

Honest-binding quantum bit commitment from separable operations

Ziad Chaoui  and Anna Pappa *

Electrical Engineering and Computer Science Department, *Technical University of Berlin*, Einsteinufer 17, 10587 Berlin, Germany

Matteo Rosati 

Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche, *Università degli Studi Roma Tre*,
Via Vito Volterra 62, 00146 Rome, Italy



(Received 22 December 2025; accepted 5 May 2026; published 1 June 2026)

Bit commitment is a fundamental cryptographic primitive and a cornerstone for numerous two-party cryptographic protocols, including zero-knowledge proofs. However, it has been proven that unconditionally secure bit commitment, both classical and quantum, is impossible. In this work, we demonstrate that imposing a restriction on the committing party to perform only separable operations enables secure quantum bit-commitment schemes. Specifically, we prove that in any perfectly hiding bit-commitment protocol, an honestly committing party limited to separable operations will be detected with high probability if they attempt to alter their commitment. To illustrate our findings, we present an example protocol.

DOI: [10.1103/58t8-dj5y](https://doi.org/10.1103/58t8-dj5y)

I. INTRODUCTION

Bit commitment is a cryptographic primitive between two mistrustful parties that allows the committer (Alice) to commit to a bit and reveal it to another party (Bob) at a later stage. More specifically, a bit-commitment protocol consists of two phases. In the commit phase, Alice secretly chooses a bit $b \in \{0, 1\}$ and sends Bob proof of her commitment without revealing the bit. In the opening phase, Alice announces her bit, and Bob verifies that it is indeed the bit she had committed to. Informally, it is required that a bit-commitment protocol is *binding* (i.e., Alice cannot change her bit after the commit phase) and, at the same time, *hiding* (i.e., Bob does not learn the bit before the opening phase).

Quantum bit commitment is a fundamental primitive in quantum cryptography. Indeed, it can be used to build quantum oblivious transfer [1] and, consequently, any two-party computation. However, Mayers [2] and, independently, Lo and Chau [3] proved that unconditionally secure quantum bit commitment is not possible, thus bringing into question the conditions under which it can actually be realized. A lot of research has therefore been focused on restricting the power of the adversaries involved in the quantum bit-commitment protocol. The most common examples include putting bounds on their quantum memory, both in size [4] and in quality [5], and considering (relativistic) constraints on the location of the parties [6]. Relatively unexplored are models in which restric-

tions are placed on the operations accessible to the parties, motivated by realistic hardware limitations. One such model was proposed in [7], in which the adversary, i.e., a dishonest Alice, has access to a large quantum memory but cannot act upon its entirety in a coherent fashion. More precisely, Alice has n qubits but can act on only up to $k \leq n$ of them at a time. These operations can be modeled as local operations and classical communication (LOCC) channels. LOCC channels are indeed a natural way to model realistic hardware assumptions; they precisely allow us to represent that in practice, quantum devices rarely allow large, joint coherent operations across many qubits, as is the case, for example, in modular (see Fig. 1) and distributed quantum computing setups [8,9]. However, the security proof of the proposed protocol in [7] was erroneous [10], and therefore, the question of whether secure bit-commitment protocols exist in such models remained.

In this work, we present a set of conditions that, if fulfilled after the commit phase, allows for secure quantum bit commitment under the restriction that the committing party (Alice) can perform only separable operations on her quantum registers. This restriction includes the restriction proposed in [7] since LOCC channels are a subset of the more general separable channels [11]. Further, we propose a protocol in which said conditions are satisfied and show that Alice's attempts to switch commitment after the commit phase will be detected with high probability.

We first define what it means for a bit-commitment scheme to be secure. We then study the properties of the shared states following Alice's commitment, focusing on scenarios where her reduced state is either a product state or an absolutely maximally entangled state, depending on whether she committed to 0 or 1, respectively. In these settings, we prove that restricting her actions to separable operations leads to security. Finally, we present a bit-commitment protocol in

*Contact author: ziad.chaoui@tu-berlin.de

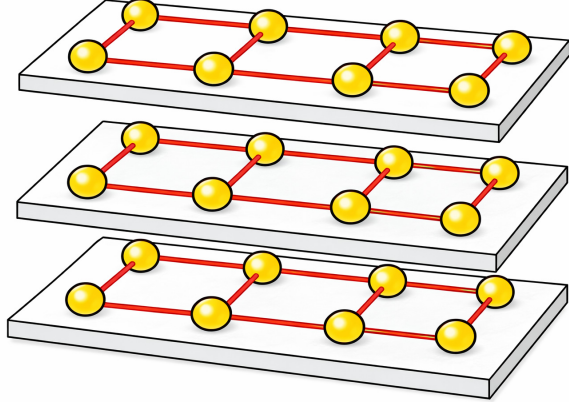


FIG. 1. Schematic representation of a modular quantum processor. The system is composed of multiple quantum chips arranged in a stack, where coherent measurement operations are restricted to individual chips rather than across the full device.

which Alice has a three-qudit register and can operate on only two of these qudits. We prove that she is not able to change her commitment except with probability $\frac{1}{d}$, where d is the dimension of the qudits used to communicate.

II. SECURITY DEFINITIONS

As previously mentioned, a bit-commitment protocol is desired to be, at the same time, hiding and binding. The definition of the first property is quite straightforward.

Definition 1: μ -hiding. A quantum bit-commitment protocol is μ -hiding, with $\mu \geq 0$, if Bob can guess the committed bit before the opening phase only with probability $\frac{1}{2} + \mu$. It is said to be *perfectly hiding* if $\mu = 0$, i.e., Bob can hazard only a random guess.

On the other hand, there are different ways to define what it means for a protocol to be binding. There is a composable definition given in [12], while the most common definition was first presented in [13]. In the latter, the authors define a bit-commitment protocol as binding if Alice cannot significantly increase the total probability of successfully opening both 0 and 1 after the commit phase. In [12] this property is referred to as *weak-binding*, and the authors of [14,15] call this property *sum-binding*, while also defining the notion of *honest-binding*. Informally, a protocol is honest-binding if Alice cannot successfully open the bit $1 - b$ after she honestly committed to the bit b . We formally define sum-binding and honest-binding as follows.

Definition 2: δ -sum-binding. A bit-commitment protocol is δ -sum-binding if, for any strategy that Alice follows, the probabilities p_b of successfully opening the bit $b \in \{0, 1\}$ satisfy

$$p_0 + p_1 \leq 1 + \delta.$$

Definition 3: ε -honest-binding. In a bit-commitment protocol, for $b \in \{0, 1\}$, let p_b be the probability that Alice successfully opens bit $1 - b$ after having honestly committed bit b . We say the protocol is ε -honest-binding if

$$\max\{p_0, p_1\} \leq \varepsilon.$$

Although sum-binding implies honest-binding, it is still interesting to study the latter because it is precisely the honest-binding property that fails in the unconditional setting, leading to the no-go result [2,3]. Gaining a better understanding of how to evade this no-go result could help design protocols that are conditionally binding and hiding. In the following, we show that restricting Alice to separable operations can guarantee honest-binding, without comprising perfect hiding. We first take a closer look at the properties of Alice and Bob's shared state after Alice committed honestly.

