Noname manuscript No.
(will be inserted by the editor)

A search for quantum coin-flipping protocols using optimization techniques - SUPPLEMENTAL MATERIAL

Ashwin Nayak · Jamie Sikora · Levent Tunçel

Received: date / Accepted: date

Contents

1 An example protocol

Here we describe a construction of strong coin-flipping protocols based on quantum *bit-commitment* [1], [3], [11], [6] that consists of three messages. First, Alice chooses a uniformly random bit a, creates a state of the form

$$\psi_a \in \mathbb{C}^A \otimes \mathbb{C}^{A'}$$

A. Nayak
Department of Combinatorics and Optimization, and Institute for Quantum Computing, University of Waterloo. Address: 200 University Ave. W., Waterloo, ON, N2L 3G1, Canada.
Tel.: +1 519 888-4567 extension 33601
E-mail: ashwin.nayak@uwaterloo.ca

J. Sikora
Centre for Quantum Technologies, National University of Singapore. Address: Block S15, 3 Science Drive 2, Singapore 117543.
E-mail: cqtjwjs@nus.edu.sg

L. Tunçel
Department of Combinatorics and Optimization, University of Waterloo. Address: 200 University Ave. W., Waterloo, ON, N2L 3G1, Canada.
Tel.: +1 519 888-4567 ext. 35598
E-mail: ltuncel@uwaterloo.ca

and sends A to Bob, i.e., the first message consists of qubits corresponding to the space $\mathbb{C}^A$. (For ease of exposition, we use this language throughout, i.e., refer to qubits by the labels of the corresponding spaces.) This first message is the *commit stage* since she potentially gives some information about the bit a, for which she may be held accountable later. Then Bob chooses a uniformly random bit b and sends it to Alice. Alice then sends a and A' to Bob. Alice's last message is the *reveal stage*. Bob checks to see if the qubits he received are in state ψ_a (we give more details about this step below). If Bob is convinced that the state is correct, they both output 0 when $a = b$, or 1 if $a \neq b$, i.e., they output the XOR of a and b.

This description can be cast in the form of a quantum protocol as presented in [7]: we can encode 0 as basis state e_0 and 1 as e_1, we can simulate the generation of a uniformly random bit by preparing a uniform superposition over the two basis states, and we can "send" qubits by permuting their order (a unitary operation) so that they are part of the message subsystem. In fact, we can encode an entirely classical protocol using a quantum one in this manner.

We present a protocol from [6] which follows the above framework.

Definition 1 (Coin-flipping protocol example)
Let $A := \{0, 1, 2\}$, $A' := A$, and let $\mathbb{C}^A$ and $\mathbb{C}^{A'}$ be spaces for Alice's two messages.

- Alice chooses $a \in \{0, 1\}$ uniformly at random and creates the state
$$\psi_a = \frac{1}{\sqrt{2}}\, e_a \otimes e_a + \frac{1}{\sqrt{2}}\, e_2 \otimes e_2 \in \mathbb{C}^A \otimes \mathbb{C}^{A'},$$
where $\{e_0, e_1, e_2\}$ are standard basis vectors. Alice sends the A part of ψ_a to Bob.
- Bob chooses $b \in \{0, 1\}$ uniformly at random and sends it to Alice.
- Alice reveals a to Bob and sends the rest of ψ_a, i.e., she sends A'.
- Bob checks to see if the state sent by Alice is ψ_a, i.e., he checks to see if Alice has tampered with the state during the protocol. The measurement on $\mathbb{C}^A \otimes \mathbb{C}^{A'}$ corresponding to this check is
$$(\Pi_{\text{accept}} := \psi_a \psi_a^*, \quad \Pi_{\text{abort}} := \mathrm{I} - \Pi_{\text{accept}}).$$
If the measurement outcome is "abort" then Bob aborts the protocol.
- Each player outputs the XOR of the two bits, i.e., Alice outputs $a \oplus b'$, where b' is the bit she received in the second round, and if he does not abort, Bob outputs $a' \oplus b$, where a' is the bit received by him in the third round.

In the honest case, Bob does not abort since $\langle \Pi_{\text{abort}}, \psi_a \psi_a^* \rangle = 0$. Furthermore, Alice and Bob get the same outcome which is uniformly random. Therefore, this is a well-defined coin-flipping protocol. We now sketch a proof that this protocol has bias $\epsilon = 1/4$.

Bob cheating. We consider the case when Bob cheats towards 0; the analysis of cheating towards 1 is similar. If Bob wishes to maximize the probability of outcome 0, he has to maximize the probability that the bit b he sends equals a. In other words, he may only cheat by measuring Alice's first message to try to learn a, then choose b suitably to force the desired outcome. Define $\rho_a := \mathrm{Tr}_{A'}(\psi_a \psi_a^*)$. This is the reduced state of the A-qubits Bob has after the first message. Recall Bob can learn the value of a with probability

$$\frac{1}{2} + \frac{1}{2}\Delta(\rho_0, \rho_1) = 3/4 \ ,$$

and this bound can be achieved. This strategy is independent of the outcome Bob desires, thus $P^*_{\mathrm{B},0} = P^*_{\mathrm{B},1} = 3/4$.

Alice cheating. Alice's most general cheating strategy is to send a state in the first message such that she can decide the value of a after receiving b, and yet pass Bob's cheat detection step with maximum probability. For example, if Alice wants outcome 0 then she returns $a = b$ and if she wants outcome 1, she returns $a = \bar{b}$. Alice always gets the desired outcome as long as Bob does not detect her cheating. As a primer for more complicated protocols, we show an SDP formulation for a cheating Alice based on the above cheating strategy description. There are three important quantum states to consider here. The first is Alice's first message, which we denote as $\sigma \in \mathbb{S}^A_+$. The other two states are the states Bob has at the end of the protocol depending on whether $b = 0$ or $b = 1$, we denote them by $\sigma_b \in \mathbb{S}^{A \otimes A'}_+$. Note that $\mathrm{Tr}_{A'}(\sigma_0) = \mathrm{Tr}_{A'}(\sigma_1) = \sigma$ since they are consistent with the first message σ—Alice does not know b when σ is sent. However, they could be different on A' because Alice may apply some quantum operation depending upon b before sending the A' qubits. Then Alice can cheat with probability given by the optimal objective value of the following SDP:

$$\begin{array}{rrl} & \sup \ \frac{1}{2}\langle \psi_0 \psi_0^*, \sigma_0 \rangle + \frac{1}{2}\langle \psi_1 \psi_1^*, \sigma_1 \rangle & \\ \text{subject to} & \mathrm{Tr}_{A'}(\sigma_b) = \sigma, & \text{for all } b \in \{0,1\}, \\ & \mathrm{Tr}(\sigma) = 1, & \\ & \sigma \in \mathbb{S}^A_+, & \\ & \sigma_b \in \mathbb{S}^{A \otimes A'}_+, & \text{for all } b \in \{0,1\}, \end{array}$$

recalling that the partial trace is trace-preserving, any unit trace, positive semidefinite matrix represents a valid quantum state, and that two purifications of the same density matrix are related to each other by a unitary transformation on the part that is traced out.

It has been shown [11], [3], [9] that the optimal objective function value of this problem is

$$\frac{1}{2} + \frac{1}{2}\sqrt{\mathrm{F}(\rho_0, \rho_1)} = 3/4$$

given by the optimal solution $(\sigma_0, \sigma_1, \sigma) = (\psi\psi^*, \psi\psi^*, \mathrm{Tr}_{A'}(\psi\psi^*))$, where

$$\psi = \sqrt{\frac{1}{6}}\, e_0 \otimes e_0 + \sqrt{\frac{1}{6}}\, e_1 \otimes e_1 + \sqrt{\frac{2}{3}}\, e_2 \otimes e_2 \ .$$

Therefore, the bias of this protocol is

$$\max\{P^*_{\mathrm{A},0}, P^*_{\mathrm{A},1}, P^*_{\mathrm{B},0}, P^*_{\mathrm{B},1}\} - 1/2 = 3/4 - 1/2 = 1/4.$$

Using the Fuchs-van de Graaf inequalities [5], it was shown in [3] that for any ρ_0 and ρ_1, we have

$$\max\left\{\frac{1}{2} + \frac{1}{2}\sqrt{\mathrm{F}(\rho_0, \rho_1)}, \frac{1}{2} + \frac{1}{2}\Delta(\rho_0, \rho_1)\right\} - 1/2 \quad \geq \quad 1/4 \ .$$

Thus, we cannot improve the bias by simply changing the starting states in this type of protocol, suggesting a substantial change of the form of the protocol is necessary to find a smaller bias.

2 SDP characterization of cheating strategies

We start by formulating strategies for cheating Bob and cheating Alice as semidefinite programs as proposed by Kitaev [7] restricting to the protocols examined in this paper. The communication of such a protocol is depicted in Figure 1, below.

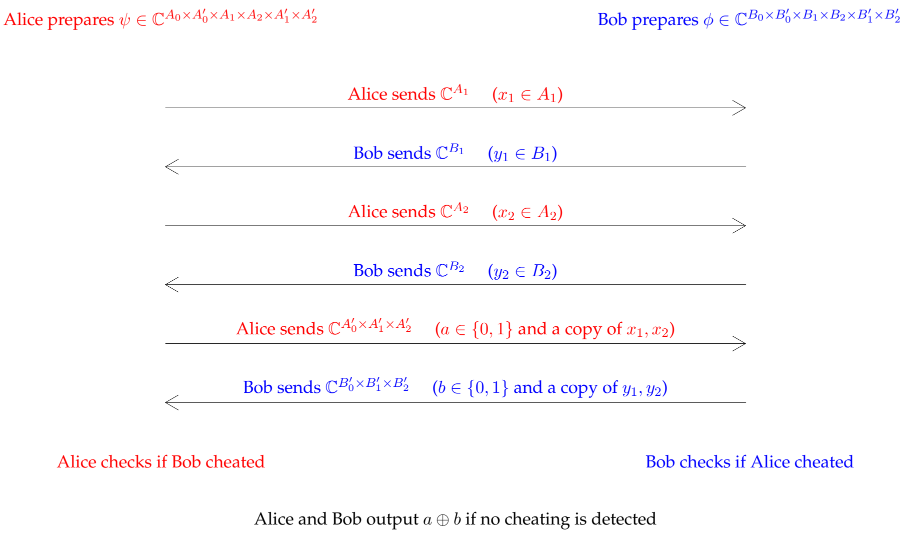

Fig. 1 A six-round protocol.

The extent to which Bob can cheat is captured by the following lemma.

Lemma 1 *The maximum probability with which cheating Bob can force honest Alice to accept $c \in \{0, 1\}$ is given by the optimal objective value of the following*

SDP*:*

$$
\begin{array}{rl}
\sup & \langle\, \rho_F, \Pi_{\mathrm{A},c}\,\rangle \\
\text{s.t.} & \mathrm{Tr}_{B_1}(\rho_1) = \mathrm{Tr}_{A_1}\,(\psi\psi^*)\,, \\
& \mathrm{Tr}_{B_j}(\rho_j) = \mathrm{Tr}_{A_j}(\rho_{j-1}),\;\; \forall j \in \{2,\dots,n\}, \\
& \mathrm{Tr}_{B'\times B'_0}(\rho_F) = \mathrm{Tr}_{A'\times A'_0}(\rho_n), \\
& \rho_j \in \mathbb{S}_+^{A_0\times A'_0\times B_1\times\cdots\times B_j\times A_{j+1}\times\cdots\times A_n\times A'},\;\; \forall j\in\{1,\dots,n\}, \\
& \rho_F \in \mathbb{S}_+^{A_0\times B'_0\times B\times B'}.
\end{array}
$$

Furthermore, an optimal cheating strategy for Bob may be derived from an optimal feasible solution of this SDP*.*

Proof The matrix constraints in the SDP may readily be rewritten as linear constraints on the variables ρ_j, so the optimization problem is an SDP. The variables are the density matrices of qubits under Alice's control after each of Bob's messages. The partial trace is trace-preserving, so any feasible solution satisfies

$$\mathrm{Tr}(\rho_F) = \mathrm{Tr}(\rho_n) = \cdots = \mathrm{Tr}(\rho_1) = \mathrm{Tr}(\psi\psi^*) = 1.$$

Since $\rho_1, \dots, \rho_n, \rho_F$ are constrained to be positive semidefinite, they are quantum states.

Bob sends the B_1 qubits to Alice replacing the A_1 part already sent to him. Being the density matrix Alice has after Bob's first message, ρ_1 satisfies

$$\mathrm{Tr}_{B_1}(\rho_1) = \mathrm{Tr}_{A_1}(\psi\psi^*),$$

since the state of the qubits other than those in A_1, B_1 remains unchanged. Similarly, we have the constraint

$$\mathrm{Tr}_{B_j}(\rho_j) = \mathrm{Tr}_{A_j}(\rho_{j-1}), \quad \text{for} \quad j \in \{2,\dots,n\},$$

for each ρ_j after Bob's j'th message. Also ρ_F, the state Alice has at the end of the protocol, satisfies

$$\mathrm{Tr}_{B'\times B'_0}(\rho_F) = \mathrm{Tr}_{A'\times A'_0}(\rho_n).$$

She then measures ρ_F and accepts c with probability $\langle \rho_F, \Pi_{\mathrm{A},c}\rangle$.

These constraints are necessary conditions on the states under Alice's control. We may further restrict the states to be real matrices: the real parts of any complex feasible solution also form a feasible solution with the same objective function value.

We now show that every feasible solution to the above problem yields a valid cheating strategy for Bob with success probability equal to the objective function value of the feasible solution. He can find such a strategy by maintaining a purification of each density matrix in the feasible solution. For example, suppose the protocol starts in the state $\eta := \psi \otimes \phi'$, where $\phi' \in \mathbb{C}^K := \mathbb{C}^{B_0} \otimes \mathbb{C}^{B'_0} \otimes \mathbb{C}^{B} \otimes \mathbb{C}^{B'} \otimes \mathbb{C}^{K'}$ where $\mathbb{C}^{K'}$ is extra space Bob uses to cheat. Consider $\tau \in \mathbb{C}^{A_0} \otimes \mathbb{C}^{A'_0} \otimes \mathbb{C}^{A} \otimes \mathbb{C}^{A'} \otimes \mathbb{C}^{K}$ a purification of ρ_1. Since $\mathrm{Tr}_{B_1}(\rho_1) = \mathrm{Tr}_{A_1}(\psi\psi^*)$, we have

$$\mathrm{Tr}_{A_1\times K}(\tau\tau^*) = \mathrm{Tr}_{B_1}(\rho_1) = \mathrm{Tr}_{A_1}(\psi\psi^*) = \mathrm{Tr}_{A_1\times K}(\eta\eta^*).$$

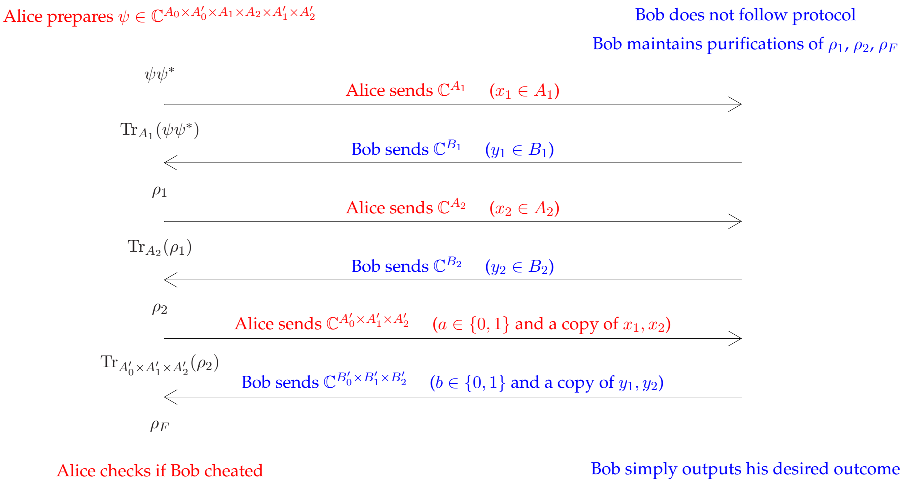

Fig. 2 Bob cheating in a six-round protocol.

Thus, there exists a unitary U which acts on $\mathbb{C}^{A_1} \otimes \mathbb{C}^K$ which maps η to τ. If Bob applies this unitary after Alice's first message and sends the B_1 qubits back then he creates ρ_1 under Alice's control. The same argument can be applied to the remaining constraints.

The states corresponding to honest Bob yield a feasible solution. Attainment of an optimal solution then follows from continuity of the objective function and from the compactness of the feasible region. An optimal solution yields an optimal cheating strategy. $\square$

We call the SDP in Lemma 1 Bob's cheating SDP and depict Bob cheating, and the context of the SDP variables, in a six-round protocol in Figure 2, above.

In a similar fashion, we can formulate Alice's cheating SDP.

Lemma 2 *The maximum probability with which cheating Alice can force honest Bob to accept $c \in \{0,1\}$ is given by the optimal objective value of the following* SDP*:*

$$
\begin{array}{lrcl}
\sup & \multicolumn{3}{l}{\left\langle \sigma_F, \Pi_{\mathrm{B},c} \otimes \mathrm{I}_{B_0' \times B'} \right\rangle} \\
\text{s.t.} & \mathrm{Tr}_{A_1}(\sigma_1) & = & \phi\phi^*, \\
& \mathrm{Tr}_{A_2}(\sigma_2) & = & \mathrm{Tr}_{B_1}(\sigma_1), \\
& & \vdots & \\
& \mathrm{Tr}_{A_n}(\sigma_n) & = & \mathrm{Tr}_{B_{n-1}}(\sigma_{n-1}), \\
& \mathrm{Tr}_{A' \times A_0'}(\sigma_F) & = & \mathrm{Tr}_{B_n}(\sigma_n), \\
& \sigma_j & \in & \mathbb{S}_+^{B_0 \times B_0' \times A_1 \times \cdots \times A_j \times B_j \times \cdots \times B_n \times B'}, \forall j \in \{1, \ldots, n\}, \\
& \sigma_F & \in & \mathbb{S}_+^{B_0 \times B_0' \times A_0' \times A \times A' \times B'}.
\end{array}
$$

Furthermore, we may derive an optimal cheating strategy for Alice from an optimal feasible solution to this SDP*.*

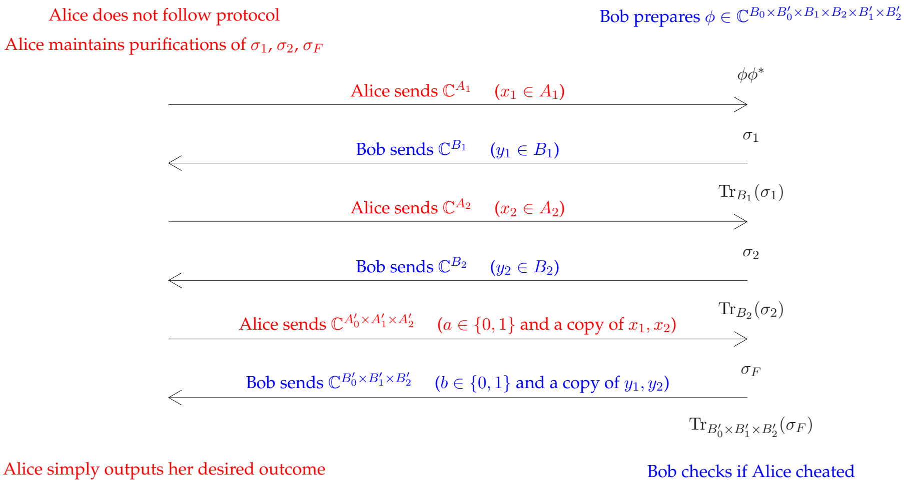

Fig. 3 Alice cheating in a six-round protocol.

