A Constant Lower Bound for Any Quantum Protocol for Secure Function Evaluation

Sarah A. Osborn
Virginia Polytechnic Institute and State University, Blacksburg, VA, USA

Jamie Sikora
Virginia Polytechnic Institute and State University, Blacksburg, VA, USA

Abstract

Secure function evaluation is a two-party cryptographic primitive where Bob computes a function of Alice's and his respective inputs, and both hope to keep their inputs private from the other party. It has been proven that perfect (or near perfect) security is impossible, even for quantum protocols. We generalize this no-go result by exhibiting a constant lower bound on the cheating probabilities for any quantum protocol for secure function evaluation, and present many applications from oblivious transfer to the millionaire's problem. Constant lower bounds are of practical interest since they imply the impossibility to arbitrarily amplify the security of quantum protocols by any means.

2012 ACM Subject Classification Theory of computation → Cryptographic primitives; Theory of computation → Cryptographic protocols; Security and privacy → Mathematical foundations of cryptography; Theory of computation → Quantum information theory

Keywords and phrases Quantum cryptography, security analysis, secure function evaluation

Digital Object Identifier 10.4230/LIPIcs.TQC.2022.8

Related Version *Full Version*: `https://arxiv.org/abs/2203.08268`

Funding *Sarah A. Osborn*: Department of Defense Cyber Scholarship Program (DoD CySP).

1 Introduction

The first paper studying quantum cryptography was written by Stephen Wiesner in the 1970s (published in 1983) [34]. In that paper, he presented a (knowingly insecure) protocol for *multiplexing* where a receiver could choose to learn one of two bits of their choosing. Since then, this task has been referred to as 1-*out-of*-2 oblivious transfer, and has been extensively studied in the quantum community [16, 29, 33, 30, 21, 11, 15, 12, 18, 20]. Indeed, since the development of quantum key distribution in 1984 [9], it has been of great interest to use quantum mechanics to develop protocols for classical tasks and push the limits of quantum theory to find optimal protocols (and their limitations).

On the other hand, it was shown in the late 1990s (and a few times since) that perfect security for a number of cryptographic tasks, including secure function evaluation, could not attain perfect, or even near perfect, security [24, 22, 23, 21, 11]. Indeed, some popular two-party cryptographic protocols, including bit commitment [14], strong coin flipping [19], oblivious transfer [15], strong die rolling [2], as well as many others, have all seen constant lower bounds presented. Constant lower bounds are of great interest for several reasons, of which we note a few. The first reason, a practical one, is that they imply that there is no way to arbitrarily amplify the security by any means (such as repeating the protocol many times and combining them in some way). The second reason, a theoretical one, now opens the question as to what are the optimal security parameters. Assuming quantum mechanics offers *some* advantage over their classical counterparts, the question now becomes to what extent is this advantage.

Note that two-party cryptography has some strange behavior, making its study very intriguing. For example, in the case of die rolling (where Alice and Bob wish to roll a die over the (possibly quantum) telephone) there can sometimes be classical protocols that offer decent security [31]. On the other hand, having classical protocols for something like coin flipping, bit commitment, and oblivious transfer is impossible [19]. And while quantum mechanics seems to deny us strong coin flipping (we have a constant lower bound [19]), it does give us arbitrarily good security for weak coin flipping [25, 3, 7, 6]. Therefore, classifying the behavior of two-party cryptographic primitives is a fruitful, and sometimes surprising, endeavor. To this end, we study the broad class of two-party cryptography known as secure function evaluation which we now discuss.

1.1 Secure function evaluation

Secure function evaluation (SFE) is a two-party cryptographic primitive in which Alice begins with an input $x \in X$ and Bob begins with an input $y \in Y$ (each input is chosen uniformly at random[1]) and Bob has a deterministic function $f : X \times Y \to B$. Here, we take X, Y, and B to have finite cardinality. See Figure 1 below.

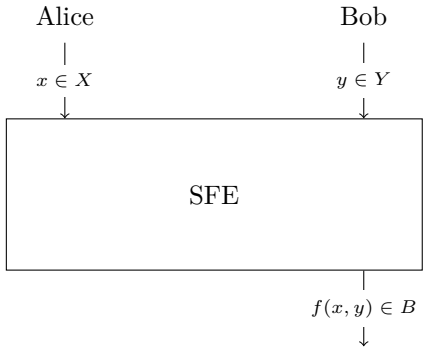

Figure 1 A pictorial representation of SFE. Bob wants to compute his function f while he and Alice keep their inputs private.

The goals when designing a (quantum) protocol for SFE are:

1. *Completeness:* If both parties are honest then Bob learns f, evaluated on their inputs x and y.
2. *Soundness against cheating Bob:* Cheating Bob obtains no extra information about honest Alice's input x other than what is logically implied from knowing $f(x, y)$.
3. *Soundness against cheating Alice:* Cheating Alice obtains no information about honest Bob's input y.

It is natural to assume perfect completeness of a protocol and then to quantify the extent to which they can be made sound. In other words, we consider protocols for SFE that do what they are meant to do when Alice and Bob follow them (that is, they compute f), and then we try to find the ones which hide their respective inputs the best.

To quantify soundness against cheating Bob, for each such protocol we define the following symbols.

[1] We believe our analysis works for other probability distributions over the inputs as well, as long as they are uncorrelated. The assumption of uniformity makes certain expressions cleaner, such as the probability of Alice being able to blindly guess Bob's input.