III. BINDING FROM SEPARABLE OPERATIONS

A. Postcommitment states

Let $\mathcal{A}$ be Alice's Hilbert space and $\mathcal{B}$ be Bob's Hilbert space, associated with an n -qudit and an m -qudit quantum register, respectively. We set $N := \dim(\mathcal{A}) = d^n$ and $M := \dim(\mathcal{B}) = d^m$, where $d \geq 2$ is the dimension of the qudits. After the commit phase, Alice and Bob share one of two quantum states $\Psi_0, \Psi_1 \in \mathcal{A} \otimes \mathcal{B}$, depending on Alice's commitment to 0 or 1, respectively. We assume the states are pure [16], and we write $\Psi_b = |\Psi_b\rangle\langle\Psi_b|$ for $b \in \{0, 1\}$. For the protocol to be hiding, the reduced states on Bob's side have to be indistinguishable [17]. This means that

$$\text{Tr}_{\mathcal{A}}(|\Psi_0\rangle\langle\Psi_0|) = \text{Tr}_{\mathcal{A}}(|\Psi_1\rangle\langle\Psi_1|). \quad (1)$$

We study the situation where Alice and Bob share the postcommitment state Ψ_b and Alice wants to open $1 - b$, meaning she wants to convince Bob that they are sharing the state Ψ_{1-b} . We denote with p_b the probability of her successfully doing so, i.e., Bob accepting her opening. To this end, Alice performs an operation on her space $\mathcal{A}$, described by $\mathcal{N} \in C(\mathcal{A})$, where $C(\mathcal{A})$ is the set of completely positive trace-preserving maps, i.e., quantum channels, from the space of linear operators on $\mathcal{A}$ to itself. Her goal is to maximize p_b , the probability that Bob identifies the shared state as Ψ_{1-b} after she applied her channel to the committed state Ψ_b ; this is expressed by the fidelity between the two states [18]:

$$p_b = \max_{\mathcal{N} \in C(\mathcal{A})} F(|\Psi_{1-b}\rangle\langle\Psi_{1-b}|, (\mathcal{N} \otimes \mathbb{1}_{\mathcal{B}})(|\Psi_b\rangle\langle\Psi_b|)).$$

We fix a channel $\mathcal{N}$ and denote by $\{K_j\}$ its set of Kraus operators, i.e., $\mathcal{N}(X) = \sum_j K_j X K_j^\dagger$. Since Ψ_{1-b} is pure, it follows that

$$\begin{aligned} & F(|\Psi_{1-b}\rangle\langle\Psi_{1-b}|, (\mathcal{N} \otimes \mathbb{1}_{\mathcal{B}})(|\Psi_b\rangle\langle\Psi_b|)) \\ &= \sum_j |\langle\Psi_{1-b}|(K_j \otimes \mathbb{1}_{\mathcal{B}})|\Psi_b\rangle|^2. \end{aligned} \quad (2)$$

We now take a closer look at states Ψ_0 and Ψ_1 . From (1), it follows that orthonormal sets $\{|x_i\rangle\}_{i=0}^{N-1}$, $\{|y_i\rangle\}_{i=0}^{M-1} \subset \mathcal{A}$, and $\{|b_i\rangle\}_{i=0}^{M-1} \subset \mathcal{B}$, as well as $\lambda_i \geq 0$, exist, so we can write the Schmidt decompositions [19] of $|\Psi_0\rangle$ and $|\Psi_1\rangle$ as

$$|\Psi_0\rangle = \sum_{i=0}^{M-1} \sqrt{\lambda_i} |x_i\rangle |b_i\rangle, \quad (3)$$

$$|\Psi_1\rangle = \sum_{i=0}^{M-1} \sqrt{\lambda_i} |y_i\rangle |b_i\rangle. \quad (4)$$

We can now compute (see Appendix A for details)

$$p_0 = \sum_j \left| \sum_i \lambda_i \langle y_i | K_j | x_i \rangle \right|^2, \quad (5)$$

$$p_1 = \sum_j \left| \sum_i \lambda_i \langle x_i | K_j | y_i \rangle \right|^2. \quad (6)$$

By the unitary equivalence of purifications, a unitary operator U exists such that $U|x_i\rangle = |y_i\rangle$ for every i . Therefore, if Alice's operations are unrestricted, she can choose the unitary channel with the single Kraus operator U and perfectly cheat without being detected; this is exactly the famous no-go result [2,3]. We can, however, avert this by restricting Alice to performing only separable channels, as we show in the next section.

B. Binding from separable operations

A separable channel is defined with respect to a bipartition of Alice's space. A separable channel $\mathcal{N} \in C(\mathcal{A})$ with respect to the bipartition $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ is a convex combination of product maps $\mathcal{N}_{\mathcal{A}_1} \otimes \mathcal{N}_{\mathcal{A}_2}$, where $\mathcal{N}_{\mathcal{A}_i}$ are completely positive maps on $\mathcal{A}_i$ and the convex combination is also trace preserving. Let $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ be such a bipartition, and denote $N_1 := \dim(\mathcal{A}_1)$ and $N_2 := \dim(\mathcal{A}_2)$ (without loss of generality, we assume that $N_2 \leq N_1$). $S(\mathcal{A}_1, \mathcal{A}_2)$ is the set of separable channels with respect to this bipartition. An important feature of separable channels is that their Kraus operators are also separable with respect to the same partition. For a separable channel $\mathcal{N} \in S(\mathcal{A}_1, \mathcal{A}_2)$ we can write its Kraus operators as $K_j = K_{j1} \otimes K_{j2}$.

In line with the notation chosen for the Schmidt decomposition (3) and (4), we investigate the situation where $|x_i\rangle$ are maximally entangled orthonormal states and $|y_i\rangle$ are orthonormal product states (so that Alice's reduced state is separable). This means that unit vectors $|v_i\rangle \in \mathcal{A}_1$ and $|w_i\rangle \in \mathcal{A}_2$ exist such that

$$|y_i\rangle = |v_i\rangle |w_i\rangle. \quad (7)$$

We can write $K_j |y_i\rangle = (K_{j1} \otimes K_{j2}) (|v_i\rangle |w_i\rangle) = |v_{ji}\rangle |w_{ji}\rangle$, where $|v_{ji}\rangle \in \mathcal{A}_1$ and $|w_{ji}\rangle \in \mathcal{A}_2$ are of norm less than 1.

In contrast, $|x_i\rangle$ are maximally entangled with respect to the bipartition $\mathcal{A}_1 \otimes \mathcal{A}_2$. This implies that, for every i , bases $\{|e_{ik}\rangle\}_{k=0}^{N_1-1} \subset \mathcal{A}_1$ and $\{|f_{ik}\rangle\}_{k=0}^{N_2-1} \subset \mathcal{A}_2$ exist such that

$$|x_i\rangle = \frac{1}{\sqrt{N_2}} \sum_{k=0}^{N_2-1} |e_{ik}\rangle |f_{ik}\rangle. \quad (8)$$

With this we find the following upper bounds for p_0 and p_1 (see Appendix A for detailed calculations):

$$p_0 \leq \lambda_{\max}^2 N_2, \quad (9)$$

$$p_1 \leq \frac{1}{N_2}, \quad (10)$$

which depend on the maximum eigenvalue of Ψ_0 and on N_2 , the dimension of the *smaller* of the two bipartitions of Alice's space.

If Bob can now choose $M = N_2$ and $\lambda_i = \frac{1}{N_2}$ for every i , then the states in (3) and (4) are both uniform superpositions.

It follows from (9) and (10) that Alice's cheating probability is bounded by $\frac{1}{N_2}$. We stress that this can be achieved under the motivated assumption that it is Bob who creates the states and therefore fixes M and $\lambda_{\max}$; indeed, if we allowed Alice to create an entangled state while being restricted to separable operations, that would be conceptually a contradiction regarding her capabilities. Furthermore, we note that Bob could also choose $M > N_2$ and reduce p_0 even more, but that would not affect Alice's overall cheating probability.