The characterization of Alice's cheating strategies is almost the same as that for cheating Bob; we only sketch the parts that are different.

Proof There are two key differences from the proof of Lemma 1. One is that Alice sends the first message and Bob sends the last, explaining the slightly different constraints. Secondly, Bob measures only the $\mathbb{C}^{B_0} \otimes \mathbb{C}^{A_0'} \otimes \mathbb{C}^{A} \otimes \mathbb{C}^{A'}$ part of his state after Alice's last message, i.e., he measures $\mathrm{Tr}_{B_0' \times B'}(\sigma_F)$. Note that the adjoint of the partial trace can be written as

$$\mathrm{Tr}^*_{B_0' \times B'}(Y) = Y \otimes \mathrm{I}_{B_0' \times B'}.$$

Therefore we have $\langle \mathrm{Tr}_{B_0' \times B'}(\sigma_F), \mathit{\Pi}_{\mathrm{B},c} \rangle = \langle \sigma_F, \mathit{\Pi}_{\mathrm{B},c} \otimes \mathrm{I}_{B_0' \times B'} \rangle$, which explains the objective function. $\square$

We depict Alice cheating, and the context of her SDP variables, in a six-round protocol in Figure 3 above.

Analyzing and solving these problems computationally gets increasingly difficult and time consuming as n increases, since the dimension of the variables increases exponentially in n. This is precisely why we develop the reduced problems which are conceptually simpler and much easier to solve numerically.

3 Derivations of the reduced SDPs

We now show the derivation of Alice's reduced cheating strategies (the derivation of Bob's is very similar and the arguments are the same). We show that if we are given an optimal solution to Alice's cheating SDP, then we can assume it has a special form while retaining the same objective function value. Then we show this special form for an optimal solution can be written in the way desired.

We now discuss some of the tools used in the upcoming proofs.

Lemma 3 *Suppose A is a finite set. Suppose $p = \sum_{x \in A} p_x \, e_x \otimes e_x \in \mathrm{Prob}^{A \times A}$ and $\sigma \in \mathbb{S}_+^A$ is a density matrix. Then we have*

$$\max_{\rho \in \mathbb{S}_+^{A \times A}} \left\{ \langle \sqrt{p}\sqrt{p}^{\mathrm{T}}, \rho \rangle : \mathrm{Tr}_A(\rho) = \sigma \right\} \leq \max_{\rho \in \mathbb{S}_+^{A \times A}} \left\{ \langle \sqrt{p}\sqrt{p}^{\mathrm{T}}, \rho \rangle : \mathrm{Tr}_A(\rho) = \mathrm{Diag}(\sigma) \right\},$$

where Diag *restricts to the diagonal of a square matrix. Moreover, an optimal solution to the problem on the right is $\overline{\rho} := \sqrt{q}\sqrt{q}^{\mathrm{T}}$, where*

$$q = \sum_{x \in A} [\sigma]_{x,x} \, e_x \otimes e_x \in \mathrm{Prob}^{A \times A},$$

yielding an objective function value of $\mathrm{F}(p, q)$.

Proof Consider $\bar{\rho}$ as defined in the statement of the lemma. Since we have $\mathrm{Tr}_A(\bar{\rho}) = \mathrm{Diag}(\sigma)$, it suffices to show that for any density matrix $\rho \in \mathbb{S}_+^{A \times A}$ satisfying either $\mathrm{Tr}_A(\rho) = \sigma$ or $\mathrm{Tr}_A(\rho) = \mathrm{Diag}(\sigma)$, we have

$$\left\langle \sqrt{p}\sqrt{p}^{\mathrm{T}}, \rho \right\rangle \leq \left\langle \sqrt{p}\sqrt{p}^{\mathrm{T}}, \bar{\rho} \right\rangle = \mathrm{F}(p, q).$$

Expanding the first inner product, and using the Cauchy-Schwartz inequality, we get

$$\begin{aligned} \left\langle \sqrt{p}\sqrt{p}^{\mathrm{T}}, \rho \right\rangle &= \sum_{x,y \in A} \sqrt{p_x p_y} (e_x \otimes e_x)^{\mathrm{T}} \rho \, (e_y \otimes e_y) \\ &\leq \sum_{x,y \in A} \sqrt{p_x p_y} \, \| \sqrt{\rho} \, (e_x \otimes e_x) \| \cdot \| \sqrt{\rho} \, (e_y \otimes e_y) \| \, . \end{aligned}$$

We can simplify this by noting

$$\begin{aligned} \| \sqrt{\rho} \, (e_x \otimes e_x) \|^2 &= (e_x \otimes e_x)^{\mathrm{T}} \rho \, (e_x \otimes e_x) \\ &\leq \sum_{z \in A} (e_z \otimes e_x)^{\mathrm{T}} \rho \, (e_z \otimes e_x) \\ &= e_x^{\mathrm{T}} \mathrm{Tr}_A(\rho) e_x \\ &= [\sigma]_{x,x} \end{aligned}$$

implying

$$\left\langle \sqrt{p}\sqrt{p}^{\mathrm{T}}, \rho \right\rangle \leq \sum_{x,y \in A} \sqrt{p_x p_y} \left([\sigma]_{x,x} [\sigma]_{y,y} \right)^{\frac{1}{2}} = \left(\sum_{x \in A} \sqrt{p_x [\sigma]_{x,x}} \right)^2 = \mathrm{F}(p, q),$$

as desired. □

Definition 2 We define the *partial* Diag *operator* over the subspace $\mathbb{C}^A$, denoted Diag_A, as the operator that projects density matrices over $\mathbb{C}^B \otimes \mathbb{C}^A$ onto the diagonal only on the subspace $\mathbb{C}^A$:

$$\mathrm{Diag}_A(\rho) \quad = \quad \sum_{x \in A} (\mathrm{I}_B \otimes e_x^{\mathrm{T}})\, \rho\, (\mathrm{I}_B \otimes e_x) \otimes e_x e_x^{\mathrm{T}}.$$

We may write Diag_A as the superoperator $\mathbb{I} \otimes \mathrm{Diag}_A$, where $\mathbb{I}$ is the identity superoperator acting on the rest of the space. Similarly, we may write the partial trace over A as the superoperator $\mathrm{Tr}_A := \mathbb{I} \otimes \mathrm{Tr}(\cdot)$ where $\mathrm{Tr}(\cdot)$ acts only on $\mathbb{C}^A$. Using this perspective, we see that the partial trace and the partial Diag operators commute when they act on different subspaces. Also, $\mathrm{Tr}_A \circ \mathrm{Diag}_A = \mathrm{Tr}_A$ since the trace only depends on the diagonal elements.

We also make use of the following lemma.

Lemma 4 *Consider a matrix $\rho \in \mathbb{S}_+^{A \times B}$. If $\mathrm{Tr}_A(\rho) = \psi\psi^*$ for some vector $\psi \in \mathbb{C}^B$, then ρ can be written as $\rho = \tilde{\rho} \otimes \psi\psi^*$, for some $\tilde{\rho} \in \mathbb{S}_+^A$.*

This is easily proven using the fact that the half-line emanating through a rank one positive semidefinite matrix forms an extreme ray of the cone of positive semidefinite matrices, or more directly by expressing ρ using an orthogonal basis for $\mathbb{C}^B$ that includes ψ.

3.1 Derivation of Alice's reduced cheating strategies

Assume $(\sigma_1, \sigma_2, \ldots, \sigma_n, \sigma_F)$ is optimal for Alice's cheating SDP. We now define new variables $(\sigma_1', \sigma_2', \ldots, \sigma_n', \sigma_F')$ from this optimal solution as

$$(\sigma_1, \mathrm{Diag}_{B_1'}(\sigma_2), \ldots, \mathrm{Diag}_{B_1' \times \cdots \times B_{n-1}'}(\sigma_n), \mathrm{Diag}_{B' \times A_0'}(\sigma_F))$$

and show it is also optimal. All we need to show is feasibility since the objective function value is preserved because $\Pi_{\mathrm{B},c} \otimes \mathrm{I}_{B_0' \times B'}$ is diagonal in the space $\mathbb{S}_+^{B' \times A_0'}$. The context of this "reduced strategy" is very simple, Alice simply changes the probability of which the next message is chosen, controlled on the messages sent and received so far (doing so in superposition). This is a very simple form, Alice's cheating is certainly not limited to such a strategy. However, here we show that such a strategy is optimal.

The first constraint is satisfied since $\sigma_1' = \sigma_1$ is part of a feasible solution. From Lemma 4, we can write $\sigma_1' = \phi\phi^* \otimes \tilde{\sigma}_1$ for some $\tilde{\sigma}_1 \in \mathbb{S}_+^{A_1}$. We can write

$$\mathrm{Tr}_{B_1}(\sigma_1') = \sum_{y_1 \in B_1'} e_{y_1} e_{y_1}^* \otimes \phi_{y_1} \phi_{y_1}^* \otimes \tilde{\sigma}_1,$$

where

$$\phi_{y_1,\ldots,y_j} := \sum_{b \in B_0} \sum_{y_{j+1} \in B_{j+1}'} \cdots \sum_{y_n \in B_n'} \frac{1}{\sqrt{2}} \sqrt{\beta_{b,y}}\, e_b \otimes e_b \otimes e_{y_{j+1}} \otimes e_{y_{j+1}} \otimes \cdots \otimes e_{y_n} \otimes e_{y_n},$$

which is in $\mathbb{C}^{B_0\times B_0'\times B_{j+1}\times B_{j+1}'\times\cdots\times B_n\times B_n'}$. Therefore, $\mathrm{Tr}_{B_1}(\sigma_1')$ is diagonal in B_1' and

$$\begin{aligned}\mathrm{Tr}_{B_1}(\sigma_1') &= \mathrm{Diag}_{B_1'}(\mathrm{Tr}_{B_1}(\sigma_1'))\\ &= \mathrm{Diag}_{B_1'}(\mathrm{Tr}_{B_1}(\sigma_1))\\ &= \mathrm{Diag}_{B_1'}(\mathrm{Tr}_{A_2}(\sigma_2))\\ &= \mathrm{Tr}_{A_2}(\sigma_2'). \end{aligned} \tag{1}$$

Therefore, the second constraint is satisfied. Since σ_2' is diagonal in B_1' we can write it as

$$\sigma_2' = \sum_{y_1\in B_1'} e_{y_1}e_{y_1}^*\otimes\sigma_{2,y_1}, \text{for some } \sigma_{2,y_1}\in\mathbb{S}_+^{B_0\times B_0'\times A_1\times A_2\times B_2\times\cdots\times B_n\times B_2'\times\cdots\times B_n'}.$$

By feasibility,

$$\mathrm{Tr}_{A_2}(\sigma_2')=\sum_{y_1\in B_1'} e_{y_1}e_{y_1}^*\otimes \mathrm{Tr}_{A_2}(\sigma_{2,y_1})=\mathrm{Tr}_{B_1}(\sigma_1')=\sum_{y_1\in B_1'} e_{y_1}e_{y_1}^*\otimes\phi_{y_1}\phi_{y_1}^*\otimes\tilde{\sigma}_1,$$

therefore $\sigma_2' = \sum_{y_1\in B_1'} e_{y_1}e_{y_1}^*\otimes\phi_{y_1}\phi_{y_1}^*\otimes\tilde{\sigma}_{2,y_1}$, where $\tilde{\sigma}_{2,y_1}\in\mathbb{S}_+^{B_0\times B_0'\times A_1\times A_2}$ satisfies $\mathrm{Tr}_{A_2}(\tilde{\sigma}_{2,y_1})=\tilde{\sigma}_1$ for all $y_1\in B_1'$. Using similar arguments, we may show that the rest of the first n constraints are satisfied. For every $j\in\{3,\ldots,n\}$, we have

$$\sigma_j' = \sum_{y_1\in B_1'}\cdots\sum_{y_{j-1}\in B_{j-1}'} e_{y_1}e_{y_1}^*\otimes\cdots\otimes e_{y_{j-1}}e_{y_{j-1}}^*\otimes\phi_{y_1,\ldots,y_{j-1}}\phi_{y_1,\ldots,y_{j-1}}^*\otimes\tilde{\sigma}_{j,y_1,\ldots,y_{j-1}},$$

where

$$\tilde{\sigma}_{j,y_1,\ldots,y_{j-1}}\in\mathbb{S}_+^{B_0\times B_0'\times A_1\times\cdots\times A_j} \text{ satisfies } \mathrm{Tr}_{A_j}(\tilde{\sigma}_{j,y_1,\ldots,y_{j-1}})=\tilde{\sigma}_{j-1,y_1,\ldots,y_{j-2}}$$

for each $y_1\in B_1',\ldots,y_{j-1}\in B_{n-1}'$. Note that

$$\mathrm{Tr}_{B_n}(\sigma_n') = \sum_{y\in B'} e_ye_y^*\otimes\phi_y\phi_y^*\otimes\tilde{\sigma}_{n,y_1,\ldots,y_{n-1}}$$

which is helpful in proving feasibility of the last constraint. For the last constraint, we can use a similar reduction as in Equation (1) to show σ_F' satisfies $\mathrm{Tr}_{A'\times A_0'}(\sigma_F')=\mathrm{Tr}_{B_n}(\sigma_n')$ proving $(\sigma_1',\ldots,\sigma_n',\sigma_F')$ is feasible. We now use this feasible solution to simplify the problem.

We can clean up σ_F' by noting that it is diagonal in $\mathbb{C}^{B'}$ and $\mathbb{C}^{A_0'}$ and write it as

$$\sigma_F' = \sum_{a\in A_0'}\sum_{y\in B'} e_ae_a^*\otimes e_ye_y^*\otimes\sigma_{F,a,y}, \quad \text{for some} \quad \sigma_{F,a,y}\in\mathbb{S}_+^{B_0\times B_0'\times A\times A'}.$$

Thus,

$$\mathrm{Tr}_{A'\times A_0'}(\sigma_F')=\sum_{a\in A_0'}\sum_{y\in B'} e_ye_y^*\otimes\mathrm{Tr}_{A'}(\sigma_{F,a,y})=\sum_{y\in B'} e_ye_y^*\otimes\left(\sum_{a\in A_0'}\mathrm{Tr}_{A'}(\sigma_{F,a,y})\right).$$

Similarly, by feasibility, we have

$$\mathrm{Tr}_{A' \times A'_0}(\sigma'_F) = \mathrm{Tr}_{B_n}(\sigma'_n) = \sum_{y \in B'} e_y e_y^* \otimes \phi_y \phi_y^* \otimes \sigma_{n,y_1,\ldots,y_{n-1}}.$$

Thus,

$$\sigma'_F = \sum_{a \in A'_0} \sum_{y \in B'} e_a e_a^* \otimes e_y e_y^* \otimes \phi_y \phi_y^* \otimes \tilde{\sigma}_{F,a,y},$$

by writing $\sigma_{F,a,y} = \phi_y \phi_y^* \otimes \tilde{\sigma}_{F,a,y}$ where $\tilde{\sigma}_{F,a,y} \in \mathbb{S}_+^{A \times A'}$ satisfies

$$\sum_{a \in A'_0} \mathrm{Tr}_{A'}(\tilde{\sigma}_{F,a,y}) = \sigma_{n,y_1,\ldots,y_{n-1}}$$

for all $a \in A'_0$ and $y \in B'$.

The objective function becomes

$$\left\langle \sigma'_F, \Pi_{\mathrm{B},0} \otimes \mathrm{I}_{B'_0 \times B'} \right\rangle = \frac{1}{2} \sum_{a \in A'_0} \sum_{y \in B'} \beta_{a,y} \left\langle \tilde{\sigma}_{F,a,y}, \psi_a \psi_a^* \right\rangle.$$

At this point, we note that

$$\left\langle \sigma'_F, \Pi_{\mathrm{B},1} \otimes \mathrm{I}_{B'_0 \times B'} \right\rangle = \frac{1}{2} \sum_{a \in A'_0} \sum_{y \in B'} \beta_{\bar{a},y} \left\langle \tilde{\sigma}_{F,a,y}, \psi_a \psi_a^* \right\rangle,$$

proving that evaluating Alice's success probability of cheating towards 0 or 1 with this strategy is a matter of switching Bob's two probability distributions.

Carrying on with $P^*_{\mathrm{A},0}$, we get the following SDP

$$\begin{array}{lrll}
\sup \frac{1}{2} \displaystyle\sum_{a \in A'_0,\, y \in B'} & \beta_{a,y} \left\langle \tilde{\sigma}_{F,a,y}, \psi_a \psi_a^* \right\rangle & & \\
\text{s.t.} & \mathrm{Tr}_{A_1}(\tilde{\sigma}_1) & = 1, & \\
& \mathrm{Tr}_{A_j}(\tilde{\sigma}_{j,y_1,\ldots,y_{j-1}}) & = \tilde{\sigma}_{j-1,y_1,\ldots,y_{j-2}}, & \forall j \in \{2,\ldots,n\}, \\
& & & \forall y_1 \in B'_1, \\
& & & \vdots \\
& & & \forall y_{j-1} \in B'_{j-1}, \\
& \sum_{a \in A'_0} \mathrm{Tr}_{A'}(\tilde{\sigma}_{F,a,y}) & = \tilde{\sigma}_{n,y_1,\ldots,y_{n-1}}, & \forall y \in B', \\
& \tilde{\sigma}_{j,y_1,\ldots,y_{j-1}} & \in \mathbb{S}_+^{A_1 \times \cdots \times A_j}, & \forall j \in \{1,\ldots,n\}, \\
& & & \forall y_1 \in B'_1, \\
& & & \vdots \\
& & & \forall y_{j-1} \in B'_{j-1}, \\
& \tilde{\sigma}_{F,a,y} & \in \mathbb{S}_+^{A' \times A}, & \forall a \in A'_0, y \in B'.
\end{array}$$

By Lemma 3, the following restrictions can only improve the objective function value:

$$\begin{aligned}
s_1 &:= \operatorname{diag}(\tilde{\sigma}_1), && \\
s_2^{(y_1)} &:= \operatorname{diag}(\tilde{\sigma}_{2,y_1}), && \forall y_1 \in B_1', \\
&\vdots && \\
s_n^{(y_1,\ldots,y_{n-1})} &:= \operatorname{diag}(\tilde{\sigma}_{n,y_1,\ldots,y_{n-1}}), && \forall y_1 \in B_1', \ldots, y_{n-1} \in B_{n-1}', \\
s^{(a,y)} &:= \operatorname{diag}(\operatorname{Tr}_{A'}(\tilde{\sigma}_{F,a,y})), && \forall a \in A_0',\, y \in B', \\
\operatorname{Tr}_{A'}(\tilde{\sigma}_{F,a,y}) &= \operatorname{Diag}(s^{(a,y)}), && \forall a \in A_0',\, y \in B',
\end{aligned}$$

where the superscripts are the restrictions of the vectors as before. With these new variables, and using Lemma 3, we can write the new objective function as

$$\frac{1}{2} \sum_{a \in \{0,1\}} \sum_{y \in B} \beta_{a,y} \, \mathrm{F}(s^{(a,y)}, \alpha_a),$$

where $(s_1, \ldots, s_n, s) \in \mathcal{P}_{\mathrm{A}}$. Any feasible solution to the reduced SDP also gives us a feasible solution to the original SDP, so their optimal values are equal. □

This proof shows that the reduced cheating problem does not eliminate all of the optimal solutions of the corresponding SDP. We can also show that the reduced problems capture optimal solutions to the corresponding SDPs by examining the dual SDPs. However, the primal SDPs are more important for the purposes of this paper and this proof is more illustrative.

