Multi-photon and side-channel attacks in mistrustful quantum cryptography

Mathieu Bozio,\textsuperscript{1, 2} Adrien Cavaillès,\textsuperscript{2} Eleni Diamanti,\textsuperscript{2} Adrian Kent,\textsuperscript{3, 4} and Damián Pitalúa-García\textsuperscript{3, 4}

\textsuperscript{1}Faculty of Physics, University of Vienna, VCQ, Boltzmanngasse 5, 1090 Vienna, Austria
\textsuperscript{2}Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, F-75005 Paris, France
\textsuperscript{3}Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, United Kingdom
\textsuperscript{4}Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada

(Dated: March 15, 2021)

Mistrustful cryptography includes important tasks like bit commitment, oblivious transfer, coin flipping, secure computations, position authentication, digital signatures and secure unforgeable tokens. Practical quantum implementations presently use photonic setups. In many such implementations, Alice sends photon pulses encoding quantum states and Bob chooses measurements on these states. In practice, Bob generally uses single photon threshold detectors, which cannot distinguish the number of photons in detected pulses. Also, losses and other imperfections require Bob to report the detected pulses. Thus, malicious Alice can send and track multi-photon pulses and thereby gain information about Bob’s measurement choices, violating the protocols’ security. Here, we provide a theoretical framework for analysing such multi-photon attacks, and present known and new attacks. We illustrate the power of these attacks with an experiment, and study their application to earlier experimental demonstrations of mistrustful quantum cryptography. We analyse countermeasures based on selective reporting and prove them inadequate. We also discuss side-channel attacks where Alice controls further degrees of freedom or sends other physical systems.

Quantum cryptography promises that cryptographic tasks can be implemented with provable security, assuming only the validity of quantum theory. As with most guarantees, though, one needs to study the small print. Security proofs are based on idealized models of quantum cryptosystems, which do not necessarily characterize the behaviour of real world equipment. Hence apparently faithful implementations of provably secure protocols can be vulnerable to attacks. A wide range of attacks on practical quantum key distribution systems have been noted \textsuperscript{[1–8]} along with countermeasures. Less attention has so far been paid to attacks on practical implementations of quantum protocols for mistrustful cryptographic tasks. We consider such attacks here.

In mistrustful cryptography, two or more parties collaborate to implement a cryptographic task without trusting each other. Significant mistrustful cryptographic tasks include bit commitment \textsuperscript{[9–18]}, various types of oblivious transfer \textsuperscript{[19–25]}, coin flipping \textsuperscript{[26–32]}, secure computations \textsuperscript{[33]}, position authentication \textsuperscript{[34–36]}, digital signature schemes \textsuperscript{[37, 38]} and money or secure unforgeable tokens \textsuperscript{[39–47]}. Some of these tasks cannot be implemented with unconditional security using standard quantum cryptography \textsuperscript{[48–52]}, but can be when relativistic signalling constraints are taken into account \textsuperscript{[6, 18, 27]}. For others, even relativistic quantum protocols cannot provide unconditional security \textsuperscript{[35, 53, 57]}, but there may be protocols that are provably unbreakable when realistic practical assumptions are made on the amounts of entanglement \textsuperscript{[54, 55]}, quantum memory \textsuperscript{[58–61]}, or other technologically challenging resources. Some tasks are only properly defined in a relativistic setting \textsuperscript{[22, 24, 34, 55, 62–66]}.

At present, quantum implementations of mistrustful cryptography generally use photonic systems. A common step in these protocols is for (say) Alice to send Bob quantum states encoding some secret data of hers in photonic degrees of freedom (usually polarization), and for Bob to apply quantum measurements on the received states, chosen from a predetermined set, where his choice encodes secret data of his. Idealized protocols often assume that Alice has ideal single photon sources, the channel is lossless, and Bob has perfectly efficient ideal detectors. In practice, there are preparation and measurement errors and losses. Moreover, most implementations use weak coherent pulses rather than near-perfect single photon sources. Another issue is that Bob generally uses threshold photon detectors, which cannot distinguish the number of photons in pulses activating a detection and which are not close to perfectly efficient. Because of losses and imperfect detectors, realistic implementations tend to require Bob to report during the protocol the labels of pulses activating a detection.

Realistic security analyses need to take all these points into account. The full range of attacks that they allow in mistrustful quantum cryptographic scenarios seems not to have been appreciated. In such scenarios, Bob cannot assume that Alice sends independent light pulses with identically randomly distributed photon numbers, or the pulses have similar frequencies, or any variations are statistical fluctuations that Alice has no more information about than he does. If Alice can advantageously vary the distributions in a controlled way or obtain information about individual pulses, then she might. An uncon-
ditionally secure real world implementation must allow for these possibilities and still provide security guarantees. Bob also cannot assume that his detectors have precisely equal efficiencies, nor that Alice has no information about their efficiencies. Even if the latter were true at the start of a protocol, Alice can learn information about their efficiencies during the protocol. In this respect she has advantages over Bob, since she knows the states sent, while he does not, and can send states other than those prescribed by the protocol.