On the other hand, Alice can freely choose the particular bipartition $\mathcal{A}_1 \otimes \mathcal{A}_2$ on which to act with separable operations, whereas (7) and (8) guarantee only that $|x_i\rangle$ is maximally entangled and $|y_i\rangle$ is separable with respect to this particular bipartition of $\mathcal{A}$. To ensure the binding property, we then need to consider states that fit structures (7) and (8) with respect to *any* bipartition of $\mathcal{A}$. We want the $|y_i\rangle$'s to be separable with respect to any bipartition of $\mathcal{A}$ and will therefore consider the product states $|y_i\rangle = |a_{i1}\rangle \otimes \cdots \otimes |a_{in}\rangle$, where, for every j , $|a_{ij}\rangle$ is a unit vector in the d -dimensional Hilbert space $\mathcal{H}_d$. As for the $|x_i\rangle$'s, the states that are maximally entangled with respect to any bipartition of $\mathcal{A}$ are precisely the absolutely maximally entangled (AME) states.

Definition 4: *Absolutely maximally entangled states* [20]. An AME(n, d) state of n qudits of dimension d is a pure state $|\gamma\rangle \in (\mathcal{H}_d)^{\otimes n} = \mathcal{A}$ such that for any bipartition of the system $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, with $N_2 = \dim(\mathcal{A}_2) \leq \dim(\mathcal{A}_1) = N_1$, $|\gamma\rangle$ is maximally entangled, i.e., $\text{Tr}_{\mathcal{A}_1}(|\gamma\rangle\langle\gamma|) = \frac{1}{N_2} \mathbb{1}_{N_2}$.

We are now equipped to prove the following theorem.

Theorem 1. We consider a bit-commitment scheme between Alice and Bob, who hold an n -qudit register $\mathcal{A}$ and an m -qudit register $\mathcal{B}$, respectively, with d being the qudit dimension. If after the commit phase Alice and Bob share either the state Ψ_0 or Ψ_1 of the form (3) or (4), respectively, then the bit-commitment protocol is $\frac{1}{d}$ -binding under the following two conditions.

(1) Alice can perform only separable channels on $\mathcal{A}$.

(2) In line with notation in (3) and (4) for every $i \in \{0, \dots, N-1\}$ it holds that $|x_i\rangle \in \text{AME}(n, d)$ and $|y_i\rangle$ is a separable state with respect to any bipartition of $\mathcal{A}$.

Proof. The two conditions given in Theorem 1 imply that the analysis presented so far holds for *any* bipartition of Alice's space $\mathcal{A}$. As discussed above, Bob creates the states and therefore can freely choose $\lambda_{\max}$ and M in the Schmidt decompositions (3) and (4). From (9) and (10) it then follows that Alice's maximal cheating probability is

$$\max_{N_2} \min_{\lambda_{\max}} \max \left\{ \frac{1}{N_2}, \lambda_{\max}^2 N_2 \right\}.$$

Alice can maximize $\frac{1}{N_2}$ by choosing the smallest possible N_2 which corresponds to her acting on a single qudit, obtaining $\max_{N_2} \frac{1}{N_2} = \frac{1}{d}$. If she wants to maximize $\lambda_{\max}^2 N_2$, she can pick N_2 to be as large as possible, i.e., $\lfloor \frac{N}{2} \rfloor$ (because $\mathcal{A}_2$ is the smaller partition), but since Bob has control over $\lambda_{\max}$, he can choose it to be $\lfloor \frac{N}{2} \rfloor^{-1}$. Alice acting on a partition of dimension $\lfloor \frac{N}{2} \rfloor$ corresponds to her operating on $\lfloor \frac{n}{2} \rfloor$ of her qudits, and we can conclude that her maximum cheating probability is then

$$p_{\text{switch}} = \max \left\{ \frac{1}{d}, \frac{1}{d^{\lfloor \frac{n}{2} \rfloor}} \right\} = \frac{1}{d}.$$

■

Therefore, we are left with the challenge of designing a quantum bit-commitment protocol where, after commitment, Alice's reduced state is either a product state or an AME state depending on her commitment. If there is a protocol where Alice's reduced state satisfies this condition regardless of her strategy up to the end of the commit phase, then our analysis proves that the protocol is sum-binding. If the protocol leads to the desired situation only if Alice is honest up to the commitment, then our analysis proves that the protocol is honest-binding. Crucially, in either case the protocol is perfectly hiding since the postcommitment states satisfy (3) and (4). In the following we present an example of an honest-binding protocol for any d using $\text{AME}(3, d)$ states, where Alice has a three-qudit register and is restricted to perform coherent operations on up to two of them.

IV. $\text{AME}(3, d)$ QUANTUM BIT COMMITMENT

We consider the following setup: Alice has a three-qudit register $\mathcal{A}$, Bob has a single-qudit register $\mathcal{B}$, and we also consider ancilla registers $\mathbf{a}$. The Fourier gate for qudits is $F = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kl} |k\rangle\langle l|$, where $\omega := e^{\frac{2\pi i}{d}}$ is the primitive d th root of unity; the gate transforms the generalized Z eigenbasis $\mathbf{B}_1 = \{|k\rangle\}_{k=0}^{d-1}$ to the generalized X eigenbasis $\mathbf{B}_0 = \{|\tilde{k}\rangle\}_{k=0}^{d-1}$, with $|\tilde{k}\rangle = F^\dagger |k\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{-kl} |l\rangle$ [19]. We can now state the protocol and prove its security.

Theorem 2. The bit-commitment protocol (Protocol 1) is perfectly hiding and $1/d$ -honest-binding if Alice is restricted to perform only separable operations.

In the following we outline the main steps of the proof of Theorem 2. We refer the reader to Appendix B for details.

We first show that the commitment does not reveal any information and is always accepted when both parties are being honest. If Alice commits to 1, the postmeasurement state given the permutation π and the measurement outcome m is

$$|\Xi_{\pi, m}^1\rangle = |\Phi_{\pi(m)}\rangle.$$

Similarly, if Alice commits to 0, the postmeasurement state is

$$|\Xi_{\pi, m}^0\rangle = \left(\frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\pi(m)l} |\Phi_l\rangle \right).$$

We assume that Alice decides randomly to commit to 0 or 1; this means that given her measurement outcome m , the shared state of Alice and Bob is equally likely to be $|\Xi_{\pi, m}^0\rangle$ or $|\Xi_{\pi, m}^1\rangle$. We need to guarantee that these states are indistinguishable to Bob. Indeed, it holds that

$$\text{Tr}_{\mathcal{A}}(|\Xi_{\pi, m}^0\rangle\langle\Xi_{\pi, m}^0|) = \text{Tr}_{\mathcal{A}}(|\Xi_{\pi, m}^1\rangle\langle\Xi_{\pi, m}^1|) = \frac{\mathbb{1}}{d},$$

where $\mathbb{1}$ is the identity matrix. Furthermore, since, for a given $\pi \in S_d$ and $b \in \{0, 1\}$, $\{|\Xi_{\pi, j}^b\rangle\}_{j=0}^{d-1}$ forms a basis, when Alice announces her parameters m , π , and b in step 5, Bob can measure in that basis and finally accept Alice's opening if the outcome is indeed m .

We prove Theorem 2 by separately showing that the protocol is $\frac{1}{d}$ -honest-binding and perfectly hiding. For the former we show that it fulfills the conditions of Theorem 1 if Alice acts honestly in the commit phase; as for the hiding, we show

PROTOCOL 1. $\text{AME}(3, d)$ quantum bit commitment.

