# The Impossibility Of Secure Two-Party Classical Computation

Roger Colbeck*
*Centre for Quantum Computation, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, UK and Homerton College, Hills Road, Cambridge CB2 8PH, UK*
(August 21, 2007)

We present attacks that show that unconditionally secure two-party classical computation is impossible for many classes of function. Our analysis applies to both quantum and relativistic protocols. We illustrate our results by showing the impossibility of oblivious transfer.



## I. INTRODUCTION

Consider two parties wishing to compute some joint function of their data (two millionaires might wish to know who is richer, for example). A secure computation of such a function is one for which the only information the first party gets on the input of the second is that implied by the outcome of the computation, and vice versa.

In this work, we focus on *unconditional* security, whereby we seek to construct a protocol whereby the two mistrustful parties can communicate in order to achieve the task. Security will rely on a belief in the laws of physics. We allow each party to exploit the properties of both quantum mechanics and relativity in order to achieve security. While the security benefits of the former are well known, relatively little investigation has been made into the extra security afforded by the latter. One positive result in relativistic cryptography is that it allows variable-bias coin tossing to be realized [1]. In this paper, we show that even using both relativistic and quantum protocols, there are a large class of functions for which secure two-party computation is impossible. A discussion of relativistic cryptography can be found in Refs. [1, 2].

We call a computation classical, in spite of it potentially relying on quantum communication for its implementation, because its inputs and outputs are classical data.

Two-party computations can be divided into several classes, depending on the number of parties that receive the output (the *sidedness* of the function) and whether the function is deterministic or random. In the two-sided case, we will further specialize to *single function* computations, where both parties receive identical outcomes. What is presently known about such functions is summarized in Table I. For a longer introduction to secure two-party computation, see Ref. [1].

In this paper, we will show the impossibility of various secure two-party computations, by giving an explicit cheating attack. A summary of the argument is as follows. In a classical computation, each party is supposed to input one of a finite set of classical values. However, the impossibility of classical certification [4] means that one party cannot

| | | | |
|---|---|---|---|
| Zero-input | Deterministic | ✓ | Trivial |
| | Random one-sided | ✓ | Trivial |
| | Random two-sided | ✓ | Biased $n$-faced die roll (see [1] for discussion) |
| One-input | Deterministic | ✓ | Trivial |
| | Random one-sided | ✗* | One-sided variable-bias $n$-faced die roll (this paper) |
| | Random two-sided | ✓* | Variable-bias $n$-faced die roll cf. [1] |
| Two-input | Deterministic one-sided | ✗ | cf. [3] |
| | Deterministic two-sided | ✗* | This paper |
| | Random one-sided | ✗* | This paper |
| | Random two-sided | ✗* | This paper |

TABLE I: Functions computable with unconditional security in two-party computations using (potentially) both quantum and relativistic protocols. ✓ indicates that all functions of this type are possible, ✗ indicates that all functions of this type are impossible, ✓* indicates that some functions of this type are possible and all functions of this type are conjectured to be possible, and ✗* indicates that some functions of this type are impossible.

*r.a.colbeck@damtp.cam.ac.uk

detect when the other inputs a superposition of such inputs. By keeping all decisions at the quantum level until the end of the protocol, we can model the entire computation as unitary. The insecurity of the computation then follows because there exists a measurement on the output state generated by the superposed input, which allows the cheating party to better distinguish between the possible inputs of the other party than if they had been honest. In most cases, we have impossibility proofs for the simplest non-trivial cases of each class of function. We discuss at the end of the paper the possible generalizations.

In this paper we consider *perfectly secure* protocols—i.e. those for which the probability of cheating is strictly zero. Further, our protocols are *perfectly correct*; that is, the probability of error is strictly zero in the case where both parties are honest. One would like to extend our results to cover the case of protocols for which the probability of cheating and of error tend to zero in the limit that some security parameter tends to infinity.

## II. COMPUTATIONAL MODEL

We use a black box model for secure computation. A black box represents an idealized version of a protocol. It can be thought of as an unbreakable box which has an input and output port for each party. It features an authentication system (e.g., an unalterable label) so that each party can be sure of the function it computes. An appropriately constructed protocol will prescribe a sequence of information exchanges mimicking the essential features of such a black box. If one of the parties deviates from the prescribed exchanges, the protocol should abort. The question of whether or not it is possible to construct a protocol mimicking a given black box will not be addressed[1]. Rather, we show that cheating is possible even if such black boxes do exist.

Since in any real protocol all measurements can be delayed until the end, we consider only black boxes which perform unitary operations. The outcomes of such unitary operations are distributed amongst the parties. At the end of a classical computation they are measured to generate the outcome. For a general two-sided function, we consider the unitary, $U_f$, such that

$$U_f \left|i\right\rangle_A \left|j\right\rangle_B \left|0\right\rangle \left|0\right\rangle = \left|i\right\rangle_A \left|j\right\rangle_B \sum_k \alpha_{i,j}^k \left|kk\right\rangle_{AB}, \tag{1}$$

where $\{\alpha_{i,j}^k\}$ depend on the function being computed, and the index $k$ runs over all possible outputs. $i$ and $j$ correspond to Alice's and Bob's inputs respectively, and their output[2] is $k$ which is read by measurement in an orthonormal basis. Outcome $k$ occurs with probability $|\alpha_{i,j}^k|^2$. If the function is deterministic, then, for each $i$ and each $j$, $|\alpha_{i,j}^k| = 1$ for one value of $k$, and is zero for all others. More generally, the unitary, $U_f'$ performing