$\mathrm{B}_{\mathrm{SFE}}$: The maximum probability with which cheating Bob can guess honest Alice's input x.

$\mathrm{B}'_{\mathrm{SFE}}$: The maximum probability with which cheating Bob can guess every $f(x,y)$, *for each* $y \in Y$.

Note that often these two *cheating probabilities* are the same. For instance, in 1-out-of-2 oblivious transfer we have $x \in X = \{0,1\}^2$ as a 2-bit string, $y \in Y = \{1,2\}$ as an index, and $f(x,y) = x_y$, i.e., the y-th bit of x. Then clearly $\mathrm{B}_{\mathrm{SFE}} = \mathrm{B}'_{\mathrm{SFE}}$, since knowing each bit is equivalent to knowing the full string. In general, $\mathrm{B}_{\mathrm{SFE}} \leq \mathrm{B}'_{\mathrm{SFE}}$, since if Bob is able to correctly learn Alice's input x, then he can compute any function of it he wants.

Similarly, to quantify soundness against cheating Alice, we define the following symbols.

$\mathrm{A}_{\mathrm{SFE}}$: The maximum probability with which cheating Alice can guess honest Bob's input y.

Note that there is only the one definition for a cheating probability for Alice since she has no output.

1.2 Main result

We now present our main result, a trade-off curve relating Alice and Bob's cheating probabilities that must be satisfied for any quantum protocol for SFE.

▶ **Theorem 1.** *In any quantum protocol for secure function evaluation, it holds that*

$$\mathrm{B}'_{\mathrm{SFE}} \geq \frac{1}{|Y|\,\mathrm{A}_{\mathrm{SFE}}} - 2\left(|Y|-1\right)\sqrt{1-\frac{1}{|Y|\,\mathrm{A}_{\mathrm{SFE}}}} \tag{1}$$

where Y is the set of choices for Bob's input.

We now discuss this bound. Note that

$$\mathrm{A}_{\mathrm{SFE}} \geq \frac{1}{|Y|}, \tag{2}$$

since she can always blindly, or randomly, guess the value of $y \in Y$. Since Alice has no output function (like Bob does) she may not be able to infer anything about y from the protocol if she is honest. Therefore, sometimes her best strategy is to randomly guess, and in this case we would have

$$\mathrm{A}_{\mathrm{SFE}} = \frac{1}{|Y|}, \tag{3}$$

which translates to perfect security against a cheating Alice. However, in that case, our bound implies that

$$\mathrm{B}'_{\mathrm{SFE}} = 1, \tag{4}$$

meaning Bob can compute his function perfectly for *every choice of input on his side*, i.e., complete insecurity against a cheating Bob. This implication exactly recovers Lo's conclusion in his 1997 paper [21], and also the conclusion in a more recent paper by Buhrman, Christandl, and Schaffner [11]. It should be mentioned that the above two papers also discuss the "Alice can cheat with a small probability" case as well. A key component in their proofs is the application of Uhlmann's theorem on purifications of the protocol to find unitaries with which Bob can use to cheat. As evidenced later on, this is very different from our proof. In fact, at no point in our protocol do we assume anything is pure and we only deal with POVMs, not

unitaries. The "magic ingredient" in our proof is a generalization of Kitaev's lower bound for strong coin flipping [19]. Moreover, we chose to quantify the security solely in terms of Alice and Bob's cheating probabilities, which is complementary to the results in [11].

Before continuing, we now discuss what we mean by having a "constant lower bound." To this end, we define the following symbols.

$\mathrm{A}_{\mathrm{rand}}$: The maximum probability with which cheating Alice can guess honest Bob's input y *given only black-box access to the SFE task.*

$\mathrm{B}'_{\mathrm{rand}}$: The maximum probability with which cheating Bob can learn every $f(x, y)$, *for each* $y \in Y$, *given only black-box access to the SFE task.*

In other words, the cheating definitions above correspond to the information Alice and Bob can infer only from their outputs. Of course, Alice has no output, so clearly

$$\mathrm{A}_{\mathrm{rand}} = \frac{1}{|Y|}. \tag{5}$$

However, as is illustrated in our examples, it is less clear how to write $\mathrm{B}'_{\mathrm{rand}}$ in terms of the parameters of a general SFE protocol.

Equipped with these symbols, we are now ready to state our constant lower bound on SFE.

▶ **Theorem 2.** *In any quantum protocol for secure function evaluation, either* $\mathrm{B}'_{\mathrm{rand}} = 1$ *(in which case the protocol is* completely *insecure), or there exists a constant* $c > 1$ *such that*

$$\mathrm{A}_{\mathrm{SFE}} \geq c \cdot \mathrm{A}_{\mathrm{rand}} \qquad \textit{or} \qquad \mathrm{B}'_{\mathrm{SFE}} \geq c \cdot \mathrm{B}'_{\mathrm{rand}}. \tag{6}$$

Before discussing how to find this constant, a word on our lower bound is in order. We chose to define what it means for a constant lower bound to be a multiplicative factor. This is because $\mathrm{A}_{\mathrm{rand}}$ and $\mathrm{B}'_{\mathrm{rand}}$ may be dramatically different (as we demonstrate shortly). Therefore, having a constant additive factor could be unevenly weighted between cheating Alice and Bob and, we feel, would be less insightful in those cases. However, using our bound one can optimize and find an additive constant if one so desires.