1: Bob creates the state

$$|\Xi\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |l\rangle_{\mathbf{a}} |\Phi_l\rangle_{\mathcal{AB}}, \quad (11)$$

where

$$|\Phi_l\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{jl} |jj\rangle_{\mathcal{A}} |j+l\rangle_{\mathcal{B}}. \quad (12)$$

Commit Phase

2: Bob sends Alice the registers $\mathbf{a}$ and $\mathcal{A}$.

3: Alice picks a permutation $\pi \in S_d$ and chooses $b \in \{0, 1\}$ she wants to commit.

1. To commit $b = 0$ Alice measures $\mathbf{a}$ in the basis

$$\mathbf{B}_{0, \pi} = \{|\pi(\tilde{k})\rangle\}_{k=0}^{d-1}.$$

2. To commit $b = 1$ Alice measures $\mathbf{a}$ in the basis

$$\mathbf{B}_{1, \pi} = \{|\pi(k)\rangle\}_{k=0}^{d-1}.$$

4: Alice obtains outcome $|\pi(m)\rangle$ or $|\pi(\tilde{m})\rangle$ and announces $m \in \{0, \dots, d-1\}$. The shared state dependent on b , π , and m is $|\Xi_{\pi, m}^b\rangle$.

Opening Phase

5: Alice announces b and π and sends Bob the register $\mathcal{A}$.

6: Bob projects the full state onto the expected state

$$|\Xi_{\pi, m}^b\rangle\langle\Xi_{\pi, m}^b|_{\mathcal{AB}} \text{ to verify that Alice's announcement was truthful.}$$

that even if Bob sends an arbitrary state of his choice, he cannot infer any information on the bit Alice committed after the commit phase.

Lemma 1. If Alice acts honestly in the commit phase, then Alice and Bob share a state $|\Xi_{\pi, m}^b\rangle$ that satisfies condition 2 of Theorem 1, making the protocol $\frac{1}{d}$ -honest-binding.

Proof. We show that after honest commitment, Alice's reduced state is an AME state if she committed 0 and a separable state if she committed 1. Indeed, if Alice selects the permutation π and commits to 1, the postmeasurement state given outcome m is

$$|\Xi_{\pi, m}^1\rangle = |\Phi_{\pi(m)}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |y_j^{m, \pi}\rangle |j\rangle,$$

where $|y_j^{m, \pi}\rangle$ are product qudit states and $\{|y_j^{m, \pi}\rangle\}_{j=0}^{d-1}$ is an orthonormal set. On the other hand, if Alice commits to 0, the postmeasurement state given outcome m is

$$|\Xi_{\pi, m}^0\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\pi(m)l} |\Phi_l\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |x_j^{m, \pi}\rangle |j\rangle,$$

where $|x_j^{m, \pi}\rangle$ is an $\text{AME}(3, d)$ state for every j and $\{|x_j^{m, \pi}\rangle\}_{j=0}^{d-1}$ is an orthonormal set. We refer the reader to Appendix B for more detailed explanations.

It therefore follows from Theorem 1 that $p_b \leq \frac{1}{d}$ for $b \in \{0, 1\}$. This means that Alice can successfully reveal a bit different from the one she committed to with probability $\frac{1}{d}$. ■

We emphasize that if Alice had not been restricted to separable operations, then her cheating probability would have been 1, whereas for qutrits our cheating probability is already smaller than or equal to $\frac{1}{3}$. Next, we prove that the protocol is perfectly hiding.

Lemma 2. For any state that Bob creates and sends in the AME(3, d) quantum bit-commitment protocol, he does not get any information on the bit Alice commits.

Proof. Bob can try to cheat in step 1 of the protocol by sending a different state that could potentially improve his probability of guessing the committed bit before the opening phase. Alice's measurements can be modeled as quantum channels, and thus, Bob's cheating probability is the probability of successfully distinguishing between Alice's two choices.

Alice's commitment b is implemented in terms of a measurement channel on the register a ; she chooses a permutation $\pi \in S_d$ at random and then measures in the $\mathbf{B}_{0,\pi}$ or $\mathbf{B}_{1,\pi}$ basis. For a given π , we can write the measurement channels as follows:

$$\mathcal{M}_0^\pi(\rho) = \sum_{m=0}^{d-1} (|m\rangle\langle\pi(m)| \otimes \mathbb{1}_{AB}) \rho (|\pi(m)\rangle\langle m| \otimes \mathbb{1}_{AB}),$$

$$\mathcal{M}_1^\pi(\rho) = \sum_{m=0}^{d-1} (|m\rangle\langle\pi(m)| \otimes \mathbb{1}_{AB}) \rho (|\pi(m)\rangle\langle m| \otimes \mathbb{1}_{AB}).$$

Since π is chosen at random, Alice's measurement channels corresponding to 0 and 1 commitments are

$$\mathcal{M}_0(\rho) = \frac{1}{d!} \sum_{\pi \in S_d} \mathcal{M}_0^\pi(\rho),$$

$$\mathcal{M}_1(\rho) = \frac{1}{d!} \sum_{\pi \in S_d} \mathcal{M}_1^\pi(\rho).$$

For any ρ , we then have (see Appendix B for details)

$$\mathcal{M}_0(\rho) = \mathcal{M}_1(\rho).$$

Therefore, the postmeasurement state reveals no information on Alice's choice to Bob, no matter which state he sends Alice. The protocol is therefore perfectly hiding. ■

V. CONCLUSION

While unconditionally secure quantum bit commitment cannot exist, in this work we presented conditions under which one could design a protocol that is binding if the committing party is restricted to separable operations. Specifically, we proved that if the shared postcommitment state is either an absolutely maximally entangled state or a product state after tracing out the receiver's system, then the probability of the committer successfully cheating can be bounded by $\frac{1}{d}$, where d is the dimension of the qudits in the communicated state. We further strengthened our result by presenting an example protocol that is perfectly hiding and that saturates the $\frac{1}{d}$ bound if the committer is honest during the first phase of the protocol. The proposed AME(3, d) bit-commitment protocol provides a foundational example of how honest-binding bit commitment can be designed within this restricted operational framework, leveraging the properties of AME states to ensure

security. However, in our proposed protocol, Alice can easily defer her commitment, making the protocol honest-binding but not sum-binding.

Our results present an approach to circumventing the no-go theorem for unconditionally secure bit commitment in the quantum setting, emphasizing the role of operational restrictions on the committing party. Theorem 1 offers a set of conditions that, if fulfilled by a protocol, will lead to $\frac{1}{d}$ -sum-binding and perfectly hiding quantum bit commitment. While we have established security under the honest-binding criterion, developing protocols where the restriction to separable operations can also guarantee sum-binding security remains an important challenge which has strong implications for the implementation of secure bit-commitment schemes.

Furthermore, the security of the proposed protocol scales with the dimension of the communicated qudits, rather than with the number of qubits used, as is often the case for other cryptographic protocols in particular [7]. The binding condition presented in the latter requires a large number of qubits (roughly calculated at 7800) with a restriction of acting on a maximum of one qubit at a time to be close to our bound offered by qutrits, highlighting the qubit-qutrit trade-off between scaling in numbers and in dimension. Qudits, however, remain significantly difficult to control and use with current technological resources [21–23]. A possible implementation of the proposed protocol using qutrits could, however, already be envisioned by using a ten-qubit entangled state [24]; however, this would need to be further investigated.