$$U_f' \left|i\right\rangle_A \left|j\right\rangle_B \left|0\right\rangle \left|0\right\rangle \left|0\right\rangle = \left|i\right\rangle_A \left|j\right\rangle_B \sum_k \alpha_{i,j}^k \left|kk\right\rangle_{AB} \left|\psi_{i,j}^k\right\rangle_{AB}, \tag{2}$$

would be of use to compute such a function, where the final Hilbert space corresponds to an ancillary system the black box uses for the computation (and has arbitrary dimension). In the protocol mimicking such a box, this final state must be distributed between Alice and Bob in some way, such that the part that goes to Bob, for instance, contains no information on Alice's input.

If black boxes implementing such unitaries were to exist, then each party has two ways of cheating. The first is by inputting a superposition of states into the protocol, rather than a member of the computational basis as they should. The second involves using a different measurement on the output of the black box than that dictated by the protocol. It follows from the impossibility of classical certification [4] that a real protocol cannot prevent the first attack. Under these attacks, insecurity of functions under $U_f$ implies insecurity under $U_f'$, as we show below. Hence it is sufficient to consider only the former.

Consider the case where Alice makes a superposed input, $\sum_i a_i \left|i\right\rangle$, rather than a single member of the computational basis. Then, at the end of the protocol, her reduced density matrix takes either the form

$$\sigma_j = \sum_{i,i',k} a_i a_{i'}^* \alpha_{i,j}^k (\alpha_{i',j}^k)^* |i\rangle\langle i'| \otimes |k\rangle\langle k| \tag{3}$$

---

[1] However, we do eliminate certain types of black box, e.g. ones that allow classical certification (see later).

[2] Recall that we have restricted to single function computations.

or

$$\sigma'_j = \sum_{i,i',k} a_i a^*_{i'} \alpha^k_{i,j} (\alpha^k_{i',j})^* |i\rangle\langle i'| \otimes |k\rangle\langle k| \otimes \mathrm{tr}_B |\psi^k_{i,j}\rangle\langle\psi^k_{i',j}|, \tag{4}$$

where the first case applies to $U_f$, and the second to $U'_f$.

Alice is then to make a measurement on her state in order to distinguish between the different possible inputs Bob could have made, as best she could. We will show that there exists a trace-preserving quantum operation that Alice can use to convert $\sigma'_j$ to $\sigma_j$ for all $j$. It follows that Alice's ability to distinguish between $\{\sigma'_j\}_j$ is at least as good as her ability to distinguish between $\{\sigma_j\}_j$.

In order that the protocol functions correctly when both Alice and Bob are honest, we require $\mathrm{tr}_B |\psi^k_{i,j}\rangle\langle\psi^k_{i,j}| \equiv \rho^{i,k}$ to be conditionally independent of $j$ given $k$ (otherwise Alice can gain more information on Bob's input than that implied by $k$ by a suitable measurement on her part of this state). By expressing $\rho^{i,k}$ in its diagonal basis, $\rho^{i,k} = \sum_m \lambda^{i,k}_m U^{i,k}_A |m\rangle\langle m|_A (U^{i,k}_A)^\dagger$, we have

$$\left|\psi^k_{i,j}\right\rangle = \sum_m \sqrt{\lambda^{i,k}_m} U^{i,k}_A \left|m\right\rangle_A \otimes U^{i,j,k}_B \left|m\right\rangle_B, \tag{5}$$

where $\{|m\rangle_A\}_m$ form an orthogonal basis set on Alice's system and likewise $\{|m\rangle_B\}_m$ is an orthogonal basis for Bob's system. Bob then holds

$$\mathrm{tr}_A |\psi^k_{i,j}\rangle\langle\psi^k_{i,j}| = \sum_m \lambda^{i,k}_m U^{i,j,k}_B |m\rangle\langle m|_B (U^{i,j,k}_B)^\dagger. \tag{6}$$

This must be conditionally independent of $i$ given $k$, hence so must $\lambda^{i,k}_m$ and $U^{i,j,k}_B$. Thus

$$\left|\psi^k_{i,j}\right\rangle = \sum_m \sqrt{\lambda^k_m} (U^{i,k}_A \otimes U^{j,k}_B) \left|m\right\rangle_A \left|m\right\rangle_B. \tag{7}$$

It hence follows that there is a unitary on Alice's system converting $\left|\psi^k_{i_1,j}\right\rangle$ to $\left|\psi^k_{i_2,j}\right\rangle$ for all $i_1$, $i_2$, and that, furthermore, this unitary is conditionally independent of $j$ given $k$. Likewise, there is a unitary on Bob's system converting $\left|\psi^k_{i,j_1}\right\rangle$ to $\left|\psi^k_{i,j_2}\right\rangle$ for all $j_1$, $j_2$, with this unitary being conditionally independent of $i$ given $k$.