Here we analyse various strategies of Bob to report the labels of pulses activating a detection, some of which were considered before, and discuss their vulnerability to multi-photon attacks, in which dishonest Alice controls the number of photons in the transmitted pulses to her advantage. The analysed reporting strategies fit within a broad class of probabilistic reporting strategies introduced here in which Bob reports the label of a pulse with a probability that depends on which of his detectors are activated. Our main result (Theorem 1) states that the only reporting strategy within this class that provides perfect protection against arbitrary multi-photon attacks when Bob’s detection efficiencies are different is a trivial strategy in which Bob reports all detection events with the same probability. This implies that the strategy of symmetrization of losses [64], which is commonly used (e.g. [13, 30, 60, 61]), does not protect against arbitrary multi-photon attacks. We discuss how multi-photon attacks apply to the experimental demonstrations of mistrustful quantum cryptography of Refs. [13, 14, 30, 60, 61]. We report an experiment suggesting that multi-photon attacks can be implemented in practice. We also discuss side-channel attacks in mistrustful quantum cryptography, where Alice controls degrees of freedom not previously agreed with Bob. We propose some countermeasures to investigate against multi-photon and side-channel attacks.

I. RESULTS

A. Private measurement of an unknown qubit state

Many interesting protocols in mistrustful quantum cryptography (e.g. [12, 13, 23, 24, 30, 44, 47, 60, 61]) use some version of a task we call private measurement of an unknown qubit state. An ideal protocol to implement this task is the following:

1. Alice prepares a qubit state $|\psi\rangle$ randomly from a set $\mathcal{S} = \{|\psi_{ij}\rangle\}_{(i,j) \in \{0,1\}^2}$ and sends it to Bob.

2. Bob generates a random bit $\beta \in \{0,1\}$ privately and measures $|\psi\rangle$ in a qubit orthogonal basis $\mathcal{B}_\beta = \{|\psi_0\rangle, |\psi_1\rangle\}$. Commonly, $\mathcal{B}_0$ and $\mathcal{B}_1$ are the computational and Hadamard bases, respectively, and $\mathcal{S}$ is the set of Bennett-Brassard 1984 (BB84) states. We consider here the more general situation in which $\mathcal{B}_0$ and $\mathcal{B}_1$ are arbitrary distinct qubit orthogonal bases. We assume that Alice and Bob know these bases precisely.

We are primarily interested in the security attainable against Alice in various realistic implementations of the task. This is parametrised by Alice’s probability $P_{\text{guess}}$ to guess Bob’s chosen bit $\beta$, assuming Bob honestly follows the version of the protocol defined for the given implementation. We say the protocol is $\epsilon_{\text{guess}}$-secure against Alice if

$$P_{\text{guess}} \leq \frac{1}{2} + \epsilon_{\text{guess}},$$

for any possible strategy (not necessarily honestly following the protocol) of Alice. We say it is secure against Alice if $\epsilon_{\text{guess}} \to 0$ as some protocol security parameter is increased. In general, a dishonest Alice may deviate in any way from the protocol. For example, she may send Bob quantum states that are not only outside the agreed set $\mathcal{S}$ but outside its Hilbert space.

Different experimental setups correspond to different protocols to implement versions of this task. Here we consider setups and protocols with photonic systems, where Alice encodes quantum states in degrees of freedom of photons, for example in polarization, and Bob measures quantum states using single photon detectors.

We focus here on attacks by Alice, and assume that Bob honestly follows the given protocols. However, we have in mind applications in which these are sub-protocols for mistrustful cryptographic tasks in which cheating by Bob is equally relevant. These applications motivate two correctness criteria:

1. If Alice and Bob follow the protocol, the pulse sent by Alice must produce a measurement outcome with probability $P_{\text{det}}$ satisfying

$$P_{\text{det}} \geq \delta_{\text{det}},$$

for some $\delta_{\text{det}} > 0$ predetermined by Alice and Bob.

2. If Alice and Bob follow the protocol, Bob measures the received qubit in the basis of Alice’s prepared state, and Bob gets a measurement outcome, then the outcome is the state $|\psi\rangle$ prepared by Alice, with probability $1 - P_{\text{error}}$, where

$$P_{\text{error}} \leq \delta_{\text{error}},$$

for some $\delta_{\text{error}} \geq 0$ predetermined by Alice and Bob.

In an ideal setup, Alice’s and Bob’s laboratories are perfectly secure, their preparation and measurement devices are perfect, Alice has a perfect single photon source, the probability that a transmitted photon is lost in the quantum channel is zero, Bob has a perfect random number generator and single photon detectors with unit detection efficiency and without dark counts.
Since Bob’s detectors are ideal and the quantum channel is lossless, Bob obtains a measurement outcome with unit probability if Alice sends a single photon: precisely one of his detectors clicks for each photon sent. Thus, \( P_{\text{det}} = 1 \) and condition (2) is trivially satisfied. Since the preparation and measurement devices are perfect, \( P_{\text{error}} = 0 \) and (3) is also trivially satisfied.