Further work should also include a thorough analysis of the protocol's robustness under realistic noise conditions. A starting point could be considering separable noise channels, for example, depolarizing channels acting on each qudit of Alice's reduced state. This would not alter our results because the effect of the noise channel would be absorbed by Alice's separable channel, leaving her cheating probability unchanged. In contrast, correlated noise is destructive and decreases entanglement, and we believe that while it might increase Alice's cheating probability in one direction (switching her commitment from 0 to 1), it would reduce it in the other direction. Additionally, such noise could lead to Bob rejecting Alice's commitment even when she has been acting honestly. Typically, this would be resolved with some mitigation mechanism (e.g., repetition of the protocol), which could impact the cheating strategies. A careful treatment of these noise effects is left for future work.

Another direction for future research is to investigate separable channels over more than two partitions and eventually return to the physically more realistic restriction of LOCC operations mentioned in the Introduction. Given that the latter do not have a closed-form expression [11,25], we anticipate the mathematical analysis will be more challenging. We expect, however, Alice's inability to create entanglement to remain the backbone of the security proof.

Finally, we believe that the insights from this work can be extended to other two-party cryptographic primitives, such as oblivious transfer and secure multiparty computation, where similar operational restrictions might enable new secure protocols.

ACKNOWLEDGMENTS

All the authors would like to particularly thank Jamie Sikora for insightful discussions throughout the project. M.R. also acknowledges discussions with Andreas Winter on an alternative swap-based protocol. Finally, A.P. would like to thank Louis Salvail for introducing the original problem to her while she was on an academic stay at the University of Montreal and for discussing potential solutions. Z.C. and A.P. acknowledge support from the Hector Fellow Academy, the Emmy Noether grant from the Deutsche Forschungsge-

meinschaft (Grant No. 41829458), and the Berlin Quantum Alliance. M.R. is supported by Ministero dell'università e della ricerca via Project No. 816000-2022-SQUID - CUP F83C22002390007 (Young Researchers).

DATA AVAILABILITY

There are no publicly available research data or software supporting this manuscript. Requests for further information or data should be sent to the authors.

APPENDIX A: DERIVING THE GENERAL CHEATING BOUND

We derive (5) and (6) by plugging (3) and (4) into (2); indeed,

$$p_0 = \sum_j |\langle \Psi_1 | (K_j \otimes \mathbb{1}_B) | \Psi_0 \rangle|^2 = \sum_j \left| \left(\sum_{i=0}^{M-1} \sqrt{\lambda_i} \langle y_i | b_i \rangle \right) (K_j \otimes \mathbb{1}_B) \left(\sum_{l=0}^{M-1} \sqrt{\lambda_l} \langle x_l | b_l \rangle \right) \right|^2 = \sum_j \left| \sum_{i=0}^{M-1} \lambda_i \langle y_i | K_j | x_i \rangle \right|^2.$$

Similarly, we find $p_1 = \sum_j \left| \sum_{i=0}^{M-1} \lambda_i \langle x_i | K_j | y_i \rangle \right|^2$.

We now present detailed computations of (9) and (10). We start with the latter. Using (7) and (8), we find

$$\begin{aligned} p_1 &= \sum_j \left| \sum_{i=0}^{M-1} \lambda_i \langle x_i | K_j | y_i \rangle \right|^2 = \sum_j \left| \sum_{i=0}^{M-1} \lambda_i \left(\sum_{k=0}^{N_2-1} \frac{1}{\sqrt{N_2}} \langle e_{ik} | v_{ji} \rangle \langle f_{ik} | w_{ji} \rangle \right) \right|^2 \\ &= \sum_j \frac{1}{N_2} \left| \sum_{i=0}^{M-1} \sum_{k=0}^{N_2-1} \sqrt{\lambda_i} \langle e_{ik} | v_{ji} \rangle \sqrt{\lambda_i} \langle f_{ik} | w_{ji} \rangle \right|^2 \leq \frac{1}{N_2} \sum_j \left(\sum_{i=0}^{M-1} \sum_{k=0}^{N_2-1} |\sqrt{\lambda_i} \langle e_{ik} | v_{ji} \rangle|^2 \right) \left(\sum_{s=0}^{M-1} \sum_{t=0}^{N_2-1} |\sqrt{\lambda_s} \langle f_{st} | w_{js} \rangle|^2 \right) \\ &= \frac{1}{N_2} \sum_j \left(\sum_{i=0}^{M-1} \lambda_i \sum_{k=0}^{N_2-1} |\langle e_{ik} | v_{ji} \rangle|^2 \right) \left(\sum_{s=0}^{M-1} \lambda_s \sum_{t=0}^{N_2-1} |\langle f_{st} | w_{js} \rangle|^2 \right) = \frac{1}{N_2} \sum_j \left(\sum_{i=0}^{M-1} \lambda_i \langle v_{ji} | v_{ji} \rangle \right) \left(\sum_{s=0}^{M-1} \lambda_s \langle w_{js} | w_{js} \rangle \right) \\ &= \frac{1}{N_2} \sum_j \sum_{i,s=0}^{M-1} \lambda_i \lambda_s \langle v_i | K_{j1}^\dagger K_{j1} | v_i \rangle \langle w_s | K_{j2}^\dagger K_{j2} | w_s \rangle \\ &= \frac{1}{N_2} \text{Tr} \left[\sum_j (K_{j1} \otimes K_{j2}) \left(\sum_{i=0}^{M-1} \lambda_i |v_i\rangle \langle v_i| \otimes \sum_{s=0}^{M-1} \lambda_s |w_s\rangle \langle w_s| \right) (K_{j1} \otimes K_{j2})^\dagger \right] \\ &= \frac{1}{N_2} \text{Tr} \left[\mathcal{N} \left(\sum_{i=0}^{M-1} \lambda_i |v_i\rangle \langle v_i| \otimes \sum_{s=0}^{M-1} \lambda_s |w_s\rangle \langle w_s| \right) \right] = \frac{1}{N_2}. \end{aligned}$$

The upper bound in the second line follows from using the Cauchy-Schwarz inequality on the double sum, treated as the sum of all the terms indexed by i and k . The last equality holds because $\mathcal{N}$ is trace preserving.

The case for $b = 0$ is a bit more convoluted. Again, we use (7) and (8), and we denote by $\lambda_{\max}$ the maximum eigenvalue of Φ_0 given in (3) and by Π_K (where $K \in \mathbb{N}$) a projector onto a subspace of dimension of K :