We note here that we can get similar SDPs and reductions if Alice chooses a with a non-uniform probability distribution and similarly for Bob. It only changes the multiplicative factor $1/2$ in the reduced problems to something that depends on a (or b) and the proofs are nearly identical. Note that this causes the honest outcome probabilities to not be uniformly random and this no longer falls into our definition of a coin-flipping protocol. However, sometimes such "unbalanced" coin-flipping protocols are useful, see [4].

4 Second-order cone programming formulations and analysis

Here we define second-order cone programs and discuss such formulations of the optimal cheating probabilities for Alice and Bob.

The *second-order cone* (or *Lorentz cone*) in $\mathbb{R}^n$, $n \geq 2$, is defined as

$$\mathrm{SOC}^n := \left\{ (x,t) \in \mathbb{R}^n : t \geq \|x\|_2 \right\}.$$

A *second-order cone program*, denoted SOCP, is an optimization problem of the form

$$\begin{array}{lrl}
\text{(P)} & & \sup \ \langle c, x \rangle \\
& \text{subject to} & Ax = b, \\
& & x \in \mathrm{SOC}^{n_1} \oplus \cdots \oplus \mathrm{SOC}^{n_k},
\end{array}$$

where A is an $m \times (\sum_{i=1}^{k} n_k)$ matrix, $b \in \mathbb{R}^m$, $c \in \mathbb{R}^{\sum_{i=1}^{k} n_k}$, and k is finite.

A related cone, called the *rotated second-order cone*, is defined as

$$\mathrm{RSOC}^n := \left\{ (a, b, x) \in \mathbb{R}^n : a, b \geq 0,\ 2ab \geq \|x\|_2^2 \right\}.$$

Optimizing over the rotated second-order cone is also called second-order cone programming because $(x, t) \in \mathrm{SOC}^n$ if and only if $(t/2, t, x) \in \mathrm{RSOC}^{n+1}$ and $(a, b, x) \in \mathrm{RSOC}^n$ if and only if $(x, a, b, a + b) \in \mathrm{SOC}^{n+1}$ and $a, b \geq 0$. In fact, both second-order cone constraints can be cast as positive semidefinite constraints:

$$t \geq \|x\|_2 \iff \begin{bmatrix} t & x^{\mathrm{T}} \\ x & t\,\mathrm{I} \end{bmatrix} \succeq 0 \quad \text{and} \quad a, b \geq 0,\ 2ab \geq \|x\|_2^2 \iff \begin{bmatrix} 2a & x^{\mathrm{T}} \\ x & b\,\mathrm{I} \end{bmatrix} \succeq 0.$$

Despite second-order cone programming being a special case of semidefinite programming, there are some notable differences. One is that the algorithms for solving second-order cone programs can be more efficient and robust than those for solving semidefinite programs. We refer the interested reader to [12], [13], [8], [2] and the references therein.

4.1 SOCP formulations for the reduced problems

We now show that the reduced SDPs can be modelled using second-order cone programming. We elaborate on this below and explain the significance to solving these problems computationally.

We start by first explaining how to model fidelity as an SOCP. Suppose we are given the problem

$$\max_{q \in \mathbb{R}^n_+ \cap S} \left\{ \sqrt{\mathrm{F}(p, q)} \right\} = \max_{q \in \mathbb{R}^n_+ \cap S} \left\{ \sum_{i=1}^{n} \sqrt{p_i}\, t_i : t_i^2 \leq q_i,\ \forall i \in \{1, \ldots, n\} \right\},$$

where $p \in \mathbb{R}^n_+$ and $S \subseteq \mathbb{R}^n$. We can replace $t_i^2 \leq q_i$ with the equivalent constraint $(1/2, q_i, t_i) \in \mathrm{RSOC}^3$, for all $i \in \{1, \ldots, n\}$. Therefore, we can maximize the fidelity using n rotated second-order cone constraints.

For the same reason, we can use second-order cone programming to solve a problem of the form

$$\max \left\{ \sum_{j=1}^{m} a_j \sqrt{\mathrm{F}(p_j, q_j)} : (q_1, \ldots, q_m) \in \mathbb{R}^{mn}_+ \cap S' \right\},$$

where $a \in \mathbb{R}^m_+$ and $S' \subseteq \mathbb{R}^{mn}$. However, this does not apply directly to the reduced problems since we need to optimize over a linear combination of fidelities and $f(x) = x^2$ is not a concave function. For example, Alice's reduced problem is of the form

$$\max \left\{ \sum_{j=1}^{m} a_j\, \mathrm{F}(p_j, q_j) : (q_1, \ldots, q_m) \in \mathbb{R}^{mn}_+ \cap S' \right\}.$$

The root of this problem arises from the fact that the fidelity function, which is concave, is a composition of a concave function with a convex function, thus we cannot break it into these two steps. Even though the above analysis does not work to capture the reduced problems as SOCPs, it does have a desirable property that it only uses $O(n)$ second-order cone constraints and perhaps this formulation will be useful for future applications.

We now explain how to model the reduced problems as SOCPs directly.

Lemma 5 *For $p, q \in \mathbb{R}^n_+$, we have*

$$\mathrm{F}(p,q) = \max \left\{ \frac{1}{\sqrt{2}} \sum_{i,j=1}^{n} \sqrt{p_i p_j}\, t_{i,j} : (q_i, q_j, t_{i,j}) \in \mathrm{RSOC}^3,\ \forall i,j \in \{1,\ldots,n\} \right\}.$$

Proof For every $i, j \in \{1, \ldots, n\}$, we have $(q_i, q_j, t_{i,j}) \in \mathrm{RSOC}^3$ if and only if $q_i, q_j \geq 0$, and $2q_i q_j \geq t_{i,j}^2$. Thus, $t_{i,j} = \sqrt{2q_i q_j}$ is optimal with objective function value $\mathrm{F}(p,q)$. □

This lemma provides an SOCP representation for the hypograph of the fidelity function. Recall that the hypograph of a concave function is a convex set. Also, the dimension of the hypograph of $\mathrm{F}(\cdot, q) : \mathbb{R}^n_+ \to \mathbb{R}$ is equal to n (assuming $q > 0$). Since the hypograph is $O(n)$-dimensional and convex, there exists a so-called *self-concordant barrier function* for the set with complexity parameter $\mathrm{O}(n)$, shown by Nesterov and Nemirovski [10]. The details of such functions are not necessary for this paper, but we mention that such a function allows the derivation of interior-point methods for the underlying convex optimization problem which use $\mathrm{O}(\sqrt{n}\log(1/\varepsilon))$ iterations, where ε is an accuracy parameter. The above lemma uses $\Omega(n^2)$ second-order cone constraints and the usual treatment of these "cone constraints" with optimal self-concordant barrier functions lead to interior-point methods with an iteration complexity bound of $\mathrm{O}(n \log(1/\varepsilon))$. It is conceivable that there exist better convex representations of the hypograph of the fidelity function than the one we provided in Lemma 5.

We can further simplify the reduced problems using fewer SOC constraints than derived above. We first consider the dual formulation of the reduced problems, so as to avoid the hypograph of the fidelity function.

Using the SDP characterization of the fidelity function, we write Alice's reduced problem for forcing outcome 0 as an SDP. The dual of this SDP is

$$\begin{array}{rrcll}
\inf & z_1 & & & \\
\text{subject to} & z_1 \cdot e_{A_1} & \geq & \mathrm{Tr}_{B_1}(z_2), & \\
& z_2 \otimes e_{A_2} & \geq & \mathrm{Tr}_{B_2}(z_3), & \\
& & \vdots & & \\
& z_n \otimes e_{A_n} & \geq & \mathrm{Tr}_{B_n}(z_{n+1}), & \\
& \mathrm{Diag}(z_{n+1}^{(y)}) & \succeq & \frac{1}{2}\beta_{a,y}\sqrt{\alpha_a}\sqrt{\alpha_a}^{\mathrm{T}}, & \forall a \in \{0,1\}, y \in B\ , \\
& z_1 & \in & \mathbb{R}, & \\
& z_i & \in & \mathbb{R}^{A_1 \times B_1 \times \cdots \times A_{i-1} \times B_{i-1}}, & \forall i \in \{2,\ldots,n+1\}\ , \\
\text{where} & z_{n+1,x}^{(y)} & = & z_{n+1,x_1 y_1 x_2 y_2 \cdots, x_n y_n}, & \forall x \in A, y \in B\ .
\end{array}$$

The only nonlinear constraint in the above problem is of the form

$$\mathrm{Diag}(z) \succeq \sqrt{q}\sqrt{q}^{\mathrm{T}},$$

for some fixed $q \geq 0$. Recall that for z which is positive in every coordinate, we have

$$\mathrm{Diag}(z) \succeq \sqrt{q}\sqrt{q}^{\mathrm{T}} \iff \langle z^{-1}, q \rangle \leq 1.$$

So, it suffices to characterize inverses using SOCP constraints which can be done by considering

$$(z_i, r_i, \sqrt{2}) \in \mathrm{RSOC} \iff r_i \geq z_i^{-1}.$$

With this observation, we can write the dual of Alice and Bob's reduced problems using $\mathrm{O}(n)$ RSOC constraints for each fidelity function in the objective function as opposed to $\Omega(n^2)$ RSOC constraints had we combined the reduced problems with Lemma 5 above.

4.2 Numerical performance of SDP formulation vs. SOCP formulation

Since the search algorithm designed in this paper examines the optimal cheating probabilities of many protocols (more than 10^{16}) we are concerned with the efficiency of solving the reduced problems. In this subsection, we discuss the efficiency of this computation. Our computational platform is an SGI XE C1103 with 2x 3.2 GHz 4-core Intel X5672 x86 CPUs processor, and 10 GB memory, running Linux. The reduced problems were solved using SeDuMi 1.3, a program for solving semidefinite programs and rotated second-order cone programs in Matlab (Version 7.12.0.635) [12], [13].

Table 1 (on the next page) compares the computation of Alice's reduced problem in a four-round protocol for forcing an outcome of 0 with 5-dimensional messages. The top part of the table presents the average running time, the maximum running time, and the worst gap (the maximum of the extra time needed to solve the problem compared to the other formulation (SOCP vs. SDP)). The bottom part of the table presents the average number of iterations, the average feasratio, the average timing (the time spent in preprocessing, iterations, and postprocessing, respectively), and the average cpusec.

Table 1 suggests that solving the rotated second-order cone programs are comparable to solving the semidefinite programs. However, before testing the other three cheating probabilities, we test the performance of the two formulations from Table 1 in a setting that appears more frequently in the search. In particular, most the searches dealt with in this paper involve many protocols with very sparse parameters. We retest the values in Table 1 when we force the first entry of α_0, the second entry of α_1, the third entry of β_0, and the fourth entry of β_1 to all be 0. The results are shown in Table 2.

As we can see, the second-order cone programming formulation stumbles when the data does not have full support. Notice the feasratio in that scenario is 0.5172, suggesting SeDuMi ran into some numerical problems. Since we search over many vectors without full support, we use the SDP formulations for the search algorithm.

Table 1 Comparison of solving the SOCP formulation (the $O(n)$ RSOC constraints version) and the reduced SDP formulations for Alice forcing outcome 0 with 5-dimensional messages in four-rounds (averaged over $1,000$ randomly selected protocols).

INFO parameters	SOCP	SDP
Average running time (s)	0.1551	0.1529
Max running time (s)	0.7491	0.2394
Worst gap (s)	$+\,0.5098$	$+\,0.0927$
Average iteration	14.4420	12.2940
Average feasratio	0.9990	1.0000
Average timing	$[0.0270, 0.1267, 0.0010]^{\mathrm{T}}$	$[0.0024, 0.1494, 0.0009]^{\mathrm{T}}$
Average cpusec	0.9283	0.6588

Table 2 Comparison of solving the SOCP formulation (the $O(n)$ RSOC constraints version) and the reduced SDP formulations for Alice forcing outcome 0 with 5-dimensional messages in four-rounds (averaged over $1,000$ randomly selected protocols with forced 0 entries).

INFO parameters	SOCP	SDP
Average running time (s)	0.4104	0.1507
Max running time (s)	0.7812	0.2084
Worst gap (s)	$+\,0.6323$	$+\,0$
Average iterations	32.7370	12.2530
Average feasratio	0.5172	1.0000
Average timing	$[0.0279, 0.3814, 0.0010]^{\mathrm{T}}$	$[0.0023, 0.1473, 0.0009]^{\mathrm{T}}$
Average cpusec	2.4953	0.5605

5 Developing the strategies in the filter

5.1 Cheating Alice

We now reproduce Theorem 4, give brief descriptions of the cheating strategies, then derive them and the corresponding bounds.

Theorem 4 *For a protocol parameterized by $\alpha_0, \alpha_1 \in \mathrm{Prob}^A$, $\beta_0, \beta_1 \in \mathrm{Prob}^B$, we can bound Alice's optimal cheating probability as follows:*

$$P^*_{\mathrm{A},0} \geq \frac{1}{2} \sum_{y \in B} \mathrm{conc}\left\{\beta_{a,y} \mathrm{F}(\cdot, \alpha_a) : a \in \{0,1\}\right\}(v) \tag{2}$$

$$\geq \frac{1}{2} \lambda_{\max}\left(\eta \sqrt{\alpha_0}\sqrt{\alpha_0}^{\mathrm{T}} + \tau \sqrt{\alpha_1}\sqrt{\alpha_1}^{\mathrm{T}}\right) \tag{3}$$

$$\geq \left(\frac{1}{2} + \frac{1}{2}\sqrt{\mathrm{F}(\alpha_0, \alpha_1)}\right)\left(\frac{1}{2} + \frac{1}{2}\Delta(\beta_0, \beta_1)\right), \tag{4}$$

where

$$\eta := \sum_{\substack{y \in B: \\ \beta_{0,y} \geq \beta_{1,y}}} \beta_{0,y} \quad \text{and} \quad \tau := \sum_{\substack{y \in B: \\ \beta_{0,y} < \beta_{1,y}}} \beta_{1,y} \;,$$

and $\sqrt{v}$ is the normalized principal eigenvector of $\eta \sqrt{\alpha_0}\sqrt{\alpha_0}^{\mathrm{T}} + \tau \sqrt{\alpha_1}\sqrt{\alpha_1}^{\mathrm{T}}$.

Furthermore, in a six-round protocol, we have

$$P^*_{\mathrm{A},0} \geq \frac{1}{2} \lambda_{\max}\left(\eta' \sqrt{\mathrm{Tr}_{A_2}(\alpha_0)}\sqrt{\mathrm{Tr}_{A_2}(\alpha_0)}^{\mathrm{T}} + \tau' \sqrt{\mathrm{Tr}_{A_2}(\alpha_1)}\sqrt{\mathrm{Tr}_{A_2}(\alpha_1)}^{\mathrm{T}}\right) \tag{5}$$

$$\geq \left(\frac{1}{2} + \frac{1}{2}\sqrt{\mathrm{F}(\mathrm{Tr}_{A_2}(\alpha_0), \mathrm{Tr}_{A_2}(\alpha_1))}\right)\left(\frac{1}{2} + \frac{1}{2}\Delta(\mathrm{Tr}_{B_2}(\beta_0), \mathrm{Tr}_{B_2}(\beta_1))\right) \tag{6}$$

where

$$\eta' := \sum_{\substack{y_1 \in B_1: \\ [\mathrm{Tr}_{B_2}(\beta_0)]_{y_1} \geq [\mathrm{Tr}_{B_2}(\beta_1)]_{y_1}}} [\mathrm{Tr}_{B_2}(\beta_0)]_{y_1} \quad \text{and} \quad \tau' := \sum_{\substack{y_1 \in B_1: \\ [\mathrm{Tr}_{B_2}(\beta_0)]_{y_1} < [\mathrm{Tr}_{B_2}(\beta_1)]_{y_1}}} [\mathrm{Tr}_{B_2}(\beta_1)]_{y_1}.$$

We have analogous bounds for $P^*_{\mathrm{A},1}$, which are obtained by interchanging β_0 and β_1 in the above expressions.

We call (2) Alice's *improved eigenstrategy*, (3) her *eigenstrategy*, and (4) her *three-round strategy*. For six-round protocols, we call (5) Alice's *eigenstrategy* and (6) her *measuring strategy*.

Note that only the improved eigenstrategy is affected by switching β_0 and β_1 (as long as we are willing to accept a slight modification to how we break ties in the definitions of η, η', τ, and τ').

We now briefly describe the strategies that yield the corresponding cheating probabilities in Theorem 4. Her three-round strategy is to prepare the qubits AA' in the state $\psi' = (\psi_0 + \psi_1)/\left\|\psi_0 + \psi_1\right\|$ instead of ψ_0 or ψ_1, send the first n messages accordingly, then measure the qubits received from Bob to try to learn b, and reply with a bit a using the measurement outcome (along with the rest of the state ψ'), to bias the coin towards her desired output. Her eigenstrategy is the same as her three-round strategy, except that the first message is further optimized. The improved eigenstrategy has the same first message as in her eigenstrategy, but the last message is further optimized. For a six-round protocol, Alice's measuring strategy is to prepare the qubits AA' in the following state $\psi' = (\psi'_0 + \psi'_1)/\left\|\psi'_0 + \psi'_1\right\|$ where ψ'_0 and ψ'_1 are purifications of $\mathrm{Tr}_{A_2,A'}(\psi_0\psi_0^*)$ and $\mathrm{Tr}_{A_2,A'}(\psi_1\psi_1^*)$, respectively. She measures Bob's first message to try to learn b, then depending on the outcome, she applies a (fidelity achieving) unitary before sending the rest of her messages. Her six-round eigenstrategy is similar to her measuring strategy, except her first message is optimized in a way described in the proof.

