Fidelity of Quantum Strategies with Applications to Cryptography*†

Gus Gutoski‡[1], **Ansis Rosmanis**[2], **and Jamie Sikora**§[3]

1 **Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada**
gus.gutoski@isara.com
2 **Centre for Quantum Technologies, National University of Singapore, Singapore and Nanyang Technological University, Singapore**
ansis@ntu.edu.sg
3 **Centre for Quantum Technologies, National University of Singapore, Singapore and MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, Singapore**
cqtjwjs@nus.edu.sg

Abstract

We introduce a definition of the fidelity function for multi-round quantum strategies, which we call the *strategy fidelity*, that is a generalization of the fidelity function for quantum states. We provide many interesting properties of the strategy fidelity including a Fuchs-van de Graaf relationship with the strategy norm. We illustrate an operational interpretation of the strategy fidelity in the spirit of Uhlmann's Theorem and discuss its application to the security analysis of quantum protocols for interactive cryptographic tasks such as bit-commitment and oblivious string transfer. Our analysis is very general in the sense that the actions of the protocol need not be fully specified, which is in stark contrast to most other security proofs. Lastly, we provide a semidefinite programming formulation of the strategy fidelity.

1998 ACM Subject Classification G.1.6 Optimization, K.6.5 Security and Protection, J.2 Physical Sciences and Engineering

Keywords and phrases Quantum strategies, cryptography, fidelity, semidefinite programming

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.8

1 Introduction

1.1 Review of quantum strategies

In this paper we consider multiple-round interactions between two parties involving the exchange of quantum information. There is a natural asymmetry between the parties as only one of the parties can send the first message or receive the final message. Since we are not

* Research at the Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. Research at the Centre for Quantum Technologies at the National University of Singapore is partially funded by the Singapore Ministry of Education and the National Research Foundation, also through the Tier 3 Grant "Random numbers from quantum processes," (MOE2012-T3-1-009). This material is based on research supported in part by the Singapore National Research Foundation under NRF RF Award No. NRF-NRFF2013-13.
† A full version of the paper is available at https://arxiv.org/abs/1704.04033.
‡ GG also acknowledges support from CryptoWorks21.
§ JS acknowledges support from NSERC Canada.

© Gus Gutoski, Ansis Rosmanis and Jamie Sikora;
licensed under Creative Commons License CC-BY

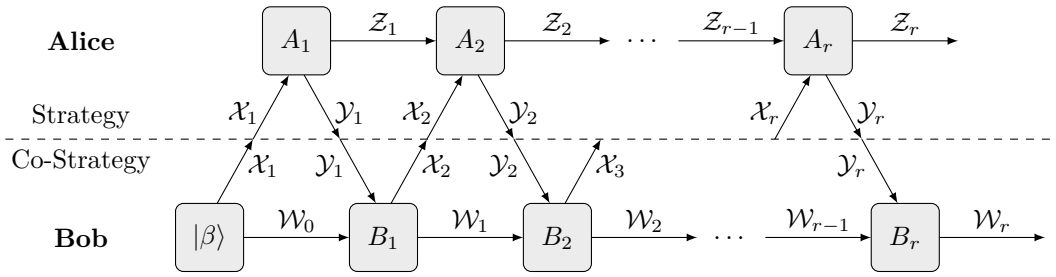

Figure 1 An r-round interaction between a pure strategy of Alice (the linear isometries above the dashed line) and a pure co-strategy of Bob (the linear isometries below the dashed line). Arrows crossing the dashed line represent messages exchanged between the parties, while horizontal arrows represent private memory.

concerned about optimizing the number of messages exchanged, without loss of generality both of these tasks are done by the same party, which, for convenience, we call *Bob*. Let us call the other party *Alice*. The interaction between Alice and Bob decomposes naturally into a finite number r of *rounds* (see Figure 1).

Such interactions are conveniently described by the formalism of quantum strategies introduced in Ref. [13]. We closely follow that formalism here with the exception that we consider two mathematically different objects: *strategies* and *pure strategies*. Pure strategies are implemented using linear isometries and preserve their final memory space, while strategies trace out the final memory space. The object we call a strategy is called a *non-measuring strategy* in Ref. [13]. For additional details on quantum strategies, one may refer to [13, 9, 11].

▶ **Definition 1** (Pure strategy and pure co-strategy)**.** Let $r \geq 1$ and let $\mathcal{X}_1, \ldots, \mathcal{X}_r, \mathcal{Y}_1, \ldots, \mathcal{Y}_r$, $\mathcal{Z}_r, \mathcal{W}_r$ be complex Euclidean spaces and, for notational convenience, let $\mathcal{X}_{r+1} := \mathbb{C}$ and $\mathcal{Z}_0 := \mathbb{C}$. An *$r$-round pure strategy* $\tilde{A}$ having *input spaces* $\mathcal{X}_1, \ldots, \mathcal{X}_r$, *output spaces* $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$, and *final memory space* $\mathcal{Z}_r$, consists of:

1. complex Euclidean spaces $\mathcal{Z}_1, \ldots, \mathcal{Z}_{r-1}$, called *intermediate memory spaces*, and
2. an r-tuple of linear isometries $(A_1, \ldots, A_r)$ of the form $A_i : \mathcal{X}_i \otimes \mathcal{Z}_{i-1} \to \mathcal{Y}_i \otimes \mathcal{Z}_i$.

An *r-round pure co-strategy* having input spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$, output spaces $\mathcal{X}_1, \ldots, \mathcal{X}_r$, and final memory space $\mathcal{W}_r$, consists of:

1. complex Euclidean intermediate memory spaces $\mathcal{W}_0, \ldots, \mathcal{W}_{r-1}$,
2. a pure quantum state $|\beta\rangle \in \mathcal{X}_1 \otimes \mathcal{W}_0$, called the *initial state*, and
3. an r-tuple of linear isometries $(B_1, \ldots, B_r)$ of the form $B_i : \mathcal{Y}_i \otimes \mathcal{W}_{i-1} \to \mathcal{X}_{i+1} \otimes \mathcal{W}_i$.

