Quantum Protocol for Cheat-Sensitive Weak Coin Flipping

R.W. Spekkens[1,*] and Terry Rudolph[2,3,†]

[1]*University of Toronto, 60 St. George Street, Toronto, Ontario, Canada M5S 1A7*
[2]*Bell Labs, 600-700 Mountain Avenue, Murray Hill, New Jersey 07974*
[3]*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, 1090 Vienna, Austria*

(Received 27 February 2002; published 6 November 2002)

We present a quantum protocol for the task of weak coin flipping. We find that, for one choice of parameters in the protocol, the maximum probability of a dishonest party winning the coin flip if the other party is honest is $1/\sqrt{2}$. We also show that if parties restrict themselves to strategies wherein they cannot be caught cheating, their maximum probability of winning can be even smaller. As such, the protocol offers additional security in the form of cheat sensitivity.

DOI: 10.1103/PhysRevLett.89.227901 PACS numbers: 03.67.Dd

In 1981, Blum [1] introduced the following cryptographic problem: Alice and Bob have just divorced and are trying to determine who will keep the car. They agree to decide the issue by the flip of a coin, but they can communicate only by telephone. The question is whether there is a protocol that allows them to decide on a winner in such a way that both parties feel secure that the other cannot fix the outcome.

Two-party protocols, of which this is an example, are some of the most problematic in classical cryptography. In fact, there are no two-party classical protocols whose security does not rely upon assumptions (many of which are threatened by quantum computation) about the complexity of a computational task. Kilian explains [2]: "[In a two-party protocol] both parties possess the entire transcript of the conversation that has taken place between them. [...] Because of this knowledge symmetry condition there are impossibility proofs for seemingly trivial problems. Cryptographic protocols "cheat" by setting up situations in which A may determine exactly what B can infer about her data, from an information-theoretic point of view, but does *not* know what he can easily (i.e., in probabilistic polynomial time) infer about her data. *From an information-theoretic point of view, of course, nothing has been accomplished.*" (Emphasis added.) Conversely, when we move from classical to quantum cryptography, we find many two-party protocols whose security rests only upon the validity of quantum mechanics. Thus, from a quantum information-theoretic point of view, something significant *can* be accomplished. Furthermore, quantum protocols can naturally exhibit a type of security known as *cheat sensitivity* [3]: Whenever a party cheats above some threshold amount, he or she runs a risk of being caught. This can provide a strong deterrent to cheating. For instance, if two parties need to implement a protocol many times, they may stand to gain more from the preservation of the trust of the other party than they do from cheating in a single implementation. Such considerations can be treated quantitatively by assigning numerical costs to the various possible results. Given the striking contrasts between what can be accomplished in classical and quantum two-party protocols, the analysis of such protocols provides valuable insights into the differences between classical and quantum information theory.

In this Letter, we will be concerned with a cryptographic task called *coin flipping.* We begin by distinguishing a strong and a weak form, both of which are adequate for Blum's original problem.

Strong coin flipping (SCF).—Alice and Bob engage in some number of rounds of communication, at the end of which each infers the outcome of the protocol to be either 0, 1, or *fail.* If both are honest, then they agree on the outcome and find it to be 0 or 1 with equal probability. Suppose, on the other hand, that one of the parties, X, is dishonest. In this situation, X cannot increase the probability of his/her opponent obtaining the outcome c to greater than $1/2 + \epsilon_X^c$, for either $c = 0$ or $c = 1$. The parameters ϵ_A^0, ϵ_A^1, ϵ_B^0, ϵ_B^1, which specify the degree to which the protocol resists biasing, must each be strictly less than $1/2$,

Weak coin flipping (WCF).—This is simply SCF without any constraints on ϵ_A^0 or ϵ_B^1. The parameters $\epsilon_A \equiv \epsilon_A^1$ and $\epsilon_B \equiv \epsilon_B^0$ must be strictly less than $1/2$ and specify the bias resistance of the protocol.