Proof of Theorem 4. Recall Alice's optimization problem

$$P^*_{\mathrm{A},0} = \max \left\{ \frac{1}{2} \sum_{a \in \{0,1\}} \sum_{y \in B} \beta_{a,y} \, \mathrm{F}(s^{(a,y)}, \alpha_a) \; : \; (s_1, \ldots, s_n, s) \in \mathcal{P}_{\mathrm{A}} \right\}.$$

To get a feasible solution, suppose Alice guesses b before she reveals a in the following way. If Bob reveals $y \in B$, then Alice guesses $b = 0$ if $\beta_{0,y} \geq \beta_{1,y}$ and $b = 1$ if $\beta_{0,y} < \beta_{1,y}$. Let Alice's guess be denoted by $f(y)$, so

$$f(y) = \arg\max_a \{\beta_{a,y}\} \in \{0,1\},$$

and we set $f(y) = 0$ in the case of a tie. We have chosen a way to satisfy the last constraint in Alice's cheating polytope, but we can choose how Alice sends her first n messages $s_1, \ldots, s_n$. We make one more restriction, we set $s_n = d \otimes e_{B_1 \times \cdots \times B_{n-1}}$ and optimize over $d \in \mathrm{Prob}^A$. We can easily satisfy the rest of the constraints given any d by choosing each variable as the corresponding marginal probability distribution.

Under these restrictions, we have that Alice's reduced problem can be written as

$$\max_{d \in \mathrm{Prob}^A} \left\{ \frac{1}{2} \sum_{y \in B} \beta_{f(y),y} \mathrm{F}(d, \alpha_{f(y)}) \right\} = \max_{d \in \mathrm{Prob}^A} \left\{ \eta \, \mathrm{F}(d, \alpha_0) + \tau \, \mathrm{F}(d, \alpha_1) \right\}.$$

We can simplify this using the following lemma.

Lemma 6 *For nonnegative vectors $\{z_1, \ldots, z_n\} \subset \mathbb{R}^n_+$, we have that*

$$\max \left\{ \sum_{i=1}^n \mathrm{F}(p, z_i) : p \in \mathrm{Prob}^n \right\} = \lambda_{\max} \left(\sum_{i=1}^n \sqrt{z_i} \sqrt{z_i}^{\mathrm{T}} \right).$$

Furthermore, an optimal solution is the entry-wise square of the normalized principal eigenvector.

Proof Since $\sum_{i=1}^n \mathrm{F}(p, z_i) = \sum_{i=1}^n \left\langle \sqrt{p}\sqrt{p}^{\mathrm{T}}, \sqrt{z_i}\sqrt{z_i}^{\mathrm{T}} \right\rangle = \sqrt{p}^{\mathrm{T}} \left(\sum_{i=1}^n \sqrt{z_i}\sqrt{z_i}^{\mathrm{T}} \right) \sqrt{p}$, where $\sqrt{\cdot}$ is the entry-wise square root, the maximization problem reduces to

$$\max \left\{ \sqrt{p}^{\mathrm{T}} \left(\sum_{i=1}^n \sqrt{z_i}\sqrt{z_i}^{\mathrm{T}} \right) \sqrt{p} : p \in \mathrm{Prob}^n \right\}.$$

Let $\hat{x} \in \mathbb{R}^m$ be the restriction of a vector x onto $\cup_{i=1}^n \mathrm{supp}(z_i)$. Then the optimal objective value of the above optimization problem is equal to that of

$$\max \left\{ \sqrt{\hat{p}}^{\mathrm{T}} \left(\sum_{i=1}^n \sqrt{\hat{z}_i}\sqrt{\hat{z}_i}^{\mathrm{T}} \right) \sqrt{\hat{p}} : \hat{p} \in \mathrm{Prob}^{\cup_{i=1}^n \mathrm{supp}(z_i)} \right\}.$$

If the nonnegativity constraint were not present, the optimum value would be attained by setting $\sqrt{\hat{p}}$ to be the normalized principal eigenvector of the matrix $\sum_{i=1}^n \sqrt{\hat{z}_i}\sqrt{\hat{z}_i}^{\mathrm{T}}$. Because $\sum_{i=1}^n \sqrt{\hat{z}_i}\sqrt{\hat{z}_i}^{\mathrm{T}}$ has positive entries, we know the principal eigenvector is also positive by the Perron-Frobenius Theorem. Since this does not violate the nonnegativity constraint in the problem, $\hat{p}$, where $\sqrt{\hat{p}}$ is the normalized principal eigenvector, is an optimal solution yielding an optimal objective value of $\lambda_{\max}\left(\sum_{i=1}^n \sqrt{\hat{z}_i}\sqrt{\hat{z}_i}^{\mathrm{T}}\right)$. Notice that $\sum_{i=1}^n \sqrt{\hat{z}_i}\sqrt{\hat{z}_i}^{\mathrm{T}}$ is the matrix obtained by removing the zero rows and columns from $\sum_{i=1}^n \sqrt{z_i}\sqrt{z_i}^{\mathrm{T}}$ and thus has the same largest eigenvalue. $\square$

Using this lemma, Alice can cheat with probability

$$\frac{1}{2}\lambda_{\max}\left(\eta\sqrt{\alpha_0}\sqrt{\alpha_0}^{\mathrm{T}} + \tau\sqrt{\alpha_1}\sqrt{\alpha_1}^{\mathrm{T}}\right),$$

which we call Alice's *eigenstrategy*.

We can find a lower bound on this value using the following two lemmas.

Lemma 7 *For β_0, β_1, η, and τ defined above, we have $\eta + \tau = 1 + \Delta(\beta_0, \beta_1)$.*

Proof Notice that we can write $\sum_{y \in B} \max_{a \in \{0,1\}} \{\beta_{a,y}\} + \sum_{y \in B} \min_{a \in \{0,1\}} \{\beta_{a,y}\} = 2$ and we can also write $\sum_{y \in B} \max_{a \in \{0,1\}} \{\beta_{a,y}\} - \sum_{y \in B} \min_{a \in \{0,1\}} \{\beta_{a,y}\} = 2\Delta(\beta_0, \beta_1)$. With this, we can conclude that $\eta + \tau = \sum_{y \in B} \max_{a \in \{0,1\}} \{\beta_{a,y}\} = 1 + \Delta(\beta_0, \beta_1)$, as desired. $\square$

The above lemma can be restated as $\sum_{y \in B} \max_{a \in \{0,1\}} \{\beta_{a,y}\} = 1 + \Delta(\beta_0, \beta_1)$ for any probability distributions β_0 and β_1. This is helpful when looking at Bob's cheating strategies as well.

Lemma 8 *For $\eta, \tau \in \mathbb{R}$ and $p, q \in \mathrm{Prob}^n$, we have*

$$\lambda_{\max}\left(\eta\sqrt{p}\sqrt{p}^{\mathrm{T}} + \tau\sqrt{q}\sqrt{q}^{\mathrm{T}}\right) = \frac{1}{2}\left(\eta + \tau + \sqrt{(\eta - \tau)^2 + 4\eta\tau\,\mathrm{F}(p,q)}\right).$$

Proof Since we can write $\mathrm{F}(p,q) = \left(\sqrt{p}^{\mathrm{T}}\sqrt{q}\right)^2$, we can apply a unitary to both $\sqrt{p}$ and $\sqrt{q}$ and both sides of the equality we want to prove are unaffected. Choose a unitary U such that

$$U\sqrt{p} = [1, 0, 0, \ldots, 0]^{\mathrm{T}} \quad \text{and} \quad U\sqrt{q} = [\sin\theta, \cos\theta, 0, \ldots, 0]^{\mathrm{T}},$$

for some $\theta \in [0, 2\pi)$. Then we can write $\mathrm{F}(p,q) = \sin^2\theta$. Let $\lambda_{\max}$ be the largest eigenvalue of the matrix $\eta\sqrt{p}\sqrt{p}^{\mathrm{T}} + \tau\sqrt{q}\sqrt{q}^{\mathrm{T}}$, or equivalently, of the matrix $\eta U\sqrt{p}\sqrt{p}^{\mathrm{T}}U^* + \tau U\sqrt{q}\sqrt{q}^{\mathrm{T}}U^*$, and let λ_2 be the second largest eigenvalue. Then

$$\lambda_{\max} + \lambda_2 = \mathrm{Tr}(\eta\sqrt{p}\sqrt{p}^{\mathrm{T}} + \tau\sqrt{q}\sqrt{q}^{\mathrm{T}}) = \eta + \tau$$

and, by taking the determinant of the only nonzero block, we get

$$\lambda_{\max} \cdot \lambda_2 = \eta\tau\cos^2\theta = \eta\tau(1 - \mathrm{F}(p,q))$$

implying $\lambda_{\max} = \frac{1}{2}\left(\eta + \tau + \sqrt{(\eta-\tau)^2 + 4\eta\tau\mathrm{F}(p,q)}\right)$, as desired. □

Note that Lemma 8 shows that switching the roles of η and τ does not affect the largest eigenvalue.

Using the above two lemmas, we have

$$\begin{aligned}
&\frac{1}{2}\lambda_{\max}\left(\eta\sqrt{\alpha_0}\sqrt{\alpha_0}^{\mathrm{T}} + \tau\sqrt{\alpha_1}\sqrt{\alpha_1}^{\mathrm{T}}\right)\\
&= \frac{1}{4}\left(\eta + \tau + \sqrt{(\eta-\tau)^2 + 4\eta\tau\,\mathrm{F}(\alpha_0,\alpha_1)}\right)\\
&\geq \frac{1}{4}\left(\eta + \tau + \sqrt{(\eta-\tau)^2\,\mathrm{F}(\alpha_0,\alpha_1) + 4\eta\tau\,\mathrm{F}(\alpha_0,\alpha_1)}\right)\\
&= \frac{1}{4}\left(\left(1 + \sqrt{\mathrm{F}(\alpha_0,\alpha_1)}\right)(\eta+\tau)\right)\\
&= \left(\frac{1}{2} + \frac{1}{2}\sqrt{\mathrm{F}(\alpha_0,\alpha_1)}\right)\left(\frac{1}{2} + \frac{1}{2}\Delta(\beta_0,\beta_1)\right).
\end{aligned}$$

This lower bound has a natural interpretation. This is the strategy where Alice ignores all of Bob's messages until $\mathbb{C}^{B_n}$ is sent. Then she measures it to learn b with probability $\frac{1}{2} + \frac{1}{2}\Delta(\beta_0,\beta_1)$. Conditioned on having the correct value for b, she tries to get past Bob's cheat detection and can do so with probability $\frac{1}{2} + \frac{1}{2}\sqrt{\mathrm{F}(\alpha_0,\alpha_1)}$. We call this Alice's *three-round strategy* since it combines optimal strategies for the three-round protocol example in Subsection 1. It makes sense that this is a lower bound on the success probability of Alice's eigenstrategy since her eigenstrategy is optimized from the same restrictions that apply to her three-round strategy.

We can also examine how Alice can choose her last message optimally supposing she has already sent her first n messages in a particular way. I.e., suppose $s_n := c \otimes e_{B_1 \times \cdots \times B_{n-1}}$ for some $c \in \mathrm{Prob}^A$ (as in the eigenstrategy). From this we can find $s_1, \ldots, s_{n-1}$ satisfying the first $n-1$ constraints of her cheating polytope by taking the corresponding marginal distributions of c. We want to optimize over s satisfying $\mathrm{Tr}_{A_0'}(s) = s_n \otimes e_{B_n} = c \otimes e_B$. In this case, this constraint can be written as $\sum_{a\in\{0,1\}} s^{(a,y)} = c$, for each $y \in B$, where again, $s^{(a,y)}$ is the restriction of s with a and y fixed. Now we get the following optimization problem

$$\begin{array}{rr}\max \frac{1}{2}\sum_{a\in\{0,1\}}\sum_{y\in B}\beta_{a,y}\,\mathrm{F}(s^{(a,y)},\alpha_a) & \\ \text{subject to} \qquad\qquad \sum_{a\in\{0,1\}} s^{(a,y)} & = c, \text{ for all } y\in B,\\ s^{(a,y)} & \geq 0,\end{array}$$

where c is now constant. If we rewrite this as

$$\begin{array}{rr}\max \frac{1}{2}\sum_{y\in B}\sum_{a\in\{0,1\}}\mathrm{F}(s^{(a,y)},\beta_{a,y}\alpha_a) & \\ \text{subject to} \qquad\qquad \sum_{a\in\{0,1\}} s^{(a,y)} & = c, \text{ for all } y\in B,\\ s^{(a,y)} & \geq 0,\end{array}$$

we have a separable problem over $y \in B$. That is, for each fixed $\tilde{y} \in B$, Alice needs to solve the optimization problem

$$G_{\tilde{y}}(c) := \max\left\{\frac{1}{2}\sum_{a\in\{0,1\}}\mathrm{F}(s^{(a,\tilde{y})},\beta_{a,\tilde{y}}\alpha_a) : \sum_{a\in\{0,1\}} s^{(a,\tilde{y})} = c, s^{(a,\tilde{y})} \geq 0, \forall a\in\{0,1\}\right\}.$$

This optimization problem has a special structure.

Definition 3 The *infimal convolution* of the convex functions $f_1, f_2, \ldots, f_n$, where
$f_1, \ldots, f_n : \mathbb{R}^m \to \mathbb{R}\cup\{\infty\}$, is

$$(f_1 \square f_2 \square \cdots \square f_n)(d) := \inf_{x_1,\ldots,x_n\in\mathbb{R}^m}\left\{\sum_{i=1}^n f_i(x_i) : \sum_{i=1}^n x_i = d\right\}.$$

We do not need to worry about the nonnegativity constraints on the variables since we can define our convex function $-\mathrm{F}(p,q) = +\infty$ if p or q is not nonnegative. Note for every $p \in \mathbb{R}^m_+$, that $-\mathrm{F}(p,\cdot)$ is a *proper, convex function*, i.e., it is convex and $-\mathrm{F}(p,q) < +\infty$ for some $q \in \mathbb{R}^m_+$ and $-\mathrm{F}(p,q) > -\infty$ for every $q \in \mathbb{R}^m_+$. Proper, convex functions have many useful properties as detailed in this section. Using these properties and the fact that $-\mathrm{F}(p,\cdot)$ is positively homogeneous, we show a way to express $G_{\tilde{y}}$.

Recall that for proper, convex functions $f_1, \ldots, f_n : \mathbb{R}^m \to \mathbb{R}\cup\{\infty\}$, the convex hull of $\{f_1, \ldots, f_n\}$ is the greatest convex function f such that $f(x) \leq f_1(x), \ldots, f_n(x)$ for every $x \in \mathbb{R}^m$. To write down explicitly what the convex hull is, we use the following lemma.

Lemma 9 ([Roc70, page 37]) *Let $f_1, \ldots, f_n : \mathbb{R}^m \to \mathbb{R}\cup\{\infty\}$ be proper, convex functions. Then we have*

$$\operatorname{conv}\{f_1,\ldots,f_n\}(d) = \inf\left\{\sum_{i=1}^n \lambda_i f_i(x_i) : \sum_{i=1}^n \lambda_i x_i = d\right\}.$$

For a positively homogeneous function f, we have $\lambda f\left(\lambda^{-1}x\right) = f(x)$, for $\lambda > 0$. Therefore, we have the following corollary.

Corollary 1 *Let* $f_1, \ldots, f_n : \mathbb{R}^m \to \mathbb{R} \cup \{\infty\}$ *be positively homogeneous, proper, convex functions. Then we have*

$$\mathrm{conv}\left\{f_1, \ldots, f_n\right\} = f_1 \square f_2 \square \cdots \square f_n.$$

Therefore, we can write Alice's cheating probability using concave hulls as shown below

$$\begin{aligned}
G_{\tilde{y}}(c) &= \max\left\{\frac{1}{2}\sum_{a \in \{0,1\}} \mathrm{F}(s^{(a,\tilde{y})}, \beta_{a,\tilde{y}}\alpha_a) : \sum_{a \in \{0,1\}} s^{(a,\tilde{y})} = c,\ s^{(a,\tilde{y})} \geq 0,\ \forall a\right\} \\
&= -\min\left\{-\frac{1}{2}\sum_{a \in \{0,1\}} \mathrm{F}(s^{(a,\tilde{y})}, \beta_{a,\tilde{y}}\alpha_a) : \sum_{a \in \{0,1\}} s^{(a,\tilde{y})} = c,\ s^{(a,\tilde{y})} \geq 0,\ \forall a\right\} \\
&= -\left(-\frac{1}{2}\mathrm{F}(\cdot, \beta_{0,\tilde{y}}\alpha_0)\right) \square \left(-\frac{1}{2}\mathrm{F}(\cdot, \beta_{1,\tilde{y}}\alpha_1)\right)(c) \\
&= -\mathrm{conv}\left\{\frac{-1}{2}\beta_{0,\tilde{y}}\mathrm{F}(\cdot, \alpha_0), \frac{-1}{2}\beta_{1,\tilde{y}}\mathrm{F}(\cdot, \alpha_1)\right\}(c) \\
&= \mathrm{conc}\left\{\frac{1}{2}\beta_{0,\tilde{y}}\mathrm{F}(\cdot, \alpha_0), \frac{1}{2}\beta_{1,\tilde{y}}\mathrm{F}(\cdot, \alpha_1)\right\}(c).
\end{aligned}$$

Thus, for each $c \in \mathrm{Prob}^A$, we can write Alice's cheating probability as

$$\sum_{y \in B} \mathrm{conc}\left\{\frac{1}{2}\beta_{0,y}\mathrm{F}(\cdot, \alpha_0), \frac{1}{2}\beta_{1,y}\mathrm{F}(\cdot, \alpha_1)\right\}(c).$$

Note this way of optimizing the last message works for any strategy. For a general strategy, we would have a different c for every $y_1, \ldots, y_{n-1}$.

Thus, we have Alice's *improved eigenstrategy* which is when Alice chooses her first n messages according to her eigenstrategy, yet reveals a optimally.