To find this constant $c > 1$, note that our lower bound on $\mathrm{B}'_{\mathrm{SFE}}$ (the right-hand side of Inequality (1)) is a continuous, decreasing function with respect to $\mathrm{A}_{\mathrm{SFE}}$. Therefore, if we assume

$$\mathrm{A}_{\mathrm{SFE}} \leq \frac{c_A}{|Y|}, \tag{7}$$

for some fixed constant $c_A \geq 1$, then we may conclude via our bound that

$$\mathrm{B}'_{\mathrm{SFE}} \geq \frac{1}{c_A} - 2\left(|Y| - 1\right)\sqrt{1 - \frac{1}{c_A}}. \tag{8}$$

Now, assuming that

$$\mathrm{B}'_{\mathrm{SFE}} = c_B \cdot \mathrm{B}'_{\mathrm{rand}} \tag{9}$$

for some $c_B \geq 1$, we now have the inequality

$$c_B \geq \frac{1}{\mathrm{B}'_{\mathrm{rand}}}\left(\frac{1}{c_A} - 2\left(|Y| - 1\right)\sqrt{1 - \frac{1}{c_A}}\right). \tag{10}$$

We shall now assume that $\mathrm{B}'_{\mathrm{rand}} < 1$ so that $\frac{1}{\mathrm{B}'_{\mathrm{rand}}} > 1$. Note that when $c_A = 1$, we have the right-hand side of (10) equalling $\frac{1}{\mathrm{B}'_{\mathrm{rand}}} > 1$ and when $c_A = \frac{1}{\mathrm{B}'_{\mathrm{rand}}}$ we have the right-hand side being strictly less than 1. Thus, by continuity of the right-hand side and the intermediate value theorem, we know there exists a constant $c > 1$ satisfying the equation

$$c = \frac{1}{\mathrm{B}'_{\mathrm{rand}}} \left(\frac{1}{c} - 2\left(|Y| - 1\right) \sqrt{1 - \frac{1}{c}} \right). \tag{11}$$

Note that this constant $c > 1$ is exactly what we want, since if $c_A \leq c$ then we have $c_B \geq c$.

Now, in theory one can solve for c above for a general SFE task, but it is complicated and perhaps not very insightful. However, when it comes to particular instances or families of SFE, then one can easily solve the above equation and get a constant (and possibly decent) lower bound for any quantum protocol for that task. We demonstrate this several times below.

1.3 Applications

Since our bound is general, we can apply it to many different scenarios. However, since each scenario is quite different and requires discussion, we delegate these discussions to the full version of the paper and simply summarize the cryptographic tasks below and a few of the special cases in which we found some exact formulas for lower bounds. Note that all of the special cases presented below are *new lower bounds* as far as we are aware.

- **1-out-of-n oblivious transfer.** This is where Alice has a database and Bob wishes to learn one item (his input is an index). We present lower bounds on either how much Alice can learn Bob's index or how much Bob can learn all of Alice's database. A special case is when Alice has 3 bits and Bob wants to learn 1 of them. We present a new lower bound that either

$$\mathrm{B}_{\mathrm{OT}} \gtrapprox 0.2581 > 0.2500 \quad \text{or} \quad \mathrm{A}_{\mathrm{OT}} \gtrapprox 0.3442 > 0.3333. \tag{12}$$

  Note that we define the cheating probability symbols above in the full version, but they should be clear from context for this abbreviated discussion. This is also the case for the cheating probability symbols below.

- **k-out-of-n oblivious transfer.** This is the same as 1-out-of-n oblivious transfer except Bob's input is now a proper subset instead of an index (so Bob learns $k < n$ entries in Alice's database). We present lower bounds on either how much Alice can learn Bob's proper subset or how much Bob can learn all of Alice's database. A special case is when Alice has 4 bits and Bob wants to learn 2 of them. We present a new lower bound that either

$$\mathrm{B}_{\mathrm{knOT}} \gtrapprox 0.2514 > 0.2500 \quad \text{or} \quad \mathrm{A}_{\mathrm{knOT}} \gtrapprox 0.1676 > 0.1667. \tag{13}$$

- **XOR oblivious transfer**. This is similar to 1-out-of-2 oblivious transfer (where Alice's database consists of 2 bit *strings*) but Bob now has a third option of learning the bit-wise XOR of the two strings. We present lower bounds on either how much Alice can learn Bob's choice (first string, second string, or the XOR) or how much Bob can learn both of Alice's strings. A special case is when Alice's strings have length 1 (so, they are just bits). We present a new lower bound that either

$$\mathrm{B}_{\mathrm{XOT}} \gtrapprox 0.5073 > 0.5000 \quad \text{or} \quad \mathrm{A}_{\mathrm{XOT}} \gtrapprox 0.3382 > 0.3333. \tag{14}$$

- **Equality/one-way oblivious identification**. This is when Alice and Bob each have the same set of inputs and Bob learns whether or not their inputs are equal. We present lower bounds on either how much Alice or Bob can learn the other's input. A special case is when the input set has cardinality 3. We present a new lower bound that either

$$\mathrm{B}_{\mathrm{EQ}} \gtrapprox 0.671 > 0.667 \quad \text{or} \quad \mathrm{A}_{\mathrm{EQ}} \gtrapprox 0.3355 > 0.3333. \tag{15}$$

- **Inner product**. This is when Alice and Bob each input an n-bit string and Bob learns their inner product. We present lower bounds on either how much Alice or Bob can learn the other's input. A special case is when $n = 3$. We present a new lower bound that either

$$\mathrm{B}_{\mathrm{IP}} \gtrapprox 0.251 > 0.250 \quad \text{or} \quad \mathrm{A}_{\mathrm{IP}} \gtrapprox 0.1434 > 0.1429. \tag{16}$$