An SCF protocol ensures that neither party can fix the outcome to be 0 or fix the outcome to be 1. This protocol is appropriate when the parties do not know which outcome their opponent favors. By contrast, a WCF protocol ensures only that Alice cannot fix the outcome to be 1 and that Bob cannot fix the outcome to be 0. This is appropriate if Alice and Bob are playing a game where Alice wins if the outcome is 1 and Bob wins if the outcome is 0.

It has been shown by Lo and Chau [4] that a *perfectly bias-resistant* SCF protocol, i.e., one having $\epsilon_{A,B}^{0,1} = 0$, is impossible. Recently, Kitaev [5] has shown that it is also impossible to find an *arbitrarily bias-resistant* SCF protocol, i.e., one for which $\epsilon_{A,B}^{0,1} \longrightarrow 0$ in the limit that some security parameters go to infinity. The first *partially bias-resistant* SCF protocol, presented by Aharonov *et al.* [6], had $\epsilon_B^{0,1} \simeq 0.354$ and $\epsilon_A^{0,1} \leq 0.414$. We later showed that $\epsilon_A^{0,1} = \epsilon_B^{0,1}$ [7]. If $\epsilon_A^c = \epsilon_B^c$ for $c = 0$ and 1, we call the protocol *fair*; if $\epsilon_X^0 = \epsilon_X^1$ for $X = A$ and B, we call it *balanced.* A fair and balanced SCF protocol with $\epsilon_{A,B}^{0,1} = \frac{1}{4}$ was recently discovered by Ambainis [8]; the possibility of SCF with this degree of security also follows from our analysis [9] of quantum bit commitment. In fact, the results of Ref. [9] imply the existence of a balanced SCF protocol with $\epsilon_A^{0,1} = \alpha$ and $\epsilon_B^{0,1} = \beta$ for any pair of values α, β satisfying $\alpha + \beta = 1/2$.

Much less is known about WCF. Indeed, whether arbitrarily bias-resistant WCF is possible or not remains an open question. Since an SCF protocol yields a WCF protocol with parameters $\epsilon_A = \epsilon_A^0$ and $\epsilon_B = \epsilon_B^1$, the protocol of Ref. [9] yields a WCF protocol with $\epsilon_A + \epsilon_B = 1/2$. However, it is likely that by making a SCF protocol unbalanced one can lower the values of ϵ_A^1 and ϵ_B^0 at the expense of ϵ_A^0 and ϵ_B^1. Thus, one would expect there to exist a WCF protocol with better security than the one derived from Ref. [9]. This expectation is borne out by the results of this Letter. Specifically, we demonstrate the existence of a three-round WCF protocol for any ϵ_A, ϵ_B satisfying $(1/2 + \epsilon_A)(1/2 + \epsilon_B) = 1/2$. In particular, this implies that there exists a fair WCF protocol with $\epsilon_{A,B} = (\sqrt{2} - 1)/2 \simeq 0.207$.

We also characterize the cheat sensitivity of this protocol. Specifically, we consider each party's *threshold for cheat sensitivity*, defined as the maximum probability of winning that the party can achieve while ensuring that his or her probability of being caught cheating remains strictly zero. Since a party can achieve a probability of winning of 1/2 without cheating, the minimum possible threshold is 1/2. The maximum possible threshold is simply the party's maximum probability of winning. The protocol is said to be cheat sensitive only if the threshold is less than this maximum value. We find that, for suitably chosen parameters, the protocol presented here can be cheat sensitive against both parties simultaneously. Although no parameter choices yield a threshold of 1/2 for both parties simultaneously, it is possible to obtain such a threshold for one of the parties.

The protocol is as follows:

Round 1.—Alice prepares a pair of systems in a (typically entangled) state $|\psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$, and sends system B to Bob.

Round 2.—Bob performs the measurement associated with the positive operator-valued measure (POVM) $\{E_0, E_1\}$ on system B, and sends a classical bit b indicating the result to Alice.

Round 3.—If $b = 0$ then Bob sends system B back to Alice, while if $b = 1$ then Alice sends system A to Bob. The party that receives the system then performs the measurement associated with the projection valued measure $\{|\psi_b\rangle\langle\psi_b|, I - |\psi_b\rangle\langle\psi_b|\}$, where $|\psi_b\rangle = I \otimes \sqrt{E_b}|\psi\rangle / \sqrt{\langle\psi|I \otimes E_b|\psi\rangle}$.