A pure strategy and a pure co-strategy are said to be *compatible* when the input spaces of one are the output spaces of the other, and vice versa. The *final state* of the interaction between $\tilde{A}$ and $\tilde{B}$ is denoted by

$$|\psi(\tilde{A}, \tilde{B})\rangle := (I_{\mathcal{Z}_r} \otimes B_r)(A_r \otimes I_{\mathcal{W}_{r-1}}) \cdots (I_{\mathcal{Z}_1} \otimes B_1)(A_1 \otimes I_{\mathcal{W}_0})|\beta\rangle \in \mathcal{Z}_r \otimes \mathcal{W}_r.$$

In order to extract classical information from the interaction it suffices to permit Alice and Bob to measure their respective parts of the final state $|\psi(\tilde{A}, \tilde{B})\rangle$.

A pure strategy $\tilde{A}$ specified by linear isometries $(A_1, \ldots, A_r)$ can be represented by a single isometry

$$\tilde{A} := (A_r \otimes I_{\mathcal{Y}_{1\ldots r-1}}) \ldots (I_{\mathcal{X}_{3\ldots r}} \otimes A_2 \otimes I_{\mathcal{Y}_1})(I_{\mathcal{X}_{2\ldots r}} \otimes A_1) : \mathcal{X}_{1\ldots r} \to \mathcal{Y}_{1\ldots r} \otimes \mathcal{Z}_r,$$

where $\mathcal{X}_{i\ldots j}$ is short for $\mathcal{X}_i \otimes \cdots \otimes \mathcal{X}_j$ and $\mathcal{Y}_{i\ldots j}$ is short for $\mathcal{Y}_i \otimes \cdots \otimes \mathcal{Y}_j$. We abuse the notation[1] $\tilde{A}$ here and elsewhere in the paper by using it to denote both a pure strategy and the linear isometry representing it, and we do the same for pure co-strategies $\tilde{B}$, discussed next. A pure co-strategy $\tilde{B}$ specified by the initial state $|\beta\rangle$ and linear isometries $(B_1, \ldots, B_r)$ can be represented by a single isometry

$$\tilde{B} := (B_r \otimes I_{\mathcal{X}_{1\ldots r}}) \cdots (I_{\mathcal{Y}_{2\ldots r}} \otimes B_1 \otimes I_{\mathcal{X}_1})(I_{\mathcal{Y}_{1\ldots r}} \otimes |\beta\rangle) : \mathcal{Y}_{1\ldots r} \to \mathcal{X}_{1\ldots r} \otimes \mathcal{W}_r.$$

Note that two pure strategies that are represented by the same linear isometry are effectively indistinguishable, and the same holds true for pure co-strategies.

Any one party is not affected by what the other party does with their final memory space. Hence, from the point of view of that party, the other party can trace it out. In view of this, a *strategy* A is obtained from a pure strategy $\tilde{A}$ by tracing out the final memory space $\mathcal{Z}_r$ and a *co-strategy* B is obtained from a pure co-strategy $\tilde{B}$ by tracing out the final memory space $\mathcal{W}_r$. Multiple pure strategies (co-strategies) can yield the same strategy (co-strategy), and we call any such pure strategy (co-strategy) a *purification*. We will use tildes to indicate purifications.

Just as a pure strategy and a pure co-strategy can be specified by linear isometries $\tilde{A}$ and $\tilde{B}$, respectively, their corresponding strategy A and co-strategy B can be specified by quantum channels

$$\Phi_A : \mathbf{L}(\mathcal{X}_{1\ldots r}) \to \mathbf{L}(\mathcal{Y}_{1\ldots r}) : X \mapsto \mathrm{Tr}_{\mathcal{Z}_r}(\tilde{A} X \tilde{A}^*),$$
$$\Psi_B : \mathbf{L}(\mathcal{Y}_{1\ldots r}) \to \mathbf{L}(\mathcal{X}_{1\ldots r}) : Y \mapsto \mathrm{Tr}_{\mathcal{W}_r}(\tilde{B} Y \tilde{B}^*).$$

In turn, both of these channels can be specified using their Choi-Jamiołkowski representations, but, due to the asymmetry between strategies and co-strategies, it is convenient to specify the latter one using the Choi-Jamiołkowski representation of its adjoint map. Thus, we can represent a strategy A by $J(\Phi_A)$ and a co-strategy B by $J(\Psi_B^*)$, both of which are positive semidefinite operators acting on $\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r}$. In a similar abuse of notation as mentioned before, we refer to $J(\Phi_A)$ as the strategy A and to $J(\Psi_B^*)$ as the co-strategy B.

For compatible pure strategy $\tilde{A}$ and pure co-strategy $\tilde{B}$, let

$$\rho_A(\tilde{B}) := \mathrm{Tr}_{\mathcal{Z}_r}\left(|\psi(\tilde{A}, \tilde{B})\rangle\langle\psi(\tilde{A}, \tilde{B})|\right) \tag{1}$$

denote the reduced state of the final memory space $\mathcal{W}_r$ of $\tilde{B}$ after the interaction between $\tilde{A}$ and $\tilde{B}$. Since this state is the same for all purifications of A, we omit the tilde above A in this notation.

1.2 The definition of strategy fidelity

Recall that the fidelity $\mathrm{F}(P, Q)$ between two positive semidefinite operators P and Q is defined as

$$\mathrm{F}(P, Q) := \left\| \sqrt{P}\sqrt{Q} \right\|_{\mathrm{Tr}}.$$

When applied to density operators ρ, ξ, the fidelity function $\mathrm{F}(\rho, \xi)$ is a useful distance measure for quantum states. We would like to construct a generalization of the fidelity function that can serve as a useful distance measure for quantum strategies.

[1] It will be clear from context to which we are referring.

Just as the trace norm $\|\rho - \xi\|_{\mathrm{Tr}}$ quantifies the distinguishability of quantum states, the strategy norm $\|S - T\|_{\diamond \mathrm{r}}$ studied in [12] quantifies the distinguishability of quantum strategies S and T having the same input and output spaces. In other words, $\|S - T\|_{\diamond \mathrm{r}}$ is proportional to the maximum bias with which an interacting pure co-strategy $\tilde{B}$ can distinguish S from T. Another expression for this maximum bias can be derived as follows. Let $\mathcal{W}_r$ be the final memory space of $\tilde{B}$ and let $\rho_S(\tilde{B}), \rho_T(\tilde{B})$ be the reduced states of this final memory space after an interaction between $\tilde{B}$ and S, T, respectively, as defined in (1). It is clear that the maximum bias with which S can be distinguished from T is proportional to the maximum over all such $\tilde{B}$ with which the final state $\rho_S(\tilde{B})$ can be distinguished from $\rho_T(\tilde{B})$, which is precisely $\|\rho_S(\tilde{B}) - \rho_T(\tilde{B})\|_{\mathrm{Tr}}$.