Cheating Alice in six-round protocols. In six-round protocols, Alice's goal is to maximize the objective function

$$\frac{1}{2}\sum_{a \in \{0,1\}} \sum_{y_1 \in B_1} \sum_{y_2 \in B_2} \beta_{a,y_1 y_2}\mathrm{F}(s^{(a,y_1 y_2)}, \alpha_a)$$

over (s_1, s_2, s) satisfying:

$$\begin{aligned}
\mathrm{Tr}_{A_1}(s_1) &= 1, \\
\mathrm{Tr}_{A_2}(s_2) &= s_1 \otimes e_{B_1}, \\
\mathrm{Tr}_{A'_0}(s) &= s_2 \otimes e_{B_2}, \\
\\
s_1 &\in \mathbb{R}_+^{A_1}, \\
s_2 &\in \mathbb{R}_+^{A_1 \times B_1 \times A_2}, \\
s &\in \mathbb{R}_+^{A_1 \times A_2 \times B_1 \times B_2 \times A'_0}.
\end{aligned}$$

We suppose that Alice chooses her commitment a based on the most likely choice of b after seeing y_1 from Bob's first message. Let

$$f'(y_1) = \arg\max_{a \in A'_0} \{[\mathrm{Tr}_{B_2}(\beta_a)]_{y_1}\}$$

and 0 in the case of a tie. The last constraint can be written as the sum $\sum_{a \in A'_0} s^{(a,y_1 y_2)} = s_2^{(y_1)}$, for all $y_1 \in B_1$, where $s_2^{(y_1)}$ is the projection of s_2 with the index y_1 fixed. We set $s^{(a,y_1,y_2)} = s_2^{(y_1)}$, if $a = f'(y_1)$, and 0 otherwise. Now we set $s_2^{(y_1)} = s_2^0$, if $f'(y_1) = 0$, and $s_2^{(y_1)} = s_2^1$, if $f'(y_1) = 1$, where we optimize $s_2^0, s_2^1 \in \mathbb{R}_+^{A_1 \times A_2}$. The new objective function can be written as

$$\begin{aligned}
&\frac{1}{2} \sum_{a \in A'_0} \sum_{y_1 \in B_1, y_2 \in B_2} \beta_{a,y_1 y_2} \mathrm{F}(s^{(a,y_1 y_2)}, \alpha_a) \\
&= \frac{1}{2} \sum_{y_1 \in B_1} \left[\sum_{y_2 \in B_2} \beta_{f'(y_1),y_1 y_2} \right] \mathrm{F}(s_2^{f'(y_1)}, \alpha_{f'(y_1)}) \\
&= \frac{1}{2} \eta' \, \mathrm{F}(s_2^0, \alpha_0) + \frac{1}{2} \tau' \, \mathrm{F}(s_2^1, \alpha_1).
\end{aligned}$$

Since the only constraints remaining are $\mathrm{Tr}_{A_2}(s_2^0) = s_1 = \mathrm{Tr}_{A_2}(s_2^1)$, we now optimize over each choice of s_2^0 and s_2^1 separately using the following lemma.

Lemma 10 *For $\alpha \in \mathbb{R}_+^{A_1 \times A_2}$ and $c \in \mathbb{R}_+^{A_1}$, we have*

$$\max \{\mathrm{F}(p, \alpha) : \mathrm{Tr}_{A_2}(p) = c, \, p \geq 0\} \geq \mathrm{F}(c, \mathrm{Tr}_{A_2}(\alpha)).$$

The inequality can be shown to hold with equality by Uhlmann's theorem. However, we prove the inequality by exhibiting a feasible solution which is also useful for the analysis of cheating Bob.

Proof For each $x_1 \in A_1$, $x_2 \in A_2$, define p_{x_1,x_2} as

$$p_{x_1,x_2} := \begin{cases} c_{x_1} \frac{\alpha_{x_1,x_2}}{[\mathrm{Tr}_{A_2}(\alpha)]_{x_1}} & \text{if } [\mathrm{Tr}_{A_2}(\alpha)]_{x_1} > 0, \\ \\ c_{x_1} \frac{1}{|A_2|} & \text{if } [\mathrm{Tr}_{A_2}(\alpha)]_{x_1} = 0. \end{cases}$$

Then we have $p \geq 0$ is feasible since $[\mathrm{Tr}_{A_2}(p)]_{x_1} = c_{x_1}$ and it has objective function value $\mathrm{F}(p, \alpha) = \mathrm{F}(c, \mathrm{Tr}_{A_2}(\alpha))$, as desired. □

Using the lemma, we can write the problem as

$$\max_{c \in \mathrm{Prob}^{A_1}} \eta' \, \mathrm{F}(c, \mathrm{Tr}_{A_2}(\alpha_0)) + \tau' \, \mathrm{F}(c, \mathrm{Tr}_{A_2}(\alpha_1))$$

which has optimal value

$$\frac{1}{2} \lambda_{\max} \left(\eta' \sqrt{\mathrm{Tr}_{A_2}(\alpha_0)} \sqrt{\mathrm{Tr}_{A_2}(\alpha_0)}^{\mathrm{T}} + \tau' \sqrt{\mathrm{Tr}_{A_2}(\alpha_1)} \sqrt{\mathrm{Tr}_{A_2}(\alpha_1)}^{\mathrm{T}} \right)$$

and is lower bounded by

$$\left(\frac{1}{2}+\frac{1}{2}\sqrt{\mathrm{F}(\mathrm{Tr}_{A_2}(\alpha_0),\mathrm{Tr}_{A_2}(\alpha_1))}\right)\left(\frac{1}{2}+\frac{1}{2}\Delta(\mathrm{Tr}_{B_2}(\beta_0),\mathrm{Tr}_{B_2}(\beta_1))\right).$$

Again, this last quantity has context. This is the strategy where Alice measures the first message to learn b early and then tries to change the value of a. She can learn b with probability $\frac{1}{2}+\frac{1}{2}\Delta(\mathrm{Tr}_{B_2}(\beta_0),\mathrm{Tr}_{B_2}(\beta_1))$. She can successfully change the value of a with probability $\frac{1}{2}+\frac{1}{2}\sqrt{\mathrm{F}(\mathrm{Tr}_{A_2}(\alpha_0),\mathrm{Tr}_{A_2}(\alpha_1))}$. Thus, she can cheat with probability at least

$$\left(\frac{1}{2}+\frac{1}{2}\sqrt{\mathrm{F}(\mathrm{Tr}_{A_2}(\alpha_0),\mathrm{Tr}_{A_2}(\alpha_1))}\right)\left(\frac{1}{2}+\frac{1}{2}\Delta(\mathrm{Tr}_{B_2}(\beta_0),\mathrm{Tr}_{B_2}(\beta_1))\right).$$

5.2 Cheating Bob

We now turn to cheating Bob. We reproduce Theorem 5, give brief descriptions of the cheating strategies, then derive them and the corresponding bounds.

Theorem 5 *For a protocol parameterized by $\alpha_0,\alpha_1\in\mathrm{Prob}^A$, $\beta_0,\beta_1\in\mathrm{Prob}^B$, we can bound Bob's optimal cheating probability as follows:*

$$P^*_{\mathrm{B},0}\geq\frac{1}{2}+\frac{1}{2}\sqrt{\mathrm{F}(\beta_0,\beta_1)},\tag{7}$$

and

$$P^*_{\mathrm{B},0}\geq\frac{1}{2}+\frac{1}{2}\Delta(\mathrm{Tr}_{A_2\times\cdots\times A_n}(\alpha_0),\mathrm{Tr}_{A_2\times\cdots\times A_n}(\alpha_1)).\tag{8}$$

In a four-round protocol, we have

$$\begin{aligned}P^*_{\mathrm{B},0}&\geq\frac{1}{2}\sum_{a\in\{0,1\}}\mathrm{F}\left(\sum_{x\in A}\alpha_{a,x}v_x,\beta_a\right)&(9)\\&\geq\frac{1}{2}\sum_{x\in A}\lambda_{\max}\left(\sum_{a\in\{0,1\}}\alpha_{a,x}\sqrt{\beta_a}\sqrt{\beta_a}^{\mathrm{T}}\right)&(10)\\&\geq\max\left\{\frac{1}{2}+\frac{1}{2}\Delta(\alpha_0,\alpha_1),\ \frac{1}{2}+\frac{1}{2}\sqrt{\mathrm{F}(\beta_0,\beta_1)}\right\}\ ,\end{aligned}$$

where $\sqrt{v_x}$ is the normalized principal eigenvector of $\sum_{a\in\{0,1\}}\alpha_{a,x}\sqrt{\beta_a}\sqrt{\beta_a}^{\mathrm{T}}$.

In a six-round protocol, we have

$$\begin{aligned}P^*_{\mathrm{B},0}&\geq\frac{1}{2}\sum_{a\in A'_0}\mathrm{F}\left(\sum_{x\in A}\alpha_{a,x}\,\tilde{p_2}^{(x)},\beta_a\right)&(11)\\&\geq\frac{1}{2}\lambda_{\max}\left(\kappa\sqrt{\mathrm{Tr}_{B_2}(\beta_0)}\sqrt{\mathrm{Tr}_{B_2}(\beta_0)}^{\mathrm{T}}+\zeta\sqrt{\mathrm{Tr}_{B_2}(\beta_1)}\sqrt{\mathrm{Tr}_{B_2}(\beta_1)}^{\mathrm{T}}\right)&(12)\\&\geq\left(\frac{1}{2}+\frac{1}{2}\sqrt{\mathrm{F}(\mathrm{Tr}_{B_2}(\beta_0),\mathrm{Tr}_{B_2}(\beta_1))}\right)\left(\frac{1}{2}+\frac{1}{2}\Delta(\alpha_0,\alpha_1)\right),&(13)\end{aligned}$$

where

$$[\tilde{p_2}^{(x)}]_{y_1,y_2} := \begin{cases} c_{y_1} \frac{\beta_{g(x),y_1,y_2}}{[\mathrm{Tr}_{B_2}(\beta_{g(x)})]_{y_1}} & \textit{if} \quad [\mathrm{Tr}_{B_2}(\beta_{g(x)})]_{y_1} > 0 \ , \\ c_{y_1} \frac{1}{|B_2|} & \textit{if} \quad [\mathrm{Tr}_{B_2}(\beta_{g(x)})]_{y_1} = 0 \ , \end{cases}$$

$$\kappa = \sum_{\substack{x \in A: \\ \alpha_{0,x} \geq \alpha_{1,x}}} \alpha_{0,x} \ , \qquad \zeta = \sum_{\substack{x \in A: \\ \alpha_{0,x} < \alpha_{1,x}}} \alpha_{1,x} \ , \qquad g(x) = \arg\max_a \{\alpha_{a,x}\} \ ,$$

and $\sqrt{c}$ *is the normalized principal eigenvector of*

$$\frac{1}{2} \lambda_{\max}\left(\kappa \sqrt{\mathrm{Tr}_{B_2}(\beta_0)} \sqrt{\mathrm{Tr}_{B_2}(\beta_0)}^{\mathrm{T}} + \zeta \sqrt{\mathrm{Tr}_{B_2}(\beta_1)} \sqrt{\mathrm{Tr}_{B_2}(\beta_1)}^{\mathrm{T}} \right) .$$

Furthermore, if $|A_i| = |B_i|$ *for all* $i \in \{1, \ldots, n\}$*, then*

$$P^*_{\mathrm{B},0} \geq \frac{1}{2} \sum_{a \in \{0,1\}} \mathrm{F}(\alpha_a, \beta_a) \ . \tag{14}$$

We get analogous lower bounds for $P^*_{\mathrm{B},1}$ *by switching the roles of* β_0 *and* β_1 *in the above expressions.*

We call (7) Bob's *ignoring strategy* and (8) his *measuring strategy*. For four-round protocols, we call (9) Bob's *eigenstrategy* and (10) his *eigenstrategy lower bound*. For six-round protocols, we call (11) Bob's *six-round eigenstrategy*, (12) his *eigenstrategy lower bound*, and (13) his *three-round strategy*. We call (14) Bob's *returning strategy*.

Note that the only strategies that are affected by switching β_0 and β_1 are the eigenstrategy and the returning strategy.

We now briefly describe the strategies that yield the corresponding cheating probabilities in Theorem 5. Bob's ignoring strategy is to prepare the qubits BB' in the state $\phi' = (\phi_0 + \phi_1)/\left\|\phi_0 + \phi_1\right\|$ instead of ϕ_0 or ϕ_1, send the first n messages accordingly, then send a value for b that favours his desired outcome (along with the rest of ϕ'). His measuring strategy is to measure Alice's first message, choose b according to his best guess for a and run the protocol with ϕ_b. His returning strategy is to send Alice's messages right back to her. For the four-round eigenstrategy, Bob's commitment state is a principal eigenvector depending on Alice's first message. For a six-round protocol, Bob's three-round strategy is to prepare the qubits BB' in the following state $\phi' = (\phi'_0 + \phi'_1)/\left\|\phi'_0 + \phi'_1\right\|$ where ϕ'_0 and ϕ'_1 are purifications of $\mathrm{Tr}_{B_2,B'}(\phi_0 \phi_0^*)$ and $\mathrm{Tr}_{B_2,B'}(\phi_1 \phi_1^*)$, respectively. He measures Alice's second message to try to learn a, then depending on the outcome, he applies a (fidelity achieving) unitary before sending the rest of his messages. His six-round eigenstrategy is similar to his three-round strategy except that the first message is optimized in a way described in the proof.

Proof of Theorem 5. Bob's returning strategy is to send Alice's messages right back to her (if the dimensions agree). This way, the state that Alice checks at the end of the protocol is her own state. This is a good strategy when Alice and Bob share the same starting states, i.e., for a protocol with parameters $\alpha_0 = \beta_0$ and $\alpha_1 = \beta_1$. To calculate the cheating probability of this strategy, for any choice of parameters, it is easier to use the original cheating SDP as opposed to the reduced cheating SDP. This cheating strategy corresponds to the feasible solution

$$\bar{\rho}_1 = \bar{\rho}_2 = \cdots = \bar{\rho}_n = \bar{\rho}_F = \psi\psi^*$$

which has success probability given by the objective function value

$$\langle \bar{\rho}_F, \Pi_{\mathrm{A},0} \rangle = \langle \psi\psi^*, \Pi_{\mathrm{A},0} \rangle = \frac{1}{2} \sum_{a \in \{0,1\}} \mathrm{F}(\alpha_a, \beta_a).$$

This is clearly optimal when $\alpha_0 = \beta_0$ and $\alpha_1 = \beta_1$.

Recall Bob's reduced problem below

$$P^*_{\mathrm{B},0} = \max \left\{ \frac{1}{2} \sum_{a \in \{0,1\}} \mathrm{F}\left((\alpha_a \otimes \mathrm{I}_B)^{\mathrm{T}} p_n, \, \beta_a \right) : (p_1, \ldots, p_n) \in \mathcal{P}_{\mathrm{B}} \right\}.$$

There is a strategy for Bob that works for any n and is very important in the search algorithm. This is the strategy where Bob ignores all of Alice's messages and tries to choose b after learning a from Alice. By ignoring Alice's messages, he effectively sets $p_n = e_A \otimes d$, for some $d \in \mathrm{Prob}^B$, which we optimize. Under this restriction, he can cheat with probability

$$\begin{aligned} \max_{d \in \mathrm{Prob}^B} \frac{1}{2} \sum_{a \in \{0,1\}} \mathrm{F}\left((\alpha_a \otimes \mathrm{I}_B)^{\mathrm{T}} (e_A \otimes d), \, \beta_a \right) &= \max_{d \in \mathrm{Prob}^B} \frac{1}{2} \sum_{a \in \{0,1\}} \mathrm{F}\left(d, \beta_a \right) \\ &= \frac{1}{2} \lambda_{\max} \left(\sqrt{\beta_0} \sqrt{\beta_0}^{\mathrm{T}} + \sqrt{\beta_1} \sqrt{\beta_1}^{\mathrm{T}} \right) \\ &= \frac{1}{2} + \frac{1}{2} \sqrt{\mathrm{F}(\beta_0, \beta_1)} \end{aligned}$$

using Lemma 6 and Lemma 8. Note this is similar to the three-round case (discussed in Subsection 1). The reason this strategy is important is that it is easy to compute, only depends on half of the parameters, and is effective in pruning sub-optimal protocols. We call this Bob's *ignoring strategy.*

Another strategy for Bob is to measure Alice's first message, choose b accordingly, then play honestly. This is called Bob's *measuring strategy* and succeeds with probability

$$\frac{1}{2} + \frac{1}{2} \Delta(\mathrm{Tr}_{A_2 \times \cdots \times A_n}(\alpha_0), \mathrm{Tr}_{A_2 \times \cdots \times A_n}(\alpha_1)),$$

when $n \geq 2$.

Cheating Bob in four-round protocols. There are cheating strategies that apply to four-round protocols, that do not extend to a larger number of rounds. For example, Bob has all of Alice's $\mathbb{C}^A$ space before he sends any messages. We show that Bob can use this to his advantage. One example is Bob's measuring strategy, which leads to a cheating probability of

$$\frac{1}{2} + \frac{1}{2}\Delta(\alpha_0, \alpha_1) \ .$$

Similar to cheating Alice, we can develop an eigenstrategy for Bob. For the special case of four-round protocols, notice that Bob's cheating polytope contains only the constraints $\mathrm{Tr}_B(p) = e_A$ and $p \in \mathbb{R}_+^{A \times B}$. This can be rewritten as $p_x \in \mathrm{Prob}^B$ for all $x \in A$. Also, $\mathrm{F}\left((\alpha_a \otimes \mathrm{I}_B)^{\mathrm{T}} p_n, \, \beta_a\right)$ can be written as $\mathrm{F}\left(\sum_{x \in A} \alpha_{a,x} p_n^{(x)}, \beta_a\right)$, where $p_n^{(x)}$ is the projection of p_n with x fixed. Thus, we can simplify Bob's reduced problem as

$$P_{\mathrm{B},0}^* = \max \left\{ \frac{1}{2} \sum_{a \in \{0,1\}} \mathrm{F}\left(\sum_{x \in A} \alpha_{a,x} p_n^{(x)}, \beta_a \right) : p_n^{(x)} \in \mathrm{Prob}^B, \text{ for all } x \in A \right\}.$$

Since fidelity is concave, we have that

$$\mathrm{F}\left(\sum_{x \in A} \alpha_{a,x} p_n^{(x)}, \beta_a \right) \geq \sum_{x \in A} \alpha_{a,x} \, \mathrm{F}(p_n^{(x)}, \beta_a).$$

Therefore Bob's optimal cheating probability is bounded below by

$$\max \left\{ \frac{1}{2} \sum_{x \in A} \sum_{a \in \{0,1\}} \alpha_{a,x} \, \mathrm{F}(p_n^{(x)}, \beta_a) : p_n^{(x)} \in \mathrm{Prob}^B, \text{ for all } x \in A \right\}$$

which separates over $x \in A$. That is, we choose each $p_n^{(x)} \in \mathrm{Prob}^B$ separately to maximize $\sum_{a \in \{0,1\}} \alpha_{a,x} \, \mathrm{F}(p_n^{(x)}, \beta_a)$, which has optimal objective value $\lambda_{\max}\left(\sum_{a \in \{0,1\}} \alpha_{a,x} \sqrt{\beta_a} \sqrt{\beta_a}^{\mathrm{T}} \right)$ using Lemma 6. Thus, we know that

$$P_{\mathrm{B},0}^* \geq \frac{1}{2} \sum_{x \in A} \lambda_{\max} \left(\sum_{a \in \{0,1\}} \alpha_{a,x} \sqrt{\beta_a} \sqrt{\beta_a}^{\mathrm{T}} \right).$$

Since we use the concavity of the objective function, the bound we get may not be tight. Notice that solving the smaller separated problems yields a solution which is feasible for the original problem. Therefore, we can substitute this into the original objective function to get a better lower bound on Bob's optimal cheating probability. We call this Bob's *eigenstrategy*.