Returning now to the case where Alice makes a superposed input. The final state of the entire system can be written

$$\sum_{i,k} a_i \alpha^k_{i,j} \left|i\right\rangle_A \left|j\right\rangle_B \left|k\right\rangle_A \left|k\right\rangle_B (U^{i,k}_A \left|m\right\rangle_A)(U^{j,k}_B \left|m\right\rangle_B). \tag{8}$$

Alice can then apply the unitary

$$V = \sum_{i,k} |i\rangle\langle i|_A \otimes \mathbb{1}_B \otimes |k\rangle\langle k|_A \otimes \mathbb{1}_B \otimes (U^{i,k}_A)^\dagger \otimes \mathbb{1}_B \tag{9}$$

to her systems leaving the state as

$$\sum_{i,k} a_i \alpha^k_{i,j} \left|i\right\rangle_A \left|j\right\rangle_B \left|k\right\rangle_A \left|k\right\rangle_B \sum_m \sqrt{\lambda^k_m} \left|m\right\rangle_A (U^{j,k}_B \left|m\right\rangle_B). \tag{10}$$

Alice is thus in possession of density matrix

$$\sum_{i,i',k} a_i a^*_{i'} \alpha^k_{i,j} (\alpha^k_{i',j})^* |i\rangle\langle i'| \otimes |k\rangle\langle k| \otimes \rho^k_A, \tag{11}$$

where $\rho^k_A = \sum_m \lambda^k_m |m\rangle\langle m|_A$. On tracing out the final system, we are left with $\sigma_j$ as defined by (3).

We have hence shown that there is a trace-preserving quantum operation Alice can perform which converts $\sigma'_j$ to $\sigma_j$ for all $j$, and that this operation is conditionally independent of $j$ given $k$. Hence Alice's ability to distinguish between Bob's inputs after computations of the type $U'_f$ is at least as good as her ability to distinguish Bob's inputs after computations of the type $U_f$, and so, under the type of attack we consider, insecurity of computations specified by $U_f$ implies insecurity of those specified by $U'_f$. We will therefore consider only type $U_f$ in our analysis. An analogous argument follows for the one-sided case, and likewise for the deterministic cases (which are special cases of the non-deterministic ones).

We now state the security condition that will be shown to be breakable for a large class of computation.

**Security Condition.** Consider the case where Bob is honest. For a computation to be considered secure, there can be no input, together with a measurement on the corresponding output that gives Alice a better probability of guessing Bob's input than she would have gained by following the protocol honestly and making her most informative input. This condition must hold for all forms of prior information Alice holds on Bob's input.

Let us emphasize that the use of the black box model does not restrict the scope of our proofs: these apply to all real protocols. The model is common to discussions of universal composability (see Section V) and makes manifest that is sufficient for parties to behave dishonestly only in the initial and final steps of any protocol in order to break our security condition[3].

## III. DETERMINISTIC FUNCTIONS

We first focus on the deterministic case. Lo showed that two-input deterministic one-sided computations are impossible to compute securely [3], hence only two-sided deterministic functions remain[4]. There is a further consideration when discussing deterministic functions that leads us to restrict the class of functions further.

Suppose that the outcome of such a protocol leads to some real-world consequence. In the dating problem [5], for example, one requires a secure computation of $k = i \times j$, where $i, j \in \{0, 1\}$. If the computation returns $k = 1$, then the protocol dictates that Alice and Bob go on a date. This additional real-world consequence is impossible to enforce, although both Alice and Bob have some incentive not to stand the other up, since this results in a loss of the other's trust. A cost function could be introduced to quantify this, but since suitable cost assignments must be assessed case by case, it is difficult to develop general results. To eliminate such an issue, we restrict to the case where the sole purpose of the computation is to learn something about the input of the other party. No subsequent action of either party based on this information will be specified.

We say that a function is *potentially concealing* if there is no input by Alice which will reveal Bob's input with certainty, and vice versa. If the aim of the computation is only to learn something about the input of the other party, and if Bob's data is truly private, he will not enter a secure computation with Alice if she can learn his input with certainty. We hence only consider potentially concealing functions in what follows. In addition, we will ignore *degenerate* functions in which two different inputs are indistinguishable in terms of the outcomes they afford. If the sole purpose of the computation is to learn something about the other party's input, then, rather than compute a degenerate function, Alice and Bob could instead compute the simpler function formed by combining the degenerate inputs of the original.

An alternative way of thinking about such functions is that they correspond to those in which there is no cost for ignoring the real world consequence implied by the computation. At the other extreme, one could invoke the presence of an enforcer who would compel each party to go ahead with the computation's specified action. This would have no effect on security for a given function (a cheating attack that works without an enforcer also works with one) but introduces a larger set of functions that one might wish to compute. There exist functions within this larger set for which the attack we present does not work.

We specify functions by giving the matrix of outcomes. For convenience the outputs of the function are labelled with consecutive integers starting with 0. We consider functions that satisfy the following conditions:

1. (Potentially concealing requirement) Each row and each column must contain at least two elements that are the same.

2. (Non degeneracy requirement) No two rows or columns should be the same.

For instance, if $i, j \in \{0, 1, 2\}$ (which we term a $3 \times 3$ function), the function $f(i, j) = 1 - \delta_{ij}$ is

| $f(i,j)$ | | $i$ | | |
|---|---|---|---|---|
| | | 0 | 1 | 2 |
| | 0 | 0 | 1 | 1 |
| $j$ | 1 | 1 | 0 | 1 |
| | 2 | 1 | 1 | 0 |

.