▶ Remark. All purifications $\tilde{B}$ of B are equivalent up to a unitary acting on $\mathcal{W}_r$. Thus, unitarily invariant distance measures between $\rho_S(\tilde{B})$ and $\rho_T(\tilde{B})$ (including the trace distance and the fidelity) depend only upon B and not upon the specific purification $\tilde{B}$.

The strategy norm is defined so that

$$\|S - T\|_{\diamond \mathrm{r}} = \max_B \|\rho_S(\tilde{B}) - \rho_T(\tilde{B})\|_{\mathrm{Tr}}. \tag{2}$$

In light of this observation, we define the strategy fidelity by replacing the maximization of the trace distance between $\rho_S(\tilde{B})$ and $\rho_T(\tilde{B})$ with the minimization of the fidelity between $\rho_S(\tilde{B})$ and $\rho_T(\tilde{B})$.

▶ **Definition 2** (Strategy fidelity)**.** For any r-round strategies S and T having the same input and output spaces, the *strategy fidelity* is defined as

$$\mathrm{F}_{\mathrm{r}}(S, T) := \min_B \mathrm{F}(\rho_S(\tilde{B}), \rho_T(\tilde{B})) \tag{3}$$

where the minimization is over all compatible co-strategies B and the states $\rho_S(\tilde{B}), \rho_T(\tilde{B})$ are as defined in (1).

In the following discussion, we argue that this definition is a meaningful one by proving analogues of the Fuchs-van de Graaf inequalities and Uhlmann's Theorem for the strategy fidelity, among many other properties.

▶ Remark. The same definition of fidelity has been considered for the case of channels [2]. In that setting, they establish several properties which we generalize to the strategy setting.

First, let us observe that the fidelity for quantum states is recovered as a special case of the strategy fidelity when S, T are one-round strategies with no input (that is, $\mathcal{X}_1 = \mathbb{C}$) and only one output message. To see this, observe that one-round strategies such as S, T are simply states ρ, ξ acting on $\mathcal{Y}_1$. Bob's most general pure co-strategy is an isometry $\tilde{B} : \mathcal{Y}_1 \to \mathcal{W}_1$. In this case the effect of Bob's purified strategy $\tilde{B}$ is cancelled in the computation of $\mathrm{F}_{\mathrm{r}}(S, T)$ so that

$$\mathrm{F}_1(S, T) = \min_B \mathrm{F}(\rho_S(\tilde{B}), \rho_T(\tilde{B})) = \mathrm{F}(\tilde{B}\rho\tilde{B}^*, \tilde{B}\xi\tilde{B}^*) = \mathrm{F}(\rho, \xi)$$

as claimed.

1.2.1 Basic properties of the strategy fidelity

We now list several other properties of the strategy fidelity, all of which immediately hold using the corresponding properties of the fidelity of quantum states.

▶ **Proposition 3** (Basic properties).

- *(Fuchs-van de Graaf inequalities for strategies) For any r-round strategies S and T, it holds that*

$$1 - \frac{1}{2}\|S - T\|_{\diamond \mathrm{r}} \leq \mathrm{F}_{\mathrm{r}}(S,T) \leq \sqrt{1 - \frac{1}{4}\|S - T\|_{\diamond \mathrm{r}}^2}. \tag{4}$$

- *(Symmetry) For any r-round strategies S and T, it holds that $\mathrm{F}_{\mathrm{r}}(S,T) = \mathrm{F}_{\mathrm{r}}(T,S)$.*
- *(Joint concavity) For any r-round strategies $S^1, \ldots, S^n$ and $T^1, \ldots, T^n$, and nonnegative scalars $\lambda_1, \ldots, \lambda_n$ satisfying $\sum_{i=1}^n \lambda_i = 1$, we have*

$$\mathrm{F}_{\mathrm{r}}\left(\sum_{i=1}^n \lambda_i S^i, \sum_{i=1}^n \lambda_i T^i\right) \geq \sum_{i=1}^n \lambda_i \, \mathrm{F}_{\mathrm{r}}\left(S^i, T^i\right).$$

- *(Bounds on the strategy fidelity) For any r-round strategies S and T, it holds that $0 \leq \mathrm{F}_{\mathrm{r}}(S,T) \leq 1$. Moreover, $\mathrm{F}_{\mathrm{r}}(S,T) = 1$ if and only if $S = T$ and $\mathrm{F}_{\mathrm{r}}(S,T) = 0$ if and only if S and T are perfectly distinguishable.*

We later discuss that the strategy version of the Fuchs-van de Graaf inequalities is crucial to our cryptographic applications. This was also used implicitly in [10].

1.2.2 Operational interpretation (min-max properties)

Here we propose an operationally motivated generalization of Uhlmann's Theorem [24] to the strategy fidelity. In so doing we elucidate the need for a min-max theorem. Recall that Uhlmann's Theorem for quantum states asserts that the fidelity $\mathrm{F}(\rho, \xi)$ between any two quantum states ρ and ξ, acting on $\mathcal{X}$, is given by

$$\mathrm{F}(\rho, \xi) = \max_U |\langle \phi | (U \otimes I_{\mathcal{X}}) | \psi \rangle|$$

where $|\phi\rangle, |\psi\rangle \in \mathcal{X} \otimes \mathcal{Y}$ are any purifications of ρ, ξ and the maximization is over all unitaries U acting on $\mathcal{Y}$ alone.

Intuitively, $\mathrm{F}_{\mathrm{r}}(S,T)$ should quantify the extent to which any purifications $\tilde{S}, \tilde{T}$ of two strategies S, T can be made to look the same by acting only on the final memory space $\mathcal{Z}_r$. It follows immediately from the definition of the strategy fidelity and Uhlmann's Theorem that

$$\mathrm{F}_{\mathrm{r}}(S,T) = \min_B \mathrm{F}(\rho_S(\tilde{B}), \rho_T(\tilde{B})) = \min_B \max_U \left| \langle \psi(\tilde{S}, \tilde{B}) | \left(U \otimes I_{\mathcal{W}_r}\right) | \psi(\tilde{T}, \tilde{B}) \rangle \right| \tag{5}$$

where, again, the maximization is over all unitaries U acting on $\mathcal{Z}_r$ alone.

