Breaking barriers in two-party quantum cryptography via stochastic semidefinite programming

Akshay Bansal and Jamie Sikora

Department of Computer Science, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, USA

In the last two decades, there has been much effort in finding secure protocols for two-party cryptographic tasks. It has since been discovered that even with quantum mechanics, many such protocols are limited in their security promises. In this work, we use stochastic selection, an idea from stochastic programming, to circumvent such limitations. For example, we find a way to *switch* between bit commitment, weak coin flipping, and oblivious transfer protocols to improve their security. We also use stochastic selection to turn trash into treasure yielding the first quantum protocol for Rabin oblivious transfer.

1 Introduction

The first work in the quantum cryptography was by Wiesner in [1]. In that seminal paper, he introduced two cryptographic tasks which are still very much studied by the quantum community, quantum money and a task which he called *multiplexing*. Multiplexing is now better known as 1-out-of-2 oblivious transfer in which Bob wishes to send to Alice one bit while keeping the other bit hidden. Wiesner's protocol was knowingly insecure in the unconditional security model, where no computational bounds are put on the adversaries, but he argued that it would be infeasible to break using (then) current technology (which is an argument which could still be made to this day, some 40 years later).

The term *oblivious transfer* was first introduced by Rabin in 1981 (see [2]). The task studied in that paper was Alice sending to Bob a single bit which he receives with probability 1/2 and is lost with probability 1/2. This task which is sometimes now referred to Rabin oblivious transfer has been showed to be equivalent to 1-out-of-2 oblivious transfer (for some definition of equivalent) by Crépeau in 1994 [3]. In this work, we shall refer to multiplexing/1-out-of-2 oblivious transfer simply as *oblivious transfer* and Rabin's similar task as *Rabin oblivious transfer*.

In addition to these tasks, there are several other two-party cryptographic tasks studied in this work. We briefly introduce them below, but we note now a common story; that most of them are provably insecure by a significant margin. Indeed, there are general results proving the insecurity of many such cryptographic tasks, see for example [4, 5]. This brings us to the main question which motivates this work.

Can we do anything about the limited unconditional security of quantum two-party cryptography?

Akshay Bansal: akshaybansal14@gmail.com

Jamie Sikora: sikora@vt.edu, https://sites.google.com/site/jamiesikora/

To better understand these limitations, we now give a glimpse into the history of quantum protocols for two-party cryptography (with rigorous definitions deferred to more formal discussions later).

1.1 A brief history of two-party cryptography

We now give a brief history of several cryptographic tasks and in doing so, indicate bounds on their security. When relevant, we also discuss further limitations when considering *simple* protocols.

Oblivious transfer. Several constant lower bounds on oblivious transfer have been presented in [6, 7, 4, 8] with the largest being in [9]. In that work, it was shown that Alice or Bob can cheat with probability at least 2/3, a large gap above the perfect security bound of 1/2. The best known explicit protocol[1] that we have is from [6] which attains cheating probabilities both equal to 3/4. (Definitions of cheating probabilities are deferred to formal discussions later.)

We also discuss Rabin oblivious transfer in this paper. As far as we are aware, there are no quantum protocols known for Rabin oblivious transfer. However, there is a constant lower bound known for a particular variant of it [4].

Bit commitment. Bit commitment is the task where Alice commits to a bit y, then wishes to reveal it at a later time. Cheating Alice wants to be able to reveal any bit she chooses later and a cheating Bob wants to learn y before it is revealed. It has been showed that Alice or Bob can cheat with probability at least 0.739. Simple protocols have since been introduced where Alice and Bob can both cheat with probability 3/4 with a matching lower bound for such protocols in [10]. Since we wish to have the cheating probabilities close to 1/2, there is a significant security gap here as well.

Weak coin flipping. Weak coin flipping is the task where Alice and Bob use a communication channel to generate a random bit but Alice and Bob want different outcomes. Mochon proved that it is possible to find arbitrarily good quantum protocols for this task [11] (see also [12]) which have been made explicit in [13, 14]. However, these are quite complicated and it has since been shown that any such protocol requires a huge communication cost [15]. Mochon also gave a fairly simple protocol called Dip-dip-boom, see [16], where Alice and Bob cannot influence the outcome with probability greater than 2/3. This is, again, a constant above the preferred cheating probabilities of 1/2, but it has the benefit of being relatively simple.

Strong coin flipping and die rolling. Strong coin flipping is the same as weak coin flipping but Alice or Bob may try to influence the outcome towards either 0 or 1 (i.e., we do not assume they want different outcomes). Die rolling is the generalization of strong coin flipping to D possible outcomes (strong coin flipping being the case when $D = 2$). Kitaev used semidefinite programming [17] to prove that Alice or Bob can cheat with probability at least $1/\sqrt{2}$ in any quantum protocol for strong coin flipping which is easily extended to $1/\sqrt{D}$ for the general case of die rolling (see [18] for details). In each case, the lower bound is a constant above the desired bound of $1/D$.

[1] Using slightly different security definitions, the protocol in [8] has better security parameters concerning one of the cheating parties.

1.2 Our stochastic switching framework

We now illustrate our idea to improve the security of cryptographic tasks. Suppose we have two communication tasks between Alice and Bob (or even more parties) such that the first several rounds of communication are identical. These two protocols may end up diverging from one another and ultimately result in accomplishing two completely different goals. What we do is have Alice and Bob start the communication, then at some point, one of the parties (selected beforehand, say Bob) flips a coin and announces whether to continue with either the first task or the second. Then they agree to continue to complete the announced task.

To take an example, suppose one task is oblivious transfer and the other task is bit commitment. They then communicate and at some pre-agreed upon point Bob announces "Alice, we are finishing this protocol as a bit commitment protocol", to which Alice agrees.

Is this a realistic setting? Notice that in the above example, even though Alice and Bob end up doing bit commitment, this may not have been the case. Moreover, this protocol does not adhere to the traditional definition of a proper bit commitment protocol since there is a chance that it accomplishes something else entirely (oblivious transfer). In a way, this suggests a protocol for *bit commitment or oblivious transfer* decided randomly from within the protocol itself. However, we argue that this is a realistic setting. In most scenarios, Alice and Bob are not set up to communicate in order to accomplish a single task a single time, but rather many varied tasks in succession. In this work, we study basic cryptographic tasks, sometimes referred to as primitives, which are used as building blocks in much more elaborate, more complicated protocols. Thus, it is entirely likely that Alice and Bob do not want to perform a single bit commitment protocol or a single weak coin flipping protocol, but rather perform them hundreds or thousands of times.

Moreover, our stochastic switch framework is so versatile that it can be used to switch between many tasks, cryptographic or otherwise. Many of our tasks start with Alice creating the EPR state

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{1}$$

and sending half to Bob. This is reminiscent of many other basic tasks in quantum computing such as superdense coding, teleportation, and entanglement-swapping, to list a few. These do not a priori have anything to do with cryptography, but are communication primitives in their own right. Therefore, many of our examples in this paper can be used in a setting more general than just two-party cryptography; they can be used in general communication tasks. One setting to which our framework could easily be applied is a node-to-node communication point in a quantum internet where the two nodes may need to sometimes generate random numbers (weak coin flipping), retrieve information from a database (oblivious transfer), or use it as a quantum repeater to aid in quantum key distribution (entanglement-swapping).

A familiar example where the stochastic switch is useful. We now illustrate our switching idea in a simple, yet familiar, communication task.

Protocol 1 (A seemingly pointless protocol)**.**

- Suppose Alice creates a qubit $|\psi\rangle$ (unknown to Bob). She sends it to Bob who then returns a two-qubit state $|\phi\rangle$ to Alice with the intention that the first qubit of $|\phi\rangle$ is $|\psi\rangle$.
- Alice checks if the first qubit is $|\psi\rangle$ with the POVM:

$$\{|\psi\rangle\langle\psi| \otimes \mathbb{1}_2, \mathbb{1}_4 - (|\psi\rangle\langle\psi| \otimes \mathbb{1}_2)\}. \tag{2}$$

We note that Bob can easily pass Alice's test by simply returning $|\psi\rangle \otimes |0\rangle$.

Protocol 2 (Another seemingly pointless protocol)**.**
The same as Protocol 1, except Alice checks if the second qubit is $|\psi\rangle$ instead.

Again, Bob can easily pass Alice's test, this time by returning $|0\rangle \otimes |\psi\rangle$.

While these two protocols each allow Bob to pass the test, we now use a stochastic switch to make the game harder for Bob.

Protocol 3 (Switching between Protocols 1 and 2)**.**

- Suppose Alice creates a qubit $|\psi\rangle$ (unknown to Bob). She sends it to Bob who then returns a two-qubit state $|\phi\rangle$.
- *Alice selects* $c \in \{0, 1\}$ *uniformly at random and sends it to Bob.*
- If $c = 0$, Alice checks to see if the *first* qubit is in state $|\psi\rangle$. If $c = 1$, Alice checks to see if the *second* qubit is in state $|\psi\rangle$.

For Bob to pass this test, he must somehow make the first qubit equal to $|\psi\rangle$ and also the second qubit. Since this qubit is unknown to Bob it is impossible to win this game with certainty by the *no-broadcasting theorem* (see, e.g., [19]) which is a refinement of the no-cloning theorem [20]. We could calculate the maximum probability with which Bob could pass the test (if more details about the states are given), but since it must be strictly less than 1, we have illustrated our point; the switch decreases Bob's probability to pass this test.

Why would this improve security, and does it always? A moment's thought reveals why switching between Protocols 1 and 2 ruins Bob's chances of passing Alice's test. The message Bob would send back to Alice in Protocol 1 is different than the state Bob would send back to Alice in Protocol 2. Since the stochastic switch (Alice's selection of $c \in \{0, 1\}$) occurs *after* Bob's returned message, he cannot simultaneously use both strategies. Thus, this limits what Bob can do.

In fact, a specialized variant of stochastic switch also finds its application in interactive proof systems where an honest *verifier* wishes to verify the zero-knowledge(ness) of a *prover* by randomly picking a challenge (from a predefined set of challenges) independent of the prior interaction with the prover. This switching method can ensure the zero-knowledge behaviour of the *prover*. In our work, we generalize this framework of stochastic switching by also allowing a selection amongst fundamentally different tasks and analyzing the statistical security by formulating it as stochastic semidefinite programming problem (discussed in detail in the later sections). Although the formulation and the ideas remain general, we mostly focus on quantum protocols where a natural analysis follows via semidefinite programming. It is worth noting that some of the more well-known techniques in classical cryptography, e.g., the *cut-and-choose* methods and their application in secure two-party computation [21] also falls conceptually within our framework.

We now discuss this idea further and pin down, conceptually, when this may work and when it may not. For simplicity, suppose Alice sends a single message to Bob who then does the stochastic switch between two tasks, call them Task_1 and Task_2. Note that the first message must be modeled by the same density operator for them to be considered for this framework. However, Alice might be tempted to digress from this "honest" message in each task. Suppose for Task_1 Alice's optimal strategy involves her sending a first message modeled by the density operator σ_1 and, similarly,

Alice's optimal strategy for Task_2 involves her sending a first message modeled by the density operator σ_2. Then if $\sigma_1 \neq \sigma_2$, then the two tasks could be good candidates to switch between to see a decrease in Alice's cheating. The story is a bit more nuanced than this though. Alice could have multiple choices for her first message in an optimal strategy. Therefore, we must consider the *set of optimal first messages* in each scenario. Fig. 1 illustrates two scenarios.

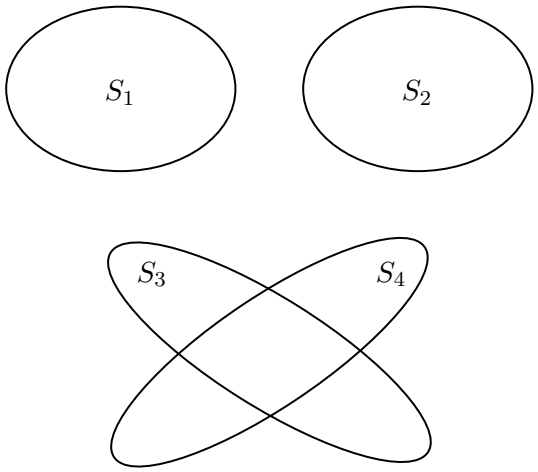

Figure 1: Let S_j denote the set of optimal first messages Alice could send in Task_j. Then if two sets are disjoint, Alice would have to hedge her cheating attempts if Bob switches between those two tasks (e.g., Task_1 and Task_2). If the two sets have a nonempty intersection, Alice would have no difficulty cheating if Bob switches between those two tasks (e.g., Task_3 and Task_4).

As the above figure suggests, if the two sets of optimal first messages have no intersection, then Alice's cheating attempts are strictly decreased in this setting. A similar story can be said when considering switching between three or more protocols as well.

If this setting is to improve security, we would require Bob to not be able to break the protocol by abusing his power to control the stochastic switch. We now describe the general model of a cheating Alice and cheating Bob (and give explicit formulations when analyzing specific instances in later sections).

Modeling cheating Alice and cheating Bob. We discuss the following notions of security for a *complete* switch protocol with multiple possible subtasks.

- *Completeness:* A switch protocol is said to be (conditionally) *complete* if whenever Alice and Bob are honest, then the protocol resulting from Bob's selection is *complete*. In other words, if Bob chooses Task_j, the resulting protocol does exactly what Task_j is supposed to do.
- *Cheating Alice:* A cheating Alice could in general try to find a strategy which can accommodate for a good cheating attempt for every task choice of Bob. The cheating probability for dishonest Alice against honest Bob is given by

$$P_A = \max \left\{ \sum_j p_j \, P_A^{\text{Task}_j} \right\} \tag{3}$$

  where the maximum is taken over all possible strategies of Alice, p_j is the probability honest Bob chooses Task_j, and $P_A^{\text{Task}_j}$ is the maximum cheating probability for Alice conditioned on Bob choosing Task_j in the context of the switching protocol.

- *Cheating Bob:* Bob's cheating attempts could involve using his protocol switching choice to his advantage. As an example, if one task allows Bob to cheat with a large probability, he has the power to simply choose that task. A slightly more sophisticated approach is for him to perform a measurement and then, conditioned on the outcome, make his choice on how to proceed.

  The cheating probability for dishonest Bob against honest Alice is given by

$$P_B = \max \left\{ \sum_j \Pr[\text{Bob chooses Task}_j] P_B^{\text{Task}_j} \right\} \tag{4}$$

  where the maximum is taken over all strategies of Bob and $P_B^{\text{Task}_j}$ is the maximum cheating probability for Bob conditioned on him choosing Task_j. Note that the probability Bob chooses Task_j comes from the cheating strategy; it may not be equal to the probability had he been honest.

Where does this idea come from? The idea of the stochastic switch comes directly from stochastic programming. Indeed, optimization is an inherent task when studying the security of any cryptographic protocol since we care about an adversary's *optimal* cheating capability. In other words, a security analysis often involves maximizing over allowable cheating strategies. In this work, we model Alice and Bob's cheating strategies in the same way Kitaev modeled those for coin flipping [17] which involves semidefinite programming.

Semidefinite programming is the study of optimizing linear functions over positive semidefinite variables subject to affine constraints. Since the study of quantum computing (and hence quantum cryptography) often involves positive semidefinite objects (density operators, POVMs, channels, etc.) this is a very natural setting in which to optimize quantum quantities.

A semidefinite program (SDP) can be written in a standard form as

$$\begin{aligned} \text{maximize: } & \langle C, X \rangle \\ \text{subject to: } & \Phi(X) = B \\ & X \succcurlyeq 0, \end{aligned} \tag{5}$$

where C and B are Hermitian matrices, and Φ is a Hermiticity-preserving linear map. An important feature of SDPs is that they can often be solved efficiently and many computational solvers exist [22, 23, 24].

A stochastic semidefinite program is a variant of an SDP where decisions are made during multiple stages based on certain scenarios chosen probabilistically by the adversary at each stage. (The protocols devised in this work are primarily based on two stages with only a finite number of possible scenarios where each scenario corresponds to a certain protocol.) The optimization for a decision-maker within these stochastic protocols is based on the following formulation:

$$\begin{aligned} \text{maximize: } & \mathbb{E}_\omega[\langle C_\omega, Y_\omega \rangle] \\ \text{subject to: } & \Phi_\omega(Y_\omega) = B_\omega, \forall \omega \in \Omega \\ & \Xi_\omega(Y_\omega) = X, \forall \omega \in \Omega \\ & Y_\omega \succcurlyeq 0, \forall \omega \in \Omega \\ & X \succcurlyeq 0, \end{aligned} \tag{6}$$

where Ω is the set of possible scenarios, C_ω and B_ω are Hermitian for each ω, and Φ_ω and Ξ_ω are Hermiticity-preserving linear maps for each ω.