[3] In any case, if a protocol mimicks a black box correctly, then there is no scope for cheating during its implementation.
[4] Lo did not consider relativistic cryptography, but his results apply to this case as well [1].

| $f(i,j)$ | | $i$ | | |
|---|---|---|---|---|
| | | 0 | 1 | 2 |
| $j$ | 0 | 0 | $a$ | . |
| | 1 | 0 | $b$ | . |
| | 2 | 1 | $b$ | . |

TABLE II: This function can be taken as the most general $3 \times 3$ function satisfying conditions 1 and 2, where $a \neq b$, and $a = 0$ or $b = 0$ or $b = 1$. The dots represent unspecified (and not necessarily identical) entries consistent with the conditions.

This function is potentially concealing, and non-degenerate.

We consider the case of $3 \times 3$ functions. We first give a non-constructive proof that Alice can always cheat, and then an explicit cheating strategy.

Let us assume that we have a black box that can implement the protocol, i.e., that performs the following operation:

$$U_f \left|i\right\rangle_A \left|j\right\rangle_B \left|0\right\rangle \left|0\right\rangle = \left|i\right\rangle_A \left|j\right\rangle_B \left|f(i,j)\right\rangle_A \left|f(i,j)\right\rangle_B . \tag{12}$$

The states $\{\left|i\right\rangle_A\}$ are mutually orthogonal, as are the members of the sets $\{\left|j\right\rangle_B\}$, $\{\left|f(i,j)\right\rangle_A\}$ and $\{\left|f(i,j)\right\rangle_B\}$. This ensures that Alice and Bob always obtain the correct output if both have been honest. The existence of such a black box would allow Alice to cheat in the following way. She can first input a superposition, $\sum_{i=0}^{2} a_i \left|i\right\rangle_A$ in place of $\left|i\right\rangle_A$. Her output from the box is one of $\rho_0, \rho_1, \rho_2$, the subscript corresponding to Bob's input, $j$, where (using the shorthand $\mathrm{tr}_B(\left|\Psi\right\rangle) \equiv \mathrm{tr}_B(\left|\Psi\right\rangle\!\left\langle\Psi\right|)$)

$$\rho_j \equiv \mathrm{tr}_B \left( U_f \sum_{i=0}^{2} a_i \left|i\right\rangle_A \left|j\right\rangle_B \left|0\right\rangle_A \left|0\right\rangle_B \right). \tag{13}$$

Alice can then attempt to distinguish between these using any measurement of her choice.

The main result of this section is the following theorem.

**Theorem 1.** *Consider the computation of a $3 \times 3$ deterministic function satisfying conditions 1 and 2. For each function of this type, there exists a set of coefficients, $\{a_i\}$ such that when Alice has a uniform prior distribution over Bob's inputs and she inputs $\sum_{i=0}^{2} a_i \left|i\right\rangle_A$ into the protocol, there exists a measurement that gives her a better probability of distinguishing the three possible (j dependent) output states than that given by her best honest strategy.*

*Proof.* We will rely on the following lemma.

**Lemma 1.** *All $3 \times 3$ functions satisfying conditions 1 and 2 can be put in the form of the function in Table II.*

*Proof.* The essential properties of any function are unchanged under permutations of rows or columns (which correspond to relabelling of inputs), and under relabelling of outputs. In order that the function is potentially concealing, there can be at most one column whose elements are identical. By relabelling the columns if necessary, we can ensure that this corresponds to $i = 2$. Relabelling the outputs and rows, if necessary, the column corresponding to $i = 0$ has entries $(f(0,0), f(0,1), f(0,2)) = (0,0,1)$. The column corresponding to $i = 1$ then must have entries $(a,a,b)$ or $(a,b,b)$, with $a \neq b$. In the case $(a,a,b)$, the $i = 2$ column must have the form $(c,d,d)$, for $c \neq d$, in which case we can permute the $i = 1$ and $i = 2$ columns to recover the form $a,b,b$ for the $i = 1$ column. Relabellings always put such cases into forms with $a = 0$ or $b = 0$ or $b = 1$. $\mathcal{QED}$

Suppose Alice inputs $\frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle)$ into a function of the form given in Table II. After tracing out Bob's systems, Alice holds one of

$$\rho_0 = \frac{1}{2}\left(\left|00\right\rangle\!\left\langle 00\right| + \delta_{a,0}\left(\left|00\right\rangle\!\left\langle 10\right| + \left|10\right\rangle\!\left\langle 00\right|\right) + \left|1a\right\rangle\!\left\langle 1a\right|\right) \tag{14}$$

$$\rho_1 = \frac{1}{2}\left(\left|00\right\rangle\!\left\langle 00\right| + \delta_{b,0}\left(\left|00\right\rangle\!\left\langle 10\right| + \left|10\right\rangle\!\left\langle 00\right|\right) + \left|1b\right\rangle\!\left\langle 1b\right|\right) \tag{15}$$

$$\rho_2 = \frac{1}{2}\left(\left|01\right\rangle\!\left\langle 01\right| + \delta_{b,1}\left(\left|01\right\rangle\!\left\langle 11\right| + \left|11\right\rangle\!\left\langle 01\right|\right) + \left|1b\right\rangle\!\left\langle 1b\right|\right). \tag{16}$$