Notice the order of minimization and maximization in (5). This could be viewed as a competitive game between Alice (who plays according to S or T) and Bob (who plays according to any arbitrary co-strategy B) in which Bob is trying to distinguish S from T and Alice is trying to make S and T look the same. To these ends, Bob chooses his strategy B so as to minimize the overlap $|\langle \psi(\tilde{S}, \tilde{B}) | \psi(\tilde{T}, \tilde{B}) \rangle|$; given such a choice B for Bob, Alice's responds with a unitary U that maximizes this overlap.

The problem is that Alice's choice of U may depend upon Bob's co-strategy B. The task of distinguishing S from T should depend only upon S and T—Alice should not be granted the ability to tweak S or T after she has acquired knowledge of Bob's specific choice of distinguishing co-strategy B. From an operational perspective, it would be much more desirable if the order of minimization and maximization in (5) were reversed. Alice should

select her unitary U so as to make S look as much as possible like T *before* Bob selects his distinguishing co-strategy B. Thus, we require a type of *min-max theorem*.

The set of all co-strategies B for Bob is compact and convex [13], but it is not at all clear that the objective function in (5) is convex in B; we show later (Lemma 9) that this is indeed the case. However, the set of all unitaries U for Alice is not a convex set. One might think that we could extend the domain of maximization to the convex hull of the unitaries in the hopes that there is a saddle point (U, B) with U unitary. Unfortunately, saddle points do not in general occur at extreme points of the domain, so we are not guaranteed that such a unitary saddle point exists. Thus, a min-max theorem for the strategy fidelity involving unitaries is not so easily forthcoming.

However, if we allow Alice to apply a general *quantum channel*, we are able to obtain a min-max result, as stated below.

▶ **Theorem 4** (Strategy generalization of Uhlmann's Theorem)**.** *Let S, T be r-round strategies and let $\tilde{S}, \tilde{T}$ be any purifications of S, T. Let $|\psi(\tilde{S}, \tilde{B})\rangle$, $|\psi(\tilde{T}, \tilde{B})\rangle$ be as defined in Definition 1. We have*

$$\mathrm{F_r}(S,T)^2 = \max_{\Xi} \min_{B} \langle\psi(\tilde{S},\tilde{B})| \left[\left(\Xi \otimes I_{\mathbf{L}(\mathcal{W}_r)}\right)\left(|\psi(\tilde{T},\tilde{B})\rangle\langle\psi(\tilde{T},\tilde{B})|\right)\right] |\psi(\tilde{S},\tilde{B})\rangle \tag{6}$$

where the minimum is over all r-round pure co-strategies $\tilde{B}$ and the maximum is over all quantum channels Ξ acting on $\mathcal{Z}_r$ alone.

Note that similar min-max results are derived in [2] and [10]. It will be convenient to define the following quantum channel.

▶ **Definition 5.** A *strategy fidelity-achieving* channel Ξ is a channel which attains the maximum in (6), above.

1.2.3 Semidefinite programming formulation of strategy fidelity

It was shown in [12] that the strategy norm has a semidefinite programming formulation. Also, the fidelity of quantum states has semidefinite programming formulations, see [26, 27] for examples. It is natural to ask whether the strategy fidelity has such a formulation. We answer this question in the affirmative, below.

▶ **Theorem 6** (Semidefinite programming formulation of strategy fidelity)**.** *Fix any purifications $\tilde{S}$ and $\tilde{T}$ of r-round strategies S and T, respectively. Then $\mathrm{F_r}(S,T)^2$ is equal to the optimal objective function value of the following semidefinite program:*

$$\begin{aligned}
\mathrm{F_r}(S,T)^2 = \quad & \max & t & & \\
& \text{subject to} & tI_{\mathcal{X}_1} & \preceq & \mathrm{Tr}_{\mathcal{Y}_1}(R_1) \\
& & R_j \otimes I_{\mathcal{X}_{j+1}} & \preceq & \mathrm{Tr}_{\mathcal{Y}_{j+1}}(R_{j+1}), \ \text{ for } j \in \{1,\ldots,r-1\}, \\
& & R_r & \preceq & \tfrac{1}{2}\,\mathrm{Tr}_{\mathcal{Z}_r}\left((K \otimes I_{\mathcal{Y}_{1\ldots r}\otimes\mathcal{X}_{1\ldots r}})\,|\tilde{T}\rangle\!\rangle\langle\!\langle\tilde{S}|\right) + h.c. \\
& & \begin{bmatrix} I_{\mathcal{Z}_r} & K \\ K^* & I_{\mathcal{Z}_r} \end{bmatrix} & \succeq & 0
\end{aligned}$$

where the variables R_j are Hermitian acting on $\mathcal{Y}_{1\ldots j} \otimes \mathcal{X}_{1\ldots j}$ for each $j \in \{1,\ldots,r\}$, and h.c. denotes the Hermitian conjugate.

1.3 Applications to two-party quantum cryptography

Since the seminal work of Wiesner [28] and Bennett and Brassard [3], there has been much interest in knowing the advantages, and limitations, of quantum protocols for cryptographic

tasks. Due to the interactive setting of such protocols, the use of quantum strategy analysis has proven to be useful. In [13], it was shown how to rederive Kitaev's lower bound for coin-flipping [15]. In [10], it was shown how to find a simple proof of the impossibility of interactive bit-commitment. Here, we find a similar proof of this and extend the argument to oblivious string transfer.

In this paper, we present our ideas using the machinery we have developed for the strategy fidelity. In particular, we show that the strategy version of the Fuchs-van de Graaf inequalities (Eqn. (4)) are of central importance in providing security lower bounds. In fact, due to the nature of the strategy norm and strategy fidelity, we are able to bound the security without even specifying the entire protocol! This is in stark contrast to many other security proofs/models studied, for example in [15, 23, 25, 19, 1, 14, 13, 5, 6, 7, 8, 20, 21, 4, 22] where Alice and Bob's actions are assumed to be fully specified (and known to cheating parties). We note that our proposed security model is implicit in the bit-commitment security bounds in [10] and in the channel setting in [2].

In this paper, we show the impossibility of ideal quantum protocols for interactive *bit-commitment* and *oblivious string transfer*.