Since eigenvalues are expensive to compute, we can bound this quantity by

$$\begin{aligned}
&\frac{1}{2}\sum_{x\in A}\lambda_{\max}\left(\sum_{a\in\{0,1\}}\alpha_{a,x}\sqrt{\beta_a}\sqrt{\beta_a}^{\mathrm{T}}\right)\\
&\geq \min_{\beta_0,\beta_1\in\mathrm{Prob}^B}\frac{1}{2}\sum_{x\in A}\lambda_{\max}\left(\sum_{a\in\{0,1\}}\alpha_{a,x}\sqrt{\beta_a}\sqrt{\beta_a}^{\mathrm{T}}\right)\\
&= \frac{1}{2}\sum_{x\in A}\max_{a\in\{0,1\}}\{\alpha_{a,x}\}\\
&= \frac{1}{2}+\frac{1}{2}\Delta(\alpha_0,\alpha_1)\ ,
\end{aligned}$$

where the last equality follows from Lemma 7.

Since $\lambda_{\max}(X+Y)\leq\lambda_{\max}(X)+\lambda_{\max}(Y)$ for all matrices X and Y, we have that

$$\begin{aligned}
\frac{1}{2}\sum_{x\in A}\lambda_{\max}\left(\sum_{a\in\{0,1\}}\alpha_{a,x}\sqrt{\beta_a}\sqrt{\beta_a}^{\mathrm{T}}\right) &\geq \frac{1}{2}\lambda_{\max}\left(\sum_{x\in A}\sum_{a\in\{0,1\}}\alpha_{a,x}\sqrt{\beta_a}\sqrt{\beta_a}^{\mathrm{T}}\right)\\
&= \frac{1}{2}\lambda_{\max}\left(\sum_{a\in\{0,1\}}\sqrt{\beta_a}\sqrt{\beta_a}^{\mathrm{T}}\right)\\
&= \frac{1}{2}+\frac{1}{2}\sqrt{\mathrm{F}(\beta_0,\beta_1)}\ .
\end{aligned}$$

Therefore, Bob's eigenstrategy performs better than both his measuring strategy and ignoring strategy.

Cheating Bob in six-round protocols. In six-round protocols, Bob's goal is to maximize the objective function

$$\frac{1}{2}\sum_{a\in\{0,1\}}\mathrm{F}((\alpha_a\otimes\mathrm{I}_{B_1\times B_2})^{\mathrm{T}}p_2,\beta_a)$$

over (p_1,p_2) satisfying:

$$\begin{aligned}
\mathrm{Tr}_{B_1}(p_1) &= e_{A_1},\\
\mathrm{Tr}_{B_2}(p_2) &= p_1\otimes e_{A_2},\\
p_1 &\in \mathbb{R}_+^{A_1\times B_1},\\
p_2 &\in \mathbb{R}_+^{A_1\times B_1\times A_2\times B_2}.
\end{aligned}$$

Like in four-round protocols, we can lower bound the objective function as

$$\frac{1}{2}\sum_{a\in A_0'}\mathrm{F}\left(\sum_{x\in A}\alpha_{a,x}p_2^{(x)},\beta_a\right)\geq\frac{1}{2}\sum_{x\in A}\sum_{a\in A_0'}\mathrm{F}(p_2^{(x)},\alpha_{a,x}\beta_a)$$

and focus our attention on optimizing the function $\sum_{a\in A_0'}\mathrm{F}(p_2^{(x)},\alpha_{a,x}\beta_a)$. We use the following lemma.

Lemma 11 *For $\beta_0, \beta_1 \in \mathbb{R}_+^{B_1 \times B_2}$ and $c \in \mathbb{R}_+^{B_1}$, we have*

$$\max \left\{ \sum_{a \in \{0,1\}} \mathrm{F}(p, \beta_a) : \mathrm{Tr}_{B_2}(p) = c,\, p \geq 0 \right\} \geq \mathrm{F}(c, \mathrm{Tr}_{B_2}(\beta_{\tilde{a}})),$$

for any $\tilde{a} \in \{0,1\}$.

Proof Fix any $\tilde{a}$ and choose $p \in \arg\max \{\mathrm{F}(p, \beta_{\tilde{a}}) : \mathrm{Tr}_{B_2}(p) = c,\, p \geq 0\}$. Since the fidelity is nonnegative, the result follows by Lemma 10. □

By setting $p_1 = c \otimes e_{A_1}$, we have the constraint $\mathrm{Tr}_{B_2}(p^{(x)}) = c$ for all $x \in A$. We now apply Lemma 11 to get

$$\max_{p_2^{(x)}} \left\{ \sum_{a \in A_0'} \mathrm{F}(p_2^{(x)}, \alpha_{a,x}\beta_a) \right\} \geq \alpha_{g(x),x}\, \mathrm{F}(c, \mathrm{Tr}_{B_2}(\beta_{g(x)})),$$

where $g(x) := \arg\max_{a \in A_0'} \{\alpha_{a,x}\}$, and 0 in the case of a tie.

Substituting this into the relaxed objective function above, we have

$$\begin{aligned}
&\max_{c \in \mathrm{Prob}^{B_1}} \frac{\kappa}{2} \mathrm{F}(c, \mathrm{Tr}_{B_2}(\beta_0)) + \frac{\zeta}{2} \mathrm{F}(c, \mathrm{Tr}_{B_2}(\beta_1)) \\
&= \frac{1}{2} \lambda_{\max} \left(\kappa \sqrt{\mathrm{Tr}_{B_2}(\beta_0)} \sqrt{\mathrm{Tr}_{B_2}(\beta_0)}^{\mathrm{T}} + \zeta \sqrt{\mathrm{Tr}_{B_2}(\beta_1)} \sqrt{\mathrm{Tr}_{B_2}(\beta_1)}^{\mathrm{T}} \right) \quad (15) \\
&\geq \left(\frac{1}{2} + \frac{1}{2} \Delta(\alpha_0, \alpha_1) \right) \left(\frac{1}{2} + \frac{1}{2} \sqrt{\mathrm{F}(\mathrm{Tr}_{B_2}(\beta_0), \mathrm{Tr}_{B_2}(\beta_1))} \right). \quad (16)
\end{aligned}$$

The quantity (16) corresponds to the strategy where Bob measures Alice's second message to try to learn a early, then tries to change the value of b. He can learn a after Alice's second message with probability $\frac{1}{2} + \frac{1}{2}\Delta(\alpha_0, \alpha_1)$. He can change the value of b with probability $\frac{1}{2} + \frac{1}{2}\sqrt{\mathrm{F}(\mathrm{Tr}_{B_2}(\beta_0), \mathrm{Tr}_{B_2}(\beta_1))}$. Thus, he can cheat with probability at least

$$\left(\frac{1}{2} + \frac{1}{2} \sqrt{\mathrm{F}(\mathrm{Tr}_{B_2}(\beta_0), \mathrm{Tr}_{B_2}(\beta_1))} \right) \left(\frac{1}{2} + \frac{1}{2} \Delta(\alpha_0, \alpha_1) \right).$$

We call this Bob's *three-round strategy.*

Although we used many bounds in developing the quantity (12), such as concavity and the lower bound in Lemma 11, we can recover some of the losses by generating its corresponding feasible solution and computing its objective function value for the original objective function. For example, we can calculate c as the entry-wise square of the normalized principal eigenvector of

$$\frac{1}{2} \lambda_{\max} \left(\kappa \sqrt{\mathrm{Tr}_{B_2}(\beta_0)} \sqrt{\mathrm{Tr}_{B_2}(\beta_0)}^{\mathrm{T}} + \zeta \sqrt{\mathrm{Tr}_{B_2}(\beta_1)} \sqrt{\mathrm{Tr}_{B_2}(\beta_1)}^{\mathrm{T}} \right),$$

then calculate $p_2^{(x)}$ for each value of x from the construction of the feasible solution in the proof of Lemma 10. We call this Bob's *eigenstrategy.*

6 Computer aided bounds on bias

The search algorithm has the potential to give us computer aided *proofs* that certain coin-flipping protocols have bias within a small interval. In this section, we describe the kind of bound we can deduce under the assumption that the software provides us an independently verifiable upper bound on the additive error in terms of the objective value.

We begin by showing that any state $\xi \in \mathbb{R}^D$ of the form used in the protocols is suitably close to a state given by the mesh used in the search algorithm. For an integer $N \geq 1$, let $\mathbb{M}_N = \{j/N : j \in \mathbb{Z}, 0 \leq j \leq N\}$.

Lemma 12 *Let $N \geq 1$ be an integer. Consider the state $\xi = \sum_{i=1}^{D} \sqrt{\gamma_i}\, e_i$ in $\mathbb{R}^D$, where $\gamma \in \mathrm{Prob}^D$. Then there is a probability distribution $\gamma' \in \mathrm{Prob}^D \cap \mathbb{M}_N^D$ such that the corresponding state $\xi' = \sum_{i=1}^{D} \sqrt{\gamma'_i}\, e_i$ satisfies $\xi^* \xi' \geq 1 - D/2N$.*

Proof Let $\tilde{\gamma}_i = \lfloor \gamma_i N \rfloor / N$ for $i \in \{1, 2, \ldots, D\}$. Note that $\sum_{i=1}^{D} \tilde{\gamma}_i \leq 1$, and that

$$1 - \sum_{i=1}^{D} \tilde{\gamma}_i = \sum_{i=1}^{D} \gamma_i - \sum_{i=1}^{D} \tilde{\gamma}_i = j/N,$$

for some $j \in \{0, 1, 2, \ldots, D\}$. We may obtain γ' by adding $1/N$ to j coordinates of $\tilde{\gamma}$. For concreteness, let $\gamma'_i = \tilde{\gamma}_i + 1/N$ for $i \in \{1, 2, \ldots, j\}$ and $\gamma'_i = \tilde{\gamma}_i$ for $i \in \{j+1, \ldots, D\}$. We therefore have $\|\gamma - \gamma'\|_1 \leq D/N$, and

$$\xi^* \xi' \quad = \quad \mathrm{F}(\gamma, \gamma')^{1/2} \quad \geq \quad 1 - \frac{D}{2N} \;,$$

by a Fuchs-van de Graaf inequality [5]. □

The above lemma helps us show that any protocol in the family we consider is approximated by one given by the mesh.

Lemma 13 *Consider a bit-commitment based coin-flipping protocol $\mathcal{A}$ with bias ϵ of the form considered in this paper. Suppose $\mathcal{A}$ is specified by the 4-tuple $(\alpha_0, \alpha_1, \beta_0, \beta_1)$, where $\alpha_i, \beta_i \in \mathrm{Prob}^D$. Then there is a protocol $\mathcal{A}'$ with bias ϵ' of the same form, defined by a 4-tuple $(\alpha'_0, \alpha'_1, \beta'_0, \beta'_1)$, satisfying the two conditions $|\epsilon - \epsilon'| \leq 2\sqrt{D/N}$ and $\alpha'_i, \beta'_i \in \mathrm{Prob}^D \cap \mathbb{M}_N^D$.*

Proof The statement of the lemma is vacuous if $1 - D/2N < 0$, we therefore assume $1 - D/2N \geq 0$. We show that $\epsilon' \leq \epsilon + 2\sqrt{D/N}$ (the other inequality $\epsilon \leq \epsilon' + 2\sqrt{D/N}$ follows similarly).

Without loss in generality, assume that bias ϵ' is achieved when Bob cheats towards 0 in protocol $\mathcal{A}'$. Recall

$$\psi = \frac{1}{\sqrt{2}} \left(e_0 \otimes e_0 \otimes \psi_0 + e_1 \otimes e_1 \otimes \psi_1 \right) \;, \qquad \text{and}$$

$$\Pi_{\mathrm{A},0} = \sum_{b \in \{0,1\}} e_b e_b^* \otimes e_b e_b^* \otimes \phi_b \phi_b^* \;.$$

Let the probability distributions $\alpha'_0, \alpha'_1, \beta'_0, \beta'_1$ and states $\psi'_0, \psi'_1, \phi'_0, \phi'_1$ corresponding to the distributions $\alpha_0, \alpha_1, \beta_0, \beta_1$, respectively, be the ones guaranteed by Lemma 12. Let

$$\begin{aligned} \psi' &= \frac{1}{\sqrt{2}} \left(e_0 \otimes e_0 \otimes \psi'_0 + e_1 \otimes e_1 \otimes \psi'_1 \right) \ , \qquad \text{and} \\ \Pi'_{\mathrm{A},0} &= \sum_{b \in \{0,1\}} e_b e_b^* \otimes e_b e_b^* \otimes \phi'_b (\phi'_b)^* \ . \end{aligned}$$

We have $\psi^* \psi' \geq 1 - \frac{D}{2N}$, by Lemma 12, and

$$\begin{aligned} \| \psi' (\psi')^* - \psi \psi^* \|_* &\leq 2 \left(1 - (\psi^* \psi')^2 \right)^{1/2} \\ &\leq 2 \sqrt{D/N} \ , \end{aligned}$$

by a Fuchs-van de Graaf inequality [5]. Further,

$$\begin{aligned} \left\| \Pi'_{\mathrm{A},0} - \Pi_{\mathrm{A},0} \right\|_{\mathrm{op}} &\leq \max \left\{ \| \phi'_0 (\phi'_0)^* - \phi_0 \phi_0^* \|_{\mathrm{op}} , \| \phi'_1 (\phi'_1)^* - \phi_1 \phi_1^* \|_{\mathrm{op}} \right\} \\ &\leq \sqrt{D/N} \ , \end{aligned}$$

using the identity $\| v v^* - u u^* \|_{\mathrm{op}} = \left(1 - (v^* u)^2 \right)^{1/2}$ for normalized real vectors v and u. Here, $\|X\|_{\mathrm{op}}$ denotes the operator norm of X, namely the largest singular value of the matrix X.

For this analysis, we assume that the protocol $\mathcal{A}'$ is of the form analyzed in this paper and the two parties start with joint initial state $e_0^{\otimes 4n}$, apply $U_1, U_2, \ldots, U_{2n}$ alternately, and finally measure their parts of the system to obtain the output.

Consider Bob's cheating strategy towards 0 (which we assumed achieves bias ϵ'). As in the proof of Lemma 1, it follows that there are spaces $\mathcal{H}_i$ and corresponding unitary operations U'_i on them for even $i \leq 2n$ that characterize his cheating strategy. When Alice measures $\zeta' = (U'_{2n} U_{2n-1} U'_{2n-2} \cdots U_1) e_0^{\otimes 4n}$, she obtains outcome 0 with probability $\left\| \Pi'_{\mathrm{A},0} \zeta' \right\|_2^2 = \frac{1}{2} + \epsilon'$. (In the expression for the final state ζ', we assume that the unitary operations extend to the combined state space by tensoring with identity over the other part.)

We consider the same cheating strategy for Bob in the protocol $\mathcal{A}$, in which Alice starts with the commitment state ψ, and performs the measurement $\{ \Pi_{\mathrm{A},0}, \Pi_{\mathrm{A},1}, \Pi_{\mathrm{A,abort}} \}$. This corresponds to a different initial unitary transformation for Alice instead of U_1. Let ζ be the corresponding final joint state. Note that ψ is mapped to ζ using the same unitary transformation that maps ψ' to ζ' since Bob is using the same cheating strategy. The probability of outcome 0 is $\| \Pi_{\mathrm{A},0} \zeta \|_2^2 \leq \frac{1}{2} + \epsilon$, as the protocol $\mathcal{A}$ has bias ϵ. We may bound the difference in probabilities as follows.

$$
\begin{aligned}
\epsilon' - \epsilon &\le \mathrm{Tr}\left(\Pi'_{\mathrm{A},0}\zeta'(\zeta')^*\right) - \mathrm{Tr}\left(\Pi_{\mathrm{A},0}\zeta\zeta^*\right) \\
&= \mathrm{Tr}\left((\Pi'_{\mathrm{A},0} - \Pi_{\mathrm{A},0})\zeta'(\zeta')^*\right) + \mathrm{Tr}\left(\Pi_{\mathrm{A},0}(\zeta'(\zeta')^* - \zeta\zeta^*)\right) \\
&\le \left\|\Pi'_{\mathrm{A},0} - \Pi_{\mathrm{A},0}\right\|_{\mathrm{op}} + \frac{1}{2}\left\|\zeta\zeta^* - \zeta'(\zeta')^*\right\|_* \\
&= \left\|\Pi'_{\mathrm{A},0} - \Pi_{\mathrm{A},0}\right\|_{\mathrm{op}} + \frac{1}{2}\left\|\psi\psi^* - \psi'(\psi')^*\right\|_* \\
&\le 2\sqrt{D/N}\ ,
\end{aligned}
$$

as claimed. □

We may infer bounds on classes of protocols using the search algorithm and the lemma above. Suppose the computational approximation to the bias obtained by the algorithm has net additive error τ due to the protocol filter and SDP solver and the finite precision arithmetic used in the computations. If the algorithm reports that there are no protocols with bias at most ϵ^* given by a mesh with precision parameter N, then it holds that there are no 4-tuples, even outside the mesh, with bias at most $\epsilon^* - 2\sqrt{D/N} - \tau$. Here D is the dimension of Alice's (or Bob's) first n messages (i.e., commitment states used, or equivalently, the size of the support of an element of the 4-tuple).

A quick calculation with $\epsilon^* = 0.2499$ and $\tau \approx 0$ shows that mesh fineness parameter $N \ge 2185 \times d$ for four-round protocols and $N \ge 2185 \times d^2$ for six-round protocols with message dimension d, would be sufficient for us to conclude that such protocols *do not achieve* optimal bias ≈ 0.2071. A slightly finer mesh would be needed if one were to expect τ to be somewhat larger than 0. We would then obtain *computer aided* lower bounds for new classes of bit-commitment based protocols. Thus, a refinement of the search algorithm that allows finer meshes for messages of larger dimension and over more rounds would be well worth pursuing.