In the setups we consider Bob has at least two detectors. If Alice sends something other than a single photon state, Bob may get zero, two or more clicks. The number of clicks may depend statistically on his measurement basis. However, since he does not report anomalous results, his laboratory is secure, and his basis choices are perfectly random, Alice still learns no information about his chosen basis. Thus, the ideal setup allows us to effectively implement the task of private measurement of an unknown qubit state, with perfect security against Alice (\( \epsilon_{\text{guess}} = 0 \)) and perfect correctness (\( P_{\text{det}} = 1 \) and \( P_{\text{error}} = 0 \)).

However, in practical implementations, the ideal protocol and setup have to be altered to allow for imperfect sources, channels and measuring devices. We show in this paper that this allows attacks by Alice that make perfect security impossible in practical implementations of the task using known technology. This is hence also true of higher-level cryptographic tasks that use the considered task as a sub-routine.

### B. Practical implementations

#### 1. A practical protocol

We make the standard cryptographic assumption that Alice’s and Bob’s laboratories are secure. We consider the realistic case in which their preparation and measurement devices are imperfect, the quantum channel is lossy. Bob’s random number generator is imperfect, Bob’s single photon detectors have nonunit efficiencies and nonzero dark count probabilities.

We assume Alice has what is usually called a single photon source, although in fact only approximates to one, i.e. the source emits a pulse with \( k \) photons with probability \( p_k \), for \( k \in \{0, 1, 2, \ldots \} \), where \( p_1 >> \sum_{k=2}^{\infty} p_k \). For the moment we suppose that Alice and Bob know the probabilities \( p_k \) but neither of them has any further information about the number of photons \( k \) in any given pulse. Most commonly, in implementations to date, Alice uses a weak coherent source (e.g. [13, 14, 30, 43]), which emits a pulse of \( k \) photons with probability \( p_k = e^{-\mu} \mu^k/k! \), where \( \mu \) is the average photon number, chosen by Alice and agreed with Bob, with \( 0 < \mu << 1 \). This emits an empty pulse with probability \( p_0 = e^{-\mu} \approx 1 \), but nonzero pulses are likely to be single photons since \( p_1 >> \sum_{k=2}^{\infty} p_k \). Another possibility is a source of pairs of entangled photons in which Alice measures one of the photons and sends the other one to Bob, with transmissions considered valid if Alice obtains a measurement outcome (e.g. [60, 61]). This gives \( p_0 << 1 \), \( p_1 \approx 1 \) and so \( p_1 >> \sum_{k=2}^{\infty} p_k \).

In either case there is a nonzero probability that none of Bob’s detectors click when a nonempty pulse is sent, because they are not perfectly efficient and the quantum channel is noisy. There is also a nonzero probability that more than one of Bob’s detectors click, because their dark counts are nonzero and the transmitted pulse may have more than one photon. As we explain below, a realistic protocol generally requires an algorithm determining a message \( m \) as a function (which may be probabilistic) of Bob’s detection results. This algorithm may in general depend on various experimental parameters known to Bob, which may include his detectors’ efficiencies, for instance. Bob sends Alice \( m = 1 \) \((m = 0)\) to report a successful (unsuccessful) measurement. As usual in cryptography, we assume the full protocol, and hence the algorithm, is known to both parties. It defines Bob’s reporting strategy.

The parameter \( \delta_{\text{det}} \) must be sufficiently small to satisfy (2). Bob’s detection efficiencies are often small. For example, Refs. [13, 30, 60, 61] report detection efficiencies of the order of 0.06, 0.08, 0.13 and 0.015, respectively. Ref. [14] reports considerably higher detection efficiencies, of the order of 0.45. Note that in this paper, we include in the term ‘detection efficiency’ the transmission efficiency of the quantum channel and the quantum efficiency of the detectors.

However, more complex protocols that have our task as a subroutine may also require that \( \delta_{\text{det}} \) be not too small in order to give security against Bob. For example, a \( N \)–parallel repetition of the task in which Bob reports to Alice that \( \ll N\delta_{\text{det}} \) pulses produce a measurement outcome could allow Bob to choose to report an appropriate subset of pulses producing measurement outcomes advantageous to him in some cheating strategy. Alice thus stipulates a minimum value of \( \delta_{\text{det}} \), and Bob must ensure his technology allows this value to be attained. Alice aborts if Bob reports less than \( N\delta_{\text{det}}(1 - \delta_{\text{dev}}) \), where \( \delta_{\text{dev}} > 0 \) is predetermined by Alice and agreed by Bob as the maximum tolerable deviation from the expected value of reported pulses.

Since the preparation and measurement devices are not perfect, there is a probability \( P_{\text{error}} > 0 \) that Bob obtains a measurement outcome different to Alice’s target state \(|\psi\rangle\) when Bob measures in the basis of preparation by Alice. Thus, \( \delta_{\text{error}} \) must be chosen large enough to guarantee the condition (3).

However, more complex protocols that have the task as a subroutine generally require Bob to be able to report correct measurement outcomes with reasonably high probability. This requires \( \delta_{\text{error}} \) not to be too large.

These constraints require that Bob identifies some subset of purportedly successful measurement outcomes to Alice, in which the proportion of actually successful measurement outcomes will be relatively high if Alice honestly followed the protocol. They motivate a practical protocol for private measurement of an unknown qubit.
state, with the above practical setup:

1. Alice prepares and sends Bob a photon pulse with an approximate single photon source, where each photon in the pulse encodes the same qubit state $|\psi\rangle$, and where $|\psi\rangle$ is chosen randomly by Alice from the set $S$.

2. Bob generates a random bit $\beta \in \{0,1\}$ and measures the pulse in the qubit basis $B_\beta$.

3. Bob sends a message $m \in \{0,1\}$ to Alice reporting whether a measurement outcome was produced ($m = 1$) or not ($m = 0$), following an agreed reporting strategy.

Unless otherwise stated, in the definition of security against Alice for the practical protocol, $P_{\text{guess}}$ is taken as Alice’s probability to guess $\beta$, independently of the value of $m$. This makes sense with the setup described below in extensions of this protocol in which $N > 1$ photon pulses are produced by Alice and all pulses are measured by Bob in the same basis $B_\beta$. Examples of these type of protocols are those of Refs. [13, 14], which we discuss in Appendix D.

Alternatively, we could define $P_{\text{guess}}$ as Alice’s probability to guess $\beta$ conditioned on Bob reporting $m = 1$. This makes more sense in extensions of the practical protocol in which Alice sends Bob $N > 1$ photon pulses and Bob measures each pulse randomly in one of the two bases, $B_0$ and $B_1$, or in protocols using a setup with four single photon detectors (setup II defined in Appendix D) instead of two as in the setup below. This is because in these scenarios Alice might only care to learn Bob’s measurement bases for the pulses that he reported as being successful. In Appendix D, we use this definition to present an attack to the protocols of Refs. [13, 61].

Some version of the practical protocol defined above is commonly used in experimental demonstrations of mistrustful cryptography [13, 14, 30, 60, 61]. Various reporting strategies have been used. We show below that they have subtle weaknesses, allowing attacks by a dishonest Alice. We show moreover that this is true of any reporting strategy of the broad class described here.

2. Details of setup

We consider a basic setup to implement the practical protocol, denoted as setup I (see Fig. 1). Another setup is discussed in Appendix D. Alice encodes a qubit state in some degrees of freedom of a photon pulse, using an approximate single photon source and a state modulator. Alice and Bob agree in advance on these degrees of freedom. These typically consist in the polarization (e.g. $13,14,30,40,60,61$), but can also be time bin (e.g. 28) or others, for example. For definiteness we focus on polarization coding in this paper, but our results apply to any choice.

A dishonest Alice may deviate arbitrarily from the protocol, limited only by her technological capabilities. Importantly, when proving the unconditional security of a protocol, we need to assume that the technology available to dishonest Alice is only limited by the laws of physics. Dishonest Alice may, for example, replace the photon source agreed with Bob for the protocol with another one that has different statistics. More generally, Alice may send Bob an arbitrary quantum state $\rho$ encoded in the polarization and other degrees of freedom.

In most of this paper we focus on multi-photon attacks performed by a dishonest Alice, in which Alice sends Bob a pulse of $k$ photons encoding an arbitrary quantum state $\rho$ of her choice, which may be pure or mixed and may be entangled with an ancilla held by Alice, and where each photon in the pulse encodes a qubit in its polarization.

We assume from here on that Bob honestly follows the agreed protocol. In setup I (see Fig. 1), Bob measures the polarization of the received pulse with a wave plate, set in one of two positions $\beta \in \{0,1\}$, followed by a polarizing beam splitter and two single photon detectors, $D_0$ and $D_1$. These are threshold detectors: they do not distinguish the number of photons of a pulse producing a detection. If $\beta = 0$ ($\beta = 1$), Bob sets the wave plate in its first (second) position, corresponding to a measurement in the basis $B_0$ ($B_1$). Let $n_{i,\beta}$ and $d_{i,\beta}$ be the detection efficiency and the dark count probability of detector $D_i$ when Bob applies the measurement $B_\beta$, where $0 < n_{i,\beta} < 1$ and $0 < d_{i,\beta} << 1$, for $i, \beta \in \{0,1\}$. In our model, dark counts and each photo-detection are independent random events. To the best of our knowledge, this is a valid assumption.

The pair of detectors produces a detection event $(\epsilon_0, \epsilon_1) \in \{0,1\}^2$ with four possible values: $(\epsilon_0, \epsilon_1) = (1,0)$ if $D_0$ clicks and $D_1$ does not click, $(\epsilon_0, \epsilon_1) = (0,1)$ if $D_0$ does not click and $D_1$ clicks, $(\epsilon_0, \epsilon_1) = (0,0)$ if no detector clicks, and $(\epsilon_0, \epsilon_1) = (1,1)$ if both detectors click.

Independently of whether Alice is honest or not, we define $P_{\text{det}}(\epsilon_0, \epsilon_1 | \beta, \rho, k)$ and $P_{\text{report}}(m | \beta, \rho, k)$ to be the
probabilities that a detection event \((c_0, c_1) \in \{0, 1\}^2\) occurs, and that Bob reports to Alice the message \(m \in \{0, 1\}\) when Alice sends Bob a pulse of \(k\) photons encoding the state \(\rho\) and Bob measures in the basis \(B_\beta\), respectively, for \((c_0, c_1, m, \beta) \in \{0, 1\}\) and \(k \in \{0, 1, 2, \ldots\}\). We define \(P_{\text{det}}(c_0, c_1 | \beta) = \sum_{k=0}^{\infty} p_k P_{\text{det}}(c_0, c_1 | \beta, \rho, k)\), for \((c_0, c_1, \beta) \in \{0, 1\}\), when Alice and Bob follow the protocol honestly.

C. Bob’s reporting strategies and Alice’s multi-photon attacks

Tables II–III summarize the multi-photon attacks, the main suggested countermeasures against them, and the reporting strategies discussed below, as well as the application of multiphoton attacks to previous experimental demonstrations of mistrustful quantum cryptography.

1. Reporting only single clicks

We define reporting strategy I by \(m = 1\) if \((c_0, c_1) \in \{(1, 0), (0, 1)\}\), and \(m = 0\) otherwise. This might seem a natural strategy. However, as Liu et al. discuss [14], if Bob uses reporting strategy I, Alice can gain information about \(\beta\) with the following attack, which we call multiphoton attack I.

To illustrate this attack, consider a setup in which Alice’s polarization preparation devices and Bob’s polarizers are precisely aligned. Alice sends a pulse with a large number of photons \(k\) in the same polarization state chosen from \(S\); for example, \(\rho = |\psi_0\rangle \langle \psi_0| \otimes k\). If Bob measures the pulse in the basis \(B_0\) then the detection event \((c_0, c_1) = (1, 0)\) occurs with high probability, giving \(m = 1\). If Bob measures in the basis \(B_1\) then the detection event \((c_0, c_1) = (1, 1)\) occurs with high probability, giving \(m = 0\). Thus, given \(m\), Alice can learn \(\beta\) with high probability.

In a different version of attack I, Alice’s pulse is prepared with a coherent source with average photon number \(\mu >> 1\). We show below (see Methods) that in this case, if \(B_0\) and \(B_1\) are the computational and Hadamard bases, Bob’s detectors have equal efficiencies \(\eta \in (0, 1)\) and zero dark count probabilities, then Alice’s probability \(P_{\text{guess}}^{\text{cs}}(\mu)\) to guess Bob’s bit \(\beta\) as a function of \(\mu\) is given by

\[
P_{\text{guess}}^{\text{cs}}(\mu) = 1 - \frac{1}{2} \left(2e^{-\mu \eta} - e^{-\mu \eta} \right).
\]

When the devices are closely but not precisely aligned, Alice can still learn significant information about \(\beta\) from \(m\) with an appropriate choice of \(k\) or \(\mu\). An experimental simulation of this attack is presented below (see Methods). The results are given in Fig. 2 and show that Alice’s probability to guess Bob’s bit \(\beta\) is very well approximated by (4), and can be very close to unity if \(\mu\) is sufficiently large. Different versions of attack I apply to the experimental protocols of Refs. [13, 30, 60, 61] if they are implemented with Bob using reporting strategy I (see Appendix [13]).

We note that multi-photon attack I still applies in a variation of reporting strategy I in which Bob also sets \(m = 1\) with some non-zero but small probability when \((c_0, c_1) = (1, 1)\), i.e. when there is a double click.

2. Reporting if at least one detector clicks

A better reporting strategy is to set \(m = 1\) if at least one detector clicks and \(m = 0\) if no detector clicks. We call this reporting strategy II.

This reporting strategy has been considered in quantum key distribution: squashing models map a multiphoton quantum state to a single-photon state by randomly assigning the measurement outcome of a double click to a single click [68]. This reporting strategy has also been implemented in the experimental demonstrations of mistrustful quantum cryptography of Refs.
As the following lemma shows, if Bob’s detectors have exactly equal efficiencies and their dark count probabilities are independent of his measurement basis, Alice cannot learn any information about $\beta$ from the message $m$. See Appendix D for proofs of the lemmas and theorem.

**Lemma 1.** Suppose that $\eta_{\beta} = \eta$ and $d_{i\beta} = d_i$, for $i, \beta \in \{0, 1\}$. If Bob uses reporting strategy II, then for an arbitrary quantum state $\rho$ encoded in a pulse of $k$ photons that Alice sends Bob, and for arbitrary qubit orthogonal bases $B_0$ and $B_1$, it holds that

$$P_{\text{report}}(1|\beta, \rho, k) = 1 - (1 - d_0)(1 - d_1)(1 - \eta)^k,$$

for $\beta \in \{0, 1\}$ and $k \in \{0, 1, 2, \ldots\}$.

In practice, Bob cannot guarantee that the efficiencies of his detectors are exactly equal. In this general case, the detection probabilities $P_{\text{det}}(c_0, c_1|\beta, \rho, k)$ depend nontrivially on $\beta$, as illustrated in Lemma 2 (see Methods). We call multi-photon attack II any strategy implemented by Alice that allows her to exploit the difference of Bob’s detection efficiencies to obtain information about $\beta$, when Bob reports double clicks with unit probability, as in reporting strategy II, or with high probability. Particularly, in this attack, we assume that Alice knows the efficiencies of Bob’s detectors and can control the number of photons and the states of her pulses. For example, in an extension of the task to $N \gg 1$ pulses in which Bob measures all pulses in the basis $B_0$ or in the basis $B_1$, Alice can prepare a subset of pulses in specific states and with specific number of photons to maximize her probability to guess $\beta$ from Bob’s messages reporting whether these pulses produced successful measurements or not. This and other versions of this attack apply (for example) to the experimental demonstrations of Refs. 13, 29.

In Appendix D we discuss how multi-photon attacks I and II apply to some experimental demonstrations of mistrustful quantum cryptography. We summarize this in Table II below.

We show below that there is no reporting strategy using setup I that guarantees perfect security against Alice when the detection efficiencies are different. However, we derive in Appendix B an upper bound on the amount of information that Alice can learn about $\beta$ from Bob’s message $m$, which approaches zero when the difference of the detection efficiencies tends to zero.

### 3. Symmetrization of losses

The symmetrization of losses strategy was introduced in Ref. 60 as follows. Bob tests his setup by preparing and measuring states as in the practical protocol, a large number of times $N$ in parallel. Then, for $c, \beta \in \{0, 1\}$, Bob computes the frequency $F_{\text{det}}(c, \bar{c}|\beta)$ of detection events $(c, \bar{c})$, which provides a good estimate of the probability $P_{\text{det}}(c, \bar{c}|\beta)$ if $N F_{\text{det}}(c, \bar{c}|\beta) > 1$. Bob then computes the numbers $S_{c0\beta} \in (0, 1]$ satisfying

$$S_{c0\beta} F_{\text{det}}(c, \bar{c}|\beta) = F_{\text{det}}^{\min},$$

for $c, \beta \in \{0, 1\}$, where

$$F_{\text{det}}^{\min} = \min_{c, \beta \in \{0, 1\}} \{F_{\text{det}}(c, \bar{c}|\beta)\}.$$

Then, in the implementation of the protocol with Alice, Bob reports a detection event $(c, \bar{c})$ with probability $S_{c0\beta}$, for $c, \beta \in \{0, 1\}$. Ref. 60 explicitly states that the detection events $(0, 0)$ and $(1, 1)$ are not reported by Bob, for $\beta \in \{0, 1\}$.

Symmetrization of losses aims to effectively make the detection probabilities of Bob’s detectors equal. As shown below in Lemma 2 a more precise definition of this strategy (reporting strategy III), achieves this if Alice’s pulse has zero or one photons. However, dishonest Alice can send Bob a pulse with an arbitrary number of photons $k$. Because the detection probabilities are not linear functions of $k$ (see Methods), and Bob does not know $k$, symmetrization of losses fails in effectively making the detection probabilities of Bob’s detectors equal. This is proved by Theorem 4 below.

Symmetrization of losses has been implemented in at least four experimental demonstrations of mistrustful quantum cryptography protocols 13, 30, 60, 61. These implementations used setups and protocols that are slight variations of ours. We discuss them, and show that they are vulnerable to multi-photon attacks by Alice, in Appendix D.

4. Generalization of symmetrization of losses to double click events

In this paper, we introduce the following generalization of symmetrization of losses and call it reporting strategy III. Let $\eta_{\min} = \min\{\eta_{00}, \eta_{01}, \eta_{10}, \eta_{11}\}$. If Bob obtains a detection event $(c_0, c_1)$, he sets $m = 1$ with probability $S_{c_0c_1\beta}$, for $c_0, c_1, \beta \in \{0, 1\}$, where

$$S_{00\beta} = 0,$$

$$S_{11\beta} \in [0, 1],$$

$$S_{01\beta} = \frac{\eta_{\min}}{\eta_{\beta}},$$

$$S_{10\beta} = \frac{\eta_{\min}}{\eta_{\beta}},$$

for $\beta \in \{0, 1\}$. Note that Bob needs to know the efficiencies of his detectors to apply this reporting strategy and that the choices of $S_{11\beta}$ and $S_{11\beta}$ are left free.

As the following lemma shows, this reporting strategy guarantees that Alice cannot obtain any information about $\beta$ if Alice’s pulse does not have more than one photon and $d_{i\beta} = 0$, for arbitrary $\eta_{\beta} \in (0, 1)$ and for $i, \beta \in \{0, 1\}$. Furthermore, it guarantees that Alice cannot obtain much information about $\beta$ if Alice’s pulse does not have more than one photon and $0 < d_{i\beta} \leq \delta$, for $0 < \delta << 1$ and $i, \beta \in \{0, 1\}$. 


| Reference | Task                                                  | Setup | Reports multiple clicks? | Covered against attack I? | Covered against attack II? |
|-----------|------------------------------------------------------|-------|--------------------------|---------------------------|---------------------------|
| [14]      | Relativistic quantum bit commitment                  | I     | Yes                      | Yes                       | No                        |
| [13]      | Relativistic quantum bit commitment                  | I     | Does not say             | Yes (no) if double clicks are (are not) reported | No                        |
| [30]      | Quantum coin flipping                                | I     | Does not say             | No, even if double clicks are reported                   | –                         |
| [61]      | Quantum 1-out-of-2 oblivious transfer in the noisy storage model | II    | Does not say             | Yes (no) if multiple clicks are (are not) reported       | –                         |
| [60]      | Quantum bit commitment in the noisy storage model    | II    | No                       | No                        | –                         |

TABLE I. Application of multi-photon attacks I and II to experimental demonstrations of mistrustful quantum cryptography. The multi-photon attacks I and II are briefly described in the main text. The table indicates whether the protocols of Refs. [13, 14, 30, 60, 61] are covered against variations of these attacks, which are discussed in detail in Appendix D. Setup I is described in Fig. 1 while setup II is a variation of Setup I with four detectors, which is described in Appendix D.1. Dashes indicate that further analysis is required to show how (or whether) attack II applies.

Lemma 2. Let $d_{i\beta} \leq \delta$, for some $0 \leq \delta < 1$ and for $i, \beta \in \{0,1\}$. Consider the practical protocol with $p_0 + p_1 = 1$ in which Alice sends Bob a single photon pulse ($k = 1$) in arbitrary qubit state $\rho$ or an empty pulse ($k = 0$). Suppose that Bob applies reporting strategy $III$. Then

$$|P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k)| \leq B_{III}^k,$$

for $k \in \{0,1\}$, where

$$B_{III}^0 = 2\delta,$$

$$B_{III}^1 = 6\delta + 2\delta^2 + S_{\text{max}}^{11}(5\delta + \delta^2),$$

and where $S_{\text{max}}^{11} = \max\{S_{110}, S_{111}\}$.

5. Probabilistic reporting strategies

In this paper, we introduce probabilistic reporting strategies, which generalize the reporting strategies considered above. If a detection event $(c_0, c_1)$ occurs when Bob measures in the basis $B_\beta$, Bob reports the message $m = 1$ to Alice with some probability $S_{c_0c_1\beta}$, for $c_0, c_1, \beta \in \{0,1\}$. Thus, if Alice sends Bob a pulse of $k$ photons encoding a state $\rho$ and Bob measures in the basis $B_\beta$, the probability that Bob reports the message $m = 1$ is given by

$$P_{\text{report}}(1|\beta, \rho, k) = \sum_{c_0=0}^1 \sum_{c_1=0}^1 S_{c_0c_1\beta} P_{\text{det}}(c_0, c_1|\beta, \rho, k),$$

for $\beta \in \{0,1\}$ and $k \in \{0,1,2,\ldots\}$. Note that the previous strategies, including symmetrization of losses, are special cases of probabilistic reporting strategies.

We define a trivial strategy as a probabilistic reporting strategy satisfying

$$S_{c_0c_1\beta} = S,$$

for $c_0, c_1, \beta \in \{0,1\}$ and for some $S \in \{0,1\}$: we exclude $S = 0$, which implies that Bob never reports a successful measurement. A trivial strategy guarantees to Bob that Alice cannot learn any information about $\beta$ from his message $m$. Indeed, if (12) holds then from (11) we have

$$P_{\text{report}}(1|\beta, \rho, k) = S \sum_{c_0=0}^1 \sum_{c_1=0}^1 P_{\text{det}}(c_0, c_1|\beta, \rho, k)$$

$$= S,$$

for $\beta \in \{0,1\}$, for any $k$-qubit state $\rho$ and for any $k \in \{0,1,2,\ldots\}$.

If Bob uses a trivial strategy, he may as well take $S = 1$, sending $m = 1$ to Alice with unit probability. As shown in Appendix A this satisfies the correctness properties [2] and [3] if losses are low and Bob’s detectors have high efficiency. However, a trivial strategy cannot satisfy [2] and [3] for a class of common experimental setups (see details in Appendix A).

In the following theorem we show that the only probabilistic reporting strategy with setup I guaranteeing to Bob perfect security against Alice is the trivial strategy [12]. This is shown explicitly for the BB84 case and numerically for the case of general bases. It follows that symmetrization of losses, being a particular probabilistic reporting strategy, does not guarantee security against Alice.

**Theorem 1.** Suppose that

$$d_{i\beta} = 0,$$

$$\eta_{i\beta} = \eta_i \in (0,1),$$

$$\eta_0 \neq \eta_i,$$

for $i, \beta \in \{0,1\}$, and $B_0$ and $B_1$ are arbitrary distinct qubit orthogonal bases. If Alice sends Bob a pulse of $k$ photons encoding a state $\rho$, with $k \in \{0,1,2\}$ chosen by Alice and unknown to Bob, then the only probabilistic reporting strategy that guarantees to Bob that Alice cannot
obtain any information about β from his message m is the trivial strategy \((T_2)\).

D. Discussion

We have highlighted known, and introduced new, attacks on photonic implementations of mistrustful quantum cryptographic protocols. These arise because Alice may send multi-photon pulses that are different from the single photon pulses envisaged in the ideal versions of the protocols and that give her statistically distinguishable results when Bob uses standard detectors. The attacks are hard to detect with standard technology, since there is no practical perfectly reliable way to distinguish a multi-photon pulse from a single photon one. They are also hard to counter by filtering, since there is no practical perfectly reliable way to filter multi-photon pulses to produce single photon outputs with the same polarization.

Lemma \(I\) suggests that a possible countermeasure against multi-photon attacks is to make the efficiencies of Bob’s detectors as close as possible. Bob could use attenuators for this purpose; but care should be taken to guarantee that these act linearly, i.e. that their action on multi-photon states is given by the product of their action on individual photons, and that their action does not depend on wavelength or other degrees of freedom that Alice could exploit to her advantage, as in the side-channel attacks discussed below. We have investigated this possibility in Appendix \(B\) by deriving security bounds when Bob applies reporting strategies II or III that provide perfect security against multi-photon attacks in the limit that the difference of the detector efficiencies equals zero (see Lemmas \(J\)–\(L\) in Appendix \(B\)). However, as discussed in Appendix \(B\) our security bounds are not useful in practical settings unless this difference is extremely small. We leave as an open problem to investigate whether this countermeasure can provide useful security guarantees against multi-photon attacks in practice.

We have focused here on the simple experimental setup of Fig. \(1\) with two detectors. However, our analyses can be extended to more general setups with more detectors. In Appendix \(D\) we have investigated a setup with two detectors, setup II, (see Fig. \(E\) in Appendix \(D\)) and leave the extension of Theorem \(I\) to this setup as an open problem.

Although there exist photon-number-resolving detectors (see e.g. Ref. \(65\) and references therein), to our knowledge, they cannot practically determine the number of photons \(k\) in a pulse, for arbitrary \(k\). Nevertheless, we think it is worth investigating their use as a countermeasure against multi-photon attacks.

In addition to the degrees of freedom of the photon pulses, like polarization, on which Alice and Bob agreed that Alice would encode the quantum states, Alice may control further degrees of freedom of the photon pulses to her advantage, giving rise to various side-channel attacks previously considered in the literature of quantum key distribution, which can be straightforwardly adapted to mistrustful quantum cryptography. These degrees of freedom may include, for example, the light reflected from Bob’s setup to Alice’s setup in Trojan-horse attacks \(1\); the time at which the pulse is sent, the pulse wavelength, polarization, spatial degrees of freedom like angle of incidence, etc. in the detection-efficiency-mismatch attacks \(2, 4\); the arrival time of the pulse in the time-shift attacks \(3\); the intensity of the pulse in the blinding \(5\) and bright-illumination \(6\) attacks; the time separation between consecutive pulses in the dead-time attacks \(1\); and the mean photon number \(7\).

More generally, in a side-channel attack, Alice may send any system \(S\) in place of the expected photon pulse. For example, \(S\) could be a different type of elementary particle, or some more complex system. It is hard to make any general statement about the resulting measurement statistics at Bob’s detectors. At the more exotic end of the range of possibilities, one can imagine \(7\) Alice sending through the quantum channel miniaturised robots that are programmed to analyse the measurement settings and to trigger detections following statistics of Alice’s choice. Although this last possibility may perhaps seem unrealistic, the limitation is ultimately technological, meaning that a security proof that excludes such cases cannot strictly be said to guarantee unconditional security \(7\). Even if Alice is restricted to photons or particles of small mass, it would be very hard for Bob to analyse all the possible detector statistics and the scope they offer for side-channel attacks.

The only countermeasure of which we are aware that provides unconditional security, in principle, is for Bob to filter Alice’s signals via teleportation, as suggested in another context by Lo-Chau \(70\). Indeed, if Bob teleports the quantum state encoded in each pulse sent by Alice to a photon entering his setup, using an ideal teleportation device, he is guaranteed that his setup does not receive anything else than a single photon. Thus, if Bob applies reporting strategy III, he is guaranteed from Lemma \(2\) that Alice can get negligible information about his bit \(β\) when the dark count probabilities of his detectors are very small. In practice, when preparing pairs of entangled photons with parametric down conversion, there is a small but nonzero probability of produc-
| Multi-photon attack | Applies if | Proposed countermeasures |
|---------------------|------------|--------------------------|
| I                   | $S_{11\beta} = 0$ or $S_{11\beta}$ is small enough | Reporting double clicks with unit or high probability, i.e. setting $S_{11\beta} \approx 1$; or, using the trivial reporting strategy if consistent with experimental parameters |
| II                  | $S_{11\beta} = 1$ or $S_{11\beta}$ is large enough and Bob’s detection efficiencies are different, or not close enough | Making Bob’s detection efficiencies exactly equal, or sufficiently close; alternatively, using the trivial reporting strategy if consistent with experimental parameters |

**TABLE