1.3.1 Interactive bit-commitment

In bit-commitment, we require Alice and Bob to interact over two communication stages:

- Commit Phase: Alice chooses a uniformly random bit a and interacts with Bob using an r-round pure strategy $\tilde{A}^a$.
- Reveal Phase: Alice sends a to Bob and continues her interaction with him (so that Bob can test if she has cheated).
- Cheat Detection: Bob, knowing which pure strategy $\tilde{B}$ he has used, measures to check if the final state is consistent with Alice's pure strategy $\tilde{A}^a$. He aborts the protocol if this measurement detects the final state is not consistent with Alice's pure strategy $\tilde{A}^a$. If Alice is honest, he never aborts.

Protocols are designed with the intention to achieve the following two important properties of interest:

- Binding: Alice cannot change her mind after the Commit Phase and reveal the other value of a (without being detected by Bob).
- Hiding: Bob cannot learn Alice's bit a before she reveals it during the Reveal Phase.

Finding a protocol with perfect binding and hiding properties is known to be impossible [18, 16, 17]. However, these security proofs rely on an assumption that we do not make, that honest Bob's actions are specified beforehand (and thus known to Alice).

We define the cheating probabilities of Alice and Bob as follows:

$\mathrm{B_{BC}}$: The maximum probability with which a dishonest Bob can *learn* an honest Alice's committed bit $a \in \{0, 1\}$ after the Commit Phase.

$\mathrm{A_{BC}}$: The maximum probability with which Alice can change her commitment from 0 to 1 (or from 1 to 0) before the Reveal Phase.

▶ Remark. Note that in the definition of cheating Alice above, we do not assume Alice knows Bob's actions. It could even be the case that Bob's sole purpose is to choose a co-strategy such as to minimize $\mathrm{A_{BC}}$.

Cheating Bob wishes to distinguish between one of two uniformly randomly chosen strategies. We know from [12] that

$$\mathrm{B_{BC}} = \frac{1}{2} + \frac{1}{4}\| A^0 - A^1 \|_{\diamond\mathrm{r}}.$$

In Section 4, we show that

$$\mathrm{A_{BC}} \geq \mathrm{F}_r(A^0, A^1)^2.$$

An interesting observation is that this only depends on Alice's honest strategies, not Bob's.

Thus, by the Fuchs-van de Graaf inequalities for strategies (Proposition 3), we have the following trade-off lower bound.

▶ **Theorem 7.** *In any interactive quantum protocol for bit-commitment, we have that*

$$\sqrt{\mathrm{A_{BC}}} + 2\mathrm{B_{BC}} \geq 2.$$

Moreover, we have that Alice or Bob can cheat with probability at least $\frac{9-\sqrt{17}}{8} \approx 61\%$.

Note that this is a similar bound to the one obtained in [10] for the interactive setting and exactly the same as in [2] in the channel setting.

We remark that, when Alice and Bob's actions are completely specified, optimal protocols are known [6].

1.3.2 1-out-of-2 interactive oblivious string transfer

This is an interactive cryptographic task between Alice and Bob where Bob has two bit-strings[2] (x_0, x_1) and Alice wishes to learn one of the two in the following manner:

- Alice chooses a uniformly random bit a which corresponds to her choice of which string she wishes to learn, and interacts with Bob via the r-round pure strategy $\tilde{A}^a$.
- For every (x_0, x_1), Bob uses a pure co-strategy $\tilde{B}^{x_0,x_1}$, such that Alice learns the string x_a with certainty by measuring her private space $\mathcal{Z}_r$ at the end of the protocol.

Note that we do not assume any structure on how Bob behaves other than the consistency condition above. For example, x_0 and x_1 may be the result of another protocol of which Alice is not part, and thus she does not even know the distribution from which they are drawn. Again, Bob's strategy may be such that, conditioned on the above requirements, he just wants to foil Alice's cheating, as defined below.

We define the cheating probabilities of Alice and Bob as follows:

$\mathrm{B_{OT}}$: The maximum probability with which a dishonest Bob can *learn* an honest Alice's choice bit a.

$\mathrm{A_{OT}}$: The maximum probability with which a dishonest Alice can learn x_0 after learning x_1 with certainty, or vice versa.

Cheating Bob behaves the exact same as in a bit-commitment protocol. Thus his cheating probability is again

$$\mathrm{B_{OT}} = \frac{1}{2} + \frac{1}{4}\|A^0 - A^1\|_{\diamond\mathrm{r}}.$$

In Section 4, we show the following bound on cheating Alice:

$$\mathrm{A_{OT}} \geq \mathrm{F}_r(A^0, A^1)^2.$$

This yields the same bound as in bit-commitment, below.

[2] The bit-length of the strings are, surprisingly, not important for the purposes of this paper.

▶ **Theorem 8.** *In any interactive quantum protocol for 1-out-of-2 oblivious string transfer, we have that*

$$\sqrt{\mathrm{A_{OT}}} + 2\mathrm{B_{OT}} \geq 2.$$

Moreover, we have that Alice or Bob can cheat with probability at least $\frac{9-\sqrt{17}}{8} \approx 61\%$.

Note that in the case where Bob has two *bits* (i.e., the strings have bit-length 1), an optimal security trade-off between Alice and Bob is known [4]:

$$\mathrm{A_{OT}} + 2\mathrm{B_{OT}} \geq 2.$$

However, this assumes perfect knowledge of Alice and Bob's honest strategies. Thus, our bound for cheating Alice is a bit weaker, but has the added benefit of only depending on her honest strategies.

2 Technical lemmas and the strategy generalization of Uhlmann's Theorem

In this section we prove two lemmas that allow us to establish nontrivial properties of the strategy fidelity. These lemmas are used to prove the strategy generalization of Uhlmann's Theorem (Theorem 4) and to provide a semidefinite programming formulation of the strategy fidelity (Theorem 6).