7 New bounds for four-round qubit protocols

We can derive analytical bounds on the bias of four-round protocols using the strengthened Fuchs-van de Graaf inequality for qubit states, below:

Proposition 1 ([11]) *For any quantum states $\rho_1, \rho_2 \in \mathbb{S}^2_+$, i.e., qubits, we have*

$$1 \quad \le \quad \Delta(\rho_1, \rho_2) + \mathrm{F}(\rho_1, \rho_2)\ .$$

Recall from Section 5 that Bob can cheat in a four-round protocol with probability bounded below by

$$P^*_{\mathrm{B},0} \quad \ge \quad \frac{1}{2} + \frac{1}{2}\sqrt{\mathrm{F}(\beta_0, \beta_1)} \tag{17}$$

and

$$P^*_{\mathrm{B},0} \quad \geq \quad \frac{1}{2} + \frac{1}{2} \Delta(\alpha_0, \alpha_1) \tag{18}$$

and Alice can cheat with probability bounded below by

$$P^*_{\mathrm{A},0} \quad \geq \quad \left(\frac{1}{2} + \frac{1}{2} \sqrt{\mathrm{F}(\alpha_0, \alpha_1)} \right) \left(\frac{1}{2} + \frac{1}{2} \Delta(\beta_0, \beta_1) \right) \quad . \tag{19}$$

If $\beta_0, \beta_1 \in \mathrm{Prob}^2$, then by (17) and Proposition 1, we have

$$\Delta(\beta_0, \beta_1) \geq 4P^*_{\mathrm{B},0}(1 - P^*_{\mathrm{B},0})$$

and if $\alpha_0, \alpha_1 \in \mathrm{Prob}^2$, then from (18) and Proposition 1, we have

$$\mathrm{F}(\alpha_0, \alpha_1) \geq 2 - 2P^*_{\mathrm{B},0}.$$

Combining these two bounds with (19), we get

$$4P^*_{\mathrm{A},0} \quad \geq \quad \left(1 + \sqrt{2 - 2P^*_{\mathrm{B},0}}\right) \left(1 + 4P^*_{\mathrm{B},0}(1 - P^*_{\mathrm{B},0})\right)$$

which is a decreasing function of $P^*_{\mathrm{B},0}$. Setting this lower bound equal to $P^*_{\mathrm{B},0}$ and solving for $P^*_{\mathrm{B},0}$, we can show $\max\{P^*_{\mathrm{A},0}, P^*_{\mathrm{B},0}\} \geq 0.7487 > 1/\sqrt{2} \approx 0.7071$. In fact, using the regular Fuchs-van de Graaf inequalities [5], we can get bounds when they are not both two-dimensional. If β_0, β_1 are two-dimensional and α_0, α_1 are not, we get a lesser bound of $\max\{P^*_{\mathrm{A},0}, P^*_{\mathrm{B},0}\} \geq 0.7140 > 1/\sqrt{2}$. On the other hand, if α_0, α_1 are two-dimensional and β_0, β_1 are not, then we get $\max\{P^*_{\mathrm{A},0}, P^*_{\mathrm{B},0}\} \geq 0.7040 \not> 1/\sqrt{2}$, so we do not rule out the possibility of protocols with bias $1/\sqrt{2} - 1/2$ with such parameters. Note that tests where α_0, α_1 are two-dimensional are subsumed in the higher-dimensional tests we performed. However, future experiments could include computationally testing the case where Alice's first message is two-dimensional and Bob's first message has dimension 10 or greater.

8 Random offset

We would like to test more protocols, and also avoid anomalies that may have arisen in the previous tests due to the structure of the mesh we use and also any special relation the protocol states may have with each other due to low precision. The six-round searches take a long time, which restricts the precision ν we can use. The resulting mesh is also highly structured. We would like to test protocol parameters that do not necessarily have such regular entries. With this end in mind, we offset all of the values in the search by some random additive term $\delta > 0$. For example, say the entries of α_0, α_1, β_0, and β_1 have been selected from the set $\{0, \nu, 2\nu, \ldots, 1 - \nu, 1\}$. With an offset parameter $\delta \in (0, \nu/2)$, we use the range

$$\{\delta, \delta + \nu, \delta + 2\nu, \ldots, \delta + 1 - \nu\} .$$

Table 3 The percentage of protocols that get stopped by each strategy in the worst case after 100 random instances of offset parameter δ.

$d = 2$	$\nu = 1/3$	$\nu = 1/4$	$\nu = 1/5$	$\nu = 1/6$
G1	71.87%	82.35%	84.06%	86.63%
G2	17.18%	29.80%	15.80%	24.15%
G3	8.17%	10.73%	13.46%	12.12%
G4	51.45%	49.68%	53.99%	48.44%
G5	70.00%	83.29%	78.02%	82.86%
G6	0%	0%	0%	0%
G7	75.00%	92.43%	87.32%	94.35%
G8	100%	100%	49.10%	100%
G9			0%	
G10			0%	
SDPB0			100%	

Table 4 The percentage of protocols that get stopped by each strategy in the average case after 100 random instances of offset parameter δ.

$d = 2$	$\nu = 1/3$	$\nu = 1/4$	$\nu = 1/5$	$\nu = 1/6$
G1	85.75%	87.30%	89.42%	90.47%
G2	17.18%	29.80%	15.80%	24.15%
G3	10.85%	13.15%	14.53%	12.35%
G4	62.49%	52.53%	55.34%	53.03%
G5	70.00%	87.11%	93.46%	93.29%
G6	0%	0%	0%	0%
G7	98.70%	99.01%	96.58%	98.77%

Note that this destroys index symmetry. The simplest way to see this is to consider the 2-dimensional probability distributions created in this way. They are

$$\left\{ \begin{bmatrix} \delta \\ 1-\delta \end{bmatrix}, \begin{bmatrix} \delta+\nu \\ 1-\delta-\nu \end{bmatrix}, \begin{bmatrix} \delta+2\nu \\ 1-\delta-2\nu \end{bmatrix}, \ldots, \begin{bmatrix} \delta+1-\nu \\ \nu-\delta \end{bmatrix} \right\}.$$

We see that the set of first entries is not the same as the set of second entries when $\delta > 0$. We choose the last entry in each vector to be such that the entries add to 1. Since we generate all four of the probability distributions in the same manner, we can still apply the symmetry arguments to suppose α_0 has the largest entry out of both α_0 and α_1 and similarly for β_0 and β_1.

Tables 3 and 4 show how well each strategy in the filter performs after testing 100 random choices of offset parameter $\delta \in [0, 1/100]$. The percentages in the table entries correspond to the amount of protocols that particular strategy stopped from the ones surviving the previous filter strategies. For each random choice of δ, a percentage is calculated and Table 3 presents the least percentage and Table 4 presents the average percentage.

Observations on the random offset tests. We notice that G6 performs very poorly on these tests. We need finer precision to see the effects of G6 in the filter. Also, G1 performs generally better as the filter precision increases. We see from the previous tables that it should stay at roughly 90%. We see that G5 and G7 perform very well. G7 sometimes filters out the rest (this is why the average case table only displays up to G7). G8 performs well most of the time, except in the $\nu = 1/5$ case in the worst case table. Few protocols made it past the entire filter, and only SDPB0 needed to be solved of the four SDPs. No protocols with bias at most 0.2499 were found.

9 Zoning-in tests

The computational tests that we performed so far suggest that there are no protocols with cheating probabilities less than 0.7499 (at least for the values of the parameters used in the tests) which is slightly less than the best known constructions. The tests also show that the number of protocols grows very large as the mesh precision increases. This poses the question of whether there are protocols that have optimal cheating probabilities just slightly less than 3/4 when one considers increased mesh precisions. In this section, we focus on searching for such protocols.

There are a few obstacles to deal with in such a search. The first is that increasing the precision of the mesh drastically increases the number of protocols to be tested. To deal with this, we restrict the set of parameters to be tested by only considering protocols which are close to optimal, i.e., near-optimal protocols. In other words, we "zone in" on some promising protocols to see if there is any hope of improving the bias by perturbing some of the entries. To do this, we fix a near-optimal protocol and create a mesh over a small ball around the entries in each probability vector. We would like a dramatic increase in precision, so we use a ball of radius $2\,\nu$ (unless stated otherwise), yielding up to 5 increments tested around each entry. This gives us the advantage of having a constant number of protocols to check, independent of the mesh precision. However, this comes at the cost that we lose symmetry, since we do not wish to permute the entries nor the probability distributions defining the protocol.

Another challenge is to find the near-optimal protocols. The approach we take is to keep track of the best protocol found, updating the filter threshold accordingly. There are two issues with this approach. One is that increasing the threshold decreases the efficiency of the filter, so we are not able to search over the same mesh precisions given earlier in this section. The second is that there is an abundance of protocols with cheating probabilities exactly equal to 3/4. As was done in the protocol example section (Section 1), we can embed an optimal three-round protocol with optimal cheating probabilities 3/4 into a four-round (or six-round) protocol. One way to do this is to set $\alpha_0 = \alpha_1$ (i.e. Alice's first n messages contain *no* information) or by setting $\beta_0 \perp \beta_1$ (i.e. Bob's first message reveals b, making the rest of his messages meaningless). So we already know many protocols with cheating probabilities equal to 3/4, but can we find others? We now discuss the structure of near-optimal protocols in the case of four-round and six-round protocols, and how we zone in on them.

Four-round version. For the four-round search, we fix a message dimension $d = 5$ and use precision parameters $\nu \in \{1/7, 1/8, 1/9, 1/10, 1/11\}$. This search yields a minimum (computer verified) bias of $\epsilon = 0.2647$ when we rule out protocols with $\alpha_0 = \alpha_1$ or $\beta_0 \perp \beta_1$. In other words, we have that all of the protocols tested had one of the following three properties:

- $\alpha_0 = \alpha_1$,
- $\langle \beta_0, \beta_1 \rangle = 0$,
- $\max \left\{ P^*_{\mathrm{A},0}, P^*_{\mathrm{A},1}, P^*_{\mathrm{B},0}, P^*_{\mathrm{B},1} \right\} \geq 0.7647$.

This suggests that near-optimal four-round protocols behave similarly to optimal three-round protocols. We now zone in on two protocols, one representing each of the first two conditions above. The first protocol is

$$\alpha_0 = \frac{1}{2} [0, 0, 0, 1, 1]^{\mathrm{T}}, \quad \alpha_1 = \frac{1}{2} [0, 0, 1, 0, 1]^{\mathrm{T}},$$

$$\beta_0 = [0, 0, 0, 0, 1]^{\mathrm{T}}, \quad \beta_1 = [0, 0, 0, 1, 0]^{\mathrm{T}}$$

which satisfies $\beta_0 \perp \beta_1 = 0$ and has all four (computationally verified) cheating probabilities equal to $3/4$. The second protocol is

$$\alpha_0 = [0, 0, 0, 0, 1]^{\mathrm{T}}, \quad \alpha_1 = [0, 0, 0, 0, 1]^{\mathrm{T}},$$

$$\beta_0 = \frac{1}{2} [0, 0, 0, 1, 1]^{\mathrm{T}}, \quad \beta_1 = \frac{1}{2} [0, 0, 1, 0, 1]^{\mathrm{T}}$$

which satisfies $\alpha_0 = \alpha_1$ and has all four (computationally verified) cheating probabilities equal to $3/4$. Tables 5 and 6 display the zoning-in searches for these two protocols with threshold exactly $3/4$. Note we use mesh precisions up to 10^{-16} which, by Lemma 13, can guarantee us a change in bias up to 4×10^{-8}. A (computationally verified) change in bias of this magnitude could be argued to be an actual decrease in bias and not an error due to finite precision arithmetic.

Observations on the four-round tests. Note that not all filter strategies are useful in the zoning-in tests. For example, if F1 $\approx 1/2 < 3/4$ for the protocol we are zoning-in on, then it never filters out any protocols with the precisions considered. Considering this, and by examining the tables, we see that most strategies filter out many protocols, or none at all. Also from the tables, we see that no protocols get through the entire filter. Notice that we needed to use more strategies than were needed in previous tables, namely F9 and F10. In the previous searches, F8 was the last filter strategy needed, thus demonstrating some protocols which F8 fails to filter out (noting a larger threshold was used here than in the previous tests). It is worth noting the efficiency of the four-round filter. The algorithm did not need to solve for any optimal cheating values in any of the four-round zoning-in tests.

These tables suggest that perturbing the entries of the parameters defining these two near-optimal protocols does not yield better bias.

Table 5 The number of four-round protocols that get past each strategy when zoning-in on the first near-optimal protocol (showing F1 and only the other strategies that helped to weed out protocols).

$d = 5$	$\nu = 1/10^{10}$	$\nu = 1/10^{11}$	$\nu = 1/10^{12}$	$\nu = 1/10^{13}$	$\nu = 1/10^{14}$	$\nu = 1/10^{15}$	$\nu = 1/10^{16}$
F1	119,574,225	119,574,225	119,574,225	119,574,225	119,574,225	119,574,225	119,574,225
F2	20,253,807	20,253,807	20,411,271	21,067,371	20,253,807	20,253,807	6,337,926
F3	493,557	493,557	493,557	581,503	493,557	498,504	33,279
F6	493,557	493,557	493,557	576,819	493,557	480,276	13,695
F7	981	981	981	1,245	981	855	0
F8	0	0	0	0	0	29	0
F10	0	0	0	0	0	0	0

Table 6 The number of four-round protocols that get past each strategy when zoning-in on the second near-optimal protocol (showing F1 and only the other strategies that helped to weed out protocols).

$d = 5$	$\nu = 1/10^{10}$	$\nu = 1/10^{11}$	$\nu = 1/10^{12}$	$\nu = 1/10^{13}$	$\nu = 1/10^{14}$	$\nu = 1/10^{15}$	$\nu = 1/10^{16}$
F1	9,277,254	9,277,254	9,277,254	9,277,254	9,277,254	8,516,178	4,953,555
F3	907,608	907,608	913,496	912,864	907,608	828,952	1,030,152
F6	693,576	693,576	695,016	713,424	693,576	412,392	8,624
F7	45,376	45,376	45,376	55,064	43,264	3,136	5,056
F8	0	0	0	0	0	68	3,140
F9	0	0	0	0	0	8	2,072
F10	0	0	0	0	0	0	0

Six-round version. For the six-round search, we fix a message dimension $d = 2$ and use precision parameters $\nu \in \{1/7, 1/8, 1/9, 1/10, 1/11, 1/12\}$. For $\nu > 1/12$, the test results were similar to the four-round version, that all of the protocols tested had one of the following three properties:

- $\alpha_0 = \alpha_1$,
- $\langle \beta_0, \beta_1 \rangle = 0$,
- $\max\left\{P^*_{A,0}, P^*_{A,1}, P^*_{B,0}, P^*_{B,1}\right\} \geq 0.7521$.

We choose the following two near-optimal protocols to represent the first two conditions:

$$\alpha_0 = \frac{1}{2}[0,0,1,1]^{\mathrm{T}}, \quad \alpha_1 = \frac{1}{2}[0,1,0,1]^{\mathrm{T}},$$
$$\beta_0 = [0,0,0,1]^{\mathrm{T}}, \quad \beta_1 = [0,0,1,0]^{\mathrm{T}},$$

which satisfies $\beta_0 \perp \beta_1 = 0$, and

$$\alpha_0 = [0,0,0,1]^{\mathrm{T}}, \quad \alpha_1 = [0,0,0,1]^{\mathrm{T}},$$
$$\beta_0 = \frac{1}{2}[0,0,1,1]^{\mathrm{T}}, \quad \beta_1 = \frac{1}{2}[0,1,0,1]^{\mathrm{T}},$$

which satisfies $\alpha_0 = \alpha_1$. Both of these protocols have all four (computationally verified) cheating probabilities equal to $3/4$.

However, when $\nu = 1/12$, we found several protocols with a (computationally found) bias of 0.25. We therefore searched for all protocols with bias 0.2501 or less. We discovered the following 4 protocols, no two of which are equivalent to each other with respect to symmetry. Note that these protocols bear no resemblance to any bias $1/4$ protocols previously discovered. These protocols are below:

$$\alpha_0 = \frac{1}{3}[0,1,1,1]^{\mathrm{T}}, \quad \alpha_1 = \frac{1}{3}[1,1,0,1]^{\mathrm{T}},$$
$$\beta_0 = \frac{1}{12}[0,3,0,9]^{\mathrm{T}}, \quad \beta_1 = \frac{1}{12}[0,3,9,0]^{\mathrm{T}}$$

and

$$\alpha_0 = \frac{1}{3}[0,1,1,1]^{\mathrm{T}}, \quad \alpha_1 = \frac{1}{3}[1,1,0,1]^{\mathrm{T}},$$
$$\beta_0 = \frac{1}{12}[1,2,0,9]^{\mathrm{T}}, \quad \beta_1 = \frac{1}{12}[1,2,9,0]^{\mathrm{T}}$$

and

$$\alpha_0 = \frac{1}{3}[0,1,1,1]^{\mathrm{T}}, \quad \alpha_1 = \frac{1}{3}[1,1,1,0]^{\mathrm{T}},$$
$$\beta_0 = \frac{1}{12}[0,3,0,9]^{\mathrm{T}}, \quad \beta_1 = \frac{1}{12}[0,3,9,0]^{\mathrm{T}}$$

and

$$\alpha_0 = \frac{1}{3}[0,1,1,1]^{\mathrm{T}}, \quad \alpha_1 = \frac{1}{3}[1,1,1,0]^{\mathrm{T}},$$

$$\beta_0 = \frac{1}{12}\,[1,2,0,9]^{\mathrm{T}}\,, \quad \beta_1 = \frac{1}{12}\,[1,2,9,0]^{\mathrm{T}}\,.$$

Note that these four protocols have the property that all the filter strategies for them have cheating probabilities strictly less than 3/4. Since many of these strategies are derived from optimal three-round strategies, this property makes them especially interesting. (Other six-round protocols were found. However, these were equivalent to the ones above via symmetry.)

We now zone-in on these six protocols as indicated in the following tables. Note that we decrease the radius of the balls to ν for the third, fourth, fifth, and sixth protocol (compared to 2ν for the other protocols). This is for two reasons. One is that most the entries are bounded away from 0 or 1, making the intersection of the ball and valid probability vectors large. Second, the filter has to work harder in this case since many of the filter cheating probabilities are bounded away from 3/4 and thus more computationally expensive cheating probabilities need to be computed.

Preliminary tests show that when zoning-in on some of these 6 protocols, the default SDP solver precision is not enough to determine whether the bias is strictly less than 3/4, or whether it is numerical round-off. To provide a further test, we add an extra step for those protocols that get through the filter and SDPs, we increase the SDP solver accuracy (set pars.eps = 0 in SeDuMi) and let the solver run until no more progress is being made. The row “Better Accuracy” shows how many protocols get through this added step. Furthermore, we use the maximum of the primal and dual values when calculating the optimal cheating values since we are not guaranteed exact feasibility of both primal and dual solutions in these computational experiments.

Observations on the six-round tests. We see in Tables 7, 8, and 9 that zoning-in on the six protocols yields no protocols with bias less than 1/4. The zoning-in tests for the second near-optimal protocol are the only ones where we needed the added step of increasing the SDP solver accuracy. We see that this added step removed the remaining protocols.

We remark on the limitations of using such fine mesh precisions. For example, when zoning-in on the fourth and sixth protocol, only two strategies were used, G1 and SDPB0. These are both strategies for Bob which suggests that there are some numerical precision issues. We expect that some perturbations would decrease Bob’s cheating probability, for example when α_0 and α_1 become “closer” and β_0 and β_1 remain the same. However, the precisions used in these searches do not find any such perturbations.

From the outcome of the zoning-in tests, along with the computational evidence from all the other tests we conducted, we conjecture that any strong coin-flipping protocol based on bit-commitment as considered in this paper has bias at least 1/4.

Table 7 The number of six-round protocols that get past each strategy when zoning-in on the first near-optimal protocol (showing G1 and only the other strategies that helped to weed out protocols).