Measurement using the set $\{E_{i,k} = \left|ik\right\rangle\!\left\langle ik\right|\}$ in effect reverts to an honest strategy. The probability of correctly guessing Bob's input using these operators is the same as that for Alice's best honest strategy. These operators can

be combined to form just three operators, $\{E_{j'}\}$ such that a result corresponding to $E_{j'}$ means that Alice's best guess of Bob's input is $j'$. Then

$$\begin{aligned} E_0 &= \alpha_1|00\rangle\langle 00| + \delta_{a,0}|10\rangle\langle 10| + \delta_{a,1}|11\rangle\langle 11| + \delta_{a,2}|12\rangle\langle 12| + \delta_{a,3}|13\rangle\langle 13| && (17)\\ E_1 &= (1-\alpha_1)|00\rangle\langle 00| + \alpha_2\delta_{b,0}|10\rangle\langle 10| + \alpha_3\delta_{b,1}|11\rangle\langle 11| + \alpha_4\delta_{b,2}|12\rangle\langle 12| + \alpha_5\delta_{b,3}|13\rangle\langle 13| && (18)\\ E_2 &= \mathbb{1} - E_0 - E_1, && (19)\end{aligned}$$

where the $\{\alpha_l\}$ are arbitrary parameters, $0 \le \alpha_l \le 1$, and do not affect the success probability. We will show that such a measurement is not optimal to distinguish between the corresponding $\{\rho_j\}$. This follows from an existing result in state estimation theory, as stated in the following theorem [6, 7, 8].

**Theorem 2.** *Consider using a set of $M$ measurement operators, $\{E_j\}$, to discriminate between a set of $M$ states, $\{\rho_j\}$, which occur with prior probabilities, $\{q_j\}$, where the outcome corresponding to operator $E_j$ indicates that the best guess of the state is $\rho_j$. The set $\{E_j\}$ is optimal if and only if*

$$\begin{aligned} E_j\left(q_j\rho_j - q_l\rho_l\right)E_l &= 0 \quad \forall\, j,l && (20)\\ \sum_j E_j q_j\rho_j - q_l\rho_l &\ge 0 \quad \forall\, l. && (21)\end{aligned}$$

In the case of uniform prior probabilities, Equations (20) and (21) imply respectively

$$\begin{aligned}(\alpha_1 = 0 \quad \text{or} \quad \alpha_2 = 0 \quad \text{or} \quad b \neq 0) \quad \text{and} \quad (\alpha_1 = 1 \quad \text{or} \quad a \neq 0) \quad \text{and} \quad (22)\\ (\alpha_1 = 1 \quad \text{or} \quad \alpha_2 = 1 \quad \text{or} \quad b \neq 0) \quad \text{and} \quad (\alpha_3 = 0 \quad \text{or} \quad b \neq 1)\,,\end{aligned}$$

and

$$\begin{aligned}\left(b = 1 \quad \text{or} \quad \alpha_3 \ge \frac{1}{4}\right) \quad \text{and} \quad \left(b = 0 \quad \text{or} \quad \alpha_2(1-\alpha_1) \ge \frac{1}{4}\right) \quad \text{and} \quad (a = 1 \quad \text{or} \quad \alpha_3 = 1 \quad \text{or} \quad b \neq 1) \quad \text{and} \quad (23)\\ (\alpha_1 = 0 \quad \text{or} \quad (b \neq 0 \quad \text{and} \quad a \neq 0)) \quad \text{and} \quad (\alpha_1 = 1 \quad \text{or} \quad b \neq 0 \quad \text{or} \quad \alpha_2 = 0)\end{aligned}$$

In addition, because the function is in the form given in Table II, we also have

$$(a = 0 \quad \text{or} \quad b = 0 \quad \text{or} \quad b = 1) \quad \text{and} \quad a \neq b. \qquad (24)$$

The system of equations (22–24) cannot be satisfied for any values of $a, b, \{\alpha_k\}$. Hence, the measurement operators (17–19) are not optimal for discriminating between Bob's inputs, so Alice always has a cheating strategy. $\mathcal{QED}$

Our proof of Theorem 1 is non-constructive—we have shown that cheating is possible, but not explicitly how it can be done. Except in special cases (e.g., where the states $\{\rho_j\}$ are symmetric), no procedure for finding the optimal POVM to distinguish between states is known [9, 10]. Nevertheless, we have found a construction based on the square root measurement [11, 12] that, while not being optimal, gives a higher probability of successfully guessing Bob's input than any honest strategy.

The strategy applies to the states, $\sigma_j$, formed when Alice inputs $\frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + |2\rangle\right)$. The set of operators are those corresponding to the square root measurement, defined by

$$E_{j'} = \left(\sum_j \sigma_j\right)^{-\frac{1}{2}} \sigma_{j'} \left(\sum_j \sigma_j\right)^{-\frac{1}{2}}. \qquad (25)$$

One can verify, case by case, that this strategy affords Alice a better guessing probability over Bob's input than any honest one for all functions of the form of Table II. The Mathematica script which we have used to check this is available on the world wide web [13].

| $p(0\|i,j)$ | | $i$ | |
|---|---|---|---|
| | | 0 | 1 |
| $j$ | 0 | $p_{00}$ | $p_{10}$ |
| | 1 | $p_{01}$ | $p_{11}$ |

TABLE III: The entries in the table give the probabilities of output 0 given inputs $i, j$. For example, if both parties input 0, then the output of the function is 0 with probability $p_{00}$, and 1 with probability $1 - p_{00}$.