The different possible outcomes are as follows:

(i) $b = 0$, Alice finds $|\psi_0\rangle\langle\psi_0|$; Bob wins.

(ii) $b = 0$, Alice finds $I - |\psi_0\rangle\langle\psi_0|$; Alice catches Bob cheating.

(iii) $b = 1$, Bob finds $|\psi_1\rangle\langle\psi_1|$; Alice wins.

(iv) $b = 1$, Bob finds $I - |\psi_1\rangle\langle\psi_1|$; Bob catches Alice cheating.

Notice that, unlike other proposed two-party protocols, at no stage does this protocol require either party to make classical random choices. While this protocol is sufficient for WCF, it is insufficient for SCF because Bob can always choose to lose by simply announcing $b = 1$. We will see that one can characterize an instance of the protocol completely by specifying the POVM element E_0 and the reduced density operator on system B, $\rho \equiv \mathrm{Tr}_A(|\psi\rangle\langle\psi|)$. In order for the parties to have equal probabilities of winning when both are honest, the constraint $\mathrm{Tr}(\rho E_0) = 1/2$ must be satisfied. This implies, in particular, that $|\psi_b\rangle = \sqrt{2}(I \otimes \sqrt{E_b}|\psi\rangle)$.

We proceed by listing the most important properties of the protocol. We then present several interesting specific choices of E_0 and ρ. The proofs are left until the end.

Property 1: Alice's maximum probability of winning is

$$P_A^{\max} = 2\mathrm{Tr}(\rho E_0^2).$$

Property 2: Alice's threshold for cheat sensitivity is

$$P_A^{\mathrm{thresh}} = \frac{1}{2\mathrm{Tr}(\rho \Pi_{(I-E_0)})},$$

where Π_X denotes the projector onto the support of X (the support of X is the set of eigenvectors of X associated with nonzero eigenvalues).

Property 3: Bob's maximum probability of winning is

$$P_B^{\max} = 2(\mathrm{Tr}\sqrt{\rho E_0 \rho})^2,$$

Property 4: Bob's threshold for cheat sensitivity is

$$P_B^{\mathrm{thresh}} = \frac{1}{2\lambda^{\max}(E_0 \Pi_\rho)},$$

where $\lambda^{\max}(X)$ denotes the largest eigenvalue of X.

An interesting family of protocols is defined by the choices $\rho = x|0\rangle\langle 0| + (1 - x)|1\rangle\langle 1|$ and $E_0 = \frac{1}{2x}|0\rangle\langle 0|$, where $1/2 < x \leq 1$. For these protocols, $P_A^{\max} = 1/2x$, $P_B^{\max} = x$, $P_A^{\mathrm{thresh}} = 1/2$, $P_B^{\mathrm{thresh}} = P_B^{\max}$. Thus, Alice runs a risk of being caught whenever she cheats, while Bob can cheat up to the maximum amount possible without running any risk of being caught. This family achieves the trade-off,

$$P_A^{\max} P_B^{\max} = 1/2. \tag{1}$$

It is easy to prove that this trade-off is optimal when E_0 and ρ have support in a 2D Hilbert space. In a preprint version of this Letter, we conjectured that it was optimal for all higher dimensional Hilbert spaces as well. Subsequently, this was proven by Ambainis [10] [who also independently discovered a WCF protocol achieving the trade-off of Eq. (1)]. It is interesting to note that, whereas the best known SCF protocols [8,9] require a qutrit for their implementation, a qubit suffices here.