For a finite number of scenarios (Ω is finite), the above formulation is also an SDP where X is the Stage-I decision made by the decision-maker before the adversary reveals the scenario ω and Y_ω is the Stage-II decision made when they follow the protocol corresponding to scenario ω. Due to the stochastic nature of scenario selection by the adversary, the decision-maker wishes to select X that maximizes his / her average (expected) probability of success and later takes a decision Y_ω which is optimal for the revealed scenario ω and chosen X. The binding constraints of the type $\Xi_\omega(Y_\omega) = X$ for the Stage-I decision X may restrict decision-maker's success probability compared to the deterministic case where they follow the protocol for scenario ω with certainty.

1.3 Our results

Our main results can be divided into two categories, breadth and depth.

Breadth. We first examine protocols that provide the ability to switch between different tasks. As discussed previously, here *switch* refers to the functionality where a party can choose to perform one of the tasks (from the allowed set of tasks) after some initial communication with the other party. Here we consider different combinations of the allowed tasks where a task can either be oblivious transfer, bit commitment, *or* weak coin flipping.

We collect all the combinations in the theorem below.

Theorem 1.1 (Switching between different protocols, informal)**.** There exists a simple protocol which performs bit commitment *or* oblivious transfer with

$$P_A \approx 0.72855 \quad \text{and} \quad P_B = 0.75. \tag{7}$$

There exists a simple protocol which performs bit commitment *or* weak coin flipping with

$$P_A \approx 0.74381 \quad \text{and} \quad P_B = 0.75. \tag{8}$$

There exists a simple protocol which performs weak coin flipping *or* oblivious transfer with

$$P_A \approx 0.70440 \quad \text{and} \quad P_B = 0.75. \tag{9}$$

There exists a simple protocol which performs bit commitment *or* weak coin flipping *or* oblivious transfer with

$$P_A \approx 0.71777 \quad \text{and} \quad P_B = 0.75. \tag{10}$$

To give some context, each of the protocols above were achieved by starting with two (or more) protocols, each with Alice and Bob's cheating probabilities equal to 3/4 then having Bob stochastically switch to thwart Alice's cheating attempts. Note that in this case, Bob's cheating probability is not expected to go down since he has the power to select whichever task he wants. Thus, the fact that $P_B = 3/4$ still and $P_A < 3/4$ means a strict improvement in the overall security in each case.

To illustrate the importance of the above theorem, we point out the protocol for oblivious transfer *or* bit commitment. In that setting, the two protocols that we switch between are either the best known (as is the case with oblivious transfer [6]) or the best possible in that setting (as is the case

with bit commitment ([25] based on [10])). At the end, at least one of the two tasks were performed with a strict decrease in Alice's cheating probability (on average we have 0.75 decreasing to 0.72855). This gives us a strictly better protocol in this sense. Moreover, in each of the cases, Alice's average cheating probability decreased below 0.75, which is better than her standalone cheating probability in each task. In summary, our switching idea circumvents a significant barrier on the design of quantum protocols in each case.

Depth. We next consider switching between two protocols both of which perform the same task. In such a case, any stochastic switch of Bob is guaranteed to be a complete protocol for said task. The task we consider here is Rabin oblivious transfer.

As far as we are aware, there are no quantum protocols for Rabin oblivious transfer in the literature. Indeed, they are hard to design and even defining what cheating Alice and cheating Bob would want to achieve is a bit tricky. However, one can easily define *bad* quantum protocols, in the sense that they are completely broken (and seemingly useless). We show that our framework is capable of taking broken protocols and creating some with decent security.

Theorem 1.2 (A quantum protocol for Rabin oblivious transfer, informal)**.** There exists a quantum protocol for Rabin oblivious transfer where Alice can correctly guess whether Bob received the message or learnt $\perp$ (the output where he receives nothing) with probability at most 0.9330 and Bob can learn Alice's bit with probability at most 0.9691.

We subsequently extend our framework to develop a quantum protocol for an alternative Rabin oblivious transfer task where dishonest Alice attempts to force Bob to receive nothing.

Theorem 1.3 (A quantum protocol for an alternative Rabin oblivious transfer, informal)**.** There exists a quantum protocol where Alice can force Bob to accept $\perp$ (the output where he learns nothing) with probability at most $\cos^2(\pi/8) \approx 0.8535$ and Bob can learn Alice's bit with probability at most 0.875.

An interesting aspect of our protocol is that it switches between two protocols where the information is sent only in one direction. This allows for an easier analysis and helps to define what a cheating Alice and a cheating Bob would want in this setting. We discuss this protocol and Rabin oblivious transfer in detail in Section 5.

Limitations. It is indeed the case that switching does not always yield a more secure protocol. We now discuss two examples, one in which switching does not help and one in which it completely breaks the protocol.

Lemma 1.4 (A protocol in which the stochastic switch does not help, informal)**.** There exists a protocol for XOR oblivious transfer *or* trit commitment in which Bob does the switching but Alice's cheating probability does not decrease.

We define these two tasks and the two protocols in Appendix A followed by the analysis of their stochastic switch.

Lemma 1.5 (A protocol in which the stochastic switch hurts the overall security, informal)**.** There exists a switching protocol for *strong* coin flipping in which Bob cannot cheat perfectly in each subtask but can cheat perfectly using his stochastic switch.

We provide the two protocols and the analysis of their stochastic switch in Appendix B.

1.4 Layout of the paper

We start by defining notation and background in Section 2. In Section 3 we detail three fundamental two-party cryptographic tasks and in each give a simple quantum protocol along with a full security analysis via semidefinite programming. We then consider a stochastic switch between every combination of these fundamental tasks in Section 4 and analyze their security using stochastic semidefinite programming. In Section 5 we introduce Rabin oblivious transfer and use our framework to give the first quantum protocol for this task. Appendix A and Appendix B discuss two instances where the stochastic switch is applicable but does not help in designing protocols with improved security.

2 Background

This section provides a brief background on the mathematical ideas used in this work. We first introduce some notations from linear algebra and matrix analysis followed by a short primer on stochastic semidefinite programming. For a detailed understanding on the relevant subject, we provide a few standard references within the related subsection.

2.1 Linear algebra notation and terminology

We denote the computational (standard) basis for $\mathbb{C}^n$ by $\{|0\rangle, |1\rangle, \dots |n-1\rangle\}$. We use the Dirac notation from quantum mechanics to represent a vector $|\psi\rangle \in \mathbb{C}^n$ and uppercase calligraphic letters (such as $\mathcal{A}, \mathcal{B}$) for denoting complex Euclidean spaces.

For a complex Euclidean space $\mathcal{X}$, the set of operators on $\mathcal{X}$ is given by $\mathrm{L}_{\mathcal{X}}$ and we define $\mathbb{1}_{\mathcal{X}}$ as the identity operator acting on $\mathcal{X}$. The set of Hermitian operators on $\mathcal{X}$ is denoted by $\mathrm{Herm}(\mathcal{X})$ where an operator $X \in \mathrm{L}_{\mathcal{X}}$ is Hermitian if it is equal to its conjugate-transpose (i.e. $X = X^\dagger$). The convex cone of positive semidefinite operators acting on $\mathcal{X}$ is denoted by $\mathrm{Pos}(\mathcal{X})$ while $\mathrm{D}(\mathcal{X})$ is the set of positive semidefinite operators with unit trace i.e., density operators. The Hilbert-Schmidt inner product between two operators $P, Q \in \mathrm{Herm}(\mathcal{X})$ is given by

$$\langle P, Q \rangle = \mathrm{Tr}(P^\dagger Q) = \mathrm{Tr}(PQ).$$

The partial trace over $\mathcal{X}$, denoted by $\mathrm{Tr}_{\mathcal{X}}$ is the linear mapping from $\mathrm{L}_{\mathcal{X}\otimes\mathcal{Y}}$ to $\mathrm{L}_{\mathcal{Y}}$ such that $\mathrm{Tr}_{\mathcal{X}}(X \otimes Y) = \mathrm{Tr}(X)Y$ for all $X \in \mathrm{L}_{\mathcal{X}}$ and $Y \in \mathrm{L}_{\mathcal{Y}}$. We also make use of the fact that the measurement of a quantum state $\rho \in \mathrm{D}(\mathcal{X})$ by a k-outcome POVM (positive operator-valued measure) $\{M_0, M_1 \dots M_{k-1}\}$ reveals outcome $i \in \{0, 1, \dots k-1\}$ with probability $\langle \rho, M_i \rangle$ (known as Born's rule).

For a more comprehensive review of quantum information theory, we refer the reader to [26, 27].

2.2 Stochastic semidefinite programming

Semidefinite programming (SDP) is a sibling framework of linear programming where we want to optimize a linear function of a positive semidefinite variable constrained to affine subspaces. A popular representation of an SDP is given by:

$$\begin{aligned} \text{maximize: } & \langle C, X \rangle \\ \text{subject to: } & \Phi(X) = B \\ & X \in \text{Pos}(\mathcal{X}), \end{aligned} \tag{11}$$

where $\Phi : \text{L}(\mathcal{X}) \to \text{L}(\mathcal{Y})$ is a Hermiticity-preserving linear map with $C \in \text{Herm}(\mathcal{X})$ and $B \in \text{Herm}(\mathcal{Y})$. A semidefinite program can often be solved for an optimal solution using interior point methods [28, 29] efficiently. We refer the reader to [30] for additional details on semidefinite programming and its theory.

Stochastic semidefinite programming is a well-studied modelling framework for problems with some degree of stochasticity in the evolution of the underlying environment. We consider a *two-stage* stochastic environment that can be modelled using the following stochastic semidefinite program:

$$\begin{aligned} \text{maximize: } & \mathbb{E}_\omega[\langle C_\omega, Y_\omega \rangle] \\ \text{subject to: } & \Phi_\omega(Y_\omega) = B_\omega, \forall \omega \in \Omega \\ & \Xi_\omega(Y_\omega) = X, \forall \omega \in \Omega \\ & Y_\omega \in \text{Pos}(\mathcal{Y}_\omega), \forall \omega \in \Omega \\ & X \in \text{Pos}(\mathcal{X}). \end{aligned} \tag{12}$$

Here X is the *here-and-now* (or Stage-I) variable whose value is assigned by the decision-maker before the adversary reveals the scenario ω (which occurs with probability $\mathbb{P}_\omega$). Y_ω is the *recourse* (or Stage-II) variable assigned by the decision-maker once ω is revealed. Note that the binding constraints $\Xi_\omega(Y_\omega) = X$ could restrict the decision-maker to achieve the maximum possible reward (objective value) for scenario ω. The maximum objective value of the program above is bounded above by $\max_{\omega \in \Omega}\{f^*_\omega\}$ where f^*_ω is the optimal objective function value for scenario ω given by the following SDP:

$$\begin{aligned} \text{maximize: } & \langle C_\omega, Y_\omega \rangle \\ \text{subject to: } & \Phi_\omega(Y_\omega) = B_\omega \\ & Y_\omega \in \text{Pos}(\mathcal{Y}_\omega), \end{aligned} \tag{13}$$

i.e., the maximum value in the absence of the binding variable in scenario ω.

If the set of allowed scenarios Ω is a discrete set, then the formulation 12 can be expressed as a regular semidefinite program 11. Often if the number of scenarios (or $|\Omega|$) for a given stochastic SDP is large, then one can exploit the block structure of the SDP to solve it efficiently using the iterative Bender's decomposition [31]. As the number of scenarios discussed in this work is relatively small, we resort to solving our stochastic programs using standard SDP solvers.

3 Fundamental tasks and simple protocols

In this section, we discuss some simple protocols for three fundamental cryptographic tasks - bit commitment, coin flipping, and oblivious transfer.

3.1 Bit commitment

Bit commitment is a cryptographic task between Alice and Bob who communicate in two phases, a *commit* phase and a *reveal* phase.

- In the *commit* phase, Alice communicates with Bob in order to commit to a bit $y \in \{0,1\}$.
- In the *reveal* phase, Alice communicates with Bob to reveal her choice bit y. We say that Alice successfully reveals if Bob accepts the revealed bit.

We define the following notions of security for a valid bit commitment protocol.

- *Completeness*: If both Alice and Bob are honest, then Bob always accepts Alice's revealed bit.
- *Cheating Alice*: A dishonest Alice tries to reveal $\hat{y} \in \{0,1\}$ chosen uniformly at random before the *reveal* phase. The cheating probability of Alice is given by

$$P_A^{BC} = \max \frac{1}{2} \Pr[\text{Alice successfully reveals } \hat{y} = 0] + \frac{1}{2} \Pr[\text{Alice successfully reveals } \hat{y} = 1], \tag{14}$$

  where the maximum is taken over all cheating strategies of Alice. Note that $P_A^{BC} \geq 1/2$ since she can always make an honest commit to y in the *commit* phase which is successfully revealed with probability 1 when $\hat{y} = y$ (which occurs with probability $1/2$).
- *Cheating Bob*: A dishonest Bob tries to learn the commit bit before the *reveal* phase. The cheating probability of Bob is given by

$$P_B^{BC} = \max \Pr[\text{Bob learns } y \text{ before the reveal phase}], \tag{15}$$

  where the maximum is taken over all cheating strategies of Bob. Note that $P_B^{BC} \geq 1/2$ since Bob can trivially guess y with probability $1/2$ by selecting one of the two possible values uniformly at random.

In some previous works, [32], [33] showed that a perfectly secure bit commitment with quantum communication is impossible while more recently, [34] provided a simple proof of this impossibility for generalized probabilistic theories. In another work, [35] extended the optimal strong coin flipping protocol [36] to come up with an optimal protocol with a value for 0.739 on $\max\{P_A^{BC}, P_B^{BC}\}$. However, these protocols are quite complicated and require an infinite number of messages (in the limit).

We now present a simple quantum bit commitment protocol.

Protocol 4. Quantum protocol for bit commitment [37].

Stage-I

- (Commitment) **Alice chooses a bit** $y \in \{0,1\}$ **uniformly at random and creates the two-qutrit state**

$$|\phi_y\rangle = \frac{1}{\sqrt{2}} |yy\rangle + \frac{1}{\sqrt{2}} |22\rangle \in \mathcal{A} \otimes \mathcal{B}.$$

- **Alice sends the qutrit** $\mathcal{B}$ **to Bob.**

Stage-II

- (Revelation) Alice reveals y to Bob and sends him the subsystem $\mathcal{A}$.
- (Verification) Bob measures the combined state in $\mathcal{A} \otimes \mathcal{B}$ to accept or reject with the POVM:

$$\{\Pi_{accept} \coloneqq |\phi_y\rangle \langle \phi_y|_{\mathcal{A}\otimes\mathcal{B}}, \Pi_{reject} \coloneqq \mathbb{1}_{\mathcal{A}\otimes\mathcal{B}} - \Pi_{accept}\}.$$

  If Bob accepts, Alice successfully reveals y.

3.1.1 Cheating Alice

In order for Alice to successfully reveal bit $\hat{y} \in \{0,1\}$ in Protocol 4, she would send $\hat{y}$ and the qutrit $\mathcal{A}$ such that Bob hopefully accepts the combined state of the two qutrits (in $\mathcal{A} \otimes \mathcal{B}$) with high probability. It is instructive to note that $\hat{y}$ is sampled uniformly at random after Alice has already sent $\mathcal{B}$ during the *commit* phase.

The success probability of Alice can be evaluated by considering the two equally likely scenarios for the observed $\hat{y}$, for each of which Alice wishes a successful verification by Bob's measurement. If $\sigma_{\hat{y}}^{BC}$ is the final state in $\mathrm{D}(\mathcal{A}\otimes\mathcal{B})$ with Bob after the *reveal* phase, then the probability of successful verification (accept) is given by $\langle \sigma_{\hat{y}}^{BC}, |\phi_{\hat{y}}\rangle\langle\phi_{\hat{y}}| \rangle$. As the qutrit $\mathcal{B}$ was already communicated to Bob in the *commit* phase independent of $\hat{y}$, the reduced state $\mathcal{B}$ in the final state $\sigma_{\hat{y}}^{BC}$ is independent of $\hat{y} \in \{0,1\}$ implying $\mathrm{Tr}_{\mathcal{A}}(\sigma_0^{BC}) = \mathrm{Tr}_{\mathcal{A}}(\sigma_1^{BC})$. The optimal cheating probability can thus be calculated by maximizing the probability $\langle \sigma_{\hat{y}}^{BC}, |\phi_{\hat{y}}\rangle\langle\phi_{\hat{y}}| \rangle$ averaged over both values of $\hat{y}$.

SDP for cheating Alice. Alice's optimal cheating probability P_A^{BC} is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \frac{1}{2}\langle \sigma_0^{BC}, |\phi_0\rangle\langle\phi_0| \rangle + \frac{1}{2}\langle \sigma_1^{BC}, |\phi_1\rangle\langle\phi_1| \rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{A}}(\sigma_0^{BC}) = \mathrm{Tr}_{\mathcal{A}}(\sigma_1^{BC}) = \sigma^{BC} \\ & \sigma_0^{BC}, \sigma_1^{BC} \in \mathrm{D}(\mathcal{A}\otimes\mathcal{B}) \\ & \sigma^{BC} \in \mathrm{D}(\mathcal{B}). \end{aligned} \tag{16}$$

Numerically solving the above SDP, we find that Alice can cheat with an optimal probability of $P_A^{BC} = 3/4$ and this is achieved when $\sigma^{BC} = \begin{bmatrix} 1/6 & 0 & 0 \\ 0 & 1/6 & 0 \\ 0 & 0 & 2/3 \end{bmatrix}$.