$$\begin{aligned} p_0 &= \sum_j \left| \sum_{i=0}^{M-1} \lambda_i \langle y_i | K_j | x_i \rangle \right|^2 = \sum_j \left| \sum_{i=0}^{M-1} \sum_{k=0}^{N_2-1} \lambda_i \langle v_i | \langle w_i | (K_{j1} \otimes K_{j2}) \frac{|e_{ik}\rangle |f_{ik}\rangle}{\sqrt{N_2}} \right|^2 \\ &= \frac{1}{N_2} \sum_j \left| \sum_{i=0}^{M-1} \sum_{k=0}^{N_2-1} \sqrt{\lambda_i} \langle v_i | K_{j1} | e_{ik} \rangle \sqrt{\lambda_i} \langle w_i | K_{j2} | f_{ik} \rangle \right|^2 \\ &\leq \frac{1}{N_2} \sum_j \left(\sum_{i=0}^{M-1} \sum_{k=0}^{N_2-1} |\sqrt{\lambda_i} \langle v_i | K_{j1} | e_{ik} \rangle|^2 \sum_{s=0}^{M-1} \sum_{t=0}^{N_2-1} |\sqrt{\lambda_s} \langle w_s | K_{j2} | f_{st} \rangle|^2 \right) \\ &= \frac{1}{N_2} \sum_j \left(\sum_{i=0}^{M-1} \sum_{k=0}^{N_2-1} \lambda_i \langle v_i | K_{j1} | e_{ik} \rangle \langle e_{ik} | K_{j1}^\dagger | v_i \rangle \sum_{s=0}^{M-1} \sum_{t=0}^{N_2-1} \lambda_s \langle w_s | K_{j2} | f_{st} \rangle \langle f_{st} | K_{j2}^\dagger | w_s \rangle \right) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{N_2} \sum_j \left[\sum_{i=0}^{M-1} \lambda_i \langle v_i | K_{j1} \left(\underbrace{\sum_{k=0}^{N_2-1} |e_{ik}\rangle \langle e_{ik}|}_{\Pi_{N_2}} \right) K_{j1}^\dagger | v_i \rangle \sum_{s=0}^{M-1} \lambda_s \langle w_s | K_{j2} \left(\underbrace{\sum_{t=0}^{N_2-1} |f_{st}\rangle \langle f_{st}|}_{\mathbb{1}_{N_2}} \right) K_{j2}^\dagger | w_s \rangle \right] \\
&= \frac{1}{N_2} \sum_j \left(\sum_{i=0}^{M-1} \lambda_i \langle v_i | K_{j1} \Pi_{N_2} K_{j1}^\dagger | v_i \rangle \sum_{s=0}^{M-1} \lambda_s \langle w_s | K_{j2} \mathbb{1}_{N_2} K_{j2}^\dagger | w_s \rangle \right) \\
&= \frac{1}{N_2} \sum_j \left[\text{Tr} \left(\sum_{i=0}^{M-1} \lambda_i |v_i\rangle \langle v_i| K_{j1} \Pi_{N_2} K_{j1}^\dagger \right) \text{Tr} \left(\sum_{s=0}^{M-1} \lambda_s |w_s\rangle \langle w_s| K_{j2} \mathbb{1}_{N_2} K_{j2}^\dagger \right) \right] \\
&\leq \frac{\lambda_{\max}^2}{N_2} \sum_j \left[\text{Tr} \left(\sum_{i=0}^{M-1} |v_i\rangle \langle v_i| K_{j1} \Pi_{N_2} K_{j1}^\dagger \right) \text{Tr} \left(\sum_{s=0}^{M-1} |w_s\rangle \langle w_s| K_{j2} \mathbb{1}_{N_2} K_{j2}^\dagger \right) \right] \\
&= \frac{\lambda_{\max}^2}{N_2} \sum_j [\text{Tr}(\Pi_M K_{j1} \Pi_{N_2} K_{j1}^\dagger) \text{Tr}(\Pi_M K_{j2} \mathbb{1}_{N_2} K_{j2}^\dagger)] = \frac{\lambda_{\max}^2}{N_2} \sum_j [\text{Tr}(K_{j1} \Pi_{N_2} K_{j1}^\dagger \Pi_M) \text{Tr}(K_{j2} \mathbb{1}_{N_2} K_{j2}^\dagger \Pi_M)] \\
&= \frac{\lambda_{\max}^2}{N_2} \text{Tr} \left(\sum_j (K_{j1} \otimes K_{j2}) (\Pi_{N_2} \otimes \mathbb{1}_{N_2}) (K_{j1} \otimes K_{j2})^\dagger (\Pi_M \otimes \Pi_M) \right) \\
&= \frac{\lambda_{\max}^2}{N_2} \text{Tr}[\mathcal{N}(\Pi_{N_2} \otimes \mathbb{1}_{N_2}) (\Pi_M \otimes \Pi_M)] \leq \frac{\lambda_{\max}^2}{N_2} \text{Tr}[\mathcal{N}(\Pi_{N_2} \otimes \mathbb{1}_{N_2})] \\
&= \frac{\lambda_{\max}^2}{N_2} \text{Tr}(\Pi_{N_2} \otimes \mathbb{1}_{N_2}) = \frac{\lambda_{\max}^2}{N_2} N_2^2 = \lambda_{\max}^2 N_2.
\end{aligned}$$

The first inequality again follows the Cauchy-Schwarz inequality, while the last inequality holds because $\Pi_{N_2} \otimes \mathbb{1}_{N_2}$ is a positive operator and $\mathcal{N}$ is a completely positive map, therefore mapping positive operators to positive operators.

APPENDIX B: SECURITY PROOF OF THE AME(3, d)-QUANTUM BIT COMMITMENT PROTOCOL

1. The honest case

We first provide detailed calculations showing that the protocol indeed allows for bit commitment if both parties are honest. We need to show that the states when Alice commits to 0 or 1 are indistinguishable to Bob. We show that Bob's reduced state is always the maximally mixed state. We first properly derive the postcommitment states. When Alice commits to $b = 1$, we have

$$(|m\rangle \langle \pi(m)| \otimes \mathbb{1}) |\Xi\rangle = (|m\rangle \langle \pi(m)| \otimes \mathbb{1}) \left(\frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |l\rangle |\Phi_l\rangle \right) = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |m\rangle \delta_{\pi(m)l} |\Phi_l\rangle = \frac{1}{\sqrt{d}} |m\rangle_{\text{a}} |\Phi_{\pi(m)}\rangle_{\text{AB}}.$$

Therefore, $\frac{\langle |m\rangle \langle \pi(m)| \otimes \mathbb{1} | \Xi \rangle}{\sqrt{\langle \Xi | \Xi \rangle}} = |m\rangle_{\text{a}} |\Phi_{\pi(m)}\rangle_{\text{AB}}.$

If she commits to $b = 0$, we have

$$\begin{aligned}
(|m\rangle \langle \widetilde{\pi(m)}| \otimes \mathbb{1}) |\Xi\rangle &= (|m\rangle \langle \widetilde{\pi(m)}| \otimes \mathbb{1}) \left(\frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |l\rangle |\Phi_l\rangle \right) = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |m\rangle \langle \widetilde{\pi(m)} | l \rangle |\Phi_l\rangle \\
&= \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \left(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{\pi(m)k} |m\rangle \langle k | l \rangle \right) |\Phi_l\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \left(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{\pi(m)k} \delta_{kl} |m\rangle \right) |\Phi_l\rangle \\
&= \frac{1}{d} |m\rangle_{\text{a}} \sum_{l=0}^{d-1} \omega^{\pi(m)l} |\Phi_l\rangle_{\text{AB}}.
\end{aligned}$$

Since ω is a d th root of unity, it holds that $\sum_{i=0}^{d-1} \omega^i = 0$, which in turn implies that, for all $j, k \in \{0, \dots, d-1\}$, we have

$$\left(\frac{1}{d} \sum_{k=0}^{d-1} \omega^{-\pi(m)k} \langle \Phi_k | \right) \left(\frac{1}{d} \sum_{l=0}^{d-1} \omega^{\pi(m)l} |\Phi_l\rangle \right) = \frac{1}{d^2} \sum_{l,k=0}^{d-1} \omega^{\pi(m)(l-k)} \delta_{kl} = \frac{1}{d}$$

and therefore

$$\frac{(|m\rangle\langle\pi(\widetilde{m})| \otimes \mathbb{1})|\Xi_\pi\rangle}{\sqrt{\langle\Xi_\pi|(|\pi(\widetilde{m})\rangle \otimes \mathbb{1})|\Xi_\pi\rangle}} = |m\rangle_a \left(\frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{m\pi(l)} |\Phi_l\rangle_{AB} \right).$$

Since the state of the ancilla register $|m\rangle_a$ is fixed after the commitment and therefore contains classical information, it can be dropped for the remainder of the analysis. We will therefore consider the states $|\Xi_{\pi,m}^0\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{m\pi(l)} |\Phi_l\rangle$ and $|\Xi_{\pi,m}^1\rangle = |\Phi_{\pi(m)}\rangle$.