## IV. NON-DETERMINISTIC FUNCTIONS

### A. Two-sided case

Initially, we specialize to the case $i, j, k \in \{0, 1\}$. We specify such functions via a matrix of probabilities as given in Table III. For the two-sided case, the relevant black box implements the unitary, $U$, given by

$$U \left|i\right\rangle_A \left|j\right\rangle_B \left|0\right\rangle \left|0\right\rangle = \left|i\right\rangle_A \left|j\right\rangle_B \left(\sqrt{p_{ij}} \left|00\right\rangle_{AB} + \sqrt{1 - p_{ij}} \left|11\right\rangle_{AB}\right). \tag{26}$$

Suppose that Alice has prior information about Bob's input such that, from her perspective, he will input 0 with probability $q_0$, and 1 with probability $q_1 = 1 - q_0$. The maximum probability of correctly guessing Bob's input using an honest strategy is

$$p_h = \max_i (\max_j (p_{ij} q_j) + \max_j ((1 - p_{ij}) q_j)). \tag{27}$$

Denote Alice's final state by $\rho_j$, where $j$ is Bob's input. The optimal strategy to distinguish $\rho_0$ and $\rho_1$ is successful with probability [8]

$$\frac{1}{2} \left(1 + \mathrm{tr} \left|q_0 \rho_0 - q_1 \rho_1\right|\right). \tag{28}$$

**Theorem 3.** *Let Alice input $\frac{1}{\sqrt{2}} (\left|0\right\rangle + \left|1\right\rangle)$ and Bob input $j$ into the computation given in (26). Let Alice implement the optimal measurement to distinguish the corresponding $\rho_0$ and $\rho_1$ and call the probability of a correct guess using this measurement $p_c$. Then, for all $\{p_{00}, p_{01}, p_{10}, p_{11}\}$, there exists a value of $q_0$ such that $p_c > p_h$, unless,*

1. *$p_{00} = p_{10}$ and $p_{01} = p_{11}$, or*
2. *$p_{00} = p_{01}$ and $p_{10} = p_{11}$.*

The two exceptional cases correspond to functions for which only one party can make a meaningful input. We hence conclude that all genuinely two-input functions of this type are impossible to compute securely.

*Proof.* Take $q_0 = 1 - \epsilon$. For sufficiently small $\epsilon > 0$, (27) implies $p_h = q_0$. We then seek $p_c$. The eigenvalues of $q_0 \rho_0 - q_1 \rho_1$ are

$$\lambda_\pm = \frac{1}{4} \left(a(\{p_{i,j}\}) \pm \sqrt{a^2(\{p_{i,j}\}) + b(\{p_{i,j}\})}\right) \tag{29}$$

$$\mu_\pm = \frac{1}{4} \left(a(\{\overline{p_{i,j}}\}) \pm \sqrt{a^2(\{\overline{p_{i,j}}\}) + b(\{\overline{p_{i,j}}\})}\right), \tag{30}$$

where $a(\{p_{i,j}\}) = (p_{00} + p_{10}) q_0 - (p_{01} + p_{11}) q_1$, $b(\{p_{i,j}\}) = 4(\sqrt{p_{01} p_{10}} - \sqrt{p_{00} p_{11}})^2 q_0 q_1$, and $\overline{p_{ij}} \equiv 1 - p_{ij}$.

For $\epsilon$ sufficiently small, we have $a \gg b > 0$. Using $\sqrt{1 + x} \leq 1 + \frac{x}{2}$, we find, $\lambda_+ \geq \frac{1}{4}(2a(\{p_{i,j}\}) + \frac{b(\{p_{i,j}\})}{2a(\{p_{i,j}\})})$, $\lambda_- \leq -\frac{b(\{p_{i,j}\})}{8a(\{p_{i,j}\})}$, $\mu_+ \geq \frac{1}{4}(2a(\{\overline{p_{i,j}}\}) + \frac{b(\{\overline{p_{i,j}}\})}{2a(\{\overline{p_{i,j}}\})})$, and $\mu_- \leq -\frac{b(\{\overline{p_{i,j}}\})}{8a(\{\overline{p_{i,j}}\})}$, with equality iff $b(\{p_{i,j}\}) = 0$ and $b(\{\overline{p_{i,j}}\}) = 0$. We hence have $\frac{1}{2} (1 + \mathrm{tr}|q_0 \rho_0 - q_1 \rho_1|) \geq q_0$ and so $p_c \geq p_h$, with equality iff $p_{00} = p_{10}$ and $p_{01} = p_{11}$, or $p_{00} = p_{01}$ and $p_{10} = p_{11}$. $\mathcal{QED}$

The explicit form of the cheating measurement is given in [8].

| $p(k\|i)$ | | $i$ | |
|---|---|---|---|
| | | 0 | 1 |
| $k$ | 0 | $\frac{1}{2}$ | 0 |
| | 1 | 0 | $\frac{1}{2}$ |
| | ? | $\frac{1}{2}$ | $\frac{1}{2}$ |

TABLE IV: Probability table for oblivious transfer.

### B. One-sided case

For one-sided computations of non-deterministic functions, Alice can cheat without inputting a superposed state. In this case, the black box performs the unitary

$$U\left|i\right\rangle_A\left|j\right\rangle_B\left|0\right\rangle=\left|i\right\rangle_A\left|j\right\rangle_B\left(\sqrt{p_{ij}}\left|0\right\rangle_A+\sqrt{1-p_{ij}}\left|1\right\rangle_A\right), \tag{31}$$

where the last qubit goes to Alice at the end of the protocol. The following theorem shows that such computations cannot be securely implemented.