3.1.2 Cheating Bob

Typically, a security analysis for dishonest Bob involves him performing a state discrimination on the two possible states that could be sent during the *commit* phase. A slightly different way to quantify the success probability of Bob in identifying Alice's commit bit is to introduce a verification process on Alice's side where Bob sends back his guess for the state chosen by Alice and is subsequently verified by her for its correctness. Note that this is just a hypothetical phase introduced to capture Bob's cheating probability; it is not part of the protocol.

Mathematically, Alice prepares a pure state $|\psi\rangle = \sum_{y\in\{0,1\}} \frac{1}{\sqrt{2}} |y\rangle_{\mathcal{Y}} |\phi_y\rangle_{\mathcal{A}\otimes\mathcal{B}}$ at the beginning of the protocol and sends the qutrit $\mathcal{B}$ to Bob who subsequently returns a guess g in $\mathcal{G}$. Alice checks if $g = y$ using the POVM:

$$\{Q_{accept} \coloneqq \sum_{g\in\{0,1\}} \sum_{y\in\{0,1\}} \delta_{y,g} |y\rangle\langle y|_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}} \otimes |g\rangle\langle g|_{\mathcal{G}}, Q_{reject} \coloneqq \mathbb{1}_{\mathcal{Y}\otimes\mathcal{A}\otimes\mathcal{G}} - Q_{accept}\}.$$

The optimal probability of correctly guessing y is obtained by maximizing $\langle \tau^{BC}, Q_{accept} \rangle$ where τ^{BC} is the state with Alice in $\mathrm{D}(\mathcal{Y}\otimes\mathcal{A}\otimes\mathcal{G})$ after receiving the guess g in $\mathcal{G}$ from Bob.

SDP for cheating Bob. The optimal cheating probability for Bob is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \langle \tau^{BC}, Q_{accept} \rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{G}}(\tau^{BC}) = \mathrm{Tr}_{\mathcal{B}}(|\psi\rangle\langle\psi|) \\ & \tau^{BC} \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{A} \otimes \mathcal{G}) \end{aligned} \tag{17}$$

where recall, $|\psi\rangle = \sum_{y\in\{0,1\}} \frac{1}{\sqrt{2}} |y\rangle_{\mathcal{Y}} |\phi_y\rangle_{\mathcal{A}\otimes\mathcal{B}}$ and

$$Q_{accept} = \sum_{g\in\{0,1\}} \sum_{y\in\{0,1\}} \delta_{y,g} |y\rangle\langle y|_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}} \otimes |g\rangle\langle g|_{\mathcal{G}} .$$

Numerically solving the above SDP, we find that Bob can cheat with an optimal probability of $P_B^{BC} = 3/4$.

3.2 Weak coin flipping

Coin flipping is the cryptographic task between two parties (Alice and Bob) where they communicate to agree on a common binary outcome (0 or 1). A weak version of this task is a variant where Alice *wins* if the common outcome is 1 while Bob *wins* if the outcome is 0.

We consider the following notions of security for a given weak coin flipping protocol.

- *Completeness:* If both Alice and Bob are honest, then neither party aborts and the shared outcome is generated uniformly at random.
- *Cheating Alice:* If Bob is honest, then Alice's cheating probability is defined as

  $$P_A^{WCF} = \max \Pr[\text{Alice successfully forces the outcome 1}],$$

  where the maximum is taken over all possible cheating strategies of Alice. Note that here $P_A^{WCF} \geq 1/2$ since Alice can simply choose to follow the protocol honestly to observe the outcome 1 uniformly at random.
- *Cheating Bob:* If Alice is honest, then Bob's cheating probability is defined as

  $$P_B^{WCF} = \max \Pr[\text{Bob successfully forces the outcome 0}],$$

  where the maximum is taken over all possible cheating strategies of Bob. As before, here $P_B^{WCF} \geq 1/2$ since Bob can simply choose to follow the protocol honestly to observe the outcome 0 uniformly at random.

In a previous work, [11] showed that the lower bound of 1/2 on $\max\{P_A^{WCF}, P_B^{WCF}\}$ is in fact tight up to any precision ϵ. More recently, [15] established the impossibility of efficient coin flipping by developing lower bounds of $\exp(\Omega(1/\sqrt{\epsilon}))$ on the communication complexity.

We now present a simple weak coin flipping protocol.

Protocol 5. Quantum protocol for coin flipping based on EPR [38].

Stage-I

- **Alice chooses a bit $y \in \{0,1\}$ uniformly at random and creates the two-qutrit state**

$$|\phi_y\rangle = \frac{1}{\sqrt{2}}|yy\rangle + \frac{1}{\sqrt{2}}|22\rangle \in \mathcal{A}_0 \otimes \mathcal{B}_0.$$

- **Alice sends the qutrit $\mathcal{B}_0$ to Bob**.

Stage-II

- Alice creates another two-qutrit state

$$|\phi_y\rangle = \frac{1}{\sqrt{2}}|yy\rangle + \frac{1}{\sqrt{2}}|22\rangle \in \mathcal{A}_1 \otimes \mathcal{B}_1$$

and sends the qutrit $\mathcal{B}_1$ to Bob.

- Bob chooses an independent bit $z \in \{0,1\}$ uniformly at random and sends it to Alice.
- Alice reveals y to Bob and sends him the qutrit $\mathcal{A}_z$.
- Bob measures the combined state $\mathcal{A}_z \otimes \mathcal{B}_z$ to accept or reject with the POVM:

$$\{\Pi_{accept} \coloneqq |\phi_y\rangle\langle\phi_y|_{\mathcal{A}_z\otimes\mathcal{B}_z}, \Pi_{reject} \coloneqq \mathbb{1}_{\mathcal{A}_z\otimes\mathcal{B}_z} - \Pi_{accept}\}.$$

- If Bob accepts, Alice and Bob measures their respective subsystems with the POVM:

$$\{\Pi_0 \coloneqq |0\rangle\langle 0| + |1\rangle\langle 1|, \Pi_1 \coloneqq |2\rangle\langle 2|\}$$

to get the outcome of the protocol.

3.2.1 Cheating Alice

The idea here is that dishonest Alice attempting to force the outcome 1 in Protocol 5 would want Bob to accept the combined state in $\mathcal{A}_z \otimes \mathcal{B}_z$ and obtain the measurement outcome 1 on the subsystem $\mathcal{B}_{\bar{z}}$. As Bob measures just the qutrit $\mathcal{B}_{\bar{z}}$ to obtain his outcome, we can assume that Alice sends both $\mathcal{A}_z \otimes \mathcal{A}_{\bar{z}}$ (instead of just $\mathcal{A}_z$) to Bob. Note that this does not affect the success probability of Alice and greatly simplifies her overall security analysis. The combined success probability can be evaluated by the inner product $\langle \sigma_z^{WCF}, P_z\rangle$ where σ_z^{WCF} is the state with Bob after receiving y and $\mathcal{A}_z \otimes \mathcal{B}_z$ where

$$P_z = \sum_{y\in\{0,1\}} |y\rangle\langle y|_{\mathcal{Y}} \otimes |\phi_y\rangle\langle\phi_y|_{\mathcal{A}_z\otimes\mathcal{B}_z} \otimes \mathbb{1}_{\mathcal{A}_{\bar{z}}} \otimes |2\rangle\langle 2|_{\mathcal{B}_{\bar{z}}}$$

is the joint measurement that evaluates the combined probability of Bob accepting the state $|\phi_y\rangle$ in $\mathcal{A}_z \otimes \mathcal{B}_z$ and obtaining the outcome 1 on $\mathcal{B}_{\bar{z}}$ for both choices of y. As the qutrits $\mathcal{B}_0$ and $\mathcal{B}_1$ were sent to Bob at the beginning of the protocol before y and $\mathcal{A}_0, \mathcal{A}_1$, the reduced state in $\mathcal{B}_0 \otimes \mathcal{B}_1$ is independent of them implying $\mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_0^{WCF}) = \mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_1^{WCF})$. The optimal cheating probability is thus calculated by maximizing the probability $\langle \sigma_z^{WCF}, P_z\rangle$ averaged over both choices of z.

SDP for cheating Alice. The optimal cheating probability for Alice attempting to force the outcome 1 is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \frac{1}{2}\langle \sigma_0^{WCF}, P_0\rangle + \frac{1}{2}\langle \sigma_1^{WCF}, P_1\rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_0^{WCF}) = \mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_1^{WCF}) = \sigma_B^{WCF} \\ & \mathrm{Tr}_{\mathcal{B}_1}(\sigma_B^{WCF}) = \sigma^{WCF} \\ & \sigma_0^{WCF}, \sigma_1^{WCF} \in \mathrm{D}(\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{B}_0\otimes\mathcal{A}_1\otimes\mathcal{B}_1) \\ & \sigma_B^{WCF} \in \mathrm{D}(\mathcal{B}_0\otimes\mathcal{B}_1) \\ & \sigma^{WCF} \in \mathrm{D}(\mathcal{B}_0) \end{aligned} \tag{18}$$

where,

$$P_0 = \sum_{y\in\{0,1\}} |y\rangle\langle y|_{\mathcal{Y}} \otimes |\phi_y\rangle\langle\phi_y|_{\mathcal{A}_0\otimes\mathcal{B}_0} \otimes \mathbb{1}_{\mathcal{A}_1} \otimes |2\rangle\langle 2|_{\mathcal{B}_1}$$
$$P_1 = \sum_{y\in\{0,1\}} |y\rangle\langle y|_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}_0} \otimes |2\rangle\langle 2|_{\mathcal{B}_0} \otimes |\phi_y\rangle\langle\phi_y|_{\mathcal{A}_1\otimes\mathcal{B}_1}.$$

Numerically solving the above SDP, we find that Alice can cheat with an optimal probability of $P_A^{WCF} = 3/4$ and this is achieved when $\sigma^{WCF} = \begin{bmatrix} 1/12 & 0 & 0 \\ 0 & 1/12 & 0 \\ 0 & 0 & 5/6 \end{bmatrix}$.

3.2.2 Cheating Bob

To analyze Bob's cheating, consider the state with Alice $|\psi\rangle = \sum_{y\in\{0,1\}} \frac{1}{\sqrt{2}} |y\rangle_{\mathcal{Y}} |\phi_y\rangle_{\mathcal{A}_0\otimes\mathcal{B}_0} |\phi_y\rangle_{\mathcal{A}_1\otimes\mathcal{B}_1}$ in $\mathrm{D}(\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{B}_0\otimes\mathcal{A}_1\otimes\mathcal{B}_1)$ at the beginning of the protocol. After Alice sends the qutrits $\mathcal{B}_0$ and $\mathcal{B}_1$ to Bob, she receives z in return and is then holding the state $\tau^{WCF} \in \mathrm{D}(\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{A}_1\otimes\mathcal{Z})$. Note that Bob could use the qutrits $\mathcal{B}_0$ and $\mathcal{B}_1$ to obtain a preferable choice for z before sending it to Alice. Since the qutrit $\mathcal{A}_z$ sent to Bob in the final message of the protocol does not affect Alice's outcome, one can safely disregard this message just to come up with a simpler formulation for cheating Bob. The reduced state in $\mathrm{D}(\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{A}_1)$ remains unchanged from the state with Alice at the beginning of the protocol implying $\mathrm{Tr}_{\mathcal{Z}}(\tau^{WCF}) = \mathrm{Tr}_{\mathcal{B}_0\mathcal{B}_1}(|\psi\rangle\langle\psi|)$. The probability of Alice observing the outcome 0 is given by $\langle\tau^{WCF}, Q\rangle$ where

$$Q = \sum_z \mathbb{1}_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}_z} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)_{\mathcal{A}_{\bar{z}}} \otimes |z\rangle\langle z|_{\mathcal{Z}}$$

is the combined measurement that evaluates the probability of Alice observing 0 on $\mathcal{A}_{\bar{z}}$ when Bob sends back z. The optimal cheating probability for Bob can thus be calculated by maximizing $\langle\tau^{WCF}, Q\rangle$.

SDP for cheating Bob. The optimal cheating probability for Bob to force the outcome 0 is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \langle\tau^{WCF}, Q\rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{Z}}(\tau^{WCF}) = \mathrm{Tr}_{\mathcal{B}_0\mathcal{B}_1}(|\psi\rangle\langle\psi|) \\ & \tau^{WCF} \in \mathrm{D}(\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{A}_1\otimes\mathcal{Z}) \end{aligned} \tag{19}$$

where recall,

$$Q = \sum_{z\in\{0,1\}} \mathbb{1}_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}_z} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)_{\mathcal{A}_{\overline{z}}} \otimes |z\rangle\langle z|_{\mathcal{Z}} .$$

Numerically solving the above SDP, we find that Bob can cheat with an optimal probability of $P_B^{WCF} = 3/4$.

3.3 Oblivious transfer

Oblivious transfer (OT) is the fundamental cryptographic task between two parties, Alice and Bob, where Alice wants to learn one of two pieces of information while keeping Bob oblivious to what she learned. We define the task of 1-out-of-2 OT as follows.

- Bob selects $(x_0, x_1) \in \{0,1\}^2$ uniformly at random.
- Alice selects $y \in \{0,1\}$ uniformly at random.
- Alice learns x_y.

We define the following notions of security for 1-out-of-2 OT protocols.

- *Completeness:* A 1-out-of-2 OT protocol is said to be *complete* if Alice learns the selected bit x_y unambiguously.
- *Cheating Alice:* A dishonest Alice attempts to learn both x_0 and x_1. The cheating probability of Alice is given by

  $$P_A^{OT} = \max \Pr[\text{Alice correctly guesses both } x_0 \text{ and } x_1],$$

  where the maximum is taken over all cheating strategies of Alice. Note that $P_A^{OT} \geq 1/2$ since she can simply follow the protocol to learn x_y perfectly (completeness) and can correctly guess $x_{\overline{y}}$ by making a guess uniformly at random.
- *Cheating Bob:* A dishonest Bob attempts to learn the bit y. The cheating probability of Bob is given by

  $$P_B^{OT} = \max \Pr[\text{Bob correctly guesses } y],$$

  where the maximum is taken over all cheating strategies of Bob. Note that $P_B^{OT} \geq 1/2$ since he can correctly guess Alice's bit y by guessing one of the two values uniformly at random.

It was demonstrated in [6] a lower bound of 0.5852 on $\max\{P_A^{OT}, P_B^{OT}\}$ which was subsequently improved to 2/3 if we consider the setting of semi-honest oblivious transfer [9]. More recently, [8] developed tighter lower bounds for the class of OT protocols where the states outputted by Alice, when both parties are honest, are pure and symmetric. The optimality of the existing lower bound of 2/3 for the general class of OT protocols remains an open question.

We now reproduce a simple 1-out-of-2 OT protocol.

Protocol 6. Quantum protocol for 1-out-of-2 oblivious transfer [6].

Stage-I

- **Alice chooses a bit** $y \in \{0,1\}$ **uniformly at random and creates the two-qutrit state**

  $$|\phi_y\rangle = \frac{1}{\sqrt{2}}|yy\rangle + \frac{1}{\sqrt{2}}|22\rangle \in \mathcal{A}\otimes\mathcal{B}.$$

- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

  Stage-II

- Bob randomly selects $\{x_0, x_1\} \in \{0,1\}^2$ and applies the unitary

$$U_{x_0x_1} = \begin{bmatrix} (-1)^{x_0} & 0 & 0 \\ 0 & (-1)^{x_1} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

  to the received qutrit. Afterwards, Bob returns the qutrit to Alice.

- Alice determines the value of x_y using the two-outcome measurement:

$$\{\Pi_0 \coloneqq |\phi_y\rangle\langle\phi_y|_{\mathcal{A}\otimes\mathcal{B}}, \Pi_1 \coloneqq \mathbb{1}_{\mathcal{A}\otimes\mathcal{B}} - |\phi_y\rangle\langle\phi_y|\}.$$

3.3.1 Cheating Alice

A dishonest Alice in Protocol 6 could attempt to learn both bits simultaneously by creating a state that will eventually encode both bits (x_0, x_1). In doing so, Alice might fail to learn her choice bit x_y with certainty but the strategy could improve her overall chances of learning both bits.