- **Millionaire's problem**. This is when (rich) Alice and Bob have lots of money and Bob wishes to learn who is richer without either revealing their wealth. A special case is when $n = 10^9$ (bounding each of their bank accounts at a billion dollars). We present a new lower bound that either

$$\begin{aligned} &\mathrm{B}_{☺\$} \gtrapprox 2 \times 10^{-9} + 5 \times 10^{-28} > 2 \times 10^{-9} \quad \text{or} \\ &\mathrm{A}_{☺\$} \gtrapprox 1 \times 10^{-9} + 1 \times 10^{-18} + 1.25 \times 10^{-27} > 1 \times 10^{-9} + 1 \times 10^{-18} + 1 \times 10^{-27}. \end{aligned} \tag{17}$$

  We can also study a more realistic version by setting $n = 10$. We present a new lower bound that either

$$\mathrm{B}_{☺\$} \gtrapprox 0.2005 > 0.2000 \quad \text{or} \quad \mathrm{A}_{☺\$} \gtrapprox 0.1114 > 0.1111. \tag{18}$$

  Therefore, some information about either Alice or Bob's wealth is necessarily leaked.

Each of these cryptographic tasks are described further and analyzed in the full version of the paper.

1.4 Proof idea and key concepts

There are two main ingredients in proving our lower bound which we discuss at a high level below, and continue in more detail in the following sections. The magic ingredient is Kitaev's constant lower bound for die rolling [19, 2]. Effectively what we do is use a generic SFE protocol to create a die rolling protocol, then apply Kitaev's lower bound. However, the glue that makes SFE and die rolling play well together is a new technical result that we prove which deals with sequential gentle measurements, which we discuss next.

1.4.1 Sequential gentle measurements

The idea behind much of quantum cryptography is the concept of measurement disturbance. To put it simply, measuring to obtain certain information from a quantum state may cause it to collapse, possibly rendering it unusable for future purposes, or to simply alert honest parties that a cheating attempt was made. However, there is a concept of a *gentle measurement*, which is described at a high level below.

Gentle measurement lemma (ϵ-free version). *If a measurement outcome has a large probability of occurring, then the measured quantum state is not largely disturbed if that measurement outcome does indeed happen. (See references [36, 37] or Section 2 to see formal statements of gentle measurement lemmas.)*

How does this help us? Well, suppose for a cheating Bob who wishes to learn every $f(x, y)$, for all y, he may wish to measure some quantum state *several times*. Suppose for a fixed $y_1 \in Y$ that Bob can learn $f(x, y_1)$ with probability close to 1. Then, if he were to measure it, and achieve the correct value, then the state is not greatly disturbed, and thus more information can possibly be extracted. If a second measurement can extract the correct value of $f(x, y_2)$ for some $y_2 \in Y \setminus \{y_1\}$ with a high probability, we can repeat the process.

Now, we (intentionally) glossed over the concept of *learning*, that is, we did not precisely define it means to *learn* the correct value, in our cryptographic context. We elaborate on this in Section 2. However, it can be made precise and be put into a framework suitable for the application of a modified gentle measurement lemma. For now, we just state the main technical result of this paper below, and leave its proof for Subsection 2.2.

▶ **Lemma 3** (Sequential measurement lemma). *Let $f_1, \ldots, f_n : X \to B$ be fixed functions and suppose Bob has a quantum encoding of $x \in X$ (where x is chosen from a probability distribution known to Bob). Suppose Bob can learn $f_i(x)$ with probability p_i for each $i \in \{1, \ldots, n\}$ and let $p = \frac{1}{n}\sum_{i=1}^{n} p_i$ be his average success probability of learning the function values. Then Bob can learn* all *values $f_1(x), \ldots, f_n(x)$ with probability at least*

$$p - 2(n-1)\sqrt{1-p}. \tag{19}$$

Notice that if $p \approx 1$ (meaning that Bob has a high average success probability of learning the function values) then he can learn *all* the values with probability still very close to 1. Note that this aligns with the intuition one obtains from the gentle measurement lemma. The measurement that achieves the success probability in Lemma 3 is given in Subsection 2.2.

1.4.2 Die rolling

Die rolling (DR) is a two-party cryptographic task akin to coin flipping, where Alice and Bob try to agree on a value $n \in \{0, 1, \ldots, N-1\}$. The goals when designing a die rolling protocol are outlined below.

1. *Completeness:* If both parties are honest then their outcomes are uniformly random and identical.
2. *Soundness against cheating Bob:* Cheating Bob cannot influence honest Alice's outcome distribution away from uniform.
3. *Soundness against cheating Alice:* Cheating Alice cannot influence honest Bob's outcome distribution away from uniform.

For this work, we only consider perfectly complete die rolling protocols. To quantify the soundness of a die rolling protocol, we define the following symbols.

$\mathrm{B}_{\mathrm{DR,n}}$: The maximum probability with which cheating Bob can influence honest Alice to output the number n without Alice aborting.

$\mathrm{A}_{\mathrm{DR,n}}$: The maximum probability with which cheating Alice can force honest Bob to output the number n without Bob aborting.