A second interesting family of protocols is defined by the choices $\rho = x|0\rangle\langle 0| + (1-x)|1\rangle\langle 1|$ and $E_0 = (1-\frac{1}{2x})|0\rangle\langle 0| + |1\rangle\langle 1|$, with $1/2 \leq x < 1$. For these, $P_A^{\max} = 1/2x$, $P_B^{\max} = 2 + 4x^2 - 5x + 2(1-x)\sqrt{2x(2x-1)}$, $P_A^{\text{thresh}} = P_A^{\max}$, $P_B^{\text{thresh}} = 1/2$. In contrast with the previous example, Bob now runs a risk of being caught whenever he cheats, while Alice can cheat up to the maximum amount possible without running any risk of being caught. The trade-off (1) is no longer attained, however.

It can be shown that no choice of E_0 and ρ can give $P_A^{\text{thresh}} = P_B^{\text{thresh}} = 1/2$ [11]. Nonetheless, it *is* possible to have $P_A^{\text{thresh}} < P_A^{\max}$ and $P_B^{\text{thresh}} < P_B^{\max}$, i.e., cheat sensitivity against both parties simultaneously. This occurs, for example, when $\rho = \frac{1}{2}I$ and $E_0 = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$, since in this case $P_A^{\max} = 5/8$, $P_A^{\text{thresh}} = 1/2$, $P_B^{\max} = \frac{1}{2} + \frac{\sqrt{3}}{4} \simeq 0.933$, and $P_B^{\text{thresh}} = 2/3$. In this case, if the parties restrict themselves to strategies wherein they cannot be caught cheating, their maximum probability of winning is even less than $1/\sqrt{2}$. This example demonstrates that cheat sensitivity is a useful form of security in its own right.

Proof of property 1: Assume that Bob is honest. Alice's most general cheating strategy is to prepare a state $|\psi'\rangle$ instead of the honest $|\psi\rangle$. (It is obvious from what follows that she gains no advantage by preparing a mixed state, and thus no advantage by implementing strategies wherein she performs measurements on A or entangles A with a system she keeps in her possession. Moreover, since she only submits A to Bob when $b = 1$, any operation on A she wishes to perform can be done prior to Bob's announcement, and thus can be incorporated into the preparation.) The probability that Bob obtains the outcome $b = 1$ is $\langle\psi'|I \otimes E_1|\psi'\rangle$, and the probability that Alice passes Bob's test for $|\psi_1\rangle$ when she resubmits system A is $|\langle\psi_1|\psi_1'\rangle|^2$, where $|\psi_b'\rangle \equiv (I \otimes \sqrt{E_b}|\psi'\rangle)/\sqrt{\langle\psi'|I \otimes E_b|\psi'\rangle}$. Alice only wins the coin flip if the outcome is $b = 1$ *and* she passes Bob's test. This occurs with probability $P_A = \langle\psi'|I \otimes E_1|\psi'\rangle|\langle\psi_1|\psi_1'\rangle|^2 = |\langle\psi_1|I \otimes \sqrt{E_1}|\psi'\rangle|^2$. We wish to find $P_A^{\max} \equiv \sup_{|\psi'\rangle} P_A$. Thus, we must maximize the overlap of a normalized vector $|\psi'\rangle$, with the non-normalized vector $I \otimes \sqrt{E_1}|\psi_1\rangle$. Clearly, this is done by taking the two vectors parallel, so the optimal $|\psi'\rangle$ is $|\psi'^{\max}\rangle = (I \otimes \sqrt{E_1}|\psi_1\rangle)/\sqrt{\langle\psi_1|I \otimes E_1|\psi_1\rangle}$. Using the definition of $|\psi_1\rangle$ and applying some straightforward algebra, we find $P_A^{\max} = 2\text{Tr}(\rho E_1^2)$. As $E_1^2 = (I - E_0)^2$, we obtain $P_A^{\max} = 2\text{Tr}(\rho E_0^2)$. ■