To quantify the extent of Alice's cheating, consider the state

$$|\psi\rangle = \frac{1}{2} \sum_{(x_0,x_1)\in\{0,1\}^2} |x_0x_1\rangle_{\mathcal{X}_0\otimes\mathcal{X}_1}$$

held by Bob at the beginning of the protocol. On receiving the qutrit $\mathcal{B}$ from Alice, Bob now holds the joint state $|\psi\rangle\langle\psi| \otimes \sigma_B^{OT}$ in $\mathrm{D}(\mathcal{X}_0 \otimes \mathcal{X}_1 \otimes \mathcal{B})$ and applies the unitary

$$U_2 = \sum_{x_0,x_1\in\{0,1\}^2} |x_0x_1\rangle\langle x_0x_1| \otimes U_{x_0x_1}$$

(controlled on Bob's choice bits (x_0, x_1)) on this joint state. Once Bob sends back the qutrit $\mathcal{B}$, we extend the strategy similar to the one used previously in 17 to introduce a hypothetical message where Bob receives the guess (g_0, g_1) for the chosen bits (x_0, x_1) from Alice and holds the state σ^{OT} in $\mathrm{D}(\mathcal{X}_0 \otimes \mathcal{X}_1 \otimes \mathcal{G}_0 \otimes \mathcal{G}_1)$. Bob measures σ^{OT} to check if $(g_0, g_1) = (x_0, x_1)$ using the POVM:

$$\begin{aligned}\{P_{accept} \coloneqq \sum_{(g_0,g_1)} \sum_{(x_0,x_1)} \delta_{x_0,g_0}\delta_{x_1,g_1} |x_0x_1\rangle\langle x_0x_1|_{\mathcal{X}_0\otimes\mathcal{X}_1} \otimes |g_0g_1\rangle\langle g_0g_1|_{\mathcal{G}_0\otimes\mathcal{G}_1},\\ P_{reject} \coloneqq \mathbb{1}_{\mathcal{X}_0\otimes\mathcal{X}_1\otimes\mathcal{G}_0\otimes\mathcal{G}_1} - P_{accept}\},\end{aligned}$$

where the probability of correctly guessing (x_0, x_1) is given by $\langle\sigma^{OT}, P_{accept}\rangle$. As the states $\mathcal{X}_0$ and $\mathcal{X}_1$ with Bob remain unchanged, we have the constraint

$$\mathrm{Tr}_{\mathcal{G}_0\mathcal{G}_1}(\sigma^{OT}) = \mathrm{Tr}_{\mathcal{B}}\Big(U_2(|\psi\rangle\langle\psi| \otimes \sigma_B^{OT})U_2^\dagger\Big)$$

when maximizing $\langle\sigma^{OT}, P_{accept}\rangle$.

SDP for cheating Alice. The optimal cheating probability for Alice to correctly guess (x_0, x_1) is given by the optimal objective function value of the following SDP:

$$\begin{aligned}\text{maximize: } & \langle\sigma^{OT}, P_{accept}\rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{G}_0\mathcal{G}_1}(\sigma^{OT}) = \mathrm{Tr}_{\mathcal{B}}\Big(U_2(|\psi\rangle\langle\psi| \otimes \sigma_B^{OT})U_2^\dagger\Big) \\ & \sigma^{OT} \in \mathrm{D}(\mathcal{X}_0 \otimes \mathcal{X}_1 \otimes \mathcal{G}_0 \otimes \mathcal{G}_1) \\ & \sigma_B^{OT} \in \mathrm{D}(\mathcal{B})\end{aligned} \tag{20}$$

where recall,

$$|\psi\rangle = \frac{1}{2}\sum_{x_0,x_1} |x_0x_1\rangle_{\mathcal{X}_0\otimes\mathcal{X}_1}$$
$$U_2 = \sum_{x_0,x_1} |x_0x_1\rangle\langle x_0x_1|_{\mathcal{X}_0\otimes\mathcal{X}_1} \otimes U_{x_0x_1}$$
$$P_{accept} = \sum_{(g_0,g_1)\in\{0,1\}^2} \sum_{(x_0,x_1)\in\{0,1\}^2} \delta_{x_0,g_0}\delta_{x_1,g_1} |x_0x_1\rangle\langle x_0x_1|_{\mathcal{X}_0\otimes\mathcal{X}_1} \otimes |g_0g_1\rangle\langle g_0g_1|_{\mathcal{G}_0\otimes\mathcal{G}_1}.$$

Numerically solving the above SDP, we find that Alice can cheat with an optimal probability of $P_A^{OT} = 3/4$ and this is achieved for $\sigma_B^{OT} = \begin{bmatrix} 1/3 & 0 & 0 \\ 0 & 1/3 & 0 \\ 0 & 0 & 1/3 \end{bmatrix}$.

3.3.2 Cheating Bob

A dishonest Bob on receiving the qutrit $\mathcal{B}$, would devise a two-outcome measurement that maximizes his chances of correctly guessing Alice's choice bit y. The corresponding SDP formulation and the optimal strategy for Bob would be the exact same as discussed in Section 3.1 and thus P_B^{OT} evaluates to 3/4.

4 Stochastic switches between different protocols

In this section, we depict various stochastic switches with the protocols discussed in Section 3 and analyze their security with the underlying notions described in Section 1.2.

4.1 Stochastic switch between bit commitment and oblivious transfer

We present the switch protocol below.

Protocol 7. Quantum BC-OT stochastic switch protocol.

Stage-I

- **Alice chooses a bit $y \in \{0,1\}$ uniformly at random and creates the two-qutrit state**

$$|\phi_y\rangle = \frac{1}{\sqrt{2}}|yy\rangle + \frac{1}{\sqrt{2}}|22\rangle \in \mathcal{A}\otimes\mathcal{B}.$$

- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob chooses $c \in \{0, 1\}$ uniformly at random and sends it to Alice.
- If $c = 0$, Alice and Bob perform bit commitment as per Protocol 4, otherwise, they perform 1-out-of-2 oblivious transfer as per Protocol 6.

4.1.1 Cheating Alice

Dishonest Alice in Protocol 7 would like to maximize her average chances of successfully revealing $\hat{y}$ or correctly guessing (x_0, x_1) when Bob decides on either bit commitment or oblivious transfer (with equal probability) respectively. The constraints formulated in the SDPs for these two tasks in 16 and 20 should be jointly satisfied as Bob can randomly select one of the two tasks. We introduce an additional constraint in the form of $\sigma^{BC} = \sigma_B^{OT}$ to convey the fact that the message sent by Alice in the beginning of the protocol remains independent of Bob's selection of c in Stage-II of the switch protocol. We finally maximize the average success of Alice for the two tasks under the above constraints.

SDP for cheating Alice. The maximum cheating probability for Alice is given by the optimal objective function value of the following SDP:

$$\text{maximize: } \frac{1}{2}\left(\frac{1}{2}\langle\sigma_0^{BC}, |\phi_0\rangle\langle\phi_0|\rangle + \frac{1}{2}\langle\sigma_1^{BC}, |\phi_1\rangle\langle\phi_1|\rangle\right) + \frac{1}{2}\langle\sigma^{OT}, P_{accept}\rangle$$

subject to:

$$\begin{aligned}
&\mathrm{Tr}_{\mathcal{A}}(\sigma_0^{BC}) = \mathrm{Tr}_{\mathcal{A}}(\sigma_1^{BC}) = \sigma^{BC} && \mathrm{Tr}_{\mathcal{G}_0\mathcal{G}_1}(\sigma^{OT}) = \mathrm{Tr}_{\mathcal{B}}\Big(U_2(|\psi\rangle\langle\psi| \otimes \sigma_B^{OT})U_2^\dagger\Big)\\
&\sigma_0^{BC}, \sigma_1^{BC} \in \mathrm{D}(\mathcal{A}\otimes\mathcal{B}) && \sigma^{OT} \in \mathrm{D}(\mathcal{X}_0\otimes\mathcal{X}_1\otimes\mathcal{G}_0\otimes\mathcal{G}_1)\\
&\sigma^{BC} \in \mathrm{D}(\mathcal{B}) && \sigma_B^{OT} \in \mathrm{D}(\mathcal{B})
\end{aligned}$$

$$\boxed{\sigma^{BC} = \sigma_B^{OT}},$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are defined in Eq. (16) and P_{accept}, U_2 and $|\psi\rangle$ are as defined in Eq. (20).

Numerically solving the above SDP, we find that Alice can cheat with an optimal probability of $P_A = 0.728557$ and this is achieved when $\sigma^{BC} = \sigma_B^{OT} = \begin{bmatrix} 0.25 & 0 & 0 \\ 0 & 0.25 & 0 \\ 0 & 0 & 0.5 \end{bmatrix}$.

We remark that $P_A < P_A^{BC}$ and $P_A < P_A^{OT}$ implying an improvement in the security of the switch protocol compared to just Protocol 4 or Protocol 6.

4.1.2 Cheating Bob

Dishonest Bob in Protocol 7 would like to correctly guess y for both the tasks of bit commitment and oblivious transfer. Mathematically, Alice holds the state τ in $\mathrm{D}(\mathcal{C}\otimes\mathcal{Y}\otimes\mathcal{A}\otimes\mathcal{G})$ after sending the qutrit $\mathcal{B}$ and receiving the choice state in c for the selected protocol along with the guess g for y. As the qutrit $\mathcal{A}$ and the state for $y \in \mathcal{Y}$ remains unchanged from the state with Alice $|\psi\rangle = \sum_y \frac{1}{\sqrt{2}} |y\rangle_{\mathcal{Y}} |\phi_y\rangle_{\mathcal{A}\otimes\mathcal{B}}$ at the beginning of the protocol, we introduce a representative constraint

of the form $\mathrm{Tr}_{\mathcal{CG}}(\tau) = \mathrm{Tr}_{\mathcal{B}}(|\psi\rangle\langle\psi|)$. We finally maximize the probability of Bob correctly guessing y using the appropriate measurements for the two possible choices of c. Note that dishonest Bob can set c via postselection on a measurement on the qutrit $\mathcal{B}$.

SDP for cheating Bob. The maximum cheating probability for Bob is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \langle \tau, Q^{BC} \rangle + \langle \tau, Q^{OT} \rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{CG}}(\tau) = \mathrm{Tr}_{\mathcal{B}}(|\psi\rangle\langle\psi|) \\ & \tau \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y} \otimes \mathcal{A} \otimes \mathcal{G}) \end{aligned} \tag{21}$$

where,

$$\begin{aligned} |\psi\rangle &= \sum_{y\in\{0,1\}} \frac{1}{\sqrt{2}} |y\rangle_{\mathcal{Y}} |\phi_y\rangle_{\mathcal{A}\otimes\mathcal{B}} \\ Q^{BC} &= |0\rangle\langle 0|_{\mathcal{C}} \otimes \Big(\sum_{(y,g)\in\{0,1\}^2} \delta_{y,g} |y\rangle\langle y|_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}} \otimes |g\rangle\langle g|_{\mathcal{G}} \Big) \\ Q^{OT} &= |1\rangle\langle 1|_{\mathcal{C}} \otimes \Big(\sum_{(y',g')\in\{0,1\}^2} \delta_{y,g} |y'\rangle\langle y'|_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}} \otimes |g'\rangle\langle g'|_{\mathcal{G}} \Big). \end{aligned}$$

Numerically solving the above SDP, we find that Bob can cheat with an optimal probability of $P_B = 3/4$. Note that this is not surprising since Bob can cheat with a maximum probability of $3/4$ in the constituent protocols as both the protocols require him to correctly guess Alice's state once he receives qutrit $\mathcal{B}$.

4.2 Stochastic switch between bit commitment and weak coin flipping

We present the switch protocol below.

Protocol 8. Quantum BC-WCF stochastic switch protocol.

Stage-I

- **Alice chooses a bit $y \in \{0,1\}$ uniformly at random and creates the two-qutrit state**

$$|\phi_y\rangle = \frac{1}{\sqrt{2}} |yy\rangle + \frac{1}{\sqrt{2}} |22\rangle \in \mathcal{A} \otimes \mathcal{B}.$$

- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob chooses $c \in \{0,1\}$ uniformly at random and sends it to Alice.
- If $c = 0$, Alice and Bob perform bit commitment as per Protocol 4, otherwise, they perform weak coin flipping as per Protocol 5.

4.2.1 Cheating Alice

Dishonest Alice in Protocol 8 would like to maximize her average chances of successfully revealing $\hat{y}$ when Bob decides to perform bit commitment or forcing the outcome 1 when Bob instead decides to perform weak coin flipping.

The constraints formulated in the SDPs for these two tasks in 16 and 18 should be jointly satisfied as Bob can randomly select one of the two tasks. As earlier, we introduce an additional constraint in the form of $\sigma^{BC} = \sigma^{WCF}$ to depict the fact that the message sent by Alice in the beginning of the protocol remains independent of Bob's protocol selection. We finally maximize the average success of Alice for the two tasks under the above constraints.

SDP for cheating Alice. The optimal cheating probability for Alice is given by the optimal objective function value of the following SDP:

$$\text{maximize: } \frac{1}{2}\left(\frac{1}{2}\langle\sigma_0^{BC}, |\phi_0\rangle\langle\phi_0|\rangle + \frac{1}{2}\langle\sigma_1^{BC}, |\phi_1\rangle\langle\phi_1|\rangle\right) + \frac{1}{2}\left(\frac{1}{2}\langle\sigma_0^{WCF}, P_0\rangle + \frac{1}{2}\langle\sigma_1^{WCF}, P_1\rangle\right)$$

subject to:

$$\begin{aligned}
&\mathrm{Tr}_{\mathcal{A}}(\sigma_{\hat{y}}^{BC}) = \sigma^{BC},\ \forall \hat{y} \in \{0,1\} \\
&\sigma_{\hat{y}}^{BC} \in \mathrm{D}(\mathcal{A}\otimes\mathcal{B}),\ \forall \hat{y} \in \{0,1\} \\
&\sigma^{BC} \in \mathrm{D}(\mathcal{B})
\end{aligned}
\qquad
\begin{aligned}
&\mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_0^{WCF}) = \mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_1^{WCF}) = \sigma_B^{WCF} \\
&\mathrm{Tr}_{\mathcal{B}_1}(\sigma_B^{WCF}) = \sigma^{WCF} \\
&\sigma_0^{WCF}, \sigma_1^{WCF} \in \mathrm{D}(\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{B}_0\otimes\mathcal{A}_1\otimes\mathcal{B}_1) \\
&\sigma_B^{WCF} \in \mathrm{D}(\mathcal{B}_0\otimes\mathcal{B}_1) \\
&\sigma^{WCF} \in \mathrm{D}(\mathcal{B}_0)
\end{aligned}$$

$$\boxed{\sigma^{BC} = \sigma^{WCF}},$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are defined in Eq. (16) and P_0 and P_1 are as defined in Eq. (18).

Numerically solving the above SDP, we find that Alice can cheat with an optimal probability of $P_A = 0.743818$ and this is achieved when $\sigma^{BC} = \sigma^{WCF} = \begin{bmatrix} 0.1281 & 0 & 0 \\ 0 & 0.1281 & 0 \\ 0 & 0 & 0.7438 \end{bmatrix}$. Again, note that $P_A < P_A^{BC}$ and $P_A < P_A^{WCF}$ implying an improvement in the security of the switch protocol compared to just Protocol 4 or Protocol 5.

4.2.2 Cheating Bob

Dishonest Bob would like to maximize the probability of either correctly guessing Alice's commit bit (for bit commitment) or successfully forcing the outcome 0 (for weak coin flipping). In order to systematically analyze the extent of Bob's cheating, we provide a slight modification of Protocol 8 to simplify Bob's analysis. Once Alice sends the qutrit $\mathcal{B}_0$, she receives c and the guess g for y. She next sends Bob the qutrit $\mathcal{B}_1$ and receives z to obtain protocol outcome here by measuring the qutrit $\mathcal{A}_{\bar{z}}$. Note that this modification does not affect the probability of Bob successfully guessing y or forcing the outcome 0 from the actual protocol and makes the analysis for cheating Bob easier to analyze. This is because Bob sends back his guess g before $\mathcal{B}_1$ is received and furthermore, no additional information is received by Bob in this modified protocol to successfully force the outcome 0.

Mathematically, consider the state with Alice $|\psi\rangle = \sum_y \frac{1}{\sqrt{2}} |y\rangle_{\mathcal{Y}} |\phi_y\rangle_{\mathcal{A}_0\otimes\mathcal{B}_0} |\phi_y\rangle_{\mathcal{A}_1\otimes\mathcal{B}_1}$ at the beginning of the protocol. After sending the qutrit $\mathcal{B}_0$, Alice receives c and g from Bob and now holds the state $\tau_0 \in \mathrm{D}(\mathcal{C}\otimes\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{A}_1\otimes\mathcal{B}_1\otimes\mathcal{G})$. She subsequently sends Bob the qutrit $\mathcal{B}_1$ and receives z. Alice measures her state $\tau \in \mathrm{D}(\mathcal{C}\otimes\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{A}_1\otimes\mathcal{Z}\otimes\mathcal{G})$ at the end of the protocol where she accepts, if

Bob successfully guesses y, or outputs 0, if Bob successfully forces 0. The joint probability of Bob selecting $c = 0$ and successfully guessing y is given by $\langle \tau, Q_0 \rangle$ where

$$Q_0 = |0\rangle\langle 0|_{\mathcal{C}} \otimes \Big(\sum_{(y,g)\in\{0,1\}^2} \delta_{y,g} \otimes |y\rangle\langle y|_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}_0} \otimes \mathbb{1}_{\mathcal{A}_1} \otimes \mathbb{1}_{\mathcal{Z}} \otimes |g\rangle\langle g|_{\mathcal{G}} \Big).$$

Similarly, the joint probability of Bob selecting $c = 1$ and successfully forcing the outcome 0 is given by $\langle \tau, Q_1 \rangle$ where

$$Q_1 = |1\rangle\langle 1|_{\mathcal{C}} \otimes \Big(\sum_{z\in\{0,1\}} \mathbb{1}_{\mathcal{Y}} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)_{\mathcal{A}_{\bar{z}}} \otimes \mathbb{1}_{\mathcal{A}_z} \otimes |z\rangle\langle z|_{\mathcal{Z}} \otimes \mathbb{1}_{\mathcal{G}} \Big).$$

We impose the constraint $\mathrm{Tr}_{\mathcal{Z}}(\tau) = \mathrm{Tr}_{\mathcal{B}_1}(\tau_0)$ which ensures that the guess state $\mathcal{G}$ in τ remains the same at the end of the protocol and also the constraint $\mathrm{Tr}_{\mathcal{CG}}(\tau_0) = \mathrm{Tr}_{\mathcal{B}_0}(|\psi\rangle\langle\psi|)$. The previous two constraints together ensure that the state on $\mathcal{A}_0, \mathcal{A}_1$ and $\mathcal{Y}$ remains unchanged until the end of the protocol. We finally maximize $\langle \tau, Q_0 + Q_1 \rangle$ to evaluate the maximum cheating probability of Bob in Protocol 8.

