial-trace that removes the players in $\bar{A} = \{1, \ldots, n\} \setminus A$. The $|A|$ authorised players then apply a recovery channel $\mathcal{R}_A$ that maps the qudits labelled by A to a single q-dimensional system.

We then define our (t, n)-threshold QSS scheme to be δ-reconstructable if

$$\delta = \max_{A:|A|\geq t} \min_{\mathcal{R}_A} D_\diamond(\mathcal{R}_A \circ \mathcal{N}_A, \mathcal{I}), \tag{2}$$

where the reconstruction channels $\mathcal{R}_A$ is of the form above, $\mathcal{I}$ denotes the identity channel, and $D_\diamond$ denotes the diamond (or stabilised) norm distance between quantum channels (see below). Here the maximisation is over all authorised groups, but without loss of generality we can restrict to structures with $|A| = t$. The diamond norm distance between two channels $\mathcal{E}$ and $\mathcal{F}$ is defined as

$$D_\diamond(\mathcal{E}, \mathcal{F}) = \max_{|\psi\rangle \in \mathcal{H}\otimes\mathcal{H}'} \frac{1}{2} \big\| \mathcal{E} \otimes \mathcal{I}(|\psi\rangle\langle\psi|) - \mathcal{F} \otimes \mathcal{I}(|\psi\rangle\langle\psi|) \big\|_1, \tag{3}$$

where $\| \cdot \|_1$ is the Schatten 1-norm and the optimisation goes over all auxiliary Hilbert spaces $\mathcal{H}'$. The use of a stabilised distance here is crucial as it ensures that arbitrary secrets can be restored, inclusive of their correlations with a quantum memory held by a third party.

Alternatively, we can replace $D_\diamond$ with a fidelity-based stabilised distance, namely

$$F_\diamond(\mathcal{E}, \mathcal{F}) = \min_{|\psi\rangle \in \mathcal{H}\otimes\mathcal{H}'} F\big(\mathcal{E} \otimes \mathcal{I}(|\psi\rangle\langle\psi|), \mathcal{F} \otimes \mathcal{I}(|\psi\rangle\langle\psi|)\big) \tag{4}$$

where F is the Uhlmann fidelity, $F(\rho, \tau) = \|\sqrt{\rho}\sqrt{\tau}\|_1^2$. We say that the scheme is ϵ-reconstructable in fidelity if

$$\epsilon = 1 - \min_{A:t\leq|A|} \max_{\mathcal{R}_A} F_\diamond(\mathcal{R}_A \circ \mathcal{N}_A, \mathcal{I}). \tag{5}$$

We can relate the two notions of recoverability using Fuchs-van de Graaf inequalities, namely, for any quantum channel $\mathcal{F}$, we show in the Supplemental Material that

$$D_\diamond(\mathcal{F}, \mathcal{I}) \geq 1 - F_\diamond(\mathcal{F}, \mathcal{I}) \geq D_\diamond(\mathcal{F}, \mathcal{I})^2. \tag{6}$$

From this we can immediately conclude that γ-recoverability in fidelity implies $\sqrt{\gamma}$-recoverability in diamond norm, and conversely δ-recoverability in diamond norm implies also δ-recoverability in fidelity.

Next, we establish the notion of approximate secrecy. For this, we need to introduce *complementary channels* [21] for the channels $\mathcal{N}_A$, which intuitively model how much information the adversary retains after the attack. In particular, for a channel $\mathcal{N}_A$ we introduce its Stinespring isometry $\mathcal{U}$ and define $\hat{\mathcal{N}}_A = \mathrm{tr}_A \circ \mathcal{U}$, where tr_A is the partial trace removing the authorized set. Here, if $\mathcal{E}$ has Kraus operators E_i, $\mathcal{Z}_A$ has Kraus operators $Z_{A,j}$, and the partial trace on $\bar{A}$ has Kraus operators $\langle k_{\bar{A}}| \otimes I_A$, where I_A is the identity operator on the authorized set A, then $\mathcal{N}_A$ has Kraus operators $(\langle k_{\bar{A}}| \otimes I_A) Z_{A,j} E_i$. Then define the operator $W = \sum_{i,j,k} |i, j, k\rangle \otimes ((\langle k_{\bar{A}}| \otimes I_A)) Z_{A,j} E_i$. The map $\mathcal{U}$ is then defined as $\mathcal{U}(\rho) = W \rho W^\dagger$.

With this, we say that a (t, n)-threshold QSS scheme has ϵ-secrecy if

$$\epsilon = 1 - \min_{A:|A|\geq t} \max_{\sigma} F_\diamond(\hat{\mathcal{N}}_A, \mathcal{V}_{A,\sigma}), \tag{7}$$

where $\mathcal{V}_{A,\sigma}$ is a preparation channel that prepares a fixed density matrix σ. Namely, $\mathcal{V}_{A,\sigma}$ traces out the qudits of

the players in A and prepares a quantum state described by the density matrix σ, where the output σ does not contain any information about the input state, i.e., the input state is completely hidden. Hence, when $\hat{\mathcal{N}}_A = \mathcal{V}_{A,\sigma}$ for some σ, we have $\epsilon = 0$: a condition for perfect secrecy. The other extreme case is when $\hat{\mathcal{N}}_A = \mathcal{I}$, i.e., all the information is leaking through $\hat{\mathcal{N}}_A$. In this case it can be seen that $\epsilon = 1$.

Finally, we define the strength C of the adversarial model for a (t, n)-threshold QSS scheme:

$$C = \max_{A:|A|\geq t} C\big(\hat{\mathcal{N}}_A\big), \tag{8}$$

where $C(\hat{\mathcal{N}}_A)$ is the entanglement-assisted classical capacity of $\hat{\mathcal{N}}_A$, which is defined for a channel $\mathcal{N}$ with input labeled by X and output labeled by Y as

$$C(\mathcal{N}) = \max_{|\psi\rangle \in \mathcal{H}_X \otimes \mathcal{H}_X} I(X:Y)_\tau \tag{9}$$

where $\tau = \mathcal{I} \otimes \mathcal{N}(|\psi\rangle\langle\psi|)$ and $I(X:Y)_\tau$ is the quantum mutual information evaluated for the state τ. The mutual information itself can be expressed in terms of the Umegaki relative entropy, denoted $D(\cdot\|\cdot)$, namely

$$I(X:Y)_\tau = \min_{\rho_Y} D(\tau \| \rho_X \otimes \rho_Y)\,, \tag{10}$$

where ρ_X and ρ_Y are the marginals of τ. Using this, we can introduce a modified entanglement-assisted capacity, where $I(X:Y)_\tau$ is replaced by

$$\tilde{I}(X:Y)_\tau = -\max_{\rho_Y} \log F(\tau, \rho_X \otimes \rho_Y)\,, \tag{11}$$

which is a variant of the mutual information based on the sandwiched Rényi relative entropy of order $1/2$ [22, 23], given by

$$\widetilde{D}_\alpha(\rho\|\sigma) = \frac{1}{\alpha - 1} \log \mathrm{tr}\left((\sigma^{\frac{1-\alpha}{2\alpha}})^\alpha \rho \sigma^{\frac{1-\alpha}{2\alpha}})^\alpha \right)^\alpha, \tag{12}$$

where ρ and σ are quantum states and $\alpha \neq 1$. The corresponding generalized mutual information is $\tilde{I}_\alpha(X:Y)_\tau = \min_{\rho_Y} \widetilde{D}_\alpha(\tau\|\rho_X \otimes \rho_Y)$ [24], and $\tilde{I}(X:Y)_\tau = \tilde{I}_{1/2}(X:Y)_\tau$. The quantity $C_\alpha(\mathcal{N}) = \max_\tau \tilde{I}_\alpha(X:Y)_\tau$ is a generalized entanglement assisted capacity because $C(\mathcal{N}) = \lim_{\alpha\to 1} C_\alpha(\mathcal{N})$. Next, we define the modified strength of the adversarial model as $\tilde{C} = \max_{|A|\geq t} C_{1/2}(\hat{\mathcal{N}}_A)$, which corresponds to setting $\alpha = 1/2$. The value of $\alpha = 1/2$ is chosen to express the generalized mutual information in terms of fidelity. Since $\widetilde{D}_\alpha$ is monotone nondecreasing in α [22], we can deduce that $C \geq \tilde{C}$.

With all this preparation in hand, we can now state our main result.

Theorem 1. *Consider any (t, n) QSS scheme with an adversarial model. The following are equivalent:*

- *The adversarial model has modified strength $\tilde{C}$.*
- *The scheme has ϵ-secrecy with $\epsilon = 1 - \exp(-\tilde{C})$.*
- *The secret is ϵ-reconstructable in terms of fidelity.*

An immediate corollary of this, given the relations discussed above, is that if the adversarial model has strength at most C, then the secret is δ-recoverable in diamond distance with $\delta \leq \sqrt{1 - \exp(-C)}$.

Proof of Theorem 1. From Beny-Oreshkov duality [25] between channels and complementary channels, we have

$$\max_{\mathcal{R}} F_\diamond(\mathcal{R} \circ \mathcal{N}, \mathcal{M}) = \max_{\mathcal{S}} F_\diamond(\hat{\mathcal{N}}, \mathcal{S} \circ \hat{\mathcal{M}}), \tag{13}$$

where optimizations are over all quantum channels with appropriate input and output dimensions. Suppose that our scheme is ϵ-reconstructable in fidelity. By applying Beny-Oreshkov duality, we get that for any $A \subset \{1, \ldots, n\}$ that

$$\begin{aligned} \epsilon &= 1 - \min_{A:|A|\geq t} \max_{\mathcal{R}_A} F_\diamond(\mathcal{R}_A \circ \mathcal{N}_A, \mathcal{I}) \\ &= 1 - \min_{A:|A|\geq t} \max_{\mathcal{S}_A} F_\diamond(\hat{\mathcal{N}}_A, \mathcal{S}_A \circ \hat{\mathcal{I}}). \end{aligned} \tag{14}$$

As $\hat{\mathcal{I}}$ is the trace channel, $\mathcal{S}_A \circ \hat{\mathcal{I}}$ is without loss of generality a preparation channel $\mathcal{V}_{A,\sigma}$ which prepares a state σ. Since this applies for all A such that $|A| \geq t$, it follows that the QSS scheme also has ϵ-secrecy.

The crucial step in our proof relates $\max_\sigma F_\diamond(\hat{\mathcal{N}}_A, \mathcal{V}_{A,\sigma})$ to the entanglement-assisted capacity of $\hat{\mathcal{N}}_A$ using the following lemma.

Lemma 2. *For any $A \subset \{1, \ldots, n\}$,*

$$\max_\sigma F_\diamond(\hat{\mathcal{N}}_A, \mathcal{V}_{A,\sigma}) = e^{-\tilde{C}_A}, \tag{15}$$

where $\tilde{C}_A = C_{1/2}(\hat{\mathcal{N}}_A)$.

In essence, Lemma 2 connects the worst-case entanglement fidelity with a variant of the entanglement-assisted capacity that arises from generalized sandwiched Rényi divergences.

The first step in proving Lemma 2 is to show that

$$F_\diamond(\hat{\mathcal{N}}_A, \mathcal{V}_{A,\sigma}) = \min_\rho q(\rho, \sigma)^2 \tag{16}$$

where

$$q(\rho, \sigma) = F((\sqrt{\rho} \otimes I) J (\sqrt{\rho} \otimes I), \rho \otimes \sigma)^{1/2}. \tag{17}$$

Here

$$J = (\mathbb{1} \otimes \hat{\mathcal{N}}_A) \sum_{i,j} |\psi_i\rangle|\psi_i\rangle\langle\psi_j|\langle\psi_j| \tag{18}$$

is the Choi-Jamiolkowski matrix [26, 27] of the channel $\hat{\mathcal{N}}_A$, and I denotes an identity matrix. To show (16), we initially write the spectral decomposition of any density matrix ρ as $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$, where $|\psi_i\rangle$ denotes an orthonormal basis. Since λ_i are non-negative, we can

write $\sqrt{\rho} = \sum_i \sqrt{\lambda_i}|\psi_i\rangle\langle\psi_i|$. Next, the purification of ϱ is $|\psi_\varrho\rangle = \sum_i \sqrt{\lambda_i}|\psi_i\rangle|\psi_i\rangle$. If we trace out either the first or second part of the system of the purified state $|\psi_\varrho\rangle$, we will reconstruct the state ρ. Using this notation, note that when $\hat{\mathcal{N}}_A$ takes as input the state ρ, we have

$$\begin{aligned}\tau =&(\mathbb{1}\otimes\hat{\mathcal{N}}_A)(|\psi_\varrho\rangle\langle\psi_\varrho|)\\ =&\sum_{i,j}\sqrt{\lambda_i}\sqrt{\lambda_j}(\mathbb{1}\otimes\hat{\mathcal{N}}_A)(|\psi_i\rangle|\psi_i\rangle\langle\psi_j|\langle\psi_j|)\\ =&(\sqrt{\rho}\otimes I)(\mathbb{1}\otimes\hat{\mathcal{N}}_A)(\sum_{i,j}|\psi_i\rangle|\psi_i\rangle\langle\psi_j|\langle\psi_j|)(\sqrt{\rho}\otimes I)\\ =&(\sqrt{\rho}\otimes I)J(\sqrt{\rho}\otimes I). \end{aligned} \tag{19}$$

Hence we can see that

$$\begin{aligned}&F_\diamond(\hat{\mathcal{N}}_A,\mathcal{V}_{A,\sigma})\\ =&F((\mathbb{1}\otimes\hat{\mathcal{N}}_A)(|\psi_\varrho\rangle\langle\psi_\varrho|),\rho\otimes\sigma)\\ =&F((\sqrt{\rho}\otimes I)J(\sqrt{\rho}\otimes I),\rho\otimes\sigma)\\ =&\Big(\mathrm{tr}\sqrt{(\sqrt{\rho}\otimes\sqrt{\sigma})(\sqrt{\rho}\otimes I)J(\sqrt{\rho}\otimes I)(\sqrt{\rho}\otimes\sqrt{\sigma})}\Big)^2\\ =&\Big(\mathrm{tr}\sqrt{(\rho\otimes\sqrt{\sigma})J(\rho\otimes\sqrt{\sigma})}\Big)^2. \end{aligned} \tag{20}$$

Using the definition of the fidelity, we note that

$$q(\rho,\sigma) = \mathrm{tr}\sqrt{(\rho\otimes\sigma^{1/2})J(\rho\otimes\sigma^{1/2})} \tag{21}$$

$$= \mathrm{tr}\sqrt{J^{1/2}(\rho^2\otimes\sigma)J^{1/2}} \tag{22}$$

$$= \left\|J^{1/2}(\rho\otimes\sqrt{\sigma})\right\|_1. \tag{23}$$

Here in the penultimate equality, we use the fact $\mathrm{tr}(XJX)^{1/2} = \mathrm{tr}(J^{1/2}X^2J^{1/2})^{1/2}$ for positive semi-definite X and J. From (20) and (21), we can establish (16).

The second step in the proof of Lemma 2 is to show that the function $q(\rho,\sigma)$ is convex in the density matrix ρ and concave in the density matrix σ. Concavity of $q(\rho,\sigma)$ in σ is immediate from the fact that the expression in (22) $\omega \mapsto \mathrm{tr}\sqrt{\omega}$ is concave and the linearity of the expression under the square root in σ. To show convexity in ρ we simply note that any norm as in (23) is convex, and the expression inside the norm is linear in ρ. Since $q(\rho,\sigma)$ is convex in ρ and concave in σ, we can apply the minimax theorem [28] to interchange the maximization and minimization, in the sense that

$$\max_\sigma\min_\rho q(\rho,\sigma) = \min_\rho\max_\sigma q(\rho,\sigma). \tag{24}$$

Third, we use (24) along with the identity (16) to establish the equivalence between a fidelity and Rényi mutual information.

Denoting the input and output registers of $\hat{\mathcal{N}}_A$ as X and Y respectively, we see that

$$\begin{aligned}\tilde{I}(X:Y)_\tau &= \min_\sigma \tilde{D}_{1/2}\big((\mathbb{1}\otimes\hat{\mathcal{N}}_A)(|\psi_\varrho\rangle\langle\psi_\varrho|\big\|\rho\otimes\sigma)\big)\\ &= \min_\sigma\Big(-\log F\big((\mathbb{1}\otimes\hat{\mathcal{N}}_A)(|\psi_\varrho\rangle\langle\psi_\varrho|,\rho\otimes\sigma)\big)\Big)\\ &= \min_\sigma\big(-\log q(\rho,\sigma)^2\big). \end{aligned} \tag{25}$$

Because $-\log$ is a monotone decreasing function, we deduce that $\tilde{I}(X:Y)_\tau = -\log\big(\max_\sigma q(\rho,\sigma)^2\big)$. Applying the definition of the generalized entanglement assisted capacity, we get $\tilde{C}_A = -\log\big(\min_\rho\max_\sigma q(\rho,\sigma)^2\big)$. Next, the minimax result (24) implies that

$$\tilde{C}_A = -\log\big(\max_\sigma\min_\rho q(\rho,\sigma)^2\big). \tag{26}$$

Next, from (16), we can see that $\max_\sigma F_\diamond(\hat{\mathcal{N}}_A,\mathcal{V}_{A,\sigma}) = \max_\sigma\min_\rho q(\rho,\sigma)^2$. Hence

$$\exp(-\tilde{C}_A) = \max_\sigma F_\diamond(\hat{\mathcal{N}}_A,\mathcal{V}_{A,\sigma}), \tag{27}$$

and the proof of Lemma 2 follows. Putting Lemma 2 and (14) together, we complete the proof of Theorem 1. □

III. CONCLUSION, DISCUSSION, AND OPEN QUESTIONS

We have established that the entanglement-assisted capacity of a channel connecting the quantum secret to the quantum systems of the adversary determines both the approximate reconstructability and the approximate secrecy of a threshold QSS scheme. In some sense, our result can be intuitively understood from the mantra "*Quantum information cannot be learnt without disturbing it.*" This mantra can be used to obtain interpretations of multitude of topics in quantum theory, such as approximate quantum error correction [29–33], monogamy of entanglement [34], and the quantum information of black hole evaporation [35]. Particularly for quantum error correction, the encoding map in a QSS scheme takes the quantum secret to a quantum error correction code, and the approximate reconstructability of the secret is precisely the approximate reconstructability of the code. In this regard, our theorem implies that, if the adversaries trying to learn the secret have access to a channel with entanglement-assisted capacity of C, then there exists a decoding operation that reconstructs the secret up to an error of δ, quantified in terms of the diamond distance, where $\delta \leq \sqrt{1-\exp(-C)}$. It remains an open question as to how different types of capacities other than the entanglement-assisted capacity influences the theory of approximate QSS.

ACKNOWLEDGEMENTS

YO and MT are supported by the Quantum Engineering Programme grant NRF2021-QEP2-01-P06, and the National Research Foundation, Prime Minister's Office, Singapore and the Ministry of Education, Singapore under the Research Centres of Excellence program. YO also acknowledges support from EPSRC (Grant No. EP/W028115/1). This research was supported by the Australian Research Council (ARC) Discovery Project

(DP200102273) and ARC Centre of Excellence for Engineered Quantum Systems (EQUS,CE170100009). JR is supported by a Westpac Bicentennial Foundation Research Fellowship. BCS acknowledges funding from the Natural Sciences and Engineering Research Council of Canada.

Appendix A: Supplemental Material

First we define some notation. Given a Hilbert space $\mathscr{H}$, let $|\mathscr{H}|$ denote its dimension. We restrict our attention to finite dimensional Hilbert spaces. Let $\mathsf{M}(\mathscr{H})$ denote the set of matrix representations of linear operators on Hilbert space $\mathscr{H}$. Let $\mathsf{D}(\mathscr{H})$ denote the set of operators in $\mathsf{M}(\mathscr{H})$ that have unit trace and are positive semidefinite. A quantum channel is a completely positive and trace preserving map from $\mathsf{M}(\mathscr{H})$ to $\mathsf{M}(\mathscr{K})$ where $\mathscr{H}$ and $\mathscr{K}$ are Hilbert spaces. We use the shorthand ($\mathcal{N}$ CPT) to indicate that $\mathcal{N}$ is a quantum channel.

Proof of (6) in the main manuscript. Note that for a channel $\mathcal{F} : \mathsf{M}(\mathscr{H}) \to \mathsf{M}(\mathscr{H})$,

$$F(\mathcal{F}, \mathbb{1}) = \min_{\substack{|\psi\rangle \in \mathscr{H}\otimes\mathscr{H} \\ \||\psi\rangle\| = 1}} F(|\psi\rangle\langle\psi|, (\mathcal{I}\otimes\mathcal{F})(|\psi\rangle\langle\psi|)). \quad \text{(A1)}$$

Now for any pure state $|\psi\rangle\langle\psi|$ and mixed state σ, we have

$$F(|\psi\rangle\langle\psi|, \sigma) = \langle\psi|\sigma|\psi\rangle \quad \text{(A2)}$$

From the Fuchs-van de Graaf inequalities we have

$$\big(1 - \frac{1}{2}\||\psi\rangle\langle\psi| - \sigma\|_1\big)^2 \leq F(|\psi\rangle\langle\psi|, \sigma)$$
$$F(|\psi\rangle\langle\psi|, \sigma) \leq 1 - \frac{1}{4}\||\psi\rangle\langle\psi| - \sigma\|_1^2. \quad \text{(A3)}$$

We thereby deduce that

$$\begin{aligned} &F(\mathcal{F}, \mathbb{1}) \\ \leq &1 - \max_{\substack{|\psi\rangle \in \mathscr{H}\otimes\mathscr{H} \\ \||\psi\rangle\| = 1}} \frac{1}{4}\||\psi\rangle\langle\psi| - (\mathcal{I}\otimes\mathcal{F})(|\psi\rangle\langle\psi|)\|_1^2 \\ = &1 - \frac{1}{4}\|\mathbb{1} - \mathcal{F}\|_\diamond^2 \\ = &1 - D_\diamond(\mathbb{1}, \mathcal{F})^2, \end{aligned} \quad \text{(A4)}$$

and

$$\begin{aligned} &F(\mathcal{F}, \mathbb{1}) \\ \geq &(1 - \max_{\substack{|\psi\rangle \in \mathscr{H}\otimes\mathscr{H} \\ \||\psi\rangle\| = 1}} \frac{1}{2}\||\psi\rangle\langle\psi| - (\mathcal{I}\otimes\mathcal{F})(|\psi\rangle\langle\psi|)\|_1)^2 \\ = &(1 - \frac{1}{2}\|\mathbb{1} - \mathcal{F}\|_\diamond)^2 \\ = &(1 - D_\diamond(\mathbb{1}, \mathcal{F}))^2. \end{aligned} \quad \text{(A5)}$$

Hence,

$$(1 - D_\diamond(\mathbb{1}, \mathcal{F}))^2 \leq F(\mathcal{F}, \mathbb{1}) \leq 1 - D_\diamond(\mathbb{1}, \mathcal{F})^2. \quad \text{(A6)}$$

For a tighter lower bound, note that [36, Lemma 9.1.1]

$$\frac{1}{2}\|\psi\rangle\langle\psi| - \sigma\|_1 = \max_{0 \leq P \leq I} \operatorname{tr} P(|\psi\rangle\langle\psi| - \sigma), \quad \text{(A7)}$$

and by picking $P = |\psi\rangle\langle\psi|$, we get

$$\frac{1}{2}\|\psi\rangle\langle\psi| - \sigma\|_1 \geq 1 - \langle\psi|\sigma|\psi\rangle = 1 - F(|\psi\rangle\langle\psi|, \sigma), \quad \text{(A8)}$$

and hence

$$1 - D_\diamond(\mathbb{1}, \mathcal{F}) \leq F(\mathcal{F}, \mathbb{1}) \leq 1 - D_\diamond(\mathbb{1}, \mathcal{F})^2, \quad \text{(A9)}$$

and this proves (6) in the main manuscript. □

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, New York, 1984.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[3] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, pp. 1829–1834, Mar. 1999. arXiv: quant-ph/9806063.

[4] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, pp. 648–651, Jul 1999.

[5] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A*, vol. 55, pp. 900–911, Feb. 1997.

[6] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing," *Phys. Rev. A*, vol. 78, p. 042309, Oct 2008.

[7] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, "Quantum secret sharing with qudit graph states," *Phys. Rev. A*, vol. 82, p. 062315, Dec 2010.

[8] M. Fitzi, N. Gisin, and U. Maurer, "Quantum solution to the byzantine agreement problem," *Phys. Rev. Lett.*, vol. 87, p. 217901, Nov 2001.

[9] Y. Ouyang, S.-H. Tan, L. Zhao, and J. F. Fitzsimons, "Computing on quantum shared secrets," *Physical Review A*, vol. 96, no. 5, p. 052333, 2017.

[10] D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A*, vol. 61, p. 042311, Mar 2000.

[11] H. Imai, J. Mueller-Quade, A. C. A. Nascimento, P. Tuyls, and A. Winter, "A quantum information theoretical model for quantum secret sharing schemes,"

Quantum Inf. Comput., vol. 5, pp. 69–80, 2005. arXiv: quant-ph/0311136.

[12] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, pp. 1829–1834, Mar 1999.

[13] S. Nikova, C. Rechberger, and V. Rijmen, "Threshold implementations against side-channel attacks and glitches," in *International conference on information and communications security*, pp. 529–545, Springer, 2006.

[14] J. L. Park, "The concept of transition in quantum mechanics," *Found. Phys.*, vol. 1, pp. 23–33, Mar 1970.

[15] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[16] C. Crépeau, D. Gottesman, and A. Smith, "Approximate quantum error-correcting codes and secret sharing schemes," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 285–301, Springer, 2005.

[17] H. Imai, J. Müller-Quade, A. C. Nascimento, P. Tuyls, and A. Winter, "An information theoretical model for quantum secret sharing," *Quant. Inf. Comput.*, vol. 5, no. 1, pp. 69–80, 2005.

[18] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," *Phys. Rev. A*, vol. 72, p. 032318, Sep 2005.

[19] D. Kretschmann, D. W. Kribs, and R. W. Spekkens, "Complementarity of private and correctable subsystems in quantum cryptography and error correction," *Phys. Rev. A*, vol. 78, p. 032330, Sep 2008.

[20] P. Hayden and G. Penington, "Approximate Quantum Error Correction Revisited: Introducing the Alpha-Bit," *Commun. Math. Phys.*, vol. 374, pp. 369–432, Mar. 2020.

[21] I. Devetak and P. W. Shor, "The Capacity of a Quantum Channel for Simultaneous Transmission of Classical and Quantum Information," *Commun. Math. Phys.*, vol. 256, no. 2, pp. 287–303, 2005.

[22] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," *J. Math. Phys.*, vol. 54, no. 12, p. 122203, 2013.

[23] M. M. Wilde, A. Winter, and D. Yang, "Strong converse for the classical capacity of entanglement-breaking and hadamard channels via a sandwiched rényi relative entropy," *Commun. Math. Physics*, vol. 331, no. 2, pp. 593–622, 2014.

[24] M. K. Gupta and M. M. Wilde, "Multiplicativity of completely bounded p-norms implies a strong converse for entanglement-assisted capacity," *Commun. Math. Phys.*, vol. 334, no. 2, pp. 867–887, 2015.

[25] C. Bény and O. Oreshkov, "Approximate simulation of quantum channels," *Phys. Rev. A*, vol. 84, p. 022333, Aug. 2011.

[26] M.-D. Choi, "Completely positive linear maps on complex matrices," *Linear Algebra and its Applications*, vol. 10, no. 3, pp. 285–290, 1975.

[27] M. Jiang, S. Luo, and S. Fu, "Channel-state duality," *Phys. Rev. A*, vol. 87, no. 2, p. 022310, 2013.

[28] M. do Rosário Grossinho and S. A. Tersian, *An introduction to minimax theorems and their applications to differential equations*, vol. 52. Springer Science & Business Media, 2001.

[29] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto, "Approximate quantum error correction can lead to better codes," *Phys. Rev. A*, vol. 56, p. 2567, 1997.

[30] H. Barnum and E. Knill, "Reversing quantum dynamics with near-optimal quantum and classical fidelity," *J. Math. Phys.*, vol. 43, p. 2097, Jan. 2002.

[31] C. Bény and O. Oreshkov, "General Conditions for Approximate Quantum Error Correction and Near-Optimal Recovery Channels," *Phys. Rev. Lett.*, vol. 104, p. 120501, Mar. 2010.

[32] J. Tyson, "Two-sided bounds on minimum-error quantum measurement, on the reversibility of quantum dynamics, and on maximum overlap using directional iterates," *J. Math. Phys.*, vol. 51, p. 92204, June 2010.

[33] Y. Ouyang, "Permutation-invariant quantum codes," *Phys. Rev. A*, vol. 90, p. 062317, Dec 2014.

[34] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography," *New J. Phys.*, vol. 15, no. 10, p. 103002, 2013.

[35] A. Almheiri, T. Hartman, J. Maldacena, E. Shaghoulian, and A. Tajdini, "The entropy of hawking radiation," *Rev. Mod. Phys.*, vol. 93, p. 035002, Jul 2021.

[36] M. M. Wilde, *From Classical to Quantum Shannon Theory*. Cambridge University Press, 2013.