Proof of property 2: We seek to determine Alice's maximum probability of winning assuming that her probability of being caught cheating is strictly zero. Alice's most general cheating strategy is, as above, to prepare a pure state $|\psi'\rangle$. She must pass Bob's test with probability one, which implies $|\langle\psi_1|\psi_1'\rangle|^2 = 1$, or $|\psi_1'\rangle = |\psi_1\rangle$ to within a phase factor. Multiplying both sides of this latter equation by $I \otimes \sqrt{E_1}^{-1}$ (we use X^{-1} to denote the inverse of X on its support), and writing $|\psi_1'\rangle$ and $|\psi_1\rangle$ in terms of $|\psi'\rangle$ and $|\psi\rangle$, we obtain $I \otimes \Pi_{E_1}|\psi'\rangle = \alpha(I \otimes \Pi_{E_1}|\psi\rangle)$ for some constant α. It follows that $|\psi'\rangle = \alpha(I \otimes \Pi_{E_1}|\psi\rangle) + \beta|\chi\rangle$, where $I \otimes \Pi_{E_1}|\chi\rangle = 0$ and α, β are constrained to ensure that $|\psi'\rangle$ is normalized. Heuristically, Alice can pass Bob's test with probability 1 whenever she submits a state $|\psi'\rangle$ that is indistinguishable from $|\psi\rangle$ within the support of E_1. Alice's probability of winning in this case is $\langle\psi'|I \otimes E_1|\psi'\rangle = |\alpha|^2\langle\psi|I \otimes E_1|\psi\rangle = \frac{1}{2}|\alpha|^2$, which is maximized when $\beta = 0$ and $\alpha = 1/\sqrt{\langle\psi|I \otimes \Pi_{E_1}|\psi\rangle}$. This yields $P_A^{\text{thresh}} = 1/2\langle\psi|I \otimes \Pi_{E_1}|\psi\rangle = 1/2\text{Tr}(\rho\Pi_{E_1})$. ■

For proving properties 3 and 4, the following definition and lemma are useful. (For simplicity, we ignore degeneracy and support issues which are easily incorporated but do not change any of our results.)

Definition: Consider a vector $|\varphi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$, a linear operator X on $\mathcal{H}^A$, and a linear operator Y on $\mathcal{H}^B$. X and Y are said to be *Schmidt equivalent under* $|\varphi\rangle$ if the matrix elements of X in the eigenbasis of $\text{Tr}_B(|\varphi\rangle\langle\varphi|)$ are the same as the matrix elements of Y in the eigenbasis of $\text{Tr}_A(|\varphi\rangle\langle\varphi|)$.

Lemma[7]: For a vector $|\varphi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$, and a positive operator E on $\mathcal{H}^B$,

$$\text{Tr}_B[(I \otimes \sqrt{E})|\varphi\rangle\langle\varphi|(I \otimes \sqrt{E})] = \sqrt{\omega}D^T\sqrt{\omega},$$

where $\omega \equiv \text{Tr}_B(|\varphi\rangle\langle\varphi|)$, D is the operator on $\mathcal{H}^A$ that is Schmidt equivalent to E under $|\varphi\rangle$, and D^T is the transpose of D with respect to the eigenbasis of ω.

Proof of lemma: Suppose the biorthogonal decomposition of $|\varphi\rangle$ is $|\varphi\rangle = \sum_j \sqrt{\lambda_j}|e_j\rangle \otimes |f_j\rangle$. Taking the trace in terms of the basis $\{|f_i\rangle\}$, we find LHS $= \sum_{j,k}\sqrt{\lambda_j\lambda_k}|e_j\rangle\langle f_k|E|f_j\rangle\langle e_k|$. By definition, $\langle f_k|E|f_j\rangle = \langle e_k|D|e_j\rangle$ and $\langle e_k|D|e_j\rangle = \langle e_j|D^T|e_k\rangle$. With some reordering of terms, we obtain LHS $= (\sum_j \sqrt{\lambda_j}|e_j\rangle\langle e_j|)D^T(\sum_k \sqrt{\lambda_k}|e_k\rangle\langle e_k|)$. Noting that $\sqrt{\lambda_j}$ and $|e_j\rangle$ are the eigenvalues and eigenvectors of $\sqrt{\omega}$,, we have the desired result. ■

Proof of property 3: Assume that Alice is honest. Bob's most general cheating strategy can be implemented as follows. First, he performs a measurement on system B of a POVM $\{E_k'\}$, which may have an arbitrary number of outcomes. With probability $p_k' = \langle\psi|I \otimes E_k'|\psi\rangle$ the outcome is k and the state of the total system is updated to $|\psi_k'\rangle = (I \otimes \sqrt{E_k'}|\psi\rangle)/\sqrt{p_k'}$. After the measurement, Bob can perform a unitary transformation, U_k, on system B, the nature of which depends on the outcome k that was recorded. Finally, he must decide whether to announce $b = 0$ or 1 based on the result of the measurement; that is, he must decide on a set S_0 of outcomes for which he will announce $b = 0$.