SDP for cheating Bob. The optimal cheating probability for Bob is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \langle \tau, Q \rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{CG}}(\tau_0) = \mathrm{Tr}_{\mathcal{B}_0}(|\psi\rangle\langle\psi|) \\ & \mathrm{Tr}_{\mathcal{Z}}(\tau) = \mathrm{Tr}_{\mathcal{B}_1}(\tau_0) \\ & \tau_0 \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y} \otimes \mathcal{A}_0 \otimes \mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{G}) \\ & \tau \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y} \otimes \mathcal{A}_0 \otimes \mathcal{A}_1 \otimes \mathcal{Z} \otimes \mathcal{G}) \end{aligned} \tag{22}$$

where,

$$|\psi\rangle = \sum_{y\in\{0,1\}} \frac{1}{\sqrt{2}} |y\rangle_{\mathcal{Y}} |\phi_y\rangle_{\mathcal{A}_0\otimes\mathcal{B}_0} |\phi_y\rangle_{\mathcal{A}_1\otimes\mathcal{B}_1}$$

$$\begin{aligned} Q = |0\rangle\langle 0|_{\mathcal{C}} \otimes \Big(& \sum_{(y,g)\in\{0,1\}^2} \delta_{y,g} \otimes |y\rangle\langle y|_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}_0} \otimes \mathbb{1}_{\mathcal{A}_1} \otimes \mathbb{1}_{\mathcal{Z}} \otimes |g\rangle\langle g|_{\mathcal{G}} \Big) \\ & + |1\rangle\langle 1|_{\mathcal{C}} \otimes \Big(\sum_{z\in\{0,1\}} \mathbb{1}_{\mathcal{Y}} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)_{\mathcal{A}_{\bar{z}}} \otimes \mathbb{1}_{\mathcal{A}_z} \otimes |z\rangle\langle z|_{\mathcal{Z}} \otimes \mathbb{1}_{\mathcal{G}} \Big). \end{aligned}$$

Numerically solving the above SDP, we find that Bob can cheat with an optimal probability of $P_B = 0.75$.

4.3 Stochastic switch between oblivious transfer and weak coin flipping

We present the switch protocol below.

Protocol 9. Quantum OT-WCF stochastic switch protocol.

Stage-I

- **Alice chooses a bit $y \in \{0, 1\}$ uniformly at random and creates the two-qutrit state**

$$|\phi_y\rangle = \frac{1}{\sqrt{2}} |yy\rangle + \frac{1}{\sqrt{2}} |22\rangle \in \mathcal{A} \otimes \mathcal{B}.$$

- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob chooses $c \in \{0, 1\}$ uniformly at random and sends it to Alice.
- If $c = 0$, Alice and Bob perform 1-out-of-2 oblivious transfer as per Protocol 6 , otherwise, they perform weak coin flipping as per Protocol 5.

4.3.1 Cheating Alice

A dishonest Alice in Protocol 9 would like to maximize her average chances of correctly guessing (x_0, x_1) or forcing the outcome 1 when Bob decides to perform oblivious transfer or weak coin flipping (with equal probability) respectively.

The constraints formulated in the SDP for these two tasks in 20 and 18 should be jointly satisfied as Bob can randomly select one of the two tasks. As for the SDP of the previous two switch protocols, we introduce an additional constraint in the form of $\sigma_B^{OT} = \sigma^{WCF}$ to depict the fact that the message sent by Alice in the beginning of the protocol remains independent of Bob's protocol selection based on the bit c. We finally maximize the average success of Alice for the two tasks under the above constraints.

SDP for cheating Alice. The optimal cheating probability for dishonest Alice is given by the optimal objective function value of the following SDP:

$$\text{maximize: } \frac{1}{2}\langle \sigma^{OT}, P_{accept}\rangle + \frac{1}{2}\left(\frac{1}{2}\langle \sigma_0^{WCF}, P_0\rangle + \frac{1}{2}\langle \sigma_1^{WCF}, P_1\rangle\right)$$

subject to:

$$\begin{aligned}
&\mathrm{Tr}_{\mathcal{G}_0\mathcal{G}_1}(\sigma^{OT}) = \mathrm{Tr}_{\mathcal{B}}\Big(U_2(|\psi\rangle\langle\psi| \otimes \sigma_B^{OT})U_2^\dagger\Big) \\
&\sigma^{OT} \in \mathrm{D}(\mathcal{X}_0 \otimes \mathcal{X}_1 \otimes \mathcal{G}_0 \otimes \mathcal{G}_1) \\
&\sigma_B^{OT} \in \mathrm{D}(\mathcal{B}) \\
&\mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_0^{WCF}) = \mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_1^{WCF}) = \sigma_B^{WCF} \\
&\mathrm{Tr}_{\mathcal{B}_1}(\sigma_B^{WCF}) = \sigma^{WCF} \\
&\sigma_0^{WCF}, \sigma_1^{WCF} \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{A}_0 \otimes \mathcal{B}_0 \otimes \mathcal{A}_1 \otimes \mathcal{B}_1) \\
&\sigma_B^{WCF} \in \mathrm{D}(\mathcal{B}_0 \otimes \mathcal{B}_1) \\
&\sigma^{WCF} \in \mathrm{D}(\mathcal{B}_0)
\end{aligned}$$

$$\boxed{\sigma_B^{OT} = \sigma^{WCF}},$$

where P_{accept}, U_2 and $|\psi\rangle$ are defined in Eq. (20) and P_0 and P_1 are as defined in Eq. (18).

Numerically solving the above SDP, we find that Alice can cheat with an optimal probability of $P_A = 0.704407$ and this is achieved when $\sigma_B^{OT} = \sigma^{WCF} = \begin{bmatrix} 0.22 & 0 & 0 \\ 0 & 0.22 & 0 \\ 0 & 0 & 0.56 \end{bmatrix}$. Again, Alice cheating in the switch protocol gets reduced when compared to its constituent protocols.

4.3.2 Cheating Bob

As the objective of dishonest Bob is identical to the formulation of cheating Bob in Protocol 8, the optimal cheating probability is $P_B^* = 3/4$.

4.4 Stochastic switch between bit commitment, weak coin flipping, and oblivious transfer

We present the switch protocol below.

Protocol 10. Quantum BC-WCF-OT stochastic switch protocol.

Stage-I

- **Alice chooses a bit $y \in \{0,1\}$ uniformly at random and creates the two-qutrit state**

$$|\phi_y\rangle = \frac{1}{\sqrt{2}}|yy\rangle + \frac{1}{\sqrt{2}}|22\rangle \in \mathcal{A} \otimes \mathcal{B}.$$

- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob chooses $c \in \{0,1,2\}$ uniformly at random and sends it to Alice.
- If $c = 0$, Alice and Bob perform bit commitment as per Protocol 4, if $c = 1$, they perform weak coin flipping as per Protocol 5, otherwise they perform 1-out-of-2 oblivious transfer as per Protocol 6.

4.4.1 Cheating Alice

As in the previous switch protocols, a dishonest Alice wishes to maximize her average chances of either successfully revealing $\hat{y}$ (bit commitment), forcing the outcome 1 (weak coin flipping), or correctly guessing (x_0, x_1) (oblivious transfer) when Bob decides one of these three tasks (with equal probability).

The constraints formulated in the SDPs for the three tasks in 16, 18 and 20 are to be satisfied simultaneously as Bob can randomly select one of the three tasks. We introduce an additional connecting constraint $\sigma^{BC} = \sigma^{WCF} = \sigma_B^{OT}$ due to the fact that the qutrit $\mathcal{B}$ is sent by Alice before Bob makes a protocol selection based on his choice c. We finally maximize the average success of Alice for the three tasks under the above constraints.

SDP for cheating Alice. The optimal cheating probability for Alice is given by the optimal objective function value of the following SDP:

$$\text{maximize: } \frac{1}{3}\Big(\sum_{y\in\{0,1\}}\frac{1}{2}\langle\sigma_y^{BC},|\phi_y\rangle\langle\phi_y|\rangle\Big)+\frac{1}{3}\Big(\frac{1}{2}\langle\sigma_0^{WCF},P_0\rangle+\frac{1}{2}\langle\sigma_1^{WCF},P_1\rangle\Big)+\frac{1}{3}\langle\sigma^{OT},P_{accept}\rangle$$

subject to:

$$\begin{aligned}
&\mathrm{Tr}_{\mathcal{A}}(\sigma_0^{BC})=\sigma^{BC}\\
&\mathrm{Tr}_{\mathcal{A}}(\sigma_1^{BC})=\sigma^{BC}\\
&\sigma_0^{BC}\in\mathrm{D}(\mathcal{AB}),\\
&\sigma_1^{BC}\in\mathrm{D}(\mathcal{AB}),\\
&\sigma^{BC}\in\mathrm{D}(\mathcal{B})
\end{aligned}
\qquad
\begin{aligned}
&\mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_0^{WCF})=\mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_1^{WCF})\\
&\mathrm{Tr}_{\mathcal{Y}\mathcal{A}_0\mathcal{A}_1}(\sigma_1^{WCF})=\sigma_B^{WCF}\\
&\mathrm{Tr}_{\mathcal{B}_1}(\sigma_B^{WCF})=\sigma^{WCF}\\
&\sigma_0^{WCF}\in\mathrm{D}(\mathcal{Y}\mathcal{A}_0\mathcal{B}_0\mathcal{A}_1\mathcal{B}_1)\\
&\sigma_1^{WCF}\in\mathrm{D}(\mathcal{Y}\mathcal{A}_0\mathcal{B}_0\mathcal{A}_1\mathcal{B}_1)\\
&\sigma_B^{WCF}\in\mathrm{D}(\mathcal{B}_0\mathcal{B}_1)\\
&\sigma^{WCF}\in\mathrm{D}(\mathcal{B}_0)
\end{aligned}
\qquad
\begin{aligned}
&\mathrm{Tr}_{\mathcal{G}_0\mathcal{G}_1}(\sigma^{OT})=\mathrm{Tr}_{\mathcal{B}}\Big(U_2(|\psi\rangle\langle\psi|\otimes\sigma_B^{OT})U_2^\dagger\Big)\\
&\sigma^{OT}\in\mathrm{D}(\mathcal{X}_0\mathcal{X}_1\mathcal{G}_0\mathcal{G}_1)\\
&\sigma_B^{OT}\in\mathrm{D}(\mathcal{B})
\end{aligned}$$

$$\boxed{\sigma^{BC}=\sigma^{WCF}=\sigma_B^{OT}},$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are defined in Eq. (16), P_0 and P_1 are defined in Eq. (18), and P_{accept}, U_2 and $|\psi\rangle$ are as defined in Eq. (20).

Numerically solving the above SDP, we find that Alice can cheat with an optimal probability of $P_A=0.717779$ and this is achieved when $\sigma^{BC}=\sigma^{WCF}=\sigma_B^{OT}=\begin{bmatrix}0.1987&0&0\\0&0.1987&0\\0&0&0.6026\end{bmatrix}$. Note that P_A for the switch between protocols for bit commitment, weak coin flipping, and oblivious transfer is smaller that the cheating probabilities of its constituent protocols.

4.4.2 Cheating Bob

Dishonest Bob would like to maximize the combined probability of correctly guessing y (for bit commitment), successfully forcing the outcome 0 (for weak coin flipping) or again guessing y correctly (for oblivious transfer). Note that in this switch, $|0\rangle_{\mathcal{C}}$ and $|2\rangle_{\mathcal{C}}$ correspond to Bob selecting bit commitment and oblivious transfer respectively where he tries to correctly guess y, while $|1\rangle_{\mathcal{C}}$ corresponds to Bob selecting weak coin flipping where he wishes to force the outcome 0. The SDP for this three-task switch protocol can thus be formulated along the lines of 22 and is described next.

SDP for cheating Bob. The optimal cheating probability for Bob is given by the optimal objective function value of the following SDP:

$$\begin{aligned}
\text{maximize: }\ &\langle\tau,Q\rangle\\
\text{subject to: }\ &\mathrm{Tr}_{\mathcal{CG}}(\tau_0)=\mathrm{Tr}_{\mathcal{B}_0}(|\psi\rangle\langle\psi|)\\
&\mathrm{Tr}_{\mathcal{Z}}(\tau)=\mathrm{Tr}_{\mathcal{B}_1}(\tau_0)\\
&\tau_0\in\mathrm{D}(\mathcal{C}\otimes\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{A}_1\otimes\mathcal{B}_1\otimes\mathcal{G})\\
&\tau\in\mathrm{D}(\mathcal{C}\otimes\mathcal{Y}\otimes\mathcal{A}_0\otimes\mathcal{A}_1\otimes\mathcal{Z}\otimes\mathcal{G})
\end{aligned}\tag{23}$$

where,

$$|\psi\rangle = \sum_{y\in\{0,1\}} \frac{1}{\sqrt{2}} |y\rangle_{\mathcal{Y}} |\phi_y\rangle_{\mathcal{A}_0\otimes\mathcal{B}_0} |\phi_y\rangle_{\mathcal{A}_1\otimes\mathcal{B}_1}$$

$$Q = (|0\rangle\langle 0| + |2\rangle\langle 2|)_{\mathcal{C}} \otimes \Big(\sum_{(y,g)\in\{0,1\}^2} \delta_{y,g} \otimes |y\rangle\langle y|_{\mathcal{Y}} \otimes \mathbb{1}_{\mathcal{A}_0} \otimes \mathbb{1}_{\mathcal{A}_1} \otimes \mathbb{1}_{\mathcal{Z}} \otimes |g\rangle\langle g|_{\mathcal{G}} \Big)$$
$$+ |1\rangle\langle 1|_{\mathcal{C}} \otimes \Big(\sum_{z\in\{0,1\}} \mathbb{1}_{\mathcal{Y}} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)_{\mathcal{A}_{\overline{z}}} \otimes \mathbb{1}_{\mathcal{A}_z} \otimes |z\rangle\langle z|_{\mathcal{Z}} \otimes \mathbb{1}_{\mathcal{G}} \Big).$$

Numerically solving the above SDP, we find that Bob can cheat with an optimal probability of $P_B = 3/4$.

5 A quantum protocol for Rabin oblivious transfer

In the previous section, we noticed that the random subtask selection by Bob in a switch protocol could potentially limit the chances of successful cheating by Alice when compared to her chances in the constituent protocols. Therefore, it seems natural to examine the idea of stochastic switching between different protocols *for the same task*. In this section, we devise protocols for two variants of Rabin oblivious transfer and in each, we switch between a pair of unsecure protocols to find one with an improved security.

5.1 Rabin oblivious transfer

Rabin oblivious transfer (ROT) is the cryptographic task between two parties, Alice and Bob, where Alice sends a bit $y \in \{0, 1\}$ to Bob which he receives with probability 1/2 and with probability 1/2 he receives $\perp$ indicating the bit was lost.

We formally define the following notions of security for a given ROT protocol.

- *Completeness:* If both Alice and Bob are honest, then neither party aborts, Bob receives y with probability 1/2 and $\perp$ with probability 1/2.
- *Cheating Alice* (variant 1): If Bob is honest, then dishonest Alice's cheating probability is defined as

  $$P_A^{ROT1} = \max \Pr[\text{Alice correctly guesses whether Bob received } y \text{ or learnt } \perp]$$

  where the maximum is taken over all cheating strategies of Alice. Note that $P_A^{ROT1} \geq 1/2$ as Alice can simply choose to follow the protocol honestly and make a uniformly random guess to whether Bob received y or $\perp$ and succeed with probability 1/2.
- *Cheating Alice* (variant 2): If Bob is honest, then dishonest Alice's cheating probability is defined as

  $$P_A^{ROT2} = \max \Pr[\text{Alice successfully forces Bob to receive } \perp]$$

  where the maximum is taken over all cheating strategies of Alice. We have $P_A^{ROT2} \geq 1/2$ as Alice can simply choose to follow the protocol honestly and force Bob to observe y or $\perp$ with probability 1/2 each.
- *Cheating Bob:* If Alice is honest, then dishonest Bob's cheating probability is defined as

  $$P_B^{ROT} = \max \Pr[\text{Bob successfully learns } y]$$

where the maximum is taken over all cheating strategies of Bob. Note that $P_B^{ROT} \geq 3/4$ as Bob can simply choose to follow the protocol to learn y with probability $1/2$ and randomly guess y in the event of getting $\perp$.