Before we proceed, let us introduce some notation. Let $\mathcal{Y}_{i\ldots j}\mathcal{X}_{i'\ldots j'}$ be short for $\mathcal{Y}_{i\ldots j} \otimes \mathcal{X}_{i'\ldots j'}$. Let $\mathbf{L}(\mathcal{X})$, $\mathbf{U}(\mathcal{X})$, $\mathbf{Her}(\mathcal{X})$, $\mathbf{Pos}(\mathcal{X})$, and $\mathbf{Dens}(\mathcal{X})$ be, respectively, the set of all linear, unitary, Hermitian, positive semidefinite, and density operators acting on $\mathcal{X}$. Let $\mathbf{K}(\mathcal{X})$ be the convex hull of $\mathbf{U}(\mathcal{X})$, namely, the set of all operators $K \in \mathbf{L}(\mathcal{X})$ such that $\|K\| \leq 1$. Suppose $\mathcal{X}$ and $\mathcal{Y}$ are two complex Euclidean spaces with fixed standard basis. Given a linear operator $A : \mathcal{X} \to \mathcal{Y}$ written in the standard basis as

$$A = \sum_{i=1}^{\dim(\mathcal{X})} \sum_{j=1}^{\dim(\mathcal{Y})} a_{i,j}|j\rangle\langle i|,$$

the *vectorization* of A is

$$|A\rangle\!\rangle := \sum_{i=1}^{\dim(\mathcal{X})} \sum_{j=1}^{\dim(\mathcal{Y})} a_{i,j}|j\rangle \otimes |i\rangle \in \mathcal{Y} \otimes \mathcal{X}$$

and its adjoint is $\langle\!\langle A| := (|A\rangle\!\rangle)^*$.

▶ **Lemma 9** (Inner product is linear in B)**.** *Let S, T be r-round strategies and let $\tilde{S}, \tilde{T}$ be any purifications of S, T. Let B be a compatible r-round co-strategy and let $\tilde{B}$ be any purification of B. Let $|\psi(\tilde{S}, \tilde{B})\rangle, |\psi(\tilde{T}, \tilde{B})\rangle$ be as in Definition 1 and let $K \in \mathbf{L}(\mathcal{Z}_r)$. It holds that*

$$\langle\psi(\tilde{S}, \tilde{B})| \left(K \otimes I_{\mathcal{W}_r}\right) |\psi(\tilde{T}, \tilde{B})\rangle = \langle\!\langle \tilde{S}| \left(K \otimes B\right) |\tilde{T}\rangle\!\rangle.$$

Note that the inner product above depends on B but not on its purification $\tilde{B}$. This exemplifies what we stated earlier in the remark above Eqn. (2).

The proof is similar to a proof in Ref. [13, Theorem 5]. Lemma 9 is useful for proving the following lemma. Proofs of both these results will be included in the full version.

▶ **Lemma 10.** *Let S, T be r-round strategies and let $\tilde{S}, \tilde{T}$ be any purifications of S, T. It holds that*

$$\mathrm{F}_{\mathrm{r}}(S,T) = \max_{K} \min_{B} \Re \left(\langle\!\langle \tilde{S} | (K \otimes B) | \tilde{T} \rangle\!\rangle \right)$$

where the minimum is over all compatible r-round co-strategies B for Bob and the maximum is over all $K \in \mathbf{K}(\mathcal{Z}_r)$ acting on the final memory space $\mathcal{Z}_r$ for Alice.

Now, with Lemmas 9 and 10 at our disposal, we proceed to prove the strategy generalization of Uhlmann's Theorem.

Proof of Theorem 4. From Lemma 10, it follows that

$$\mathrm{F}_{\mathrm{r}}(S,T) \leq \max_{K} \min_{B} \left| \langle\!\langle \tilde{S} | (K \otimes B) | \tilde{T} \rangle\!\rangle \right|.$$

We square this inequality and apply Lemma 9 to obtain

$$\mathrm{F}_{\mathrm{r}}(S,T)^2 \leq \max_{K} \min_{B} \langle \psi(\tilde{S}, \tilde{B}) | (K \otimes I_{\mathcal{W}_r}) | \psi(\tilde{T}, \tilde{B}) \rangle \langle \psi(\tilde{T}, \tilde{B}) | (K^* \otimes I_{\mathcal{W}_r}) | \psi(\tilde{S}, \tilde{B}) \rangle.$$

Let us define $\bar{K} = \sqrt{I_{\mathcal{Z}_r} - K^* K}$ (noting that $K^* K \preceq I_{\mathcal{Z}_r}$) and

$$\Xi_K : \mathbf{L}(\mathcal{Z}_r) \to \mathbf{L}(\mathcal{Z}_r) : X \mapsto K X K^* + \bar{K} X \bar{K}^*,$$

which is a quantum channel as its Kraus representation $\{K, \bar{K}\}$ satisfies $K^* K + \bar{K}^* \bar{K} = I_{\mathcal{Z}_r}$. Since

$$\langle \psi(\tilde{S}, \tilde{B}) | \left(\bar{K} \otimes I_{\mathcal{W}_r} \right) | \psi(\tilde{T}, \tilde{B}) \rangle \langle \psi(\tilde{T}, \tilde{B}) | \left(\bar{K}^* \otimes I_{\mathcal{W}_r} \right) | \psi(\tilde{S}, \tilde{B}) \rangle \geq 0$$

for all K and all $\tilde{B}$, we have

$$\begin{aligned} \mathrm{F}_{\mathrm{r}}(S,T)^2 &\leq \max_{K} \min_{B} \langle \psi(\tilde{S}, \tilde{B}) | \left[\left(\Xi_K \otimes I_{\mathbf{L}(\mathcal{W}_r)} \right) \left(| \psi(\tilde{T}, \tilde{B}) \rangle \langle \psi(\tilde{T}, \tilde{B}) | \right) \right] | \psi(\tilde{S}, \tilde{B}) \rangle \\ &\leq \max_{\Xi} \min_{B} \langle \psi(\tilde{S}, \tilde{B}) | \left[\left(\Xi \otimes I_{\mathbf{L}(\mathcal{W}_r)} \right) \left(| \psi(\tilde{T}, \tilde{B}) \rangle \langle \psi(\tilde{T}, \tilde{B}) | \right) \right] | \psi(\tilde{S}, \tilde{B}) \rangle. \end{aligned} \tag{7}$$

However, we clearly have

$$\mathrm{F}_{\mathrm{r}}(S,T)^2 = \min_{B} \max_{\Xi} \langle \psi(\tilde{S}, \tilde{B}) | \left[\left(\Xi \otimes I_{\mathbf{L}(\mathcal{W}_r)} \right) \left(| \psi(\tilde{T}, \tilde{B}) \rangle \langle \psi(\tilde{T}, \tilde{B}) | \right) \right] | \psi(\tilde{S}, \tilde{B}) \rangle$$

due to Eqn. (5) and the fact that Uhlmann's Theorem also holds replacing unitaries with channels. Hence, the inequality (7) is in fact an equality due to the max–min inequality. ◀