Bob's probability of passing Alice's test given outcome k is $|\langle\psi_0|I \otimes U_k|\psi'_k\rangle|^2$, so his probability of winning the coin flip is $P_B = \sum_{k\in S_0} p'_k|\langle\psi_0|I \otimes U_k|\psi'_k\rangle|^2$. We must maximize this with respect to variations in $\{E'_k\}, \{U_k\}$, and S_0. By Uhlmann's theorem [12], $\sup_{U_k} |\langle\psi_0|I \otimes U_k|\psi'_k\rangle|^2 = F(\sigma_0, \sigma'_k)^2$, where $\sigma_b \equiv \mathrm{Tr}_B(|\psi_b\rangle\langle\psi_b|)$, $\sigma'_k \equiv \mathrm{Tr}_B(|\psi'_k\rangle\langle\psi'_k|)$, and $F(\omega, \tau) \equiv \mathrm{Tr}|\sqrt{\omega}\sqrt{\tau}|$ is the fidelity. Thus, we need to compute $P_B^{\max} = \sup_{\{E'_k\},S_0} \sum_{k\in S_0} F(\sigma_0, p'_k\sigma'_k)^2$. Since the fidelity squared is always positive, $\sum_{k\in S_0} F(\sigma_0, p'_k\sigma'_k)^2 \leq \sum_k F(\sigma_0, p'_k\sigma'_k)^2$. This implies that the optimal S_0 is the entire set of indices: No matter what the outcome k of Bob's measurement, he should announce bit 0. Moreover, by the concavity of the fidelity squared [12], we have $\sum_k F(\sigma_0, p'_k\sigma'_k)^2 \leq F(\sigma_0, \sum_k p'_k\sigma'_k)^2 = F(\sigma_0, \sigma)^2$, where $\sigma \equiv \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. This upper bound is saturated if Bob makes no measurement upon system B. Using the definition of $|\psi_0\rangle$ and the lemma, we find that $\sigma_0 = 2\sqrt{\sigma}D_0^T\sqrt{\sigma}$, where D_0 is Schmidt equivalent to E_0 under $|\psi\rangle$. Thus, we can write $P_B^{\max} = F(2\sqrt{\sigma}D_0^T\sqrt{\sigma}, \sigma)^2 = F(2\sqrt{\sigma}D_0\sqrt{\sigma}, \sigma)^2$, where the second equality follows from the fact that X^T and X have the same eigenvalues. By the isomorphism between $\mathcal{H}^A$ and $\mathcal{H}^B$ induced by Schmidt equivalence under $|\psi\rangle$, we have $P_B^{\max} = F(2\sqrt{\rho}E_0\sqrt{\rho}, \rho)^2$. Finally, by the definition of the fidelity, we have $P_B^{\max} = 2(\mathrm{Tr}\sqrt{\rho E_0 \rho})^2$.