To date, there is little known about the limits of Rabin oblivious transfer and some of the difficulty of defining the security of ROT protocols is in part due to vague cheating desire of Alice. Moreover, Shor's factoring algorithm [39] breaks the security of a classical ROT protocol [40] that relied on the hardness of factoring hinting at the need for developing secure quantum ROT protocols. As far as we are aware, there are no quantum protocols known for ROT in the literature. In this section, we exhibit protocols for the two variants of ROT (defined previously) with poor security which we stochastically combine to construct quantum ROT protocols with improved security.

From here on, we use the notation $|\perp\rangle$ to mean the computational basis state $|2\rangle$ for a qutrit system.

5.2 Stochastic Rabin OT switch (variant 1).

We now present a couple of insecure ROT protocols based on the first variant where Alice wishes to successfully guess whether Bob received the data or $\perp$ and construct another ROT protocol that stochastically switches between these insecure protocols. We further analyze the security of our switch protocol using semidefinite programming to depict a substantial improvement over the security of the constituent protocols.

Protocol 11. A simple ROT protocol (variant 1).

Stage-I

- **Alice chooses a bit $y \in \{0,1\}$ uniformly at random and creates the single-qutrit state**
$$|\phi_y\rangle = \frac{1}{\sqrt{2}}|y\rangle + \frac{1}{\sqrt{2}}|\perp\rangle \in \mathcal{B}.$$
- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob measures the qutrit $\mathcal{B}$ in computational basis to output y or $\perp$.

The above protocol is trivially *complete* as Bob outputs y or $\perp$ each with probability $1/2$ whenever both are honest. However, dishonest Alice can cheat perfectly by sending the qutrit $|\perp\rangle\langle\perp|$ to Bob where he outputs $\perp$ with probability 1. Alternatively, dishonest Bob can perform state discrimination on the two possible states to learn y with a maximum probability 0.9330.

Protocol 12. A simple ROT protocol with verification (variant 1).

Stage-I

- **Alice chooses a bit $y \in \{0,1\}$ uniformly at random and creates the single-qutrit state**
$$|\phi_y\rangle = \frac{1}{\sqrt{2}}|y\rangle + \frac{1}{\sqrt{2}}|\perp\rangle \in \mathcal{B}.$$
- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Alice reveals y to Bob where he measures the qutrit state in $\mathcal{B}$ to accept or reject with the POVM:
$$\{\Pi_{accept} \coloneqq |\phi_y\rangle\langle\phi_y|_{\mathcal{B}}, \Pi_{reject} \coloneqq \mathbb{1}_{\mathcal{B}} - \Pi_{accept}\}.$$
If Bob accepts, Alice and Bob restart with Protocol 11 (noting the restarted protocol will have a new choice of y for Alice).

Dishonest Alice in Protocol 12 could cheat perfectly by not deviating from the protocol until Bob *accepts* and subsequently sends $|\perp\rangle\langle\perp|$ once they restart Protocol 11. As the first choice of y is completely inconsequential and does not affect the outcome, dishonest Bob would always *accept* and perform state discrimination to successfully learn the (newly chosen) bit y with maximum probability 0.9330.

Protocol 13. A quantum protocol for ROT based on stochastic switch (variant 1).

Stage-I

- **Alice chooses a bit $y_0 \in \{0,1\}$ uniformly at random and creates the single-qutrit state**
$$|\phi_{y_0}\rangle = \frac{1}{\sqrt{2}}|y_0\rangle + \frac{1}{\sqrt{2}}|\perp\rangle \in \mathcal{B}_0.$$
- **Alice sends the qutrit $\mathcal{B}_0$ to Bob.**

Stage-II

- Bob chooses $c \in \{0,1\}$ uniformly at random and sends it to Alice.
  - If $c = 0$, Bob measures the qutrit $\mathcal{B}_0$ in computational basis to output y_0 or $\perp$.
  - If $c = 1$, Alice reveals y_0 to Bob where he measures $\mathcal{B}_0$ to accept or reject according to the POVM:
$$\{\Pi_{accept} \coloneqq |\phi_{y_0}\rangle\langle\phi_{y_0}|_{\mathcal{B}_0}, \Pi_{reject} \coloneqq \mathbb{1}_{\mathcal{B}_0} - \Pi_{accept}\}.$$
If Bob accepts,
    - Alice chooses another bit $y_1 \in \{0,1\}$ uniformly at random and creates the state
$$|\phi_{y_1}\rangle = \frac{1}{\sqrt{2}}|y_1\rangle + \frac{1}{\sqrt{2}}|\perp\rangle \in \mathcal{B}_1.$$
    - Alice sends the qutrit $\mathcal{B}_1$ to Bob.
    - Bob measures the qutrit $\mathcal{B}_1$ in the computational basis to output y_1 or $\perp$.

5.2.1 Cheating Alice (variant 1)

Dishonest Alice in Protocol 13 would like to maximize her average chances of successfully guessing Bob's outcome (y or $\perp$) when Bob selects $c = 0$ and successfully passing Bob's test when he selects $c = 1$. It is worth noting that if Bob accepts, Alice can successfully cheat with probability 1 in the restarted protocol.

The success probability of Alice can be evaluated by considering the two equally likely scenarios of Bob's selection of c. If σ_B is the state of the qutrit $\mathcal{B}$ sent by Alice in the first message of the

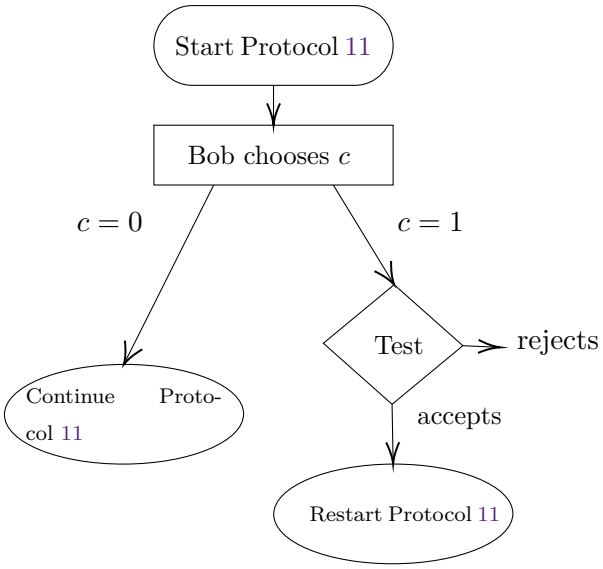

Figure 2: A schematic of our Rabin oblivious transfer protocol. Bob can either decide to continue with the now-in-progress Protocol 11 or test and restart Protocol 11 from the beginning.

protocol, then the probability with which Alice successfully guesses Bob's outcome when he selects $c = 0$ is given by $\langle \sigma_0, P_0 \rangle$ where $\sigma_0 \in \mathrm{D}(\mathcal{G} \otimes \mathcal{B})$ is the state with Bob when Alice sends her guess for the outcome and P_0 is given by

$$P_0 = |0\rangle\langle 0|_{\mathcal{G}} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)_{\mathcal{B}} + |1\rangle\langle 1|_{\mathcal{G}} \otimes |\perp\rangle\langle\perp|_{\mathcal{B}}$$

is the joint measurement that evaluates whether the guess $\mathcal{G}$ aligns with the measurement outcome. Note that $|0\rangle_{\mathcal{G}}$ means that Alice guesses that Bob has received y and $|1\rangle_{\mathcal{G}}$ means Alice guesses that Bob did not learn anything.

Alternatively, if $\sigma_1 \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{B})$ is the state with Bob when he selects $c = 1$, then the joint probability of acceptance by Bob is given by $\langle \sigma_1, P_1 \rangle$ where,

$$P_1 = \sum_{y \in \{0,1\}} |y\rangle\langle y|_{\mathcal{Y}} \otimes |\phi_y\rangle\langle\phi_y|_{\mathcal{B}}\,. \tag{24}$$

SDP for cheating Alice. The optimal cheating probability for Alice is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \frac{1}{2}\langle \sigma_0, P_0 \rangle + \frac{1}{2}\langle \sigma_1, P_1 \rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{G}}(\sigma_0) = \mathrm{Tr}_{\mathcal{Y}}(\sigma_1) = \sigma_B \\ & \sigma_0 \in \mathrm{D}(\mathcal{G} \otimes \mathcal{B}) \\ & \sigma_1 \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{B}) \\ & \sigma_B \in \mathrm{D}(\mathcal{B}) \end{aligned} \tag{25}$$

where recall,

$$\begin{aligned} P_0 &= |0\rangle\langle 0|_{\mathcal{G}} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)_{\mathcal{B}} + |1\rangle\langle 1|_{\mathcal{G}} \otimes |\perp\rangle\langle\perp|_{\mathcal{B}} \\ P_1 &= \sum_{y \in \{0,1\}} |y\rangle\langle y|_{\mathcal{Y}} \otimes |\phi_y\rangle\langle\phi_y|_{\mathcal{B}}\,. \end{aligned}$$

Numerically solving the above SDP, we find that Alice can cheat with an optimal probability $P_A^{ROT1} = 0.9330$ and this is achieved for $\sigma_B = \begin{bmatrix} 0.1890 & -0.1220 & 0.1443 \\ -0.1220 & 0.1890 & 0.1443 \\ 0.1443 & 0.1443 & 0.6220 \end{bmatrix}$.

5.2.2 Cheating Bob

Dishonest Bob would like to correctly guess y, either in the first run of the protocol or the second. In order to simplify the analysis for cheating Bob, we devise a modified protocol and claim that the extent of Bob's cheating in the modified protocol is same as in the actual protocol. For the analysis, consider the state

$$|\psi\rangle = \sum_{y_0 \in \{0,1\}} \sum_{y_1 \in \{0,1\}} \frac{1}{2} |y_0\rangle_{\mathcal{Y}_0} |y_0\rangle_{\mathcal{Y}_0'} |y_1\rangle_{\mathcal{Y}_1} |\phi_{y_0}\rangle_{\mathcal{B}_0} |\phi_{y_1}\rangle_{\mathcal{B}_1}$$

with Alice at the beginning of Protocol 13. Alice sends Bob the qutrit $\mathcal{B}_0$ while she receives c and a guess g_0 for y_0. At this point, Alice holds the state $\tau_0 \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y}_0 \otimes \mathcal{Y}_0' \otimes \mathcal{Y}_1 \otimes \mathcal{B}_1 \otimes \mathcal{G}_0)$ and sends y_0 (in $\mathcal{Y}_0'$) to Bob. Here note that Alice initially held a copy of y_0 in $\mathcal{Y}_0'$ which she reveals to Bob and keeps the other to check whether $g_0 = y_0$ at the end of the protocol. In the final set of messages, Alice sends the qutrit $\mathcal{B}_1$ to Bob and receives g_1 as the guess for y_1. At the end of the protocol, Alice holds the state $\tau \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y}_0 \otimes \mathcal{Y}_1 \otimes \mathcal{G}_0 \otimes \mathcal{G}_1)$ which she measures to accept either g_0, if $c = 0$ and Bob correctly guesses y_0, or accept g_1, if $c = 1$ and Bob correctly guesses y_1. The joint probability of Bob selecting $c = 0$ and correctly guessing y_0 is given by $\langle \tau, Q_0 \rangle$ where,

$$Q_0 = |0\rangle\langle 0|_{\mathcal{C}} \otimes \Big(\sum_{(y_0,g_0) \in \{0,1\}^2} \delta_{y_0,g_0} |y_0\rangle\langle y_0|_{\mathcal{Y}_0} \otimes \mathbb{1}_{\mathcal{Y}_1} \otimes |g_0\rangle\langle g_0|_{\mathcal{G}_0} \otimes \mathbb{1}_{\mathcal{G}_1} \Big).$$

Similarly, the joint probability of Bob selecting $c = 1$ and successfully guessing y_1 is given by $\langle \tau, Q_1 \rangle$ where,

$$Q_1 = |1\rangle\langle 1|_{\mathcal{C}} \otimes \Big(\sum_{(y_1,g_1) \in \{0,1\}^2} \delta_{y_1,g_1} \mathbb{1}_{\mathcal{Y}_0} \otimes |y_1\rangle\langle y_1|_{\mathcal{Y}_1} \otimes \mathbb{1}_{\mathcal{G}_0} \otimes |g_1\rangle\langle g_1|_{\mathcal{G}_1} \Big).$$

To ensure that Bob's guess (g_0, g_1) and Alice's input (y_0, y_1) remains unchanged, we introduce the constraints $\mathrm{Tr}_{\mathcal{Y}_0'\mathcal{B}_1}(\tau_0) = \mathrm{Tr}_{\mathcal{G}_1}(\tau)$ and $\mathrm{Tr}_{\mathcal{C}\mathcal{G}_0}(\tau_0) = \mathrm{Tr}_{\mathcal{B}_0}(|\psi\rangle\langle\psi|)$. We finally maximize $\langle \tau, Q_0 + Q_1 \rangle$ to obtain the optimal cheating probability for Bob.

SDP for cheating Bob. The optimal cheating probability for Bob is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \langle \tau, Q \rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{C}\mathcal{G}_0}(\tau_0) = \mathrm{Tr}_{\mathcal{B}_0}(|\psi\rangle\langle\psi|) \\ & \mathrm{Tr}_{\mathcal{Y}_0'\mathcal{B}_1}(\tau_0) = \mathrm{Tr}_{\mathcal{G}_1}(\tau) \\ & \tau_0 \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y}_0 \otimes \mathcal{Y}_0' \otimes \mathcal{Y}_1 \otimes \mathcal{B}_1 \otimes \mathcal{G}_0) \\ & \tau \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y}_0 \otimes \mathcal{Y}_1 \otimes \mathcal{G}_0 \otimes \mathcal{G}_1) \end{aligned} \tag{26}$$

where recall,

$$
\begin{aligned}
|\psi\rangle &= \sum_{y_0\in\{0,1\}} \sum_{y_1\in\{0,1\}]} \frac{1}{2} |y_0\rangle_{\mathcal{Y}_0} |y_0\rangle_{\mathcal{Y}_0'} |y_1\rangle_{\mathcal{Y}_1} |\phi_{y_0}\rangle_{\mathcal{B}_0} |\phi_{y_1}\rangle_{\mathcal{B}_1} \\
Q &= |0\rangle\langle 0|_{\mathcal{C}} \otimes \Big(\sum_{(y_0,g_0)\in\{0,1\}^2} \delta_{y_0,g_0} |y_0\rangle\langle y_0|_{\mathcal{Y}_0} \otimes \mathbb{1}_{\mathcal{Y}_1} \otimes |g_0\rangle\langle g_0|_{\mathcal{G}_0} \otimes \mathbb{1}_{\mathcal{G}_1} \Big) \\
&\quad + |1\rangle\langle 1|_{\mathcal{C}} \otimes \Big(\sum_{(y_1,g_1)\in\{0,1\}^2} \delta_{y_1,g_1} \mathbb{1}_{\mathcal{Y}_0} \otimes |y_1\rangle\langle y_1|_{\mathcal{Y}_1} \otimes \mathbb{1}_{\mathcal{G}_0} \otimes |g_1\rangle\langle g_1|_{\mathcal{G}_1} \Big).
\end{aligned} \tag{27}
$$

Numerically solving the above SDP, we find that Bob can cheat with an optimal probability of $P_B^{ROT} = 0.9691$.

5.3 Stochastic Rabin OT switch (variant 2)

Next, we develop and analyze another ROT protocol for the second variant where Alice wishes to force $\perp$. The constant lower bounds for such task are discussed in [4]. The ROT protocol in discussion also relies on the idea of stochastic switching between insecure protocols to develop another protocol with improved security.

Protocol 14. An alternative ROT protocol based on stochastic switch.

Stage-I

- **Alice chooses a bit $y_0 \in \{0,1\}$ uniformly at random and creates the two-qutrit state**
$$|\phi_{y_0}\rangle = \frac{1}{\sqrt{2}} |y_0 y_0\rangle + \frac{1}{\sqrt{2}} |\perp\perp\rangle \in \mathcal{A}_0 \otimes \mathcal{B}_0.$$
- **Alice sends the qutrit $\mathcal{B}_0$ to Bob.**

Stage-II

- Bob chooses $c \in \{0,1\}$ uniformly at random and sends it to Alice.
  - If $c = 0$, Bob measures the qutrit $\mathcal{B}_0$ in computational basis to output y_0 or $\perp$.
  - If $c = 1$, Alice reveals y_0 to Bob and sends him the qutrit $\mathcal{A}_0$ where Bob measures the combined state in $\mathcal{A}_0 \otimes \mathcal{B}_0$ to accept or reject according to the POVM:
$$\{\Pi_{accept} \coloneqq |\phi_{y_0}\rangle\langle\phi_{y_0}|_{\mathcal{A}_0\otimes\mathcal{B}_0}, \Pi_{reject} \coloneqq \mathbb{1}_{\mathcal{A}_0\otimes\mathcal{B}_0} - \Pi_{accept}\}.$$
  If Bob accepts,
    - Alice chooses another bit $y_1 \in \{0,1\}$ uniformly at random and creates the two-qutrit state
$$|\phi_{y_1}\rangle = \frac{1}{\sqrt{2}} |y_1 y_1\rangle + \frac{1}{\sqrt{2}} |\perp\perp\rangle \in \mathcal{A}_1 \otimes \mathcal{B}_1.$$
    - Alice sends the qutrit $\mathcal{B}_1$ to Bob.
    - Bob measures the qutrit $\mathcal{B}_1$ in computational basis to output y_1 or $\perp$.