3 Semidefinite programming formulation for strategy fidelity

In this section, we use Lemma 10 to prove Theorem 6. From Lemma 10, we have that

$$\mathrm{F}_{\mathrm{r}}(S,T)^2 = \max \{ \phi(K) : K \in \mathbf{K}(\mathcal{Z}_r) \}$$

where $\phi(K) := \min_{B} \Re \langle\!\langle \tilde{S} | (K \otimes B) | \tilde{T} \rangle\!\rangle$, and B is Bob's co-strategy. By defining

$$C := \frac{1}{2} \mathrm{Tr}_{\mathcal{Z}_r} \left((K \otimes I_{\mathcal{Y}_{1\ldots r} \mathcal{X}_{1\ldots r}}) | \tilde{T} \rangle\!\rangle \langle\!\langle \tilde{S} | \right) + \frac{1}{2} \left[\mathrm{Tr}_{\mathcal{Z}_r} \left((K \otimes I_{\mathcal{Y}_{1\ldots r} \mathcal{X}_{1\ldots r}}) | \tilde{T} \rangle\!\rangle \langle\!\langle \tilde{S} | \right) \right]^*$$

we can write

$$\phi(K) = \min_{B} \langle C, B \rangle.$$

From [13, Corollary 7], we know that B must satisfy $B = Q_r \otimes I_{\mathcal{Y}_r}$ for some $(Q_1, \ldots, Q_r)$ satisfying

$$\mathrm{Tr}(Q_1) = 1, \quad \mathrm{Tr}_{\mathcal{X}_i}(Q_i) = Q_{i-1} \otimes I_{\mathcal{Y}_{i-1}}, \text{ for } i \in \{2, \ldots, r\}$$

and $Q_1 \in \mathbf{Pos}(\mathcal{X}_1)$, $Q_i \in \mathbf{Pos}(\mathcal{Y}_{1\ldots i-1} \otimes \mathcal{X}_{1\ldots i})$, for $i \in \{2, \ldots, r\}$. Thus, $\phi(K)$ can be formulated as a semidefinite program. Its dual can be written as

$$\begin{aligned}\alpha(K) := \max \big\{\, t \;:\; & tI_{\mathcal{X}_1} \preceq \mathrm{Tr}_{\mathcal{Y}_1}(R_1),\ R_r \preceq C, \\ & R_j \otimes I_{\mathcal{X}_{j+1}} \preceq \mathrm{Tr}_{\mathcal{Y}_{j+1}}(R_{j+1}) \text{ for } j \in \{1, \ldots, r-1\} \,\big\},\end{aligned}$$

where $R_j \in \mathbf{Her}(\mathcal{Y}_{1\ldots j} \otimes \mathcal{X}_{1\ldots j})$. Since this has a strictly feasible solution, as does the primal, we know $\alpha(K) = \phi(K)$ by strong duality and $\alpha(K)$ attains an optimal solution. We now let $M = \begin{bmatrix} I_{\mathcal{Z}_r} & K \\ K^* & I_{\mathcal{Z}_r} \end{bmatrix}$ and set $M \succeq 0$ to get $\|K\| \leq 1$. We can check that C is a linear function in M (since M is Hermitian). Thus, we have that the strategy fidelity can be written as in Theorem 6.

4 Alice's cheating in interactive bit-commitment and oblivious string transfer

In this section we show that Alice can cheat with probability $\mathrm{F}_r(A^0, A^1)^2$ in either bit-commitment or oblivious string transfer. The cheating has the same flavour in both cases: Alice will follow the protocol honestly, then try to change her state as to make it look like she chose the other strategy from the beginning. Suppose Alice uses pure strategy $\tilde{A}^a$ and Bob uses pure co-strategy $\tilde{B}$. For brevity, define for each $a \in \{0, 1\}$ the following states

$$|\psi_a\rangle := |\psi(\tilde{A}^a, \tilde{B})\rangle \quad \text{and} \quad \sigma_a := (\Xi^a \otimes I_{\mathcal{W}_r})(|\psi_a\rangle\langle\psi_a|) \tag{8}$$

where Ξ_a is the strategy fidelity-achieving channel (from Definition 5) such that

$$\langle\psi_{\bar{a}}|\sigma_a|\psi_{\bar{a}}\rangle \geq \mathrm{F}_{\mathrm{r}}(A^0, A^1)^2. \tag{9}$$

Note that the aim of Ξ^a is to get σ_a as close as possible to $|\psi_{\bar{a}}\rangle\langle\psi_{\bar{a}}|$.

4.1 Bit-commitment

When we study interactive bit-commitment, we are applying the strategy/co-strategy formalism to *only* the commit phase. From the above discussion, Alice can create the state $\sigma_a \in \mathbf{Dens}(\mathcal{Z}_r \otimes \mathcal{W}_r)$ to try to change her commitment from a to $\bar{a}$. Then Alice continues her actions to "reveal" $\bar{a}$ in the Reveal Phase, as does Bob (even though Bob's actions are not specified to Alice). We just assume that this entire process is done by a unitary $U_{\bar{a}}$ acting on $\mathcal{Z}_r \otimes \mathcal{W}_r$. Then, Bob has a projective measurement $\{\Pi_{accept}, \Pi_{reject}\}$ which accepts $U_{\bar{a}}|\psi_{\bar{a}}\rangle$ with certainty, thus leading to a *non-destructive measurement*. Thus, we have

$$(I_{\mathcal{Z}_r} \otimes \Pi_{accept})U_{\bar{a}}|\psi_{\bar{a}}\rangle = U_{\bar{a}}|\psi_{\bar{a}}\rangle.$$

This implies that

$$(I_{\mathcal{Z}_r} \otimes \Pi_{accept}) \succeq U_{\bar{a}}|\psi_{\bar{a}}\rangle\langle\psi_{\bar{a}}|U_{\bar{a}}^*.$$

However, Alice's actions have led to them sharing $U_{\bar{a}}\sigma_a U_{\bar{a}}^*$ at the end of the protocol. So, we have that Alice successfully reveals $\bar{a}$ with probability

$$\mathrm{A}_{\mathrm{BC}} \geq \langle I_{\mathcal{Z}_r} \otimes \Pi_{accept}, U_{\bar{a}}\sigma_a U_{\bar{a}}^*\rangle \geq \langle U_{\bar{a}}|\psi_{\bar{a}}\rangle\langle\psi_{\bar{a}}|U_{\bar{a}}^*, U_{\bar{a}}\sigma_a U_{\bar{a}}^*\rangle = \langle|\psi_{\bar{a}}\rangle\langle\psi_{\bar{a}}|, \sigma_a\rangle \geq \mathrm{F}_r(A^0, A^1)^2$$

using Eqn. (9), as desired.