Kitaev proved in [19] that when $N = 2$, any *quantum* protocol for die rolling satisfies

$$\mathrm{A}_{\mathrm{DR},0}\mathrm{B}_{\mathrm{DR},0} \geq \frac{1}{2} \quad \text{and} \quad \mathrm{A}_{\mathrm{DR},1}\mathrm{B}_{\mathrm{DR},1} \geq \frac{1}{2}. \tag{20}$$

Note that die rolling with $N = 2$ is simply referred to as *(strong) coin flipping* as Alice and Bob decide on one of two outcomes. Note that coin flipping is a much more studied task than die rolling, the latter being a generalization of the former. Kitaev's proof of these inequalities for coin flipping easily generalizes to similar inequalities for die rolling, namely that for any *quantum* protocol for die rolling, we have

$$\mathrm{A}_{\mathrm{DR,n}}\mathrm{B}_{\mathrm{DR,n}} \geq \frac{1}{N}, \quad \text{for all} \quad n \in \{0, 1, \ldots, N-1\}. \tag{21}$$

This is indeed a constant lower bound, as we would strive to have $\mathrm{A}_{\mathrm{DR,n}} = \mathrm{B}_{\mathrm{DR,n}} = \frac{1}{N}$ for all n. However, Inequality (21) implies that

$$\max\{\mathrm{A}_{\mathrm{DR,n}}, \mathrm{B}_{\mathrm{DR,n}}\} \geq \frac{1}{\sqrt{N}}, \quad \text{for all} \quad n \in \{0, 1, \ldots, N-1\} \tag{22}$$

making it impossible to get anywhere near perfect security.

1.4.3 Die rolling via secure function evaluation - gluing the two ingredients together

The first step is to create a DR protocol from a fixed SFE protocol, as shown below.

▶ **Protocol 4** (DR from SFE).

- *Alice and Bob input uniformly random chosen inputs into a SFE protocol such that Bob learns $f(x, y)$.*
- *Alice selects a uniformly chosen $b \in Y$, independent from the SFE protocol. She sends b to Bob.*
- *Bob reveals his SFE input $y \in Y$ and also his SFE output $f(x, y)$.*
- *Alice computes $f(x, y)$ using x and y. If Bob's function value he sent to Alice does not match Alice's computation of the function, she aborts the protocol.*
- *If Alice does not abort, they both output $(b + y) \mod |Y|$. We assume an ordering of the elements of Y is known to both Alice and Bob before the protocol, i.e., we may think of them as elements of the set $\{1, \ldots, |Y|\}$.*

Protocol 4 is pictorially shown in Figure 2 below.
We now describe what Alice and Bob may do to cheat the die rolling protocol.

1.4.3.1 Cheating Alice

Suppose cheating Alice wants to force honest Bob to output the number 0. In this case, Alice must send b in the second to last message such that $b = y$. Since she may not know y, the probability she can successfully cheat is equal to the maximum probability with which she can learn y from the SFE protocol. However, this is precisely the definition of $\mathrm{A}_{\mathrm{SFE}}$. Thus, the case of cheating Alice is simple, we have that $\mathrm{A}_{\mathrm{DR},0} = \mathrm{A}_{\mathrm{SFE}}$.

1.4.3.2 Cheating Bob

Similar to cheating Alice, we wish to relate how much Bob can cheat in the DR protocol, say the quantity $\mathrm{B}_{\mathrm{DR},0}$, and how much he can cheat in the SFE protocol, namely $\mathrm{B}'_{\mathrm{SFE}}$. Suppose cheating Bob wants to force an honest Alice to output the number 0. In this case, he needs to send back y such that $y = b$ in the last message. However, for Alice to accept this last message, he must also correctly *learn* the value $f(x, y)$ from his part of the state after the

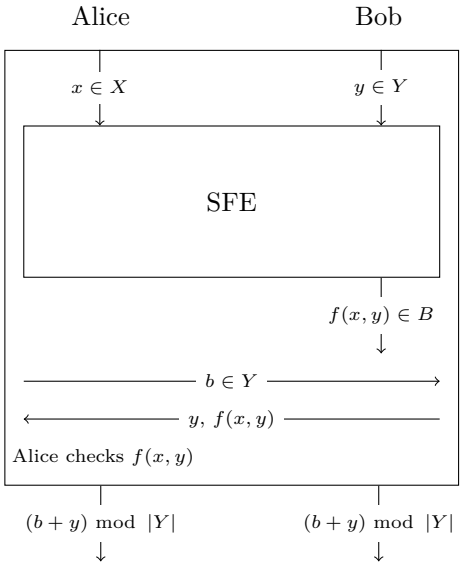

Figure 2 Protocol 4: Die rolling via secure function evaluation.

SFE subroutine. In other words, before he sends his last message, he has an *encoding* of x from which he may measure to learn something. Since Alice's message b is randomly chosen, independent of the SFE protocol, he is tasked with revealing a y with uniform probability. To say it another way, $\mathrm{B}_{\mathrm{DR},0}$ is equal to the average probability that Bob is able to learn $f(x,y)$, for each y, after the SFE subroutine.

Now, to obtain a cheating strategy for Bob in SFE, consider the following. Imagine if Bob uses his optimal die rolling strategy to communicate with Alice to create the encoding of x as described above at the end of the SFE protocol. Well, we know the average success probability of Bob learning each function value; it is equal to $\mathrm{B}_{\mathrm{DR},0}$, as explained above. If we now apply the sequential gentle measurement lemma, Lemma 3, we see that Bob can learn *all* the values of $f(x,y)$ with probability at least

$$\mathrm{B}_{\mathrm{DR},0} - 2(|Y|-1)\sqrt{1-\mathrm{B}_{\mathrm{DR},0}}. \tag{23}$$

Since this is a valid strategy for Bob to learn all the values of $f(x,y)$, it is a *lower bound* on $\mathrm{B}'_{\mathrm{SFE}}$.

