Quantum private broadcasting

Anne Broadbent,[1,*] Carlos E. González-Guillén,[2,†] and Christine Schuknecht[1,‡]

[1] *University of Ottawa, Ottawa, Canada, K1N 6N5*
[2] *Universidad Politécnica de Madrid, Madrid 28006, Spain*

(Received 26 August 2021; accepted 16 December 2021; published 10 February 2022)

In private broadcasting, a single plaintext is broadcast to multiple recipients in an encrypted form, such that each recipient can decrypt locally. When the message is classical, a straightforward solution is to encrypt the plaintext with a single key shared among all parties, and to send to each recipient a copy of the ciphertext. Surprisingly, the analogous method is insufficient in the case where the message is quantum [i.e., in quantum private broadcasting (QPB)]. In this work, we give three solutions to t-recipient quantum private broadcasting (t-QPB) and compare them in terms of key lengths. The first method is the independent encryption with the quantum one-time pad, which requires a key linear in the number of recipients, t. We show that the key length can be decreased to be logarithmic in t by using unitary t-designs. Our main contribution is to show that this can be improved to a key length that is logarithmic in the dimension of the symmetric subspace, using a concept that we define of *symmetric unitary t-designs*, which may be of independent interest.

DOI: 10.1103/PhysRevA.105.022606

I. INTRODUCTION

The secure transmission of classical information is a fundamental and well-studied problem, as it is the basis of current secure communications. Shannon [1,2] showed that in order to transmit n bits of information in an information-theoretically secure way, one needs an n-bit shared secret key. An optimal solution to this problem is given by the one-time pad, where, in order to securely transmit an n-bit message m, a random key $k \in \{0, 1\}^n$ previously shared between the parties can be used by applying the exclusive-or $m \oplus k$ to encrypt, and later to decrypt if the key is known. This encryption scheme is information-theoretic secure when the key is used only once (hence its name). Nevertheless, one can use the same single key to encrypt the same message and distribute it to as many recipients as desired or, equivalently, broadcast the ciphertext so that anyone in possession of the key can decrypt the message.

In the case of a quantum encryption scheme, where the plaintext is a quantum message, that is, an n-qubit state, $2n$ bits of shared key are needed for perfect security, and the quantum one-time pad, where a random unitary from a set of $2n$ unitaries is used to encrypt, is optimal [3,4]. The perfect security is equivalent to having a randomizing map which maps any quantum state to the maximally mixed state. In the case of approximate security, it was also proven in [3] that $2n$ bits are needed for security against side information. Whereas, if there is no side information, there are ϵ-randomizing maps with $O(n \log_2(n))$ unitaries that are approximately secure encryption schemes [5,6].

As in the one-time pad, the key from the quantum one-time pad cannot be reused to encrypt two different quantum states. Moreover, with the quantum one-time pad, one cannot even use the same key to encrypt the same state twice as it allows the ability to discard some possible original states as noted in [7]. So, how can we securely and efficiently broadcast the same quantum message to t recipients, such that the message is information-theoretically secure? This is the problem that we study here and call *t-recipient quantum private broadcasting*. More precisely, if one has available t copies of the same pure quantum state and wants to securely communicate each state to different recipients, how can this be accomplished so that each recipient decrypts with the same key? Furthermore, what is the size of such a key? We tackle these questions and enlarge the already close connection between quantum encryption schemes and unitary designs.

Unitary t-designs were introduced by Dankert *et al.* [8] from the concept of state designs. Follow-up work on unitary t-designs includes Refs. [9–14]. They are a discrete set of unitary matrices with a probability measure with the property that averaging up to t uses of the unitary yields the same result as averaging with respect to the Haar measure over the full unitary group. Unitary 1-designs are known to yield perfect encryption schemes and unitary 2-designs yield nonmalleable encryption schemes [15] (see, also, [16]). In [12], the authors consider the approximate case for unitary 2-designs and their link to approximate nonmalleable encryption schemes. Recent work [17] demonstrates that Haar random unitaries allow a private quantum channel to be implemented with multiphoton pulses, and shows that t-designs can be used to practically implement such channels when the parity of the photon source is fixed.

There are no known efficient constructions of exact unitary t-designs for $t > 3$, although there has been recent work completed regarding such constructions [14,18]. However, it has been shown that ϵ-approximate unitary t-designs on n qubits

[*] abroadbe@uottawa.ca
[†] carlos.gguillen@upm.es
[‡] cschu059@uottawa.ca

can be efficiently constructed with local random circuits that are polynomial in n, t, and $\log_2(1/\epsilon)$ [19]. In this work, we use the construction of an ϵ-approximate unitary t-design from [12], where they prove an upper bound for when the unitaries are sampled from an exact t-design (Theorem 3.1 [12]). They show that when, at most, $C(td)^t(t\log_2 d)^6/\epsilon^2$ unitaries are sampled from a t-design for some constant C, then this is an ϵ-approximate unitary t-design with probability of at least $1/2$.

In this article, we formally introduce a t-recipient quantum private broadcasting (t-QPB) scheme in the information-theoretic setting and discuss three possible ways to implement it. First is the natural idea of using the quantum one-time pad and examining the ramifications of reusing the key. Second is the use of exact and approximate t-designs as encryption schemes. Intuitively, in a t-QPB scheme there are only t uses of the unitaries, and random unitaries from the Haar measure are perfect t-QPB schemes for any number of copies t, which is made clear from Sec. II D and the formal definition of t-QPB. Therefore, it follows that t-designs can be used for t-QPB schemes. Since the key length required for unitary t-designs is logarithmic in t, this offers an exponential improvement in key length compared to the first solution. Lastly, we propose, a notion of *designs*, applicable to the scenario where the input is in the symmetric subspace. We call these *symmetric unitary t-designs*, and the resulting t-QPB schemes have the lowest key size as they exploit the full structure of the broadcasting problem that we have outlined.

We note that recent work on private communication over quantum broadcast channels [20] considers a different scenario, where recipients are *legitimate* or *malicious*; this differs from our work of broadcasting the same encrypted message to multiple recipients, who must then locally decrypt.

The paper is organized as follows. In Sec. II, we recall the basic notation, definition of unitary designs and symmetric subspace, and how they are related through representation theory. Then, in Sec. III, we introduce the definitions of t-recipient quantum private broadcasting. IVVVI analyze each of the solutions proposed, with Sec. IV devoted to the quantum one-time pad, Sec. V to unitary t-designs, and Sec. VI introducing and analyzing these symmetric unitary t-designs. Finally, Sec. VII contains a summary and some open problems.

II. PRELIMINARIES

In this section, we present the basic notation used throughout this paper. We define unitary t-designs, recall the known upper and lower bounds on their size, and briefly define and explain the symmetric subspace and concepts needed from representation theory.