Proof of property 4: We seek to determine Bob's maximum probability of winning assuming that his probability of being caught cheating is strictly zero. The latter condition constrains Bob's most general cheating strategy, described above, to be such that he must always pass Alice's test whenever he announces the outcome $b = 0$. That is, we require that $\{E'_k\}, \{U_k\}$, and S_0 be such that $I \otimes U_k|\psi'_k\rangle = |\psi_0\rangle$ for all $k \in S_0$. The probability that Bob wins the coin flip is simply $\sum_{k\in S_0} p'_k$, so we seek to determine $\sup_{\{U_k\},\{E'_k\},S_0}(\sum_{k\in S_0} p'_k)$, where the optimization is subject to the above constraint. We solve the optimization problem by establishing an upper bound and demonstrating that it can be saturated. We begin by using the definitions of $|\psi'_k\rangle$ and $|\psi_0\rangle$ to rewrite the constraint equation as $\frac{1}{p'_k}(I \otimes U_k\sqrt{E'_k})|\psi\rangle\langle\psi|(I \otimes U_k\sqrt{E'_k}) = 2(I \otimes \sqrt{E_0})|\psi\rangle\langle\psi|(I \otimes \sqrt{E_0})$. Tracing over B and applying the lemma provided above, we obtain $\sqrt{\sigma}(D'_k)^T\sqrt{\sigma} = 2p'_k\sqrt{\sigma}D_0^T\sqrt{\sigma}$, where D'_k and D_0 are the Schmidt equivalent operators to E'_k and E_0, respectively. It follows that $\Pi_\sigma D'_k \Pi_\sigma = 2p'_k\Pi_\sigma D_0 \Pi_\sigma$, which, by the isomorphism between $\mathcal{H}^A$ and $\mathcal{H}^B$ induced by Schmidt equivalence under $|\psi\rangle$, implies $\Pi_\rho E'_k \Pi_\rho = 2p'_k\Pi_\rho E_0 \Pi_\rho$. Combining this with $\sum_{k\in S_0} E'_k \leq I$, we obtain $\sum_{k\in S_0} 2p'_k\Pi_\rho E_0\Pi_\rho \leq \Pi_\rho$, which in turn implies that $\sum_{k\in S_0} p'_k \leq 1/2\lambda^{\max}(\Pi_\rho E_0 \Pi_\rho) = 1/2\lambda^{\max}(\Pi_\rho E_0)$. The upper bound can be saturated while satisfying the constraint if Bob measures the POVM, $\{E'_0, E'_1\}$, defined by $E'_0 = \Pi_\rho E_0 \Pi_\rho/\lambda^{\max}(\Pi_\rho E_0)$, and announces $b = 0$ when he obtains the outcome associated with E'_0 [13]. Thus, Bob's threshold is $P_B^{\mathrm{thresh}} = 1/2\lambda^{\max}(\Pi_\rho E_0)$. ■

R.W.S. wishes to thank the group of Anton Zeilinger at the University of Vienna for their hospitality during his visit. This research was supported in part by the Natural Sciences and Engineering Research Council of Canada, the Austrian Science Foundation FWF, the TMR programs of the European Union, Project No. ERBFMRXCT960087, and by the NSA & ARO under Contract No. DAAG55-98-C-0040.

*Electronic address: spekkens@physics.utoronto.ca
†Electronic address: rudolpht@bell-labs.com

[1] M. Blum, in *Proceedings of the 24th IEEE Computer Conference, Compcon* (IEEE, New York, 1982), p. 133.

[2] J. Kilian, in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1988), p. 20.

[3] L. Hardy and A. Kent, quant-ph/9911043.

[4] H.-K. Lo and H. F. Chau, Physica (Amsterdam) **120D**, 177 (1998).

[5] A. Kitaev (unpublished), reported to us by A. Ambainis (personal communication).

[6] D. Aharonov *et al.*, in *Proceedings of the 32nd Annual Symposium on Theory of Computing 2000* (Association for Computing Machinery, New York, 2000), p. 705.

[7] R.W. Spekkens and T. Rudolph, J. Quant. Inform. Comput. **2**, 66 (2002).

[8] A. Ambainis, in *Proceedings of the 33rd Annual Symposium on Theory of Computing 2001* (Association for Computing Machinery, New York, 2001), p. 134.

[9] R.W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).

[10] A. Ambainis, quant-ph/020463.

[11] This is unfortunate since we believe that such a protocol could be used to build WCF that is arbitrarily bias resistant against both parties.

[12] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).

[13] An alternative proof of property 4 can be found by using the following result: Given two density operators ω and τ, satisfying $\Pi_\omega \geq \Pi_\tau$, the largest probability with which τ can appear in a convex decomposition of ω is $1/\lambda^{\max}(\omega^{-1}\tau)$. This result was first pointed out to us by Michael Nielsen.