**Theorem 4.** *Having made an honest input to the black box above, Alice's optimum procedure to correctly guess Bob's input is not given by a measurement in the* $\{\left|0\right\rangle,\left|1\right\rangle\}$ *basis, except if* $p_{ij}\in\{0,1\}$ *for all* $i$, $j$.

*Proof.* From (20) of Theorem 2, if Alice inputs $i=1$, the measurement operators $\{\left|0\right\rangle\!\left\langle 0\right|,\left|1\right\rangle\!\left\langle 1\right|\}$ are optimal only if

$$q_0\sqrt{p_{10}(1-p_{10})}=(1-q_0)\sqrt{p_{11}(1-p_{11})}. \tag{32}$$

For this to hold for all $q_0$, we require that either $p_{11}=0$ or $p_{11}=1$, and either $p_{10}=0$ or $p_{10}=1$. Similarly, if Alice inputs $i=0$, we require either $p_{01}=0$ or $p_{01}=1$, and either $p_{00}=0$ or $p_{00}=1$, in order that the specified measurement operators are optimal. $\mathcal{QED}$

These exceptions correspond to functions that are deterministic, so do not properly fall into the class presently being discussed. Many are essentially single-input, hence trivial, and all such exceptions are either degenerate or not potentially concealing.

Our theorem also has the following consequence.

**Corollary 1.** *One-sided variable-bias coin tossing [1] is impossible.*

*Proof.* A one-sided variable bias coin toss is the special case where both $p_{00}=p_{10}$ and $p_{01}=p_{11}$. These cases are not exceptions of Theorem 4, and hence are impossible. $\mathcal{QED}$

### C. Example: The Impossibility Of Oblivious Transfer

Here we show explicitly how to attack a black box that performs oblivious transfer when used honestly. This is a second proof of its impossibility in a stand-alone manner (the first being Rudolph's [14]). [5] The probability table for this task is given in Table IV.

In an honest implementation of oblivious transfer, Bob is able to guess Alice's input with probability $\frac{3}{4}$. However, the final states after using the ideal black box are of the form $\left|\psi_b\right\rangle=\frac{1}{\sqrt{2}}\left(\left|b\right\rangle+\left|?\right\rangle\right)$, where $\left|0\right\rangle$, $\left|1\right\rangle$ and $\left|?\right\rangle$ are mutually orthogonal. These are optimally distinguished using the POVM $(E_0,\mathbb{1}-E_0)$, where

$$E_0=\frac{1}{6}\begin{pmatrix}2+\sqrt{3} & -1 & 1+\sqrt{3}\\ -1 & 2-\sqrt{3} & 1-\sqrt{3}\\ 1+\sqrt{3} & 1-\sqrt{3} & 2\end{pmatrix}. \tag{33}$$

This POVM allows Bob to guess Alice's bit with probability $\frac{1}{2}\left(1+\frac{\sqrt{3}}{2}\right)$, which is significantly greater than $\frac{3}{4}$.

[5] Impossibility had previously been argued on the grounds that oblivious transfer implies bit commitment and hence is impossible because bit commitment is. However, while this argument rules out the possibility of a composable oblivious transfer protocol, a stand-alone one is not excluded.

## V. DISCUSSION

We have introduced a black box model of computation, and have given a necessary condition for security. Even if such black boxes were to exist as prescribed by the model, one party can always break the security condition. Specifically, by inputting a superposed state rather than a classical one, and performing an appropriate measurement on the outcome state, one party can always gain more information on the input of the other than that gained using any honest strategy. In the case of deterministic functions, this attack has only been shown to work if the function is non-degenerate and potentially concealing. In the case where the sole purpose of the function is to learn something about the other party's input, these are the only relevant functions.

Our theorems deal only with the simplest cases of each class of function. However, the results can be extended to more general functions as described below.

**Larger input alphabets:** A deterministic function is impossible to compute securely if it possesses a $3 \times 3$ submatrix which is potentially concealing and satisfies the degeneracy requirement. This follows because Alice's prior might be such that she can reduce Bob to three possible values of $j$. This argument does not rule out the possibility of all larger functions, since some exist that are potentially concealing without possessing a potentially concealing $3 \times 3$ subfunction. Nevertheless, we conjecture that all potentially concealing functions have a cheating attack which involves inputting a superposition and then optimally measuring the outcome.

In the non-deterministic case, all functions with more possibilities for $i$ and $j$ values possess $2 \times 2$ submatrices that are ruled out by the attacks presented, or reduce to functions that are one-input. Therefore, no two-party non-deterministic computations with binary outputs can satisfy our security condition.

**Larger output alphabets:** In the non-deterministic case, we considered only binary outputs. We conjecture that the attacks we have presented work more generally on functions with a larger range of possible outputs.

We have not proven that the aforementioned attacks work for all functions within the classes given in Table I, although we conjecture this to be the case. Furthermore, for any given computation, one can use the methods presented in this work to verify its vulnerability under such attacks.