Collecting all the above pieces of information together, and adding Kitaev's lower bound, we have

- $\mathrm{A}_{\mathrm{SFE}} = \mathrm{A}_{\mathrm{DR},0}$;
- $\mathrm{B}'_{\mathrm{SFE}} \geq \mathrm{B}_{\mathrm{DR},0} - 2(|Y|-1)\sqrt{1-\mathrm{B}_{\mathrm{DR},0}}$;
- $\mathrm{A}_{\mathrm{DR},0} \cdot \mathrm{B}_{\mathrm{DR},0} \geq \frac{1}{|Y|}$.

Combining these we get a proof of our main theorem, Theorem 1.

2 Learning and gentle measurements

In this section we first discuss the gentle measurement lemma and then generalize the concept to fit our needs. Then, we discuss the context in which we consider *learning* and show how to apply our generalized gentle measurement lemma.

2.1 Gentle measurements

Before we dive into gentle measurements, we must first define some essential matrix operations. Consider two matrices A and $B \in \mathbb{C}^{m\times n}$. The trace inner product is defined as

$$\langle A, B\rangle = \mathrm{Tr}\left(A^* B\right) \tag{24}$$

where A^* represents the complex conjugate transpose of A. The trace norm of a matrix A is given by

$$\|A\|_{tr} = \mathrm{Tr}(\sqrt{A^* A}). \tag{25}$$

The operator norm of a matrix A is given by

$$\|A\|_{op} = \sup\left\{\|Av\|_2 : \|v\|_2 = 1\right\} \tag{26}$$

where $\|v\|_2$ denotes the Euclidean norm $\sqrt{\langle v, v\rangle}$.

The idea behind gentle measurements is that if a measurement operator, when applied to a quantum state, produces a given result with high probability, then the post-measured state will be relatively close to the original state. For our purposes, this allows for more information to be gleaned from the state in a successive measurement. This process is formally scoped below.

▶ **Lemma 5** (Gentle measurement operator [36, 37])**.** *Consider a density operator ρ and a measurement operator Λ where $0 \le \Lambda \le I$. Suppose that*

$$\langle \Lambda, \rho\rangle \ge 1 - \varepsilon, \tag{27}$$

where $\varepsilon \in [0, 1]$. Then we have

$$\|\rho - \sqrt{\Lambda}\rho\sqrt{\Lambda}\|_{tr} \le 2\sqrt{\varepsilon}. \tag{28}$$

We now use this to prove the following.

▶ **Lemma 6** (Sequential gentle measurement operators)**.** *Consider a density operator ρ and measurement operators $\Lambda_1, \ldots, \Lambda_n$ where $0 \le \Lambda_k \le I$ for each $k \in \{1, \ldots, n\}$, where $n \ge 2$. Suppose that*

$$\langle \Lambda_k, \rho\rangle \ge 1 - \varepsilon_k, \tag{29}$$

where $\varepsilon_k \in [0, 1]$ for each $k \in \{1, \ldots, n\}$. Then we have

$$\langle \rho, \sqrt{\Lambda_n}\cdots\sqrt{\Lambda_2}\Lambda_1\sqrt{\Lambda_2}\cdots\sqrt{\Lambda_n}\rangle \ge 1 - \epsilon_1 - 2\sum_{i=2}^{n}\sqrt{\varepsilon_i}. \tag{30}$$

Proof. We prove this by induction.

Base case: $n = 2$. Consider the following quantity

$$|\langle \rho, \Lambda_1\rangle - \langle \rho, \sqrt{\Lambda_2}\Lambda_1\sqrt{\Lambda_2}\rangle| = |\langle \rho, \Lambda_1\rangle - \langle \sqrt{\Lambda_2}\rho\sqrt{\Lambda_2}, \Lambda_1\rangle| = |\langle \rho - \sqrt{\Lambda_2}\rho\sqrt{\Lambda_2}, \Lambda_1\rangle|. \tag{31}$$

By applying Hölder's inequality, we get

$$|\langle \rho - \sqrt{\Lambda_2}\rho\sqrt{\Lambda_2}, \Lambda_1\rangle| \le \|\rho - \sqrt{\Lambda_2}\rho\sqrt{\Lambda_2}\|_{tr}\|\Lambda_1\|_{op} \le 2\sqrt{\varepsilon_2}, \tag{32}$$

where the last inequality follows from the gentle measurement operator lemma (Lemma 5) and the assumption that $0 \le \Lambda_1 \le I$. This implies that

$$\langle \rho, \sqrt{\Lambda_2}\Lambda_1\sqrt{\Lambda_2}\rangle \ge \langle \rho, \Lambda_1\rangle - 2\sqrt{\varepsilon_2} \ge 1 - \varepsilon_1 - 2\sqrt{\varepsilon_2}. \tag{33}$$