We also want Bob's reduced states to be indistinguishable and maximally mixed. Bob's reduced state when Alice commits 1 is

$$\begin{aligned} \text{Tr}_A(|\Xi_{\pi,m}^1\rangle\langle\Xi_{\pi,m}^1|) &= \text{Tr}_A(|\Phi_{\pi(m)}\rangle\langle\Phi_{\pi(m)}|) = \text{Tr}_A\left(\frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\pi(m)l} |ll\rangle\langle l + \pi(m)|\right) \left(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-\pi(m)j} \langle jj|\langle j + \pi(m)|\right) \\ &= \frac{1}{d} \sum_{j,l=0}^{d-1} \omega^{\pi(m)(l-j)} \delta_{lj} |l + \pi(m)\rangle\langle j + \pi(m)| = \frac{1}{d} \sum_{j=0}^{d-1} |j + \pi(m)\rangle\langle j + \pi(m)| = \frac{1}{d} \sum_{j'=0}^{d-1} |j'\rangle\langle j'| = \frac{\mathbb{1}_B}{d}. \end{aligned}$$

Similarly, when she commits 0, Bob's reduced state is

$$\begin{aligned} \text{Tr}_A(|\Xi_{\pi,m}^0\rangle\langle\Xi_{\pi,m}^0|) &= \text{Tr}_A\left[\left(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{\pi(m)k} |\Phi_k\rangle\right) \left(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-\pi(m)j} \langle\Phi_j|\right)\right] = \frac{1}{d} \sum_{j,k=0}^{d-1} \omega^{\pi(m)(k-j)} \text{Tr}_A[|\Phi_k\rangle\langle\Phi_j|] \\ &= \frac{1}{d} \sum_{j,k=0}^{d-1} \omega^{\pi(m)(k-j)} \text{Tr}_A\left[\left(\frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} \omega^{ks} |sss\rangle\langle s + k|\right) \left(\frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} \omega^{-jt} \langle ttt|\langle t + j|\right)\right] \\ &= \frac{1}{d^2} \sum_{j,k=0}^{d-1} \omega^{\pi(m)(k-j)} \sum_{s,t=0}^{d-1} \omega^{ks-jt} \delta_{st} |s + k\rangle\langle t + j| = \frac{1}{d^2} \sum_{j,k=0}^{d-1} \omega^{\pi(m)(k-j)} \sum_{s=0}^{d-1} \omega^{s(k-j)} |s + k\rangle\langle s + j|. \end{aligned}$$

We relabel the sum with $j' = s + j$ and $k' = s + k$ and note that $k' - j' = k - j$. Summing over roots of unity again yields

$$\begin{aligned} \frac{1}{d^2} \sum_{j,k=0}^{d-1} \omega^{\pi(m)(k-j)} \sum_{s=0}^{d-1} \omega^{s(k-j)} |s + k\rangle\langle s + j| &= \frac{1}{d^2} \sum_{j',k'=0}^{d-1} \omega^{\pi(m)(k'-j')} \left(\sum_{s=0}^{d-1} \omega^{s(k'-j')}\right) |k'\rangle\langle j'| \\ &= \frac{1}{d^2} \sum_{j',k'=0}^{d-1} \omega^{\pi(m)(k'-j')} d \delta_{j'k'} |k'\rangle\langle j'| = \frac{1}{d} \sum_{j'=0}^{d-1} |j'\rangle\langle j'| = \frac{\mathbb{1}_B}{d}. \end{aligned}$$

The states are therefore indistinguishable to Bob in the honest case.

We also want to prove that the sets $\{|\Xi_{\pi,j}^0\rangle\}_{j=0}^{d-1}$ and $\{|\Xi_{\pi,j}^1\rangle\}_{j=0}^{d-1}$ are orthonormal sets. The definition (IV) of Φ_l implies that $\{|\Xi_{\pi,j}^1\rangle\}_{j=0}^{d-1}$ is an orthonormal set. For $\{|\Xi_{\pi,j}^0\rangle\}_{j=0}^{d-1}$ we have

$$\begin{aligned} \langle\Xi_{\pi,l}^0|\Xi_{\pi,m}^0\rangle &= \left(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{-\pi(l)k} \langle\Phi_k|\right) \left(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{\pi(m)j} |\Phi_j\rangle\right) = \frac{1}{d} \sum_{k,j=0}^{d-1} \omega^{\pi(m)j - \pi(l)k} \langle\Phi_k|\Phi_j\rangle = \frac{1}{d} \sum_{k,j=0}^{d-1} \omega^{\pi(m)j - \pi(l)k} \delta_{kj} \\ &= \frac{1}{d} \sum_{k=0}^{d-1} \omega^{(\pi(m) - \pi(l))k} = \delta_{lm}. \end{aligned}$$

2. Honest binding

When Alice commits to 1, the shared state is

$$\begin{aligned} |\Xi_{\pi,m}^1\rangle &= |\Phi_{\pi(m)}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{j\pi(m)} |jj\rangle\langle j + \pi(m)| = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \underbrace{\omega^{[j - \pi(m)]\pi(m)} | [j - \pi(m)][j - \pi(m)][j - \pi(m)] \rangle}_{|y_j^{m,\pi}\rangle} |j\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |y_j^{m,\pi}\rangle |j\rangle, \end{aligned}$$

where $|y_j^{m,\pi}\rangle$ are product qudit states that form an orthonormal set.

The postcommitment state after Alice commits to 0 is

$$\begin{aligned} |\Xi_{\pi,m}^0\rangle &= \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\pi(m)l} |\Phi_l\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\pi(m)l} \sum_{j=0}^{d-1} \frac{\omega^{lj}}{\sqrt{d}} |jjj\rangle |j+l\rangle = \frac{1}{d} \sum_{j=0}^{d-1} \sum_{l=0}^{d-1} \omega^{\pi(m)l+jl} |jjj\rangle |j+l\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \left(\underbrace{\frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{\pi(m)l+(j-l)l} |(j-l)(j-l)(j-l)\rangle}_{|x_j^{m,\pi}\rangle} \right) |j\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |x_j^{m,\pi}\rangle |j\rangle. \end{aligned}$$

One can easily show that states of the form $\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{kj} |jjj\rangle$ are AMEs, and therefore, $|x_j^{m,\pi}\rangle$ are $\text{AME}(3, d)$ states that form an orthonormal set.