4.2 Oblivious string transfer

We can assume Alice uses a projective measurement $\{\Pi_z^a\}$ to learn her desired string. Note that since x_a is learned with certainty, this is a *non-destructive measurement*, as in the bit-commitment analysis above. That is, we have

$$\left(\Pi_{x_a}^a \otimes I_{\mathcal{W}_r}\right) |\psi(\tilde{A}^a, \tilde{B}^{x_0,x_1})\rangle = |\psi(\tilde{A}^a, \tilde{B}^{x_0,x_1})\rangle$$

for all a and (x_0, x_1). Again, this implies

$$\Pi_{x_a}^a \otimes I_{\mathcal{W}_r} \succeq |\psi(\tilde{A}^a, \tilde{B}^{x_0,x_1})\rangle\langle\psi(\tilde{A}^a, \tilde{B}^{x_0,x_1})|. \tag{10}$$

Thus, after learning x_a, she can create the state σ_a (defined above) to try to learn $x_{\bar{a}}$. (Here, the $\tilde{B}$ in the definition of σ_a is $\tilde{B}^{x_0,x_1}$.) Then she measures as if she had used pure strategy $\tilde{A}^{\bar{a}}$ (that is, using $\{\Pi_z^{\bar{a}}\}$) to try to learn $x_{\bar{a}}$. Then, using (10) and the definitions in (8), we have

$$\mathrm{A_{OT}} \geq \langle \Pi_{x_{\bar{a}}}^{\bar{a}} \otimes I_{\mathcal{W}_r}, \sigma_a \rangle \geq \langle \psi_{\bar{a}} | \sigma_a | \psi_{\bar{a}} \rangle \geq \mathrm{F_r}(A^0, A^1)^2,$$

as desired.

References

1 Andris Ambainis, Harry Buhrman, Yevgeniy Dodis, and Hein Röhrig. Multiparty quantum coin flipping. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259. IEEE Computer Society, 2004. doi:10.1109/CCC.2004.19.

2 Viacheslav P. Belavkin, Giacomo Mauro D'Ariano, and Maxim Raginsky. Operational distance and fidelity for quantum channels. *Journal of Mathematical Physics*, 46(6):062106, 2005. arXiv:quant-ph/0408159.

3 Charles Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. IEEE Computer Society, 1984.

4 André Chailloux, Gus Gutoski, and Jamie Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chicago Journal of Theoretical Computer Science*, 2016.

5 André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *Proceedings of the 50th IEEE Symposium on Foundations of Computer Science*, FOCS 2009, pages 527–533, 2009. arXiv:0904.1511 [quant-ph].

6 André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In Rafail Ostrovsky, editor, *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 354–362. IEEE Computer Society, 2011. doi:10.1109/FOCS.2011.42.

7 André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for quantum oblivious transfer. *Quantum Information and Computation*, 13(1&2):158–177, 2013. arXiv:1007.1875 [quant-ph].

8 André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Strong connections between quantum encodings, nonlocality, and quantum cryptography. *Phys. Rev. A*, 89:022334, 2014. arXiv:1304.0983 [quant-ph].

9 Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Physical Review A*, 80(2):022339, 2009. arXiv:0904.4483 [quant-ph].

10 Giulio Chiribella, Giacomo Mauro D'Ariano, Paolo Perinotti, Dirk Schlingemann, and Reinhard F. Werner. A short impossibility proof of quantum bit commitment. *Physics Letters A*, 377(15):1076–1087, 2013. arXiv:0905.3801v1 [quant-ph].

11 Gus Gutoski. *Quantum strategies and local operations*. PhD thesis, University of Waterloo, 2009. arXiv:1003.0038 [quant-ph].

12 Gus Gutoski. On a measure of distance for quantum strategies. *Journal of Mathematical Physics*, 53(3):032202, 2012. arXiv:1008.4636 [quant-ph].

13 Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the 39th ACM Symposium on Theory of Computing (STOC 2007)*, pages 565–574, 2007. arXiv:quant-ph/0611234.

14 Iordanis Kerenidis and Ashwin Nayak. Weak coin flipping with small bias. *Information Processing Letters*, 89(3):131–135, 2004. arXiv:quant-ph/0206121. doi:10.1016/j.ipl.2003.07.007.

15 Alexei Kitaev. Quantum coin-flipping. Presentation at the 6th Workshop on *Quantum Information Processing* (QIP 2003), 2002.

16 Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997. doi:10.1103/PhysRevLett.78.3410.

17 Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1–2):177–187, 1998. Proceedings of the Fourth Workshop on Physics and Consumption. doi:10.1016/S0167-2789(98)00053-0.

18 Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, 1997. doi:10.1103/PhysRevLett.78.3414.

19 Ashwin Nayak and Peter Shor. Bit-commitment based quantum coin flipping. *Physical Review A*, 67(1):012304, 2003. arXiv:quant-ph/0206123. doi:10.1103/PhysRevA.67.012304.

20 Ashwin Nayak, Jamie Sikora, and Levent Tunçel. Quantum and classical coin-flipping protocols based on bit-commitment and their point games. Available as arXiv.org e-Print quant-ph/1504.04217, 2015.

21 Ashwin Nayak, Jamie Sikora, and Levent Tunçel. A search for quantum coin-flipping protocols using optimization techniques. *Mathematical Programming*, 156(1):581–613, 2016.

22 Jamie Sikora. Simple, near-optimal quantum protocols for die-rolling. In *Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, pages 1–14, 2016.

23 Robert W. Spekkens and Terence Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65:012310, 2001. doi:10.1103/PhysRevA.65.012310.

24 A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

25 Salil P. Vadhan. An unconditional study of computational zero knowledge. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, pages 176–185. IEEE Computer Society, 2004. doi:10.1109/FOCS.2004.13.

26 John Watrous. Semidefinite programs for completely bounded norms. *Theory of Computing*, 5:217–238, 2009. arXiv:0901.4709v2 [quant-ph].

27 John Watrous. Simpler semidefinite programs for completely bounded norms. *Chicago Journal of Theoretical Computer Science*, 2013.

28 Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. doi:10.1145/1008908.1008920.