5.3.1 Cheating Alice (variant 2)

Dishonest Alice in Protocol 14 would like to maximize her average chances of successfully forcing $\perp$ when Bob selects $c = 0$ and successfully passing Bob's test when he selects $c = 1$ (note that if Bob accepts, Alice can successfully force $\perp$ with probability 1 in the restarted protocol). Let σ_B be the state with Bob after Alice the qutrit $\mathcal{B}$ in her first message of the protocol. Then $\langle \sigma_B, |\perp\rangle \langle\perp|\rangle$ is the probability by which Bob observes nothing ($\perp$) if he chooses $c = 0$. On the other hand, if Bob chooses $c = 1$, then Alice sends the qutrit $\mathcal{A}$ such that Bob accepts the joint state in $\mathcal{A} \otimes \mathcal{B}$ with a high probability given by $\langle \sigma, P \rangle$ where

$$P = \sum_{y \in \{0,1\}} |y\rangle \langle y|_{\mathcal{Y}} \otimes |\phi_y\rangle \langle \phi_y|_{\mathcal{A}\otimes\mathcal{B}} \,. \tag{28}$$

Note that Alice can successfully force $\perp$ to Bob with probability 1 if Alice accepts in the latter case.

SDP for cheating Alice. The optimal cheating probability for Alice is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \frac{1}{2}\langle \sigma_B, |\perp\rangle \langle\perp|\rangle + \frac{1}{2}\langle \sigma, P\rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{Y}\mathcal{A}}(\sigma) = \sigma_B \\ & \sigma \in \mathrm{D}(\mathcal{Y} \otimes \mathcal{A} \otimes \mathcal{B}) \\ & \sigma_B \in \mathrm{D}(\mathcal{B}) \end{aligned} \tag{29}$$

where recall,

$$P = \sum_{y \in \{0,1\}} |y\rangle \langle y|_{\mathcal{Y}} \otimes |\phi_y\rangle \langle \phi_y|_{\mathcal{A}\otimes\mathcal{B}} \,.$$

Numerically solving the above SDP (mapping $|\perp\rangle$ to the computational basis state $|2\rangle$), we find that Alice can cheat with an optimal probability of $P_A^{ROT2} = \cos^2(\pi/8) \approx 0.8535$ and this is achieved for $\sigma_B = \begin{bmatrix} 0.4268 & 0 & 0 \\ 0 & 0.4268 & 0 \\ 0 & 0 & 0.1464 \end{bmatrix}$.

5.3.2 Cheating Bob

As before, dishonest Bob would like to correctly guess y, either in the first run of the protocol or the second.

Consider the state

$$|\psi\rangle = \sum_{y_0 \in \{0,1\}} \sum_{y_1 \in \{0,1\}} \frac{1}{2} |y_0\rangle_{\mathcal{Y}_0} |y_0\rangle_{\mathcal{Y}_0'} |y_1\rangle_{\mathcal{Y}_1} |\phi_{y_0}\rangle_{\mathcal{A}_0\otimes\mathcal{B}_0} |\phi_{y_1}\rangle_{\mathcal{A}_1\otimes\mathcal{B}_1}$$

with Alice at the beginning of Protocol 14. Alice sends Bob the qutrit $\mathcal{B}_0$ while she receives c and a guess g_0 for y_0. At this point, Alice holds the state $\tau_0 \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y}_0 \otimes \mathcal{Y}_0' \otimes \mathcal{Y}_1 \otimes \mathcal{A}_0 \otimes \mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{G}_0)$ and sends a copy of y_0 (in $\mathcal{Y}_0'$) and $\mathcal{A}_0$ to Bob.

In the final set of messages, Alice sends the qutrit $\mathcal{B}_1$ to Bob and receives g_1 as the guess for y_1. Alice holds the state $\tau \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y}_0 \otimes \mathcal{Y}_1 \otimes \mathcal{A}_1 \otimes \mathcal{G}_0 \otimes \mathcal{G}_1)$ at the end of the protocol and measures to accept g_0 (using the remaining copy of y_0 in $\mathcal{Y}_0$), if Bob selects $c = 0$ and correctly guesses y_0,

or accept g_1, if Bob selects $c = 1$ and correctly guesses y_1. The joint probability of Bob selecting $c = 0$ and successfully guessing y_0 is given by $\langle \tau, Q_0 \rangle$ where

$$Q_0 = |0\rangle\langle 0|_{\mathcal{C}} \otimes \Big(\sum_{(y_0,g_0)\in\{0,1\}^2} \delta_{y_0,g_0} |y_0\rangle\langle y_0|_{\mathcal{Y}_0} \otimes \mathbb{1}_{\mathcal{Y}_1} \otimes \mathbb{1}_{\mathcal{A}_1} \otimes |g_0\rangle\langle g_0|_{\mathcal{G}_0} \otimes \mathbb{1}_{\mathcal{G}_1} \Big).$$

Similarly, the joint probability of Bob selecting $c = 1$ and successfully guessing y_1 is given by $\langle \tau, Q_1 \rangle$ where

$$Q_1 = |1\rangle\langle 1|_{\mathcal{C}} \otimes \Big(\sum_{(y_1,g_1)\in\{0,1\}^2} \delta_{y_1,g_1} \mathbb{1}_{\mathcal{Y}_0} \otimes |y_1\rangle\langle y_1|_{\mathcal{Y}_1} \otimes \mathbb{1}_{\mathcal{A}_1} \otimes \mathbb{1}_{\mathcal{G}_0} \otimes |g_1\rangle\langle g_1|_{\mathcal{G}_1} \Big).$$

We introduce the constraints $\mathrm{Tr}_{\mathcal{Y}_0'\mathcal{A}_0\mathcal{B}_1}(\tau_0) = \mathrm{Tr}_{\mathcal{G}_1}(\tau)$ and $\mathrm{Tr}_{\mathcal{C}\mathcal{G}_0}(\tau_0) = \mathrm{Tr}_{\mathcal{B}_0}(|\psi\rangle\langle\psi|)$ to ensure that (g_0, g_1) and Alice's input (y_0, y_1) remains unchanged. We finally maximize $\langle \tau, Q_0 + Q_1 \rangle$ over τ and τ_0 to obtain the optimal cheating probability for Bob.

SDP for cheating Bob. The optimal cheating probability for Bob is given by the optimal objective function value of the following SDP:

$$\begin{aligned} \text{maximize: } & \langle \tau, Q \rangle \\ \text{subject to: } & \mathrm{Tr}_{\mathcal{C}\mathcal{G}_0}(\tau_0) = \mathrm{Tr}_{\mathcal{B}_0}(|\psi\rangle\langle\psi|) \\ & \mathrm{Tr}_{\mathcal{Y}_0'\mathcal{A}_0\mathcal{B}_1}(\tau_0) = \mathrm{Tr}_{\mathcal{G}_1}(\tau) \\ & \tau_0 \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y}_0 \otimes \mathcal{Y}_0' \otimes \mathcal{Y}_1 \otimes \mathcal{A}_0 \otimes \mathcal{A}_1 \otimes \mathcal{B}_1 \otimes \mathcal{G}_0) \\ & \tau \in \mathrm{D}(\mathcal{C} \otimes \mathcal{Y}_0 \otimes \mathcal{Y}_1 \otimes \mathcal{A}_1 \otimes \mathcal{G}_0 \otimes \mathcal{G}_1) \end{aligned} \tag{30}$$

where recall,

$$\begin{aligned} |\psi\rangle &= \sum_{y_0\in\{0,1\}} \sum_{y_1\in\{0,1\}} \frac{1}{2} |y_0\rangle_{\mathcal{Y}_0} |y_0\rangle_{\mathcal{Y}_0'} |y_1\rangle_{\mathcal{Y}_1} |\phi_{y_0}\rangle_{\mathcal{A}_0\otimes\mathcal{B}_0} |\phi_{y_1}\rangle_{\mathcal{A}_1\otimes\mathcal{B}_1} \\ Q &= |0\rangle\langle 0|_{\mathcal{C}} \otimes \Big(\sum_{(y_0,g_0)\in\{0,1\}^2} \delta_{y_0,g_0} |y_0\rangle\langle y_0|_{\mathcal{Y}_0} \otimes \mathbb{1}_{\mathcal{Y}_1} \otimes \mathbb{1}_{\mathcal{A}_1} \otimes |g_0\rangle\langle g_0|_{\mathcal{G}_0} \otimes \mathbb{1}_{\mathcal{G}_1} \Big) \\ &\quad + |1\rangle\langle 1|_{\mathcal{C}} \otimes \Big(\sum_{(y_1,g_1)\in\{0,1\}^2} \delta_{y_1,g_1} \mathbb{1}_{\mathcal{Y}_0} \otimes |y_1\rangle\langle y_1|_{\mathcal{Y}_1} \otimes \mathbb{1}_{\mathcal{A}_1} \otimes \mathbb{1}_{\mathcal{G}_0} \otimes |g_1\rangle\langle g_1|_{\mathcal{G}_1} \Big). \end{aligned} \tag{31}$$

Numerically solving the above SDP, we find that Bob can cheat with an optimal probability of $P_B^{ROT} = 7/8$.

It is important to note the difference in nature of state preparations by Alice in the switch protocols for the two variants of the Rabin OT task (Protocol 13 and Protocol 14). The single qutrit state prepared by Alice in Protocol 13 for the first variant helps ensure that dishonest Alice is unable to learn Bob's measurement output perfectly which may not be the case when an entangled state is shared between them. Similarly, Alice sending only a part of an entangled state in her initial message to Bob in Protocol 14 lowers the overall probability of Bob successfully guessing Alice's bit when compared to Protocol 13 where she sends the entire single qutrit state in her first message to Bob.

Computational platform

The semidefinite programs formulated in this work were solved using CVX, a package for specifying and solving convex programs [41, 42], with the help of the solver MOSEK [24] and supported by the methods of QETLAB [43], a MATLAB toolbox for exploring quantum entanglement theory.

The codes developed to solve the semidefinite programs can be found at the following git repository: `https://bitbucket.org/akshaybansal14/two-party-cryptography/`.

Acknowledgements

This work is supported in part by Commonwealth Cyber Initiative SWVA grant 453136. We also thank the Computer Science Research Virtual Machine Project (CSRVM) at Virginia Tech for providing the computational resources for our work.

References

[1] Stephen Wiesner. "Conjugate coding". ACM Sigact News **15**, 78–88 (1983).

[2] Michael O. Rabin. "How to exchange secrets with oblivious transfer". Cryptology ePrint Archive, Paper 2005/187 (2005). `https://eprint.iacr.org/2005/187`.

[3] Claude Crépeau. "Quantum oblivious transfer". Journal of Modern Optics **41**, 2445–2454 (1994).

[4] Sarah A. Osborn and Jamie Sikora. "A Constant Lower Bound for Any Quantum Protocol for Secure Function Evaluation". In François Le Gall and Tomoyuki Morimae, editors, 17th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2022). Volume 232 of Leibniz International Proceedings in Informatics (LIPIcs), pages 8:1–8:14. Dagstuhl, Germany (2022). Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[5] Schaffner Christian. "Cryptography in the bounded-quantum-storage model" (2007). arXiv:0709.0289.

[6] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. "Lower bounds for quantum oblivious transfer". Quantum Information & Computation **13**, 158–177 (2013).

[7] Harry Buhrman, Matthias Christandl, and Christian Schaffner. "Complete insecurity of quantum protocols for classical two-party computation". Physical Review Letters **109**, 160501 (2012).

[8] Ryan Amiri, Robert Stárek, David Reichmuth, Ittoop V Puthoor, Michal Mičuda, Ladislav Mišta Jr, Miloslav Dušek, Petros Wallden, and Erika Andersson. "Imperfect 1-out-of-2 quantum oblivious transfer: bounds, a protocol, and its experimental implementation". PRX Quantum **2**, 010335 (2021).

[9] Gus Gutoski André Chailloux and Jamie Sikora. "Optimal bounds for semi-honest quantum oblivious transfer". Chicago Journal of Theoretical Computer Science **13**, 1–17 (2016).

[10] Andris Ambainis. "A new protocol and lower bounds for quantum coin flipping". In Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing. Page 134–142. STOC '01New York, NY, USA (2001). Association for Computing Machinery.

[11] Carlos Mochon. "Quantum weak coin flipping with arbitrarily small bias" (2007). arXiv:0711.4114.

[12] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. "A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias". SIAM Journal on Computing **45**, 633–679 (2016).

[13] Atul Singh Arora, Jérémie Roland, and Stephan Weis. "Quantum weak coin flipping". In Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing. Page 205–216. STOC 2019New York, NY, USA (2019). Association for Computing Machinery.

[14] Atul Singh Arora, Jérémie Roland, and Chrysoula Vlachou. "Analytic quantum weak coin flipping protocols with arbitrarily small bias". In Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA). Pages 919–938. (2021).

[15] Carl A. Miller. "The impossibility of efficient quantum weak coin flipping". In Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing. Page 916–929. STOC 2020New York, NY, USA (2020). Association for Computing Machinery.

[16] Carlos Mochon. "Large family of quantum weak coin-flipping protocols". Physical Review A **72**, 022341 (2005).

[17] Alexei Kitaev. "Quantum coin flipping". In 6th Annual workshop on Quantum Information Processing (Unpublished result). (2002).

[18] Nati Aharon and Jonathan Silman. "Quantum dice rolling: a multi-outcome generalization of quantum coin flipping". New Journal of Physics **12**, 033027 (2010).

[19] Howard Barnum, Jonathan Barrett, Matthew Leifer, and Alexander Wilce. "Generalized no-broadcasting theorem". Physical Review Letters **99**, 240501 (2007).

[20] WK Wootters and WH Zurek. "A single quantum cannot be cloned". Nature **299**, 802–803 (1982).

[21] Yehuda Lindell. "Fast cut-and-choose-based protocols for malicious and covert adversaries". Journal of Cryptology **29**, 456–490 (2016).

[22] Jos F Sturm. "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones". Optimization methods and software **11**, 625–653 (1999).

[23] Kim-Chuan Toh, Michael J Todd, and Reha H Tütüncü. "SDPT3—a MATLAB software package for semidefinite programming, version 1.3". Optimization Methods and Software **11**, 545–581 (1999).

[24] MOSEK ApS. "The mosek optimization toolbox for matlab manual. version 9.0.". (2019). url: `http://docs.mosek.com/9.0/toolbox/index.html`.

[25] Ashwin Nayak and Peter Shor. "Bit-commitment-based quantum coin flipping". Physical Review A **67**, 012304 (2003).

[26] Michael A Nielsen and Isaac L Chuang. "Quantum Computation and Quantum Information". Cambridge University Press. (2010).

[27] John Watrous. "The Theory of Quantum Information". Cambridge University Press. (2018).

[28] Christoph Helmberg, Franz Rendl, Robert J Vanderbei, and Henry Wolkowicz. "An interior-point method for semidefinite programming". SIAM Journal on Optimization **6**, 342–361 (1996).

[29] Farid Alizadeh, Jean-Pierre A Haeberly, and Michael L Overton. "Primal-dual interior-point methods for semidefinite programming: convergence rates, stability and numerical results". SIAM Journal on Optimization **8**, 746–768 (1998).

[30] Stephen Boyd and Lieven Vandenberghe. "Convex Optimization". Cambridge University Press. (2004).

[31] Sanjay Mehrotra and M Gökhan Özevin. "Decomposition-based interior point methods for two-stage stochastic semidefinite programming". SIAM Journal on Optimization **18**, 206–222 (2007).

[32] Hoi-Kwong Lo and Hoi Fung Chau. "Is quantum bit commitment really possible?". Physical Review Letters **78**, 3410 (1997).

[33] Dominic Mayers. "Unconditionally secure quantum bit commitment is impossible". Physical Review Letters **78**, 3414 (1997).

[34] Jamie Sikora and John H Selby. "Simple proof of the impossibility of bit commitment in generalized probabilistic theories using cone programming". Physical Review A **97**, 042302 (2018).

[35] Andre Chailloux and Iordanis Kerenidis. "Optimal bounds for quantum bit commitment". In 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science. Pages 354–362. (2011).

[36] André Chailloux and Iordanis Kerenidis. "Optimal quantum strong coin flipping". In 2009 50th Annual IEEE Symposium on Foundations of Computer Science. Pages 527–533. (2009).