3. Hiding

We will now prove that for any ρ , it holds that $\mathcal{M}_0(\rho) = \mathcal{M}_1(\rho)$ and therefore the commitment does not reveal any information to Bob. To do this we will use the following fact: If S_d is the group of all permutations over d elements, for all $j, k \in \{1, \dots, d\}$, we have $|\{\sigma \in S_d : \sigma(j) = k\}| = (d-1)!$. It then follows that

$$\begin{aligned} \mathcal{M}_0(\rho) &= \frac{1}{d!} \sum_{\pi \in S_d} \sum_{m=0}^{d-1} [|m\rangle \langle \pi(m)| \otimes \mathbb{1}_B] \rho [|\pi(m)\rangle \langle m| \otimes \mathbb{1}_B] = \frac{1}{d!} \sum_{m=0}^{d-1} \sum_{\pi \in S_d} \sum_{k,l=0}^{d-1} \frac{1}{d} \omega^{\pi(m)(k-l)} [|m\rangle \langle k| \otimes \mathbb{1}_B] \rho [|l\rangle \langle m| \otimes \mathbb{1}_B] \\ &= \frac{1}{dd!} \sum_{m=0}^{d-1} \sum_{k,l=0}^{d-1} \sum_{\pi \in S_d} \omega^{\pi(m)(k-l)} (|m\rangle \langle k| \otimes \mathbb{1}_B) \rho (|l\rangle \langle m| \otimes \mathbb{1}_B) \\ &= \frac{1}{dd!} \sum_{m=0}^{d-1} \sum_{k,l=0}^{d-1} (d-1)! \sum_{q=0}^{d-1} \omega^{q(k-l)} (|m\rangle \langle k| \otimes \mathbb{1}_B) \rho (|l\rangle \langle m| \otimes \mathbb{1}_B) \\ &= \frac{1}{d^2} \sum_{m=0}^{d-1} \sum_{k,l=0}^{d-1} d \delta_{kl} (|m\rangle \langle k| \otimes \mathbb{1}_B) \rho (|l\rangle \langle m| \otimes \mathbb{1}_B) = \frac{1}{d} \sum_{m=0}^{d-1} \sum_{k=0}^{d-1} (|m\rangle \langle k| \otimes \mathbb{1}_B) \rho (|k\rangle \langle m| \otimes \mathbb{1}_B). \end{aligned}$$

Similarly, we compute

$$\begin{aligned} \mathcal{M}_1(\rho) &= \frac{1}{d!} \sum_{\pi \in S_d} \sum_{m=0}^{d-1} [|m\rangle \langle \pi(m)| \otimes \mathbb{1}_B] \rho [|\pi(m)\rangle \langle m| \otimes \mathbb{1}_B] = \frac{1}{d!} \sum_{m=0}^{d-1} \sum_{\pi \in S_d} [|m\rangle \langle \pi(m)| \otimes \mathbb{1}_B] \rho [|\pi(m)\rangle \langle m| \otimes \mathbb{1}_B] \\ &= \frac{1}{d!} \sum_{m=0}^{d-1} (d-1)! \sum_{k=0}^{d-1} (|m\rangle \langle k| \otimes \mathbb{1}_B) \rho (|k\rangle \langle m| \otimes \mathbb{1}_B) = \frac{1}{d} \sum_{m=0}^{d-1} \sum_{k=0}^{d-1} (|m\rangle \langle k| \otimes \mathbb{1}_B) \rho (|k\rangle \langle m| \otimes \mathbb{1}_B). \end{aligned}$$

-
- [1] G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois, A quantum bit commitment scheme provably unbreakable by both parties, in *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science* (IEEE Computer Society Press, Palo Alto, CA, 1993), pp. 362–371.
- [2] D. Mayers, Unconditionally secure quantum bit commitment is impossible, *Phys. Rev. Lett.* **78**, 3414 (1997).
- [3] H.-K. Lo and H. Chau, Why quantum bit commitment and ideal quantum coin tossing are impossible, *Phys. D (Amsterdam, Neth.)* **120**, 177 (1998).
- [4] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Cryptography in the bounded-quantum-storage model, *SIAM J. Comput.* **37**, 1865 (2008).
- [5] R. Koenig, S. Wehner, and J. Wullschlegler, Unconditional security from noisy quantum storage, *IEEE Trans. Inf. Theory* **58**, 1962 (2012).
- [6] J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner, Secure bit commitment from relativistic constraints, *IEEE Trans. Inf. Theory* **59**, 4687 (2013).
- [7] L. Salvail, Quantum bit commitment from a physical assumption, in *Advances in Cryptology — CRYPTO '98*, edited by H. Krawczyk (Springer, Berlin, 1998), pp. 338–353.
- [8] A. Carrera Vazquez, C. Tornow, D. Ristè, S. Woerner, M. Takita, and D. J. Egger, Combining quantum processors with real-time classical communication, *Nature (London)* **636**, 75 (2024).

- [9] D. Main, P. Drmota, D. P. Nadlinger, E. M. Ainley, A. Agrawal, B. C. Nichol, R. Srinivas, G. Araneda, and D. M. Lucas, Distributed quantum computing across an optical network link, *Nature (London)* **638**, 383 (2025).
- [10] J. Funder, Cryptography with Quantum Mechanics, Ph.D. thesis, Aarhus University, 2012.
- [11] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, Everything you always wanted to know about LOCC (but were afraid to ask), *Commun. Math. Phys.* **328**, 303 (2014).
- [12] C. Schaffner, Cryptography in the bounded-quantum-storage model, Ph.D. thesis, University of Aarhus, 2007.
- [13] P. Dumais, D. Mayers, and L. Salvail, Perfectly concealing quantum bit commitment from any one-way permutation, in *Advances in Cryptology — EUROCRYPT 2000*, edited by G. Goos, J. Hartmanis, J. van Leeuwen, and B. Preneel, Lecture Notes in Computer Science, Vol. 1807 (Springer, Berlin, 2000), pp. 300–315.
- [14] J. Yan, General properties of quantum bit commitments (extended abstract), in *Advances in Cryptology – ASIACRYPT 2022 28th International Conference on the Theory and Application of Cryptology and Information Security* (Springer-Verlag, Taipei, Taiwan, Berlin, Heidelberg, 2022), pp. 628–657.
- [15] J. Fang, D. Unruh, J. Yan, and D. Zhou, How to base security on the perfect/statistical binding property of quantum bit commitment, in *33rd International Symposium on Algorithms and Computation (ISAAC 2022)*, edited by S. W. Bae and H. Park, Leibniz International Proceedings in Informatics, Vol. 248 (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2022), pp. 26:1–26:12.
- [16] If the states are not pure, we can purify them over a larger system that will be Bob’s since the size of his system does not matter.
- [17] This condition is necessary but not sufficient. The analysis of the hiding property is protocol specific, as is the case for our protocol in Sec. III B.
- [18] For two quantum states ρ and σ , we define the fidelity as $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2 = [\text{Tr}(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}})]^2$.
- [19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th anniversary ed. (Cambridge University Press, Cambridge, 2012).
- [20] W. Helwig, W. Cui, A. Riera, J. I. Latorre, and H.-K. Lo, Absolute maximal entanglement and quantum secret sharing, *Phys. Rev. A* **86**, 052335 (2012).
- [21] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, Qudits and high-dimensional quantum computing, *Front. Phys.* **8**, 479 (2020).
- [22] H. Zhou, H. Gao, N. T. Leitao, O. Makarova, I. Cong, A. M. Douglas, L. S. Martin, and M. D. Lukin, Robust Hamiltonian engineering for interacting qudit systems, *Phys. Rev. X* **14**, 031017 (2024).
- [23] N. Goss, A. Morvan, B. Marinelli, B. K. Mitchell, L. B. Nguyen, R. K. Naik, L. Chen, C. Jünger, J. M. Kreikebaum, D. I. Santiago, J. J. Wallman, and I. Siddiqi, High-fidelity qutrit entangling gates for superconducting circuits, *Nat. Commun.* **13**, 7481 (2022).
- [24] A. Cervera-Lierta, J. I. Latorre, and D. Goyeneche, Quantum circuits for maximally entangled states, *Phys. Rev. A* **100**, 022342 (2019).
- [25] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, 2018).