We now briefly place our results within the context of universal security definitions. In classical cryptography, there are two common models for universal security, one introduced by Canetti [15] and the other by Backes, Pfitzmann and Waidner [16, 17]. Recently, such frameworks have been extended for use in quantum protocols [18, 19, 20]. The idea is that if a protocol is universally secure (or universally composable), then it can be used as a subprotocol in any larger protocol. The large protocol can then be divided into subprotocols, each of which is assumed to behave as a black box with a defined ideal functionality[6]. The task of proving the larger protocol secure then reduces to that of proving that the subprotocols correctly mimick their ideals, together with an argument that the combination of the ideals correctly performs the overall task.

Our results imply that there is no way to define an ideal suitable for realizing secure classical computation in a quantum relativistic framework. Hence, without making additional assumptions, or invoking the presence of a trusted third party, secure classical computation is impossible using the usual notions of security. The quantum relativistic world, while offering more cryptographic power than both classical and quantum non-relativistic worlds, still does not permit a range of computational tasks.

One reasonable form of additional assumption is that the storage power of an adversary is bounded. The so-called bounded storage model has been used in both classical and quantum settings. This model evades our no-go results because limiting the quantum storage power of an adversary forces them to make measurements (or discard potentially useful parts of the system). This invalidates our unitary model of computation. In the classical bounded storage model, the adversary's memory size can be at most quadratic in the memory size of the honest parties in order to form secure protocols [21, 22]. However, if quantum protocols are considered, and an adversary's quantum memory is limited, a much wider separation is possible. Protocols exist for which the honest participants need no quantum memory, while the adversary needs to store half of the qubits transmitted in the protocol in order to cheat successfully [23].

We further remark that the cheating strategy we present for the non-deterministic case does not work for all assignments of Alice's prior over Bob's inputs—there exist functions and values of the prior for which it is impossible to cheat using the attack we have presented. This continues to be the case when we allow Alice to choose amongst the most general superposed input states. As a concrete example, consider the set $(p_{00}, p_{01}, p_{10}, p_{11}) = (\frac{47}{150}, \frac{103}{150}, \frac{8}{9}, \frac{5}{9})$, with $q_0 = \frac{1}{2}$ in the two sided version. Hence, in practice, there could be situations in which Bob would be happy to perform such a computation, for example, if he was sure Alice had no prior information over his inputs.

---

[6] Or can alternatively be described via a trusted third party

**Acknowledgments**

I would like to acknowledge Adrian Kent and Robert König for useful discussions. This work was partly supported by the European Union through the Integrated Project QAP (IST-3-015848), SCALA (CT-015714), and SECOQC and by the QIP IRC (GR/S821176/01).

---

[1] R. Colbeck and A. Kent, Physical Review A **73**, 032320 (2006).
[2] A. Kent, Journal of Cryptology **18** (2005).
[3] H.-K. Lo, Physical Review A **56**, 1154 (1997).
[4] A. Kent, *Promising the impossible: Classical certification in a quantum world*, e-print quant-ph/0409029 (2004).
[5] D. Gottesman and H.-K. Lo, Physics Today **53** (2000).
[6] A. S. Holevo, Journal of Multivariate Analysis **3**, 337 (1973).
[7] H. P. Yuen, R. S. Kennedy, and M. Lax, IEEE Transactions on Information Theory **IT-21**, 125 (1975).
[8] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, London, 1976).
[9] A. Chefles, Contemporary Physics **41**, 401 (2000).
[10] M. Ježek, J. Řeháček, and J. Fiurášek, *Finding optimal strategies for minimum-error quantum-state discrimination*, e-print quant-ph/0201109 (2002).
[11] L. P. Hughston, R. Jozsa, and W. K. Wootters, Physics Letters A **183**, 14 (1993).
[12] P. Hausladen and W. K. Wootters, Journal of Modern Optics **41**, 2385 (1994).
[13] Mathematica script available at http://qubit.damtp.cam.ac.uk/users/roger/script/PGP.nb.
[14] T. Rudolph, *The laws of physics and cryptographic security*, e-print quant-ph/0202143 (2002).
[15] R. Canetti, Journal of Cryptology **13**, 143 (2000).
[16] B. Pfitzmann and M. Waidner, in *Proceedings of the 2001 IEEE Symposium on Security and Privacy (SP01)* (IEEE Computer Society, Washington, DC, USA, 2001), pp. 184–201.
[17] M. Backes, B. Pfitzmann, and M. Waidner, in *TCC* (2004), pp. 336–354.
[18] M. Ben-Or and D. Mayers, *General security definition and composability for quantum & classical protocols*, e-print quant-ph/0409062 (2004).
[19] D. Unruh, *Simulatable security for quantum protocols*, e-print quant-ph/0409125 (2004).
[20] C. Crépeau, D. Gottesman, and A. Smith, in *Proceedings of the 34th annual ACM symposium on Theory of computing (STOC-02)* (ACM Press, New York, NY, USA, 2002), pp. 643–652.
[21] C. Cachin, C. Crépeau, and J. Marcil, in *FOCS '98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, USA, 1998), pp. 493–502.
[22] Y. Z. Ding, D. Harnik, A. Rosen, and R. Shaltiel, in *Proceedings of the First Theory of Cryptography Conference (TCC04)*, edited by M. Naor (Springer, 2004), vol. 2951 of *Lecture Notes in Computer Science*, pp. 446–472.
[23] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *FOCS '05: Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, USA, 2005), pp. 449–458.