[37] Iordanis Kerenidis and Ashwin Nayak. "Weak coin flipping with small bias". Information Processing Letters **89**, 131–135 (2004).

[38] Roger Colbeck. "An entanglement-based protocol for strong coin tossing with bias 1/4". Physics Letters A **362**, 390–392 (2007).

[39] Peter W Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". SIAM review **41**, 303–332 (1999).

[40] Michael J Fischer, Silvio Micali, and Charles Rackoff. "A secure protocol for the oblivious transfer". Journal of Cryptology **9**, 191–196 (1996).

[41] Michael Grant and Stephen Boyd. "CVX: Matlab software for disciplined convex programming, version 2.1". `http://cvxr.com/cvx` (2014).

[42] Michael Grant and Stephen Boyd. "Graph implementations for nonsmooth convex programs". In V. Blondel, S. Boyd, and H. Kimura, editors, Recent Advances in Learning and Control. Pages 95–110. Lecture Notes in Control and Information Sciences. Springer-Verlag Limited (2008).

[43] Nathaniel Johnston. "QETLAB: A MATLAB toolbox for quantum entanglement, version 0.9". `http://qetlab.com` (2016).

[44] Nati Aharon, André Chailloux, Iordanis Kerenidis, Serge Massar, Stefano Pironio, and Jonathan Silman. "Weak coin flipping in a device-independent setting". In Theory of Quantum Computation, Communication, and Cryptography: Revised Selected Papers. Pages 1–12. Springer (2011).

[45] Nati Aharon, Serge Massar, Stefano Pironio, and Jonathan Silman. "Device-independent bit commitment based on the CHSH inequality". New Journal of Physics **18**, 025014 (2016).

[46] Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. "Quantum bit escrow". In Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing. Page 705–714. STOC '00New York, NY, USA (2000). Association for Computing Machinery.

[47] Andris Ambainis, Harry Buhrman, Yevgeniy Dodis, and Hein Rohrig. "Multiparty quantum coin flipping". In Proceedings of the 19th IEEE Annual Conference on Computational Complexity. Pages 250–259. (2004).

[48] Howard Barnum, Carlton M Caves, Christopher A Fuchs, Richard Jozsa, and Benjamin Schumacher. "Noncommuting mixed states cannot be broadcast". Physical Review Letters **76**, 2818 (1996).

[49] Manuel Blum. "Coin flipping by telephone a protocol for solving impossible problems". ACM SIGACT News **15**, 23–27 (1983).

[50] Giulio Chiribella, Giacomo Mauro D'Ariano, Paolo Perinotti, Dirk Schlingemann, and Reinhard Werner. "A short impossibility proof of quantum bit commitment". Physics Letters A **377**, 1076–1087 (2013).

[51] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. "Cryptography in the bounded-quantum-storage model". SIAM Journal on Computing **37**, 1865–1890 (2008).

[52] Gus Gutoski and John Watrous. "Toward a general theory of quantum games". In Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing. Page 565–574. STOC '07New York, NY, USA (2007). Association for Computing Machinery.

[53] Gus Gutoski, Ansis Rosmanis, and Jamie Sikora. "Fidelity of quantum strategies with applications to cryptography". Quantum **2**, 89 (2018).

[54] Joe Kilian. "Founding crytpography on oblivious transfer". In Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing. Page 20–31. STOC '88New York, NY, USA (1988). Association for Computing Machinery.

[55] Srijita Kundu, Jamie Sikora, and Ernest Y-Z Tan. "A device-independent protocol for XOR oblivious transfer". Quantum **6**, 725 (2022).

[56] Hoi-Kwong Lo. "Insecurity of quantum secure computations". Physical Review A **56**, 1154 (1997).

[57] Hoi-Kwong Lo and Hoi Fung Chau. "Why quantum bit commitment and ideal quantum coin tossing are impossible". Physica D: Nonlinear Phenomena **120**, 177–187 (1998).

[58] Ashwin Nayak, Jamie Sikora, and Levent Tunçel. "Quantum and classical coin-flipping protocols based on bit-commitment and their point games" (2015). arXiv:1504.04217.

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

[60] R Tyrrell Rockafellar. "Convex Analysis". Volume 18. Princeton University Press. (1970).

[61] Christian Schaffner, Barbara Terhal, and Stephanie Wehner. "Robust cryptography in the noisy-quantum-storage model". Quantum Information and Computation **9**, 963–996 (2009).

[62] Jamie Sikora, André Chailloux, and Iordanis Kerenidis. "Strong connections between quantum encodings, nonlocality, and quantum cryptography". Physical Review A **89**, 022334 (2014).

[63] Jamie Sikora. "Simple, near-optimal quantum protocols for die-rolling". Cryptography **1**, 11 (2017).

[64] Jamie Sikora and John H Selby. "Impossibility of coin flipping in generalized probabilistic theories via discretizations of semi-infinite programs". Physical Review Research **2**, 043128 (2020).

[65] Jonathan Silman, André Chailloux, Nati Aharon, Iordanis Kerenidis, Stefano Pironio, and Serge Massar. "Fully distrustful quantum bit commitment and coin flipping". Physical Review Letters **106**, 220501 (2011).

[66] Robert W Spekkens and Terry Rudolph. "Degrees of concealment and bindingness in quantum bit commitment protocols". Physical Review A **65**, 012310 (2001).

[67] Stephanie Wehner, Christian Schaffner, and Barbara M Terhal. "Cryptography from noisy storage". Physical Review Letters **100**, 220502 (2008).

[68] Andrew Chi-Chih Yao. "How to generate and exchange secrets". In 27th Annual Symposium on Foundations of Computer Science (sfcs 1986). Pages 162–167. (1986).

A An example where the stochastic switch does not help

We now illustrate an example where the stochastic switch by Bob does not provide any improvement in the overall security of a cheating Alice. The protocol we detail switches between XOR oblivious transfer and die rolling with three possible outcomes.

A.1 XOR oblivious transfer

XOR oblivious transfer (XOT) is a cryptographic task between Alice and Bob who wish to achieve the following. Alice outputs a trit $y \in \{0,1,2\}$ while Bob outputs two bits (x_0, x_1) each by a uniformly random sampling, and they both communicate in a way that Bob learns x_y by the end of the protocol (here x_2 is defined as $x_0 \oplus x_1$).

- *Completeness:* An XOT protocol is said to be *complete* if Alice learns the selected bit (x_y) unambiguously.
- *Cheating Alice:* Dishonest Alice could deviate from an XOT protocol in order to learn both bits (x_0, x_1) with the corresponding cheating probability given by

$$P_A^{XOT} = \Pr[\text{Alice correctly guesses } (x_0, x_1)].$$

- *Cheating Bob:* Dishonest Bob on the other hand would attempt to learn Alice's choice trit y with the corresponding cheating probability given by

$$P_B^{XOT} = \Pr[\text{Bob correctly guesses } y].$$

A simple extension of the 1-out-of-2 OT Protocol (Section 3.3) for the XOT task is provided in [55] and is reproduced shortly.

The following three two-qutrit states will be used throughout this section.

Let $|\phi_y\rangle$ be the following two-qutrit state in $\mathcal{A} \otimes \mathcal{B}$:

$$|\phi_y\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|00\rangle_{\mathcal{AB}} + |22\rangle_{\mathcal{AB}}) & \text{if } y = 0, \\ \frac{1}{\sqrt{2}}(|11\rangle_{\mathcal{AB}} + |22\rangle_{\mathcal{AB}}) & \text{if } y = 1, \\ \frac{1}{\sqrt{2}}(|00\rangle_{\mathcal{AB}} + |11\rangle_{\mathcal{AB}}) & \text{if } y = 2. \end{cases} \tag{32}$$

Protocol 15. Quantum XOR oblivious transfer [55].

Stage-I

- **Alice chooses a trit $y \in \{0, 1, 2\}$ uniformly at random and creates the two-qutrit state $|\phi_y\rangle$ as defined in Eq. (32), above.**
- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob selects $(x_0, x_1) \in \{0, 1\}^2$ uniformly at random and applies the unitary

$$U_{x_0 x_1} = \begin{bmatrix} (-1)^{x_0} & 0 & 0 \\ 0 & (-1)^{x_1} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

  to the received qutrit. Afterwards, Bob returns the qutrit to Alice.

- Alice determines the value of x_y using the two-outcome measurement:

$$\{\Pi_0 \coloneqq |\phi_y\rangle \langle\phi_y|_{\mathcal{A}\otimes\mathcal{B}}, \Pi_1 \coloneqq \mathbb{1}_{\mathcal{A}\otimes\mathcal{B}} - |\phi_y\rangle \langle\phi_y|_{\mathcal{A}\otimes\mathcal{B}}\}.$$

Note that Protocol 15 above has a significant overlap with Protocol 6 for OT as Alice wants to learn (x_0, x_1) in both protocols. The only difference is the state created by Alice at the beginning of the two protocols. As the sequence and actions of Bob on the qutrit $\mathcal{B}$ remains same in both the protocols, we may infer that the optimal cheating strategy for dishonest Alice is the same in both Protocols 15 and 6 implying $P_A^{XOT} = 3/4$ achieved by Alice by sending the qutrit $\mathcal{B}$ at the beginning in the state $\begin{bmatrix} 1/3 & 0 & 0 \\ 0 & 1/3 & 0 \\ 0 & 0 & 1/3 \end{bmatrix}$.

A.2 Die rolling

Die rolling (DR) is the cryptographic task between two parties (Alice and Bob) where they communicate to agree upon a common integer outcome from the set $\{1, 2, \ldots D\}$. The security notions of a die rolling protocol are defined below.

- *Completeness:* If both Alice and Bob are honest, then neither party aborts and they obtain the same outcome uniformly at random.
- *Cheating Alice:* Dishonest Alice could deviate from the protocol to force an outcome d, the extent of which is given by

$$P_{A,d}^{DR} = \max \Pr[\text{Alice successfully forces outcome } d]$$

  where the maximum is taken over all strategies of Alice. Note that there could be different cheating probabilities for each $d \in \{1, 2, \ldots D\}$.

- *Cheating Bob:* A dishonest Bob could attempt to force an outcome $d \in \{1, 2, \dots D\}$ the extent of which is given by

$$P_{B,d}^{DR} = \max \Pr[\text{Bob successfully forces outcome } d]$$

where the maximum is taken over all strategies of Bob. As earlier, $P_{B,d}^{DR}$ could be different for each $d \in \{1, 2, \dots D\}$.

For the task of die rolling with three possible outcomes, we consider the following protocol.

Protocol 16. Quantum die rolling with three outcomes ($D = 3$) [63].

Stage-I

- **Alice chooses a trit $y \in \{0, 1, 2\}$ uniformly at random and creates the two-qutrit state $|\phi_y\rangle$ as defined in Eq. (32).**
- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob selects a uniformly random $z \in \{0, 1, 2\}$ and sends it to Alice.
- Alice reveals y to Bob and sends him the qutrit $\mathcal{A}$.
- Bob measures the combined state $\mathcal{A} \otimes \mathcal{B}$ to accept or reject with the POVM:

$$\{\Pi_{accept} \coloneqq |\phi_y\rangle \langle \phi_y|_{\mathcal{A}\otimes\mathcal{B}}, \Pi_{reject} \coloneqq \mathbb{1}_{\mathcal{A}\otimes\mathcal{B}} - \Pi_{accept}\}.$$

If Bob accepts, Alice and Bob output $d \coloneqq (y + z \mod 3) + 1$ as the outcome of the protocol.

For Protocol 16, the uniformly random selection of y and z indicates that $P_{A,0}^{DR} = P_{A,1}^{DR} = P_{A,2}^{DR} \coloneqq P_A^{DR}$ and $P_{B,0}^{DR} = P_{B,1}^{DR} = P_{B,2}^{DR} \coloneqq P_B^{DR}$. The SDP formulation for cheating Alice in Protocol 16 extends trivially from its SDP formulation in Protocol 4. Solving it numerically, we find that Alice can cheat with an optimal probability of $P_A^{DR} = 2/3$ achieved when Alice sends the qutrit $\mathcal{B}$ at the beginning in the state $\begin{bmatrix} 1/3 & 0 & 0 \\ 0 & 1/3 & 0 \\ 0 & 0 & 1/3 \end{bmatrix}$.

The Stage-I communication between Alice and Bob is common to both the Protocols 15 and 16 and hence we are able to develop a switch protocol between XOT and DR as detailed below.

Protocol 17. Quantum XOT-DR stochastic switch.

Stage-I

- **Alice chooses a trit $y \in \{0, 1, 2\}$ uniformly at random and creates the two-qutrit state $|\phi_y\rangle$ as defined in Eq. (32).**
- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob chooses $c \in \{0, 1\}$ uniformly at random and sends it to Alice.
- If $c = 0$, Alice and Bob perform XOR oblivious transfer as per Protocol 15, otherwise, they perform the three-outcome die rolling Protocol 16.

Cheating Alice. Dishonest Alice in Protocol 17 would like to send a first message such that her average success of correctly guessing (x_0, x_1) and forcing an outcome is maximized. It is interesting to note that the optimal message from Alice can be the same in both Protocol 15 and Protocol 16 implying that the optimal cheating probability of Alice in Protocol 17 is simply the average of the optimal cheating probabilities P_A^{XOT} and P_A^{DR}. The identical nature of the optimal first message in the individual protocols indicates that the stochastic switch by Bob to introduce uncertainty on Alice's side is not improving the security against cheating Alice in the switch version. We note again that if optimal sets of first messages of two or more protocols have a non-empty intersection, then it is not possible to take advantage of the switching paradigm as illustrated in Fig. 1.

B An example where Bob can take advantage of stochastic switch

Next we illustrate an example where the stochastic switch by Bob breaks the overall security of the protocol. We describe a switch protocol for strong coin flipping based on bit commitment (Section 3.1) and weak coin flipping (Section 3.2).

Strong coin flipping is the cryptographic task between Alice and Bob where they communicate to agree on a common binary outcome. The security notions of strong coin flipping (SCF) are stronger (hence the name) than weak coin flipping (WCF) because in SCF, Alice and Bob each may try to bias the outcome towards either 0 or 1. The SCF task can also be viewed as a die rolling task with only two possible outcomes (See Appendix A.2).

Consider a two-outcome variant of the die rolling protocol discussed previously in Protocol 16 and outlined below.

Protocol 18. Quantum strong coin flipping [37].

Stage-I

- **Alice chooses a bit $y \in \{0,1\}$ uniformly at random and creates the two-qutrit state**

$$|\phi_y\rangle = \frac{1}{\sqrt{2}}|yy\rangle + \frac{1}{\sqrt{2}}|22\rangle \in \mathcal{A} \otimes \mathcal{B}.$$

- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob selects a uniformly random $z \in \{0,1\}$ and sends it to Alice.
- Alice reveals y to Bob and sends him the qutrit $\mathcal{A}$.
- Bob measures the combined state $\mathcal{A} \otimes \mathcal{B}$ to accept or reject with the POVM:

$$\{\Pi_{accept} \coloneqq |\phi_y\rangle\langle\phi_y|, \Pi_{reject} \coloneqq \mathbb{1}_{\mathcal{A}\otimes\mathcal{B}} - \Pi_{accept}\}.$$

If Bob accepts, Alice and Bob output $y \oplus z$ as the outcome of the protocol.

Note that the WCF protocol given by Protocol 5 is a valid SCF protocol as well since the final outcome is a uniformly random bit when both Alice and Bob are honest. A new SCF protocol based on stochastic switch between Protocol 18 and Protocol 5 is given next.

Protocol 19. Quantum SCF based on DR-EPR stochastic switch.

Stage-I

- **Alice chooses a bit $y \in \{0,1\}$ uniformly at random and creates the two-qutrit state**

$$|\phi_y\rangle = \frac{1}{\sqrt{2}}|yy\rangle + \frac{1}{\sqrt{2}}|22\rangle \in \mathcal{A} \otimes \mathcal{B}.$$

- **Alice sends the qutrit $\mathcal{B}$ to Bob.**

Stage-II

- Bob chooses $c \in \{0,1\}$ uniformly at random and sends it to Alice.
- If $c = 0$, Alice and Bob perform SCF as per Protocol 18, otherwise, they perform SCF as per Protocol 5.

From the analysis of the previous switch protocols, one might presume that the security of Protocol 19 is at least as good as its constituent protocols. However, it is broken when Bob is dishonest. To see this consider the following strategy by Bob attempting to force the outcome 1 where he simply measures the received qutrit (at the end of Stage-I) in the computational basis. If the outcome is either 0 or 1, he already knows Alice's bit y with certainty and selects $c = 0$ to perform SCF based on bit commitment (Protocol 18). This observed value of y allows him to successfully force outcome 0 or 1 with probability 1. Alternatively, if the measurement outcome is 2, he selects $c = 1$ to perform Protocol 5. Note that the state in $\mathcal{A}$ has collapsed to $|2\rangle$. Thus, Bob can use this to force outcome 1 again with probability 1. Therefore, Bob can measure and, conditioned on the outcome, cheat in one of the protocols with certainty.