$d = 2$	$\nu = 1/10^{10}$	$\nu = 1/10^{11}$	$\nu = 1/10^{12}$	$\nu = 1/10^{13}$	$\nu = 1/10^{14}$	$\nu = 1/10^{15}$	$\nu = 1/10^{16}$
G1	1,476,225	1,476,225	1,476,225	1,476,225	1,476,225	1,476,225	1,476,225
G2	874,800	874,800	874,800	879,174	874,800	874,800	601,425
G3	533,439	533,439	533,655	538,326	533,439	448,065	149,040
G5	20,434	20,434	20,434	21,250	20,434	14,494	359
G7	656	656	668	685	579	455	0
G8	70	70	70	76	42	21	0
G9	0	0	0	0	0	0	0

Table 8 The number of six-round protocols that get past each strategy when zoning-in on the second near-optimal protocol (showing G1 and only the other strategies that helped to weed out protocols).

$d = 2$	$\nu = 1/10^{10}$	$\nu = 1/10^{11}$	$\nu = 1/10^{12}$	$\nu = 1/10^{13}$	$\nu = 1/10^{14}$	$\nu = 1/10^{15}$	$\nu = 1/10^{16}$
G1	93,312	93,312	93,312	93,312	93,312	86,022	40,824
G4	38,061	38,061	38,061	38,061	38,061	28,125	4,995
G5	2,664	2,664	2,664	2,716	2,664	1,418	0
G6	2,376	2,376	2,376	2,420	2,376	1,174	0
G9	1,270	0	0	0	0	0	0
G10	774	0	0	0	0	0	0
SDPA0	538	0	0	0	0	0	0
SDPA1	474	0	0	0	0	0	0
Better Accuracy	0	0	0	0	0	0	0

Table 9 The number of six-round protocols that get past each strategy when zoning-in on the third, fourth, fifth and sixth near-optimal protocols (showing G1 and only the other strategies that helped to weed out protocols).

$d = 2$	$\nu = 1/10^{10}$	$\nu = 1/10^{11}$	$\nu = 1/10^{12}$	$\nu = 1/10^{13}$	$\nu = 1/10^{14}$	$\nu = 1/10^{15}$	$\nu = 1/10^{16}$
G1	34,992	34,992	34,992	34,992	34,992	34,992	34,992
SDPB0	9,720	9,720	9,720	9,720	9,720	9,720	27,215
SDPA0	0	0	0	0	0	0	0

$d = 2$	$\nu = 1/10^{10}$	$\nu = 1/10^{11}$	$\nu = 1/10^{12}$	$\nu = 1/10^{13}$	$\nu = 1/10^{14}$	$\nu = 1/10^{15}$	$\nu = 1/10^{16}$
G1	99,144	99,144	93,312	99,144	99,144	99,144	99,144
SDPB0	0	0	0	0	0	0	0

$d = 2$	$\nu = 1/10^{10}$	$\nu = 1/10^{11}$	$\nu = 1/10^{12}$	$\nu = 1/10^{13}$	$\nu = 1/10^{14}$	$\nu = 1/10^{15}$	$\nu = 1/10^{16}$
G1	34,992	34,992	34,992	34,992	34,992	34,992	34,992
SDPB0	9,720	9,720	9,720	9,720	9,720	9,720	27,215
SDPA0	0	0	0	0	0	0	0

$d = 2$	$\nu = 1/10^{10}$	$\nu = 1/10^{11}$	$\nu = 1/10^{12}$	$\nu = 1/10^{13}$	$\nu = 1/10^{14}$	$\nu = 1/10^{15}$	$\nu = 1/10^{16}$
G1	99,144	99,144	93,312	99,144	99,144	99,144	99,144
SDPB0	0	0	0	0	0	0	0

10 Full data for the systematic searches for four and six-round protocols

We present in this section the full data for the searches we conducted for four and six-round protocols for various message dimensions d and precisions ν. Tables are on the following pages.

References

1. Aharonov, D., Ta-Shma, A., Vazirani, U., Yao, A.C.C.: Quantum bit escrow. In: Proceedings of 32nd Annual ACM Symposium on the Theory of Computing, pp. 705–714. ACM (2000). DOI http://doi.acm.org/10.1145/335305.335404
2. Alizadeh, F., Goldfarb, D.: Second-order cone programming. Mathematical Programming **95**, 3–51 (2003)
3. Ambainis, A.: A new protocol and lower bounds for quantum coin flipping. In: Proceedings of 33rd Annual ACM Symposium on the Theory of Computing, pp. 134 – 142. ACM (2001). DOI http://dx.doi.org/10.1109/FOCS.2004.13
4. Chailloux, A., Kerenidis, I.: Optimal quantum strong coin flipping. In: Proceedings of 50th IEEE Symposium on Foundations of Computer Science, pp. 527–533. IEEE Computer Society (2009)
5. Fuchs, C.A., van de Graaf, J.: Cryptographic distinguishability measures for quantum mechanical states. IEEE Transactions on Information Theory **45**, 1216–1227 (1999)
6. Kerenidis, I., Nayak, A.: Weak coin flipping with small bias. Information Processing Letters **89**(3), 131–135 (2004). DOI http://dx.doi.org/10.1016/j.ipl.2003.07.007
7. Kitaev, A.: Quantum coin-flipping (2002). Unpublished result. Talk in the 6th Annual workshop on Quantum Information Processing, QIP 2003, Berkeley, CA, USA, December 2002
8. Mittelmann, H.D.: An independent benchmarking of SDP and SOCP solvers. Computational semidefinite and second order cone programming: the state of the art. Mathematical Programming **95**(2), 407–430 (2003)
9. Nayak, A., Shor, P.W.: On bit-commitment based quantum coin flipping. Physical Review A **67**(1), 012,304 (2003). DOI 10.1103/PhysRevA.67.012304
10. Nesterov, Y., Nemirovskii, A.: Interior-Point Polynomial Algorithms in Convex Programming. Society for Industrial and Applied Mathematics (1994). DOI 10.1137/1.9781611970791. URL `http://epubs.siam.org/doi/abs/10.1137/1.9781611970791`
11. Spekkens, R.W., Rudolph, T.: Degrees of concealment and bindingness in quantum bit commitment protocols. Physical Review A **65**, 012,310 (2001). URL `doi:10.1103/PhysRevA.65.012310`
12. Sturm, J.F.: Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. Optimization Methods and Software **11**, 625–653 (1999)
13. Sturm, J.F.: Implementation of interior point methods for mixed semidefinite and second order cone optimization problems. Optimization Methods and Software **17**(6), 1105–1154 (2002)

Table 10 The number of four-round protocols that get past symmetry reductions and each strategy in the filter for $d = 2$.

$d = 2$	$\nu = 1/500$	$\nu = 1/1000$	$\nu = 1/1250$	$\nu = 1/1500$	$\nu = 1/2000$
No. Protocols	6.30 e+10	1.00 e+12	2.44 e+12	5.07 e+12	1.60 e+13
Symmetry	3, 969, 126, 001	63, 001, 502, 001	153, 566, 799, 376	318, 097, 128, 001	1, 004, 006, 004, 001
F1	96, 706, 535	1, 499, 479, 974	3, 636, 609, 280	7, 506, 289, 309	23, 607, 143, 560
F2	72, 336, 875	1, 123, 112, 000	2, 724, 552, 320	5, 624, 716, 125	17, 693, 560, 000
F3	5	27	50	67	124
F4	0	0	0	0	0
F5	0	0	0	0	0
F6	0	0	0	0	0
F7	0	0	0	0	0
F8	0	0	0	0	0

Table 11 The number of four-round protocols that get past symmetry reductions and each strategy in the filter for $d = 3$.

$d = 3$	$\nu = 1/5$	$\nu = 1/10$	$\nu = 1/20$	$\nu = 1/30$	$\nu = 1/50$
No. Protocols	1.94 e+05	1.89 e+07	2.84 e+09	6.05 e+10	3.09 e+12
Symmetry	4, 356	272, 484	29, 430, 625	55, 436, 7025	25, 475, 990, 544
F1	1, 254	37, 584	2, 175, 425	30, 985, 220	1, 020, 080, 292
F2	665	19, 656	1, 300, 042	19, 366, 256	662, 158, 728
F3	49	470	22, 282	225, 098	4, 414, 994
F4	29	261	11, 667	110, 931	2, 028, 518
F5	28	258	11, 495	109, 515	2, 009, 141
F6	28	241	10, 405	96, 464	1, 765, 114
F7	0	3	54	148	1, 158
F8	0	0	0	0	0

Table 12 The number of four-round protocols that get past symmetry reductions and each strategy in the filter for $d = 4$.

$d = 4$	$\nu = 1/10$	$\nu = 1/12$	$\nu = 1/16$	$\nu = 1/20$	$\nu = 1/24$	$\nu = 1/30$
No. Protocols	6.69 e+09	4.28 e+10	8.81 e+11	9.83 e+12	7.31 e+13	8.86 e+14
Symmetry	13,498,276	74,166,544	1,154,640,400	10,334,552,281	69,927,455,844	736,486,643,344
F1	2,432,188	12,616,580	146,114,000	934,856,164	5,916,006,936	49,798,933,264
F2	1,036,030	5,616,810	71,246,700	489,282,376	3,170,626,956	27,760,130,976
F3	66,623	302,547	3,185,895	19,670,642	101,703,667	738,284,522
F4	46,734	209,747	2,061,868	12,000,187	59,503,895	406,963,112
F5	46,531	208,961	2,054,891	11,962,104	59,353,374	406,099,637
F6	42,591	198,192	1,886,782	11,004,125	54,702,075	367,847,304
F7	329	756	3,439	17,144	55,929	190,699
F8	0	0	0	0	0	0

Table 13 The number of four-round protocols that get past symmetry reductions and each strategy in the filter for $d = 5$.

$d = 5$	$\nu = 1/5$	$\nu = 1/8$	$\nu = 1/10$	$\nu = 1/12$
No. Protocols	2.52 e+08	6.00 e+10	1.00 e+12	1.09 e+13
Symmetry	240,100	29,539,225	284,529,424	2,485,919,881
F1	105,840	9,467,770	66,257,504	567,544,997
F2	37,584	2,687,906	22,774,544	203,983,360
F3	8,561	241,420	2,440,765	17,794,655
F4	7,423	201,569	1,937,298	13,682,059
F5	7,417	200,965	1,933,833	13,665,087
F6	7,417	189,144	1,790,144	13,117,165
F7	0	1,415	10,790	43,459
F8	0	0	0	0

Table 14 The number of four-round protocols that get past symmetry reductions and each strategy in the filter for $d = 6$.

$d = 6$	$\nu = 1/7$	$\nu = 1/8$	$\nu = 1/9$	$\nu = 1/10$	$\nu = 1/11$	$\nu = 1/12$
No. Protocols	3.93 e+11	2.74 e+12	1.60 e+13	8.13 e+13	3.64 e+14	1.46 e+15
Symmetry	53,144,100	265,950,864	1,021,825,156	3,534,302,500	12,577,398,201	46,107,255,076
F1	25,070,310	107,583,876	387,459,886	1,034,786,700	3,605,814,648	13,370,558,568
F2	7,276,924	23,294,007	123,246,328	287,251,218	1,330,224,696	3,841,063,848
F3	1,744,038	2,811,374	25,114,451	42,503,208	258,455,916	468,218,324
F4	1,551,522	2,526,900	21,682,087	36,628,517	214,823,642	390,846,158
F5	1,550,617	2,524,052	21,666,437	36,594,682	214,698,072	390,649,931
F6	1,451,038	2,419,474	20,598,749	34,117,986	203,605,433	377,899,946
F7	9,169	13,976	57,720	174,118	526,077	1,153,864
F8	0	0	0	0	0	0

Table 15 The number of four-round protocols that get past symmetry reductions and each strategy in the filter for $d = 7$.

$d = 7$	$\nu = 1/5$	$\nu = 1/6$	$\nu = 1/7$	$\nu = 1/8$	$\nu = 1/9$	$\nu = 1/10$
No. Protocols	4.55 e+10	7.28 e+11	8.67 e+12	8.13 e+13	6.27 e+14	4.11 e+15
Symmetry	3,709,476	46,963,609	289,374,121	1,730,643,201	7,402,021,225	30,490,398,225
F1	2,270,754	26,952,849	161,111,181	841,297,023	3,456,456,125	10,915,707,495
F2	495,180	3,154,266	36,330,756	136,788,372	851,509,125	2,419,940,743
F3	149,806	369,434	10,277,699	20,469,535	216,148,269	449,464,967
F4	142,255	351,290	9,583,747	19,200,670	197,250,330	409,366,494
F5	142,241	351,219	9,582,215	19,194,692	197,214,454	409,185,885
F6	142,241	351,219	9,034,728	18,734,072	187,977,589	383,402,064
F7	0	0	60,155	91,787	512,171	1,804,382
F8	0	0	0	0	0	0

Table 16 The number of four-round protocols that get past symmetry reductions and each strategy in the filter for $d = 8$.

$d = 8$	$\nu = 1/4$	$\nu = 1/5$	$\nu = 1/6$	$\nu = 1/7$	$\nu = 1/8$	$\nu = 1/9$
No. Protocols	1.18 e+10	3.93 e+11	8.67 e+12	1.38 e+14	1.71 e+15	1.71 e+16
Symmetry	1,572,516	11,532,816	179,345,664	1,293,697,024	9,018,161,296	42,352,405,209
F1	1,054,614	7,797,216	115,131,024	814,855,040	5,050,850,268	23,061,817,617
F2	60,552	1,356,936	9,766,192	142,862,430	606,597,735	4,417,668,742
F3	0	431,956	1,254,420	44,457,239	106,851,420	1,276,499,496
F4	0	417,759	1,213,728	42,541,702	102,719,851	1,204,238,273
F5	0	417,741	1,213,629	42,539,430	102,710,139	1,204,173,244
F6	0	417,741	1,213,629	40,425,272	101,061,706	1,151,097,965
F7	0	0	0	277,225	452,792	3,194,346
F8	0	0	0	0	0	0

Table 17 The number of four-round protocols that get past symmetry reductions and each strategy in the filter for $d = 9$.

$d = 9$	$\nu = 1/3$	$\nu = 1/4$	$\nu = 1/5$	$\nu = 1/6$	$\nu = 1/7$	$\nu = 1/8$
No. Protocols	7.41 e+08	6.00 e+10	2.74 e+12	8.13 e+13	1.71 e+15	2.74 e+16
Symmetry	164,025	3,744,225	32,069,569	594,433,161	4,957,145,649	39,808,629,441
F1	131,625	2,666,430	23,348,549	414,160,047	3,423,681,189	24,851,338,155
F2	14,300	115,752	3,273,662	26,075,045	470,028,582	2,216,082,560
F3	2,700	0	1,065,271	3,484,092	153,932,946	432,754,976
F4	2,639	0	1,041,339	3,405,532	149,523,487	421,903,500
F5	2,639	0	1,041,317	3,405,403	149,520,361	421,889,260
F6	2,639	0	1,041,317	3,405,403	142,916,565	416,869,327
F7	0	0	0	0	1,053,222	1,809,800
F8	0	0	0	0	0	0

Table 18 The number of six-round protocols that get past symmetry reductions and each strategy in the filter for $d = 2$.

$d = 2$	$\nu = 1/3$	$\nu = 1/4$	$\nu = 1/5$	$\nu = 1/6$	$\nu = 1/7$	$\nu = 1/8$
No. Protocols	160,000	1,500,625	9,834,496	49,787,136	207,360,000	7.41 e+08
Symmetry	6,400	59,049	280,900	1,517,824	5,683,456	19,713,600
G1	3,200	20,412	82,680	389,312	1,397,024	4,115,880
G2	2,320	12,516	67,548	272,392	1,112,228	3,057,246
G3	1,725	9,627	52,424	223,034	899,450	2,526,712
G4	714	4,206	27,965	105,050	430,454	1,240,106
G5	210	684	7,743	20,373	112,435	228,274
G6	210	684	7,743	20,373	110,401	228,274
G7	30	48	1,285	1,856	10,979	17,831
G8	0	0	466	164	3,427	4,620
G9	0	0	466	164	3,419	4,512
G10	0	0	466	164	3,369	4,512
SDPB0	0	0	6	0	26	20
G11	0	0	6	0	26	20
SDPA0	0	0	0	0	0	0

Table 19 The number of six-round protocols that get past symmetry reductions and each strategy in the filter for $d = 2$.

$d = 2$	$\nu = 1/9$	$\nu = 1/10$	$\nu = 1/11$	$\nu = 1/12$	$\nu = 1/13$	$\nu = 1/14$	$\nu = 1/15$
No. Protocols	2.34 e+09	6.69 e+09	1.75 e+10	4.28 e+10	9.83 e+10	2.13 e+11	4.43 e+11
Symmetry	58, 247, 424	155, 276, 521	401, 080, 729	973, 502, 401	2, 052, 180, 601	4, 632, 163, 600	9, 372, 176, 100
G1	11, 020, 608	23, 862, 815	60, 761, 918	140, 154, 892	240, 820, 116	555, 641, 840	1, 048, 452, 300
G2	8, 944, 136	18, 717, 210	50, 337, 094	110, 274, 108	204, 522, 468	444, 537, 964	877, 684, 860
G3	7, 335, 617	15, 503, 308	41, 447, 668	93, 222, 286	167, 717, 637	380, 238, 435	739, 653, 758
G4	3, 477, 093	8, 534, 326	20, 503, 550	45, 888, 192	91, 991, 055	185, 971, 770	350, 105, 435
G5	696, 601	1, 367, 115	3, 435, 390	6, 577, 917	12, 425, 039	23, 210, 979	43, 785, 997
G6	688, 613	1, 367, 115	3, 435, 390	6, 577, 917	12, 258, 117	23, 097, 713	43, 188, 099
G7	57, 598	87, 303	232, 382	355, 057	678, 384	1, 051, 339	1, 977, 185
G8	17, 512	18, 105	64, 273	86, 272	177, 297	230, 146	479, 088
G9	16, 005	15, 689	50, 847	74, 114	143, 172	195, 858	411, 864
G10	15, 875	15, 124	49, 819	71, 439	137, 232	185, 696	386, 741
SDPB0	68	58	152	126	492	346	594
G11	68	58	152	126	492	346	594
SDPA0	0	0	0	0	0	0	0

Table 20 The number of six-round protocols that get past symmetry reductions and each strategy in the filter for $d = 3$.

$d = 3$	$\nu = 1/2$	$\nu = 1/3$	$\nu = 1/4$
No. Protocols	4,100,625	741,200,625	60,037,250,625
Symmetry	68,121	6,395,841	279,324,369
G1	42,282	5,222,385	180,500,400
G2	8,748	3,324,650	86,151,600
G3	5,643	1,958,070	58,038,667
G4	161	714,393	30,773,918
G5	0	464,538	15,310,116
G6	0	464,538	15,310,116
G7	0	310,518	6,557,007
G8	0	284,418	5,447,015
G9	0	284,418	5,393,911
G10	0	284,418	5,393,911
SDPB0	0	2,655	24,012
G11	0	2,655	24,012
SDPA0	0	0	0