Inductive step. Assume it is true up to some $k \in \{3, \ldots, n-1\}$. We have, again, that

$$|\langle \rho - \sqrt{\Lambda_{k+1}}\rho\sqrt{\Lambda_{k+1}}, \sqrt{\Lambda_k}\cdots\sqrt{\Lambda_2}\Lambda_1\sqrt{\Lambda_2}\cdots\sqrt{\Lambda_k}\rangle| \tag{34}$$

$$\leq \|\rho - \sqrt{\Lambda_{k+1}}\rho\sqrt{\Lambda_{k+1}}\|_{tr}\|\sqrt{\Lambda_k}\cdots\sqrt{\Lambda_2}\Lambda_1\sqrt{\Lambda_2}\cdots\sqrt{\Lambda_k}\|_{op} \tag{35}$$

$$\leq \|\rho - \sqrt{\Lambda_{k+1}}\rho\sqrt{\Lambda_{k+1}}\|_{tr}\|\sqrt{\Lambda_k}\|_{op}\cdots\|\sqrt{\Lambda_2}\|_{op}\|\Lambda_1\|_{op}\|\sqrt{\Lambda_2}\|_{op}\cdots\|\sqrt{\Lambda_k}\|_{op} \tag{36}$$

$$\leq 2\sqrt{\varepsilon_{k+1}}, \tag{37}$$

noting that the operator norm is submultiplicative. Similar to the base case, this implies that

$$\langle \rho, \sqrt{\Lambda_{k+1}}\cdots\sqrt{\Lambda_2}\Lambda_1\sqrt{\Lambda_2}\cdots\sqrt{\Lambda_{k+1}}\rangle \tag{38}$$

$$\geq \langle \rho, \sqrt{\Lambda_k}\cdots\sqrt{\Lambda_2}\Lambda_1\sqrt{\Lambda_2}\cdots\sqrt{\Lambda_k}\rangle - 2\sqrt{\varepsilon_{k+1}} \tag{39}$$

$$\geq \left(1 - \varepsilon_1 - 2\sum_{i=2}^{k}\sqrt{\varepsilon_i}\right) - 2\sqrt{\varepsilon_{k+1}} \tag{40}$$

$$= 1 - \varepsilon_1 - 2\sum_{i=2}^{k+1}\sqrt{\varepsilon_i} \tag{41}$$

as desired. ◀

This bound is related to the quantum union bound. See [27, 17] for good versions of this bound, and also [26] for a simple proof of it. While our bound is not always stronger, it can be viewed as complementary.

2.2 Quantum encodings, and proof of Lemma 3

In this section, we pin down what it means for Bob to learn something about Alice's input.

We may assume that Alice creates the following state

$$\sum_{x\in X} p_x|x\rangle\langle x| \tag{42}$$

where p_x is the probability of her choosing x, then control all of her actions on it. That is, this is a classical register that Alice holds. After some communication, Alice and Bob will share some joint state

$$\rho := \sum_{x\in X} p_x|x\rangle\langle x| \otimes \rho_x \tag{43}$$

where ρ_x is a (quantum) encoding of Alice's bit x.

Suppose Bob wants to learn some information about x. We may assume that Alice measures her classical register in the computational basis $\{N_x : x \in X\}$ to obtain the outcome x and it is this value about which Bob wants to learn some information.

Let us assume that Bob uses the measurement $\{M_b : b \in B\}$ if he wants to learn the value of the function $f : X \to B$. In the context of SFE, this function is of the same form once a $y \in Y$ has been fixed. Now, we can calculate the probability of Bob successfully learning the function f as

$$\left\langle \rho, \sum_{x\in X} N_x \otimes M_{f(x)} \right\rangle. \tag{44}$$

Note that the structure of ρ is not really all that important, only so much as to imply that we can assume N_x is a basis measurement.

Now, suppose that for a function f_i, for $i \in \{1, \ldots, n\}$, Bob has a POVM $\{M_b^i : b \in B\}$ such that he learns the correct value with probability at least $1 - \varepsilon_i$. Then from the above expression, we can write

$$\left\langle \rho, \sum_{x \in X} N_x \otimes M_{f_i(x)}^i \right\rangle \geq 1 - \varepsilon_i. \tag{45}$$

By defining

$$\Lambda_i = \sum_{x \in X} N_x \otimes M_{f_i(x)}^i \tag{46}$$

we can apply Lemma 6 to get that

$$\langle \rho, \sqrt{\Lambda_n} \cdots \sqrt{\Lambda_2} \Lambda_1 \sqrt{\Lambda_2} \cdots \Lambda_n \rangle \geq 1 - \varepsilon_1 - 2 \sum_{i=2}^{n} \sqrt{\varepsilon_i}. \tag{47}$$

Now, the neat thing is that since $\{N_x\}$ is a basis measurement, we have that

$$\sqrt{\Lambda_n} \cdots \sqrt{\Lambda_2} \Lambda_1 \sqrt{\Lambda_2} \cdots \sqrt{\Lambda_n} = \sum_{x \in X} N_x \otimes \sqrt{M_{f_n(x)}^n} \cdots \sqrt{M_{f_2(x)}^2} M_{f_1(x)}^1 \sqrt{M_{f_2(x)}^2} \cdots \sqrt{M_{f_n(x)}^n}. \tag{48}$$

This suggests we define the POVM

$$\{\tilde{M}_{b_1, \ldots, b_n} : b_1, \ldots, b_n \in B\} \tag{49}$$

where

$$\tilde{M}_{b_1, \ldots, b_n} := \sqrt{M_{b_n}^n} \cdots \sqrt{M_{b_2}^2} M_{b_1}^1 \sqrt{M_{b_2}^2} \cdots \sqrt{M_{b_n}^n}. \tag{50}$$