A. Basic notation

Let $\mathcal{H}_{d^n}$ be the Hilbert space of dimension d^n which is spanned by the basis states $\{|x\rangle : x \in \{0, 1, \dots, d-1\}^n\}$. Let $\mathcal{D}(\mathcal{H}_{d^n})$ be the set of density operators and $\mathcal{L}(\mathcal{H}_{d^n})$ be the set of linear operators on $\mathcal{H}_{d^n}$. A Hilbert space of subsystems, say M and E, is denoted with subscripts, $\mathcal{H}_{d^n} = \mathcal{H}_M \otimes \mathcal{H}_E$. Density operators on such Hilbert spaces are written as ρ_{ME}, and ρ_E denotes when subsystem M is traced out from ρ_{ME}. Transformations between quantum states are formalized by quantum channels, that is, completely positive trace preserving maps. Determining the distinguishability of the outputs from two such channels, $\Psi, \Phi : \mathcal{L}(\mathcal{H}_M) \rightarrow \mathcal{L}(\mathcal{H}_M)$, is done with the trace norm $||\cdot||_1$, where $||A||_1 = \mathrm{Tr}(\sqrt{AA^\dagger})$ for linear operator A. This trace norm is the sum of the singular values of A, while the infinity norm $||\cdot||_\infty$ is the maximum singular value. The quantum channels themselves are compared with the diamond norm $||\cdot||_\diamond$, which is the maximum trace norm when an auxiliary space E is considered, along with the original Hilbert spaces [21,22]. For example, $||\Psi - \Phi||_\diamond = \max_{\rho_{ME}} ||(\Psi \otimes \mathcal{I}_E)\rho_{ME} - (\Phi \otimes \mathcal{I}_E)\rho_{ME}||_1$, where $\mathcal{I}_E$ denotes the identity operator in $\mathcal{L}(\mathcal{H}_E)$. This is considered a better determination of the distinguishability of two quantum channels than the $1 \rightarrow 1$ norm, that is, $||\Psi - \Phi||_{1\rightarrow 1} = \max_{\rho_M} ||\Psi(\rho_M) - \Phi(\rho_M)||_1$, because it accounts for the original space $\mathcal{H}_M$ being entangled with another auxiliary space $\mathcal{H}_E$.

The notation $\mathcal{U}(d)$ denotes the unitary group of all $d \times d$ unitaries. The Pauli matrices for 2-qubits are defined as

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The quantum one-time pad (QOTP) is defined in the following way for $\varphi \in \mathcal{D}(\mathcal{H}_{2^n})$ and $a, b \in \{0, 1\}^n$:

$$\mathsf{QOTP}_{a,b}(\varphi) = X^a Z^b \varphi Z^b X^a,$$

where X and Z are Pauli operators. The quantum one-time pad is perfectly secure as defined in Definition 4, where the input need not be restricted to the symmetric subspace. This is because

$$\mathop{\mathbb{E}}_{a,b\in\{0,1\}^n} \mathsf{QOTP}_{a,b}(\varphi) = \frac{\mathbb{I}}{2^{2n}},$$

where $\mathbb{E}$ denotes the expectation value and $\mathbb{I}$ is the identity matrix of the given space, $\mathcal{D}(\mathcal{H}_{2^n})$. It can be shown that the quantum one-time pad is also perfectly secure against adversaries with side information (an auxiliary space) [3]. This is because, when considering the state of a quantum system M that is interacting with an environment E, applying the QOTP results in a joint state that is independent of the state of system M, that is, $(\mathbb{E}_{a,b}\, \mathsf{QOTP}_{a,b} \otimes \mathcal{I}_E)\varphi_{ME} = \frac{\mathbb{I}}{2^{2n}} \otimes \varphi_E$, where $\varphi_{ME} \in \mathcal{D}(\mathcal{H}_{2^{2n}} \otimes \mathcal{H}_E)$.[1]

B. Unitary t-designs

We use the definition in [10] for unitary t-designs, which we adapt to our notation.

Definition 1. Let $\{U_k\}_{k\in K}$ be a finite subset of $\mathcal{U}(d)$ and let $w : \{U_k\}_{k\in K} \rightarrow \mathbb{R}$ be a positive weight function such that $w(U_k) \geqslant 0$, $\sum_{k\in K} w(U_k) = 1$. Then, $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ is

[1] This can be generalized to $\mathcal{H}_{d^n}$ with the generalized Pauli group.

TABLE I. Known bounds on the number of unitaries for unitary t-designs.

	Lower	Upper
Wtd	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$ [10]	$\binom{d^2+t-1}{t}^2 \in O(t^{2(d^2-1)})$ [10]
Unwtd	$\binom{d^2+t-1}{t} \in \Omega(t^{d^2-1})$ [10]	$(\frac{e(d^2+t-1)}{t})^{2t}$ [13]

called a *unitary t-design* if

$$\mathbb{E}_{\mathfrak{U}}[U^{\otimes t} \otimes (U^{\dagger})^{\otimes t}] = \sum_{k\in K} w(U_k)\cdot U_k^{\otimes t} \otimes (U_k^{\dagger})^{\otimes t} \\ = \int_{\mathcal{U}(d)} U^{\otimes t} \otimes (U^{\dagger})^{\otimes t} dU, \tag{1}$$

where the integral is over the whole unitary group with respect to the Haar measure.

When $w(U_k) = 1/|K|$ for every U_k, this is an unweighted unitary t-design. Otherwise, it is a weighted unitary t-design. The known lower and upper bounds on the number of unitaries needed (i.e., $|K|$) for exact unitary t-designs for general t and dimension d are shown in Table I.

There are also approximate unitary t-designs, defined as follows.

Definition 2. Let $\{U_k\}_{k\in K}$ be a finite subset of $\mathcal{U}(d)$ and let $w : \{U_k\}_{k\in K} \to \mathbb{R}$ be a positive weight function such that $w(U_k) \geqslant 0$, $\sum_{k\in K} w(U_k) = 1$. Then, $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ is called an *ϵ-approximate unitary t-design* if

$$\left\| \mathbb{E}_{\mathfrak{U}}\left[\mathcal{E}_{U_k}^{(t)}\right] - T^{(t)} \right\|_{1\to 1} < \epsilon, \tag{2}$$

where $T^{(t)}$ is the t-twirling channel $T^{(t)}(\rho) = \int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^{\dagger})^{\otimes t} dU$ and $\mathcal{E}_{U_k}^{(t)}(\rho) = U_k^{\otimes t}\rho(U_k^{\dagger})^{\otimes t}$ for $\rho \in \mathcal{D}(\mathcal{H}_{d^t})$.

Note that there are other definitions of ϵ-approximate unitary t-designs depending on the norm used in Eq. (2). We use the $1 \to 1$ norm as it is the one needed for our application.

C. Symmetric subspace

As defined similarly in [23], the symmetric subspace for quantum states in $\mathcal{H}_d^{\otimes t}$ is the subspace formed by states invariant under any permutation of the subsystems, i.e.,

$$\mathrm{Sym}(d^t) := \{|\phi\rangle \in (\mathcal{H}_d)^{\otimes t} : P_d(\pi)\,|\phi\rangle = |\phi\rangle\,, \forall \pi \in S_t\},$$

where $P_d(\pi) : \mathcal{H}_d^{\otimes t} \to \mathcal{H}_d^{\otimes t}$ is the operator that permutes the t subsystems in $\mathcal{H}_d^{\otimes t}$ according to permutation π in the symmetric group of t elements S_t. That is,

$$P_d(\pi) = \sum_{i_1,\ldots,i_t=0}^{d-1} |i_{\pi^{-1}(1)}, \ldots, i_{\pi^{-1}(t)}\rangle\langle i_1, \ldots, i_t|.$$

The dimension for this subspace is $d_{\mathrm{Sym}} = \binom{d+t-1}{t}$ [23]. The notation $\mathcal{U}(\mathrm{Sym}(d^t))$ denotes unitaries from $\mathrm{Sym}(d^t) \otimes \mathrm{Sym}(d^t)$ of size $d_{\mathrm{Sym}} \times d_{\mathrm{Sym}}$, in the same way that $\mathcal{U}(d)$ denotes unitaries from $\mathcal{H}_d \otimes \mathcal{H}_d$ of size $d \times d$. The notation $\mathcal{D}(\mathrm{Sym}(d^t))$ is for the density operators on $\mathrm{Sym}(d^t)$. One can write density matrices in the symmetric subspace as a real linear combination of rank 1 density matrices [23], that is,

$$\mathcal{D}(\mathrm{Sym}(d^t)) \subset \mathrm{span}_{\mathbb{R}}\{(|\varphi\rangle\langle\varphi|)^{\otimes t} : |\varphi\rangle \in \mathcal{H}_d\}. \tag{3}$$

D. Representation theory

Using Schur-Weyl duality and Schur's Lemma [24] similarly to [12], one can write the following for $\rho \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$:

$$\int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^{\dagger})^{\otimes t} dU \\ = \mathrm{tr}(\Pi_{\mathrm{Sym}}\rho\Pi_{\mathrm{Sym}})\tau_{\mathrm{Sym}} + \sum_b \mathrm{tr}(\Pi_b\rho\Pi_b)\tau_b, \tag{4}$$

where Π_{Sym} is the projector into $\mathrm{Sym}(d^t)$ and $\tau_{\mathrm{Sym}} = \frac{\Pi_{\mathrm{Sym}}}{d_{\mathrm{Sym}}}$. These Π_b are projectors into subspaces orthogonal to the symmetric subspace which have dimension d_b, and $\tau_b = \frac{\Pi_b}{d_b}$. When $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$, this reduces to τ_{Sym}.

III. DEFINITIONS FOR QUANTUM PRIVATE BROADCASTING

Here we define the semantics of a t-recipient quantum private broadcast scheme, (t-QPB) along with its security definitions. We also make an observation relating t-QPB schemes to $(t-1)$-QPB schemes with perfect security and correctness.

Definition 3. Let $\mathcal{H}_M = \mathcal{H}_d$ and $\mathcal{H}_C$ be the message and ciphertext Hilbert spaces, respectively. A δ-correct, t-recipient quantum private broadcast scheme in $\mathcal{H}_M$ is a set of encryption maps $\mathsf{Enc}_k : \mathcal{H}_M^{\otimes t} \to \mathcal{H}_C^{\otimes t}$ along with decryption maps $\mathsf{Dec}_k : \mathcal{H}_C \to \mathcal{H}_M$, where $k \in K$ is the set of possible keys. We require that for each $k \in K$,

$$\left\| (\mathsf{Dec}_k^{\otimes t} \circ \mathsf{Enc}_k)\big|_{\mathrm{Sym}(d^t)} - \mathcal{I}_{\mathrm{Sym}(d^t)} \right\|_{\diamond} \leqslant 1 - \delta, \tag{5}$$

where the notation $|_{\mathrm{Sym}(d^t)}$ denotes that the input messages are restricted to being elements of $\mathrm{Sym}(d^t)$, and $\mathcal{I}_{\mathrm{Sym}(d^t)}$ is the identity map in $\mathrm{Sym}(d^t)$.

Note that in this definition, there is no reference about how the t copies of the pure quantum state (or the state in the symmetric subspace) are produced. They can be given by a third party or, if the quantum state to be transmitted is known, they can be prepared. We also note that a 1-correct t-QPB (that is, a perfect t-QPB) must necessarily be implemented via unitary matrices. Moreover, in this case, as the definition imposes local identical decryption, the decryption operation needs to be the t-fold tensor product of a unitary matrix. Thus, although the encryption maps are not necessarily t-fold tensor products of a unitary matrix, the action of each of them over the symmetric subspace can be written as a t-fold tensor product of a unitary matrix. Such a perfect t-QPB is illustrated in Fig. 1. The indistinguishability of ciphertexts for our t-QPB scheme is based on the definitions from [12], which compares the encryption scheme with that of a "state replacement channel" $\langle\sigma\rangle$. For a fixed $\sigma \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$, this is defined as $\langle\sigma\rangle(R) = \mathrm{Tr}(R)\sigma$, for any $R \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$.

Definition 4. Let K be the set of possible keys in the t-QPB. A t-QPB has ϵ-indistinguishable ciphertexts if there exists a fixed $\sigma \in \mathcal{D}(\mathcal{H}_d^{\otimes t})$ such that

$$\left\| \Big(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k - \langle\sigma\rangle \Big)\Big|_{\mathrm{Sym}(d^t)} \right\|_{1\to 1} \leqslant \epsilon. \tag{6}$$

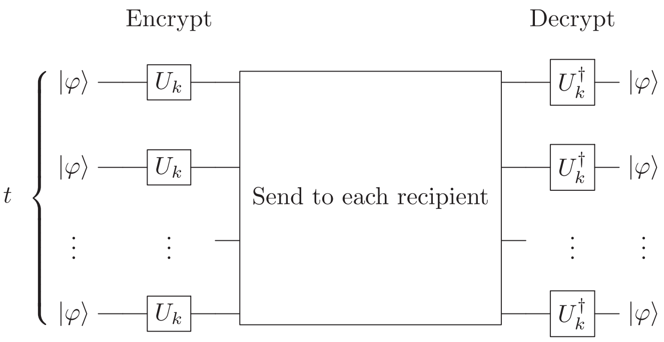

FIG. 1. Quantum private broadcasting.

We note that the above does not consider quantum side information. The encryption scheme has ϵ-indistinguishable ciphertexts against adversaries with side information if

$$\left\| \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k - \langle \sigma \rangle \right)\Big|_{\mathrm{Sym}(d^t)} \right\|_\diamond \leqslant \epsilon. \tag{7}$$

Indistinguishability against adversaries with side information necessarily implies indistinguishability since the $1 \to 1$ norm is upper bounded by the $\diamond$ norm.

When the above norms are equal to zero, we call such encryption schemes *perfectly secure* or *perfectly secure against adversaries with side information* because in this case both notions coincide.

When $t = 1$, Sec. III corresponds to the conventional information-theoretic encryption [12], where there is no restriction in the input space.

In the perfect security scenario, Sec. III implies that if all ciphertexts are intercepted by an adversary who has no information about the key, they can learn nothing. Moreover, if instead the adversary intercepts less than t copies and waits to make an attack until after the honest receivers perform their decryption, they still learn nothing. This is because from the adversary's point of view, the part of the system where the decryption is performed is traced out, and therefore the decryption operation has no effect on the adversary's view of the state.

Note that random unitaries from the Haar measure are perfectly secure 1-correct t-QPB schemes for any number of copies t with an infinite key set $K = \mathcal{U}(d)$, where $\mathsf{Enc}_U^{(t)} = \mathsf{Enc}_U^{\otimes t}$, $\mathsf{Enc}_U(\rho) = U\rho U^\dagger$, and $\mathsf{Dec}_U(\rho) = U^\dagger \rho U$ for $U \in \mathcal{U}(d)$. Indeed, correctness follows from the use of unitary matrices as encrypting and decrypting maps, while perfect security follows from Sec. II D.

The following lemma follows naturally from the setting where t copies of a pure quantum state are used as the input for a t-QPB.

Lemma 1. Let $\mathsf{Enc}_k^{(t)} : \mathcal{H}_M^{\otimes t} \to \mathcal{H}_C^{\otimes t}$ and $\mathsf{Dec}_k : \mathcal{H}_C \to \mathcal{H}_M$, defined as $\mathsf{Enc}_k^{(t)}(\rho) = U_k^{\otimes t}\rho(U_k^{\otimes t})^\dagger$ and $\mathsf{Dec}_k(\gamma) = U_k^\dagger \gamma U_k$, respectively. Let $(\mathsf{Enc}_k^{(t)}, \mathsf{Dec}_k)$ be a perfectly secure and perfectly correct t-QPB scheme. Then, $(\mathsf{Enc}_k^{(t-1)}, \mathsf{Dec}_k)$ is a perfectly secure and perfectly correct $(t-1)$-QPB scheme.

Proof. By definition of encoding and decoding maps, it is clear that for any $\rho \in \mathcal{D}(\mathcal{H}_d^{\otimes t-1} \otimes \mathcal{H}_A)$, we have $(\mathsf{Dec}_k^{\otimes t-1} \circ \mathsf{Enc}_k^{(t-1)}) \otimes \mathcal{I}_A(\rho) = \rho$ and thus $\|(\mathsf{Dec}_k^{\otimes t-1} \circ \mathsf{Enc}_k^{(t-1)})|_{\mathrm{Sym}(d^{t-1})} - \mathcal{I}_{\mathrm{Sym}(d^{t-1})}\|_\diamond = 0$ showing correctness.

Let $\rho = (|\varphi\rangle\langle\varphi|)^{\otimes t-1}$, with $|\varphi\rangle \in \mathcal{H}_d$; then we have

$$\begin{aligned} \mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k^{(t-1)}(\rho) &= \mathrm{tr}_1\Big(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k^{(t)}(\rho \otimes |\varphi\rangle\langle\varphi|)\Big) \\ &= \mathrm{tr}_1(\tau_{\mathrm{Sym},t}) = \tau_{\mathrm{Sym},t-1}, \end{aligned}$$

where the first equality follows from linearity and the second follows from the definition of a perfectly correct t-QPB scheme. We use the notation $\tau_{\mathrm{Sym},t}$ to make explicit that it is the maximally mixed state in $\mathcal{D}(\mathrm{Sym}(d^t))$. Moreover, using Eq. (3) and linearity, we know that this equation holds for any $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$. Thus,

$$\left\| \left(\mathop{\mathbb{E}}_{k\in K} \mathsf{Enc}_k^{(t-1)} - \langle \tau_{\mathrm{Sym},t-1} \rangle \right)\Big|_{\mathrm{Sym}(d^{t-1})} \right\|_{1\to 1} = 0.$$

■

IV. LIMITATIONS ON THE QUANTUM ONE-TIME PAD

When considering classical encryption, the one-time pad (OTP) can only be used once to encrypt a plaintext message since the exclusive-or (XOR) of the ciphertexts resulting from encrypting different plaintexts reveals information about these plaintexts. However, if the OTP is used to encrypt two (or more) identical plaintexts, their ciphertexts will also be identical and the XOR of these ciphertexts is the zero string. This reveals nothing about the original plaintext and therefore is still information-theoretically secure.

Since classical messages are a special case of quantum messages, the QOTP should also only be used once to encrypt a plaintext quantum state for the same reasons as the OTP. However, when the QOTP is used to encrypt two copies of the same quantum state, this is no longer information-theoretically secure, as illustrated in the following theorem.

Theorem 1. $\mathsf{QOTP}_{a,b} \otimes \mathsf{QOTP}_{a,b}$ with the same key a, b is a 1-correct, 2-recipient QPB scheme, but it does not have ϵ-indistinguishable ciphertexts for any $\epsilon < 1/2$.

Proof. This $\mathsf{QOTP}_{a,b} \otimes \mathsf{QOTP}_{a,b}$ can be defined as a "double quantum one-time pad" for $\varphi, \psi \in \mathcal{D}(\mathcal{H}_2)$ and $a, b \in \{0, 1\}$:

$$\mathsf{dQOTP}_{a,b}(\varphi \otimes \psi) = X^a Z^b \otimes X^a Z^b (\varphi \otimes \psi) Z^b X^a \otimes Z^b X^a.$$

Consider the following:

$$\begin{aligned} \rho_0 &= |0\rangle\langle 0| \otimes |0\rangle\langle 0|, \\ \rho_1 &= |+\rangle\langle +| \otimes |+\rangle\langle +|. \end{aligned}$$

Then the expectation of $\mathsf{dQOTP}_{a,b}$ applied to each state results in

$$\mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b}(\rho_0) = \tfrac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|),$$

$$\mathop{\mathbb{E}}_{a,b} \mathsf{dQOTP}_{a,b}(\rho_1) = \tfrac{1}{2}(|+\rangle\langle +| \otimes |+\rangle\langle +| + |-\rangle\langle -| \otimes |-\rangle\langle -|).$$

TABLE II. Bounds on the number of unitaries for quantum one-time pad for n qudits

	$\mathsf{QOTP}_{a,b}$	$\mathsf{QOTP}^{\otimes t}_{a_i,b_i}$
Qubits ($d = 2^n$)	$d^2 = 4^n$	$d^{2t} = 4^{nt}$
General d^n	d^{2n}	d^{2nt}

We have that for any state replacement channel $\langle\sigma\rangle$,

$$\begin{aligned}
&\Big\|\Big(\mathop{\mathbb{E}}_{a,b}\mathsf{dQOTP}_{a,b} - \langle\sigma\rangle\Big)\Big|_{\mathrm{Sym}(2^2)}\Big\|_{1\to1}\\
&\quad= \max_{\rho\in\mathcal{D}(\mathrm{Sym}(2^2))}\Big\|\mathop{\mathbb{E}}_{a,b}\mathsf{dQOTP}_{a,b}(\rho) - \langle\sigma\rangle(\rho)\Big\|_1\\
&\quad\geqslant \tfrac{1}{2}\Big(\Big\|\mathop{\mathbb{E}}_{a,b}\mathsf{dQOTP}_{a,b}(\rho_0) - \langle\sigma\rangle(\rho_0)\Big\|_1\\
&\qquad+\Big\|\mathop{\mathbb{E}}_{a,b}\mathsf{dQOTP}_{a,b}(\rho_1) - \langle\sigma\rangle(\rho_1)\Big\|_1\Big)\\
&\quad\geqslant \tfrac{1}{2}\Big\|\mathop{\mathbb{E}}_{a,b}\mathsf{dQOTP}_{a,b}(\rho_0) - \mathop{\mathbb{E}}_{a,b}\mathsf{dQOTP}_{a,b}(\rho_1)\Big\|_1 \geqslant \tfrac{1}{2}.
\end{aligned}$$

■

Therefore, encryption with the same key is not sufficient to obtain perfect security when encrypting multiple copies of the same message. Using independent encryption keys for each copy of the message is one possible solution to this problem, done by extending Sec. III so that the encryption map becomes $\mathsf{Enc}_k : \mathcal{H}_M \to \mathcal{H}_C$ to account for different encryption and decryption keys. However, as one can see in Table II, this leads to the amount of unitaries needed to be exponential in t, the number of copies. These bounds are from the known fact that to encrypt once an n-qubit state, 2^{2n} unitaries are needed [4], and this bound can be extended to general d with a general QOTP using generalized Pauli matrices [25]. We denote t independent uses of the quantum one-time pad as $\mathsf{QOTP}^{\otimes t}_{a_i,b_i}$, where $a_i, b_i \in \{0,1\}^n$ for $i = 1,\ldots,t$. In the d-dimensional case, $a_i, b_i \in \{0,1,\ldots,d-1\}^n$.

V. QPB WITH DESIGNS

In this section, we examine the case where unitary t-designs are used to solve the t-QPB problem. In order to maintain security against side information, we impose restrictions on the input message, specifically that it be an element of the symmetric subspace.

Theorem 2. Let $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ be an ϵ-approximate unitary t-design. Then the set of maps, $\mathsf{Enc}_k(\rho) = U_k^{\otimes t}\rho(U_k^{\otimes t})^\dagger$, and its local inverse maps $\mathsf{Dec}_k(\gamma) = U_k^\dagger\gamma U_k$ for $k \in K$, $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$, and $\gamma \in \mathcal{D}(\mathcal{H}_d)$ form a perfect t-QPB which has ϵ-indistinguishable ciphertexts. Moreover, in the case of exact unitary t-designs, we have a perfect t-QPB perfectly secure against adversaries with side information.

Proof. The fact that Enc_k and $\mathsf{Dec}_k^{\otimes t}$ are inverses of each other automatically shows correctness. Denote $T^{(t)}$ the t-twirling channel $T^{(t)}(\rho) = \int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^\dagger)^{\otimes t}dU$. For $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$, $T^{(t)}(\rho) = \tau_{\mathrm{Sym}}$, that is, $T^{(t)}|_{\mathrm{Sym}(d^t)} = \langle\tau_{\mathrm{Sym}}\rangle|_{\mathrm{Sym}(d^t)}$; thus, using the definition of approximate t-designs, we get

$$\begin{aligned}
&\Big\|\Big(\mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k - \langle\tau_{\mathrm{Sym}}\rangle\Big)\Big|_{\mathrm{Sym}(d^t)}\Big\|_{1\to1}\\
&\quad= \Big\|\Big(\mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k - T^{(t)}\Big)\Big|_{\mathrm{Sym}(d^t)}\Big\|_{1\to1}\\
&\quad\leqslant \Big\|\mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k - T^{(t)}\Big\|_{1\to1} < \epsilon.
\end{aligned}$$

Consider now the security against side information for the case of exact unitary t-designs. Suppose the plaintext to be encrypted is $|\psi\rangle \in \mathcal{H}_A \otimes \mathrm{Sym}(d^t)$, where A is the auxiliary space. This can be written as

$$\begin{aligned}
|\psi\rangle &= \sum_{i=1}^{D}\lambda_i\,|a_i\rangle\otimes|\varphi_i\rangle\,,\\
|\psi\rangle\langle\psi| &= \sum_i\sum_j\lambda_i\lambda_j^*|a_i\rangle\langle a_j|\otimes|\varphi_i\rangle\langle\varphi_j|,
\end{aligned}\tag{8}$$

using the Schmidt decomposition, where $|a_i\rangle$ and $|\varphi_i\rangle$ are orthonormal states for $\mathcal{H}_A$ and $\mathrm{Sym}(d^t)$, respectively. The λ_i values are non-negative real numbers such that $\sum_i\lambda_i^2 = 1$.

Applying $\mathcal{I}_A \otimes \mathsf{Enc}_k$ to $|\psi\rangle\langle\psi|$ and taking the expectation gives

$$\begin{aligned}
&\sum_i\sum_j\lambda_i\lambda_j^*|a_i\rangle\langle a_j|\otimes\sum_{k\in K}w(U_k)U_k^{\otimes t}|\varphi_i\rangle\langle\varphi_j|(U_k^\dagger)^{\otimes t}\\
&\quad= \sum_i\sum_j\lambda_i\lambda_j^*|a_i\rangle\langle a_j|\otimes\int_{\mathcal{U}(d)}U^{\otimes t}|\varphi_i\rangle\langle\varphi_j|(U^\dagger)^{\otimes t}dU\\
&\quad= \sum_i\sum_j\lambda_i\lambda_j^*|a_i\rangle\langle a_j|\\
&\quad\otimes\Big[\mathrm{tr}(\Pi_{\mathrm{Sym}}|\varphi_i\rangle\langle\varphi_j|\Pi_{\mathrm{Sym}})\tau_{\mathrm{Sym}} + \sum_b\mathrm{tr}(\Pi_b|\varphi_i\rangle\langle\varphi_j|\Pi_b)\tau_b\Big].
\end{aligned}$$

The second equality follows from Eq. (4), whose notation is explained in Sec. II D. This $\mathrm{tr}(\Pi_{\mathrm{Sym}}|\varphi_i\rangle\langle\varphi_j|\Pi_{\mathrm{Sym}}) = \langle\varphi_j|\Pi_{\mathrm{Sym}}\Pi_{\mathrm{Sym}}|\varphi_i\rangle$ will equal 0 when $i \neq j$ since $|\varphi_i\rangle$ and $|\varphi_j\rangle$ are orthonormal. For $\mathrm{tr}(\Pi_b|\varphi_i\rangle\langle\varphi_j|\Pi_b)$, this will always equal zero because $|\varphi_i\rangle, |\varphi_j\rangle \in \mathrm{Sym}(d^t)$, which is orthogonal to subspace b, and so Π_b applied to these states will give zero. Therefore, the only terms that remain are when $i = j$, which gives

$$\begin{aligned}
&\sum_i|\lambda_i|^2|a_i\rangle\langle a_i|\otimes\int_{\mathcal{U}(d)}U^{\otimes t}|\varphi_i\rangle\langle\varphi_i|(U^\dagger)^{\otimes t}dU\\
&\quad= \sum_i|\lambda_i|^2|a_i\rangle\langle a_i|\otimes\tau_{\mathrm{Sym}},
\end{aligned}\tag{9}$$

and this τ_{Sym} is independent of i. This implies that the encrypted plaintext will always look the same, regardless of what the adversary has as side information. This implies

$$\Big\|\Big(\mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k - \langle\tau_{\mathrm{Sym}}\rangle\Big)\Big|_{\mathrm{Sym}(d^t)}\Big\|_\diamond = 0.$$

■

Remark 1. Quantum private broadcasting with designs for t recipients cannot be used to broadcast states of the form $\nu^{\otimes t} \notin \mathcal{D}(\mathrm{Sym}(d^t))$. Consider, for example, the totally mixed state $\tau = \frac{\mathbb{I}}{2}\otimes\frac{\mathbb{I}}{2} \in \mathcal{D}(\mathcal{H}_{d^t})$ for $d = t = 2$. The averaged encryption of τ is naturally $\mathbb{E}_{k\in K}\mathsf{Enc}_k(\tau) = \tau$. On the other hand, any state $\rho_0 \in \mathcal{D}(\mathrm{Sym}(2^2))$ is mapped to $\mathbb{E}_{k\in K}\mathsf{Enc}_k(\rho_0) = \tau_{\mathrm{Sym}}$, the maximally mixed state in the symmetric subspace. Clearly, $\frac{\mathbb{I}}{4} \neq \tau_{\text{Sym}}$ because, when $d = t = 2$,

$$\begin{aligned}\tau_{\text{Sym}} &= \frac{\Pi_{\text{Sym}}}{d_{\text{Sym}}}\\ &= \frac{\Pi_{\text{Sym}}}{3} \neq \frac{\mathbb{I}}{4},\end{aligned} \tag{10}$$

and for any state replacement channel $\langle\sigma\rangle$,

$$\begin{aligned}&\Big\|\Big(\mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k - \langle\sigma\rangle\Big)\Big\|_{1\to 1}\\ &\quad= \max_{\rho\in\mathcal{D}(\mathbb{C}(2^2))}\Big\|\mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k(\rho) - \langle\sigma\rangle(\rho)\Big\|_1\\ &\quad\geqslant \tfrac{1}{2}\Big(\Big\|\mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k(\tau) - \langle\sigma\rangle(\tau)\Big\|_1\\ &\qquad+ \Big\|\mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k(\rho_0) - \langle\sigma\rangle(\rho_0)\Big\|_1\Big)\\ &\quad\geqslant \tfrac{1}{2}\Big(\Big\|\mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k(\tau) - \mathop{\mathbb{E}}_{k\in K}\mathsf{Enc}_k(\rho_0)\Big\|_1\Big)\\ &\quad\geqslant \tfrac{1}{2}\big\|\tau - \tau_{\text{Sym}}\big\|_1 \geqslant \tfrac{1}{4}.\end{aligned}$$

This does not fulfill a generalized version of security following Sec. III, and therefore supports why we restrict our input to the symmetric subspace in the definitions of security and correctness for t-QPB. Furthermore, we can insert a prebroadcasting stage into the t-QPB where we perform a projective measurement $\{\tau_{\text{Sym}}, \mathbb{I} - \tau_{\text{Sym}}\}$ to determine whether or not our state is in the symmetric subspace. The state provided by an adversary is either projected into the symmetric subspace, whose action leaves symmetric states unchanged, or it is projected into a subspace orthogonal to the symmetric subspace. In the first case, the state is symmetric and the t-QPB is secure, as explained above. In the second case, the projective measurement result indicates that the state is not symmetric and the encryption protocol is aborted, thus avoiding scenarios where the t-QPB is not secure.

We are interested in the key length required for the t-QPB, and we can compare the bounds from Table II to those in Table I. One can see that the upper bounds for unitary t-designs are better than the number of unitaries needed for $\mathsf{QOTP}_{a_i,b_i}^{\otimes t}$ when t is very large. The reason for this is because if one fixes the dimension d and allows t to increase, the order of unitaries needed for a t-design is polynomial in t, while the QOTP is exponential in t. See Fig. 2 for the comparison of the classical bit key length when $d = 2$ and $t = 1, \ldots, 20$.

VI. SYMMETRIC UNITARY *T* DESIGNS

Motivated by the fact that we are only working in the symmetric subspace, we propose the concept of symmetric unitary t-designs, which are a relaxation of t-designs. Namely, they are a discrete set of unitaries together with a probability distribution that mimics the action of the Haar measure in the symmetric subspace.

Definition 5. Let $\{U_k\}_{k\in K}$ be a finite subset of $\mathcal{U}(d)$ and let $w : \{U_k\}_{k\in K} \to \mathbb{R}$ be a positive weight function such that $w(U_k) \geqslant 0$ and $\sum_{k\in K} w(U_k) = 1$. Then, $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ is called an *ϵ-approximate symmetric unitary t-design* if

$$\big\|\big(\mathbb{E}_{\mathfrak{U}}\big[\mathcal{E}_{U_k}^{(t)}\big] - \langle\tau_{\text{Sym}}\rangle\big)\big|_{\text{Sym}(d^t)}\big\|_{1\to 1} < \epsilon, \tag{11}$$

where $\mathcal{E}_{U_k}^{(t)}(\rho) = U_k^{\otimes t}\rho(U_k^{\dagger})^{\otimes t}$.

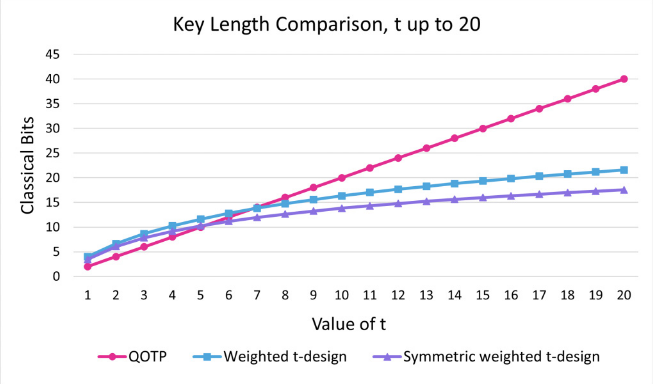

FIG. 2. QOTP, weighted t-design, and symmetric weighted t-design, $t \leqslant 20$, $d = 2$.

Note that $\langle\tau_{\text{Sym}}\rangle$ is equal to $T^{(t)}$, the t-twirling channel $T^{(t)}(\rho) = \int_{\mathcal{U}(d)} U^{\otimes t}\rho(U^{\dagger})^{\otimes t} dU$, for symmetric states $\rho \in \mathcal{D}(\text{Sym}(d^t))$ and the integral is over the whole unitary group with respect to the Haar measure.

We now connect symmetric unitary t-designs with perfect t-QPB schemes.

Corollary 1. Let $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ be an ϵ-approximate symmetric unitary t-design. Then the set of maps, $\mathsf{Enc}_k(\rho) = U_k^{\otimes t}\rho(U_k^{\otimes t})^{\dagger}$, and its local inverse maps $\mathsf{Dec}_k(\gamma) = U_k^{\dagger}\gamma U_k$ for $k \in K$, $\rho \in \mathcal{D}(\text{Sym}(d^t))$, and $\gamma \in \mathcal{D}(\mathcal{H}_d)$ form a perfect t-QPB which has ϵ-indistinguishable ciphertexts. Moreover, in the case of exact symmetric unitary t-designs, we have a perfect t-QPB perfectly secure against adversaries with side information.

Proof. Note that the only properties of approximate or exact unitary t-designs we are using in the proof of Sec. V are those fulfilled by their corresponding symmetric unitary t-designs. ∎

This shows that symmetric unitary t-designs give perfect t-QPB schemes. Moreover, every perfect t-QPB comes from a symmetric unitary t-design. Indeed, as discussed after the definition of t-QPB schemes in Sec. III, perfect t-QPB must necessarily be implemented via unitary matrices and with local identical decryption unitaries U_k. Encryption can be performed with a general unitary for each U_k, but its action over the symmetric subspace should be exactly the same as $(U_k^{\dagger})^{\otimes t}$. So, mathematically, the t-QPB comes from a symmetric unitary t-design.

Hence, Sec. III can be rephrased in terms of symmetric unitary t-designs.

Lemma 2. Let $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ be a symmetric unitary t-design; then, $\mathfrak{U}$ is a symmetric unitary $(t-1)$-design.

We now give lower and upper bounds for exact symmetric unitary t-designs.

Lemma 3. A symmetric unitary t-design has at least d_{Sym}^2 unitaries.

Proof. A symmetric t-design in $\mathcal{U}(d)$ gives a 1-design in $\mathcal{U}(\text{Sym}(d^t))$ having a particular tensor product structure, via the map $U \in \mathcal{U}(d) \mapsto V_U = U^{\otimes t}|_{\text{Sym}(d^t)} \in \mathcal{U}(\text{Sym}(d^t))$, where $U^{\otimes t}|_{\text{Sym}(d^t)} : \text{Sym}(d^t) \to \text{Sym}(d^t)$ is the restriction of $U^{\otimes t}$ to the symmetric subspace.

TABLE III. Bounds on the number of unitaries for symmetric unitary t-designs.

	Lower	Upper
Exact	d_{Sym}^2	$d_{\text{Sym}}^4 - 2d_{\text{Sym}}^2 + 3 \in O(d_{\text{Sym}}^4)$
ϵ-approximate	$(d_{\text{Sym}})^{(1-\epsilon)}$	$\alpha \frac{d_{\text{Sym}}}{\epsilon^2} \log_2(d_{\text{Sym}})^6 \log_2(1/\epsilon^2)$

Therefore, a lower bound for the number of unitaries needed in a 1-design in $\mathcal{U}(\text{Sym}(d^t))$ will also give a lower bound for those of a symmetric t-design in $\mathcal{U}(d)$. From Table I, the lower bound for a t-design in $\mathcal{U}(d)$ is $\binom{d^2+t-1}{t}$. This implies that the lower bound on the number of unitaries for a symmetric 1-design is $\binom{d_{\text{Sym}}^2+1-1}{1} = d_{\text{Sym}}^2$. ■

Lemma 4. There are symmetric unitary t-designs formed by n unitaries with $n \leqslant d_{\text{Sym}}^4 - 2d_{\text{Sym}}^2 + 3$ unitaries.

Proof. The proof follows using the results from [10] regarding the dimensions for sets of homogeneous polynomials and then applying Carathéodory's theorem.

A symmetric unitary design seen as a linear operator is an element of the convex hull of the set

$$A = \{U^{\otimes t} \otimes (\overline{U})^{\otimes t}|_{\text{Sym}(d^t)\otimes\text{Sym}(d^t)} : U \in \mathcal{U}(d)\}. \tag{12}$$

Clearly, the convex hull of A is a subset of the convex hull of $B = \{V \otimes \overline{V} : V \in \mathcal{U}(\text{Sym}(d^t))\}$, where V does not necessarily have the tensor product structure. The span of set B has the same dimension as $\text{Hom}[\mathcal{U}(\text{Sym}(d^t)), 1, 1]$, the set of homogeneous polynomials of degree 1 in the entries of V and degree 1 in the entries of $\overline{V}$ where $V \in \mathcal{U}(\text{Sym}(d^t))$, whose dimension is $d_{\text{Sym}}^4 - 2d_{\text{Sym}}^2 + 2$ (see [10]). Now applying Carathéodory's theorem, elements of the convex hull of A can be written as convex combinations of, at most, $d_{\text{Sym}}^4 - 2d_{\text{Sym}}^2 + 3$ elements in A. Therefore, there exists a weighted symmetric unitary t-design of, at most, $d_{\text{Sym}}^4 - 2d_{\text{Sym}}^2 + 3 \in O(d_{\text{Sym}}^4)$ elements. ■

This shows a gap between the lower and upper bounds, in line with the results for unitary t-designs. The bounds are summarized in Table III.

We concentrate now in giving bounds on the number of unitaries needed for approximate symmetric unitary t-designs. We adapt the randomized construction of approximate unitary t-designs from [12][2] to our case, where we are only interested in the action of the set of unitary matrices over $\text{Sym}(d^t)$, giving a construction almost linear in d_{Sym}.

Theorem 3. Let $0 < \epsilon < 1$. Let $\mathfrak{U} = (w, \{U_k\}_{k\in K})$ be a unitary t-design, and let $U_1, \ldots, U_n$ be sampled independently from $\mathfrak{U}$. Then there exists a universal constant $\alpha > 0$ such that if $n \geqslant \alpha \frac{d_{\text{Sym}}}{\epsilon^2} \log_2(d_{\text{Sym}})^6 \log_2(1/\epsilon^2)$, then, with probability at least $\frac{1}{2}$, $\forall\ \rho \in \mathcal{D}(\text{Sym}(d^t))$,

$$\left\| \frac{1}{n} \sum_{i=1}^{n} U_i^{\otimes t} \rho (U_i^\dagger)^{\otimes t} - T^{(t)}(\rho) \right\|_\infty \leqslant \frac{\epsilon}{d_{\text{Sym}}}, \tag{13}$$

where $T^{(t)}(\rho)$ is the symmetric t-twirling channel which maps $\rho \in \mathcal{D}(\text{Sym}(d^t))$ to $\int_{\mathcal{U}(d)} U^{\otimes t} \rho (U^\dagger)^{\otimes t} dU$ with respect to the Haar measure. In other words, $T^{(t)}(\rho) = \langle \tau_{\text{Sym}} \rangle(\rho) = \tau_{\text{Sym}}$ for $\rho \in \mathcal{D}(\text{Sym}(d^t))$.

Note that by relating the ∞ norm to the 1 norm, Sec. VI gives an ϵ-approximate symmetric unitary t-design and thus a perfectly correct t-QPB scheme which has ϵ-indistinguishable ciphertexts.

The proof of Sec. VI follows similarly to [12], with altered bounds due to ρ being in the symmetric subspace. To see this, we need the following result based on Lemma 5 of Ref. [6], now adjusted so that $\rho \in \mathcal{D}(\text{Sym}(d^t))$ and $U_i^{\otimes t}$ is being applied instead of simply U_i.

Lemma 5. Let $U_1, \ldots, U_n \in \mathcal{U}(d)$. For $\varepsilon_1, \ldots, \varepsilon_n$ independent Bernoulli random variables, we have

$$\begin{aligned} \mathbb{E}\left(\sup_{\rho\in\mathcal{D}(\text{Sym}(d^t))} \left\| \sum_{i=1}^{n} \varepsilon_i U_i^{\otimes t} \rho (U_i^\dagger)^{\otimes t} \right\|_\infty \right) \\ \leqslant \alpha (\log_2 d_{\text{Sym}})^{5/2} (\log_2 n)^{1/2} \\ \times \sup_{\rho\in\mathcal{D}(\text{Sym}(d^t))} \left\| \sum_{i=1}^{n} U_i^{\otimes t} \rho (U_i^\dagger)^{\otimes t} \right\|_\infty^{1/2}, \end{aligned} \tag{14}$$

where $\alpha > 0$ is a universal constant.

Proof. This proof follows from the proof in [6] since there exists an isometry that will map everything in $\text{Sym}(d^t)$ to a complex Hilbert space $\mathcal{H}_{d_{\text{Sym}}}$ of d_{Sym} dimensions. This isometry preserves scalar products and maps all nonsymmetric elements to zero. There is, therefore, an isometry between $\mathcal{D}(\text{Sym}(d^t))$ and $\mathcal{D}(\mathcal{H}_{d_{\text{Sym}}})$, and Aubrun's Lemma 5 result can be applied, where d is replaced with d_{Sym}, and U_i is now $U_i^{\otimes t}$. ■

Section VI can now be proved by directly following the proof of [12], replacing Lemma 3.2 in [12] with the known fact of $\sup_{\rho\in\mathcal{D}(\text{Sym}(d^t))} \|T^{(t)}(\rho)\|_\infty = \frac{1}{d_{\text{Sym}}}$ and substituting Sec. VI for Lemma 3.3 in [12].

From [12], their upper bound is $n \geqslant C(td)^t (t \log_2 d)^6/\epsilon^2$, while the upper bound from Sec. VI is $n \geqslant \alpha \frac{d_{\text{Sym}}}{\epsilon^2} \log_2(d_{\text{Sym}})^6 \log_2(1/\epsilon^2)$. As mentioned previously, the lower bound for symmetric unitary t-designs is d_{Sym}^2, and this upper bound for ϵ-approximate symmetric unitary t-designs is of the order of d_{Sym} along with a $\log_2 d_{\text{Sym}}$ term. The following lemma shows that this upper bound is optimal in d_{Sym} up to a sublinear term.

Lemma 6. An ϵ-approximate symmetric unitary t-design has at least $(d_{\text{Sym}})^{1-\epsilon}$ unitaries.

Proof. Similar to what is done in [12], we adapt the arguments given in [26] to our case. As proven in [26], if two quantum channels T and $\hat{T}$ on $\mathcal{L}(\mathcal{H}_d)$ are ϵ-close in the 1-norm, then the following is true:

$$\log_2 r(\hat{T}) \geqslant (1-\epsilon) \max_{\rho\in\mathcal{D}(\mathcal{H}_d)} |S(T(\rho)) - S(\rho)|, \tag{15}$$

where $r(\hat{T})$ is the Kraus rank of $\hat{T}$ and $S(\cdot)$ is the von Neumann entropy.

Moreover, if the quantum channel T has the property that $\|T(\rho)\|_\infty \leqslant \frac{c}{d}$ for $\rho \in \mathcal{D}(\mathcal{H}_d)$, then it can be said that

$$\max_{\rho\in\mathcal{D}(\mathcal{H}_d)} |S(T(\rho)) - S(\rho)| \geqslant \log_2\left(\frac{d}{c}\right), \tag{16}$$

which implies that $r(\hat{T}) \geqslant (\frac{d}{c})^{(1-\epsilon)}$.

[2] These results build on those of [6]. Note that we make explicit this $\log_2(1/\epsilon^2)$ term that is missing in the result of [6].

With respect to approximate symmetric unitary t-designs, it is known that for $\rho \in \mathcal{D}(\mathrm{Sym}(d^t))$, $\|T^{(t)}(\rho)\|_\infty = \frac{1}{d_{\mathrm{Sym}}}$. Therefore, if a quantum channel $\hat{T}^{(t)}$ is ϵ-close to $T^{(t)}$ in the 1-norm, then the rank of Kraus operators for the channel $\hat{T}^{(t)}$ satisfies

$$r(\hat{T}^{(t)}) \geqslant (d_{\mathrm{Sym}})^{(1-\epsilon)}, \tag{17}$$

which gives a lower bound for the number of unitaries for an ϵ-approximate symmetric unitary t-design. ■

VII. SUMMARY AND OPEN PROBLEMS

In this article, we have formally defined the t-recipient quantum private broadcasting (t-QPB) problem in the information-theoretic setting, and have shown three methods to achieve it. Along the way, we have defined a notion of designs, applicable to the scenario where the input is in the symmetric subspace, that may be of independent interest; we have called these symmetric unitary t-designs.

The first straightforward solution to the t-QPB problem is the encryption of each copy of the plaintext with the quantum one-time pad, using independent keys. This requires a key of length linear in t, the number of recipients, and is secure even if the adversary holds quantum side information about the plaintext. We observe, however, that this solution does not make use of the full structure of the problem, namely, that each recipient receives the same plaintext.

In order to consider the structure of the problem, we consider unitary t-designs as t-QPB schemes. Since the key length required for unitary t-designs is logarithmic in t, this offers an exponential improvement in key length compared to the first solution. Moreover, we show that unitary t-designs are secure against quantum side information, as long as the state to be encrypted is in the symmetric subspace. Note that this is not a restriction as one can ensure that the input state is always in the symmetric subspace by implementing a prebroadcasting stage. This projects the state into the symmetric subspace, aborting the encryption protocol if the resulting state is not symmetric.

Our final solution takes full advantage of the structure of the t-QPB problem, and we define symmetric unitary t-designs as a relaxation of unitary t-designs that mimic the action of the Haar measure on the symmetric subspace. We show that up to some reasonable assumptions, these are necessary and sufficient as t-QPB schemes, and that they yield a key length logarithmic in d_{Sym} (the dimension of the symmetric subspace); this is still logarithmic in t, but with a smaller constant than the key length of encryption schemes derived from unitary t-designs. We also provide lower and upper bounds for both exact and approximate symmetric unitary t-designs with respect to d_{Sym}. This lower bound of d_{Sym}^2 for exact symmetric unitary t-designs corresponds to the number of unitaries needed to perform the quantum one-time pad in the symmetric subspace, which is the t-QPB problem without the local decryption requirement.

We use the bounds for the size of weighted unitary t-designs as proven in [10] to compare the key length of a design as opposed to t uses of the quantum one-time pad (QOTP). We compare the results for the qubit case in Fig. 2, which shows that when $t > 5$, symmetric designs are a better choice than the QOTP, while it takes until $t > 6$ for regular designs to be better than the QOTP. (The data for Fig. 2 are given in the Appendix.)

We leave as an open problem further applications of symmetric unitary t-designs, and it would be interesting to see if t-designs can be relaxed in similar ways with other subspaces or depending on the application. Relaxing the correctness of the t-QPB problem to further improve the key length is left to further research. It is left open whether the techniques used to reduce the circuit depth needed for approximate unitary t-designs [27–29] can be applied to approximate symmetric unitary t-designs. We also note that we attain security against side information with t-designs by restricting our input of the broadcasting protocol to be in the symmetric subspace, and we leave as an open problem whether there is another solution to t-QPB that has the same security and similar key length but with fewer restrictions.

ACKNOWLEDGMENTS

The authors thank Cécilia Lancien for helpful discussions. A.B. acknowledges support by the Air Force Office of Scientific Research under Award No. FA9550-20-1-0375, Canada's NFRF, Canada's NSERC, an Ontario ERA, and the University of Ottawa's Research Chairs program. C.E.G.-G. acknowledges financial support from Spanish MICINN (Projects No. MTM2017-88385-P and No. PID2020-113523GB-I00) and from Comunidad de Madrid (Grant No. QUITEMAD-CM, Ref. S2018/TCS-4342). C.S. acknowledges financial support from the Government of Ontario and from the University of Ottawa.

APPENDIX: DATA FOR Fig. 2

Please refer to Table IV, which presents the data for Fig. 2.

TABLE IV. Classical bits for QOTP and upper bounds of classical bits for weighted t-design and symmetric weighted t-design when $d = 2$.

t	QOTP	Wted t-design	Sym wted t-design
1	2	4	3.46
2	4	6.64	6.04
3	6	8.64	7.83
4	8	10.26	9.17
5	10	11.61	10.26
6	12	12.78	11.17
7	14	13.81	11.96
8	16	14.73	12.64
9	18	15.56	13.26
10	20	16.32	13.81
11	22	17.02	14.32
12	24	17.66	14.78
13	26	18.26	15.21
14	28	18.82	15.61
15	30	19.34	15.99
16	32	19.84	16.34
17	34	20.31	16.67
18	36	20.75	16.98
19	38	21.18	17.28
20	40	21.58	17.56

[1] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).

[2] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[3] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 2000), pp. 547–553.

[4] P. O. Boykin and V. Roychowdhury, Phys. Rev. A **67**, 042317 (2003).

[5] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).

[6] G. Aubrun, Commun. Math. Phys. **288**, 1103 (2009).

[7] J. Bouda and V. Bužek, J. Mod. Opt. **50**, 1071 (2003).

[8] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A **80**, 012304 (2009).

[9] D. Gross, K. Audenaert, and J. Eisert, J. Math. Phys. **48**, 052104 (2007).

[10] A. Roy and A. J. Scott, Des. Codes Cryptogr. **53**, 13 (2009).

[11] R. Cleve, D. Leung, L. Liu, and C. Wang, Quantum Inf. Comput. **16**, 721 (2016).

[12] C. Lancien and C. Majenz, Quantum **4**, 313 (2020).

[13] G. Alagic, C. Majenz, and A. Russell, in *Advances in Cryptology – EUROCRYPT 2020*, Lecture Notes in Computer Science, Vol. 12107, edited by A. Canteaut and Y. Ishai (Springer, Cham, 2020), pp. 759–787.

[14] E. Bannai, Y. Nakata, T. Okuda, and D. Zhao, arXiv:2009.11170.

[15] A. Ambainis, J. Bouda, and A. Winter, J. Math. Phys. **50**, 042106 (2009).

[16] G. Alagic and C. Majenz, in *Advances in Cryptology – CRYPTO 2017*, Lecture Notes in Computer Science, Vol. 10402, edited by J. Katz and H. Shacham (Springer, Cham, 2017), pp. 310–341.

[17] J. Bouda, M. Sedlák, and M. Ziman, arXiv:2009.06067.

[18] Y. Nakata, D. Zhao, T. Okuda, E. Bannai, Y. Suzuki, S. Tamiya, K. Heya, Z. Yan, K. Zuo, S. Tamate, Y. Tabuchi, and Y. Nakamura, PRX Quantum **2**, 030339 (2021).

[19] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, Commun. Math. Phys. **346**, 397 (2016).

[20] H. Qi, K. Sharma, and M. M. Wilde, J. Phys. A: Math. Theor. **51**, 374001 (2018).

[21] J. Watrous, The Theory of Quantum Information, Lecture Notes (2011), available at https://cs.uwaterloo.ca/∼watrous/TQI-notes/ (unpublished).

[22] G. Benenti and G. Strini, J. Phys. B: At., Mol. Opt. Phys. **43**, 215508 (2010).

[23] A. W. Harrow, arXiv:1308.6595.

[24] W. Fulton and J. Harris, *Representation Theory: A First Course*, Graduate Texts in Mathematics (Springer, New York, 1991).

[25] Z. Webb, Quantum Inf. Comput. **16**, 1379 (2016).

[26] C. Lancien and A. Winter, arXiv:1711.00697.

[27] A. Harrow and S. Mehraban, arXiv:1809.06957.

[28] R. Mezher, J. Ghalbouni, J. Dgheim, and D. Markham, arXiv:1905.01504.

[29] J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, and I. Roth, arXiv:2002.09524.