One can check that this is a valid POVM and Inequality (47) and Equation (48) show that this POVM learns $f_i(x)$ for every $i \in \{1, \ldots, n\}$, with probability at least

$$1 - \varepsilon_1 - 2 \sum_{i=2}^{n} \sqrt{\varepsilon_i}. \tag{51}$$

Note that since the measurement operators have the POVM $\{M_b^1 : b \in B\}$ "in the middle," and this choice was arbitrary, then we can see that Bob can create another measurement with $\{M_b^i : b \in B\}$ "in the middle" for any choice of i he wants. Thus, if he randomly chooses which measurement is "in the middle," then we see that we can average the success probability as

$$\frac{1}{n} \sum_{j=1}^{n} \left(1 - \varepsilon_j - 2 \sum_{i \neq j}^{n} \sqrt{\varepsilon_i} \right) = 1 - \frac{\sum_{i=1}^{n} \varepsilon_i}{n} - \frac{2(n-1)}{n} \sum_{i=1}^{n} \sqrt{\varepsilon_i}. \tag{52}$$

Using Cauchy-Schwarz, one can prove that

$$\sum_{i=1}^{n} \sqrt{\varepsilon_i} \leq \sqrt{n} \sqrt{\sum_{i=1}^{n} \varepsilon_i}. \tag{53}$$

Therefore, the average success probability is bounded below by

$$1 - \frac{\sum_{i=1}^{n} \varepsilon_i}{n} - \frac{2(n-1)}{\sqrt{n}} \sqrt{\sum_{i=1}^{n} \varepsilon_i}. \tag{54}$$

In the context of Lemma 3, we have that $p_i = 1 - \varepsilon_i$ is the probability of guessing $f_i(x)$. Substituting this into (54), we finish our proof of Lemma 3.

References

1. Scott Aaronson. QMA/qpoly is contained in PSPACE/poly: de-Merlinizing quantum protocols. In *Proceedings of the 21st Annual IEEE Conference on Computational Complexity*, pages 261–273, 2006.
2. N Aharon and J Silman. Quantum dice rolling: a multi-outcome generalization of quantum coin flipping. *New Journal of Physics*, 12(3):033027, 2010.
3. 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(3):633–679, 2016.
4. Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. In *Proceedings of the 33rd Annual ACM Symposium on the Theory of Computing*, pages 134–142, 2001.
5. Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani. Dense quantum coding and quantum finite automata. *Journal of the ACM*, 49(4):496–511, 2002.
6. 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*, pages 919–938, 2021.
7. 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*, pages 205–216, 2019.
8. B. Baumgartner. An inequality for the trace of matrix products, using absolute values. Available as arXiv.org e-Print math-ph/1106.6189, 2011. `arXiv:math-ph/1106.6189`.
9. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, India, 1984.
10. Manuel Blum. Coin flipping by telephone. In *Advances in Cryptology: A Report on CRYPTO 81*, pages 11–15, 1981.
11. Harry Buhrman, Matthias Christandl, and Christian Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Physical Review Letters*, 109(16):160501, 2012.
12. André Chailloux, Gus Gutoski, and Jamie Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chicago Journal of Theoretical Computer Science*, article 13, 2016.
13. André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 527–533, 2009.
14. André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In *Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 354–362, 2011.
15. André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for quantum oblivious transfer. *Quantum Information & Computation*, 13(1-2):158–177, 2013.
16. I.B. Damgaard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 449–458, 2005.
17. Jingliang Gao. Quantum union bounds for sequential projective measurements. *Physical Review A*, 92(5):052331, 2015.
18. Gus Gutoski, Ansis Rosmanis, and Jamie Sikora. Fidelity of quantum strategies with applications to cryptography. *Quantum*, 2:89, 2018.
19. Alexei Kitaev. Quantum coin-flipping. Unpublished result, 2002. Talk at the 6th Annual workshop on Quantum Information Processing (QIP 2003).
20. Srijita Kundu, Jamie Sikora, and Ernest Y.-Z. Tan. A device-independent protocol for XOR oblivious transfer. In *Proceedings of the 15th Conference on the Theory of Quantum Computation, Communication and Cryptography*, volume 158(12), pages 1–15, 2020.
21. Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154–1162, 1997.

22 Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997.

23 Hoi-Kwong Lo and H. F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1-2):177–187, 1998.

24 Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, 1997.

25 C. Mochon. Quantum weak coin flipping with arbitrarily small bias. Available as arXiv.org e-Print quant-ph/0711.4114, 2007. `arXiv:quant-ph/0711.4114`.

26 R. O'Donnell and R. Venkateswaran. The quantum union bound made easy. Available as arXiv.org e-Print quant-ph/2103.07827, 2021. `arXiv:quant-ph/2103.07827`.

27 Samad Khabbazi Oskouei, Stefano Mancini, and Mark M. Wilde. Union bound for quantum information processing. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 475(2221):20180612, 2018.

28 Michael O. Rabin. How to exchange secrets with oblivious transfer. Technical Report TR-81, Aiken Computation Lab, Harvard University, 1981.

29 Christian Schaffner. Cryptography in the bounded-quantum-storage model. Available as arXiv.org e-Print quant-ph/0709.0289, 2007. `arXiv:quant-ph/0709.0289`.

30 Christian Schaffner, Barbara M. Terhal, and Stephanie Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Information & Computation*, 9:963–996, 2009.

31 Jamie Sikora. Simple, near-optimal quantum protocols for die-rolling. *Cryptography*, 1(2):11, 2017.

32 R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65:012310, 2001.

33 Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.

34 Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

35 Mark M. Wilde. Sequential decoding of a general classical-quantum channel. In *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, volume 469(2157), page 20130259, 2013.

36 Mark M. Wilde. *Quantum Information Theory (second edition)*. Cambridge University Press, 2017.

37 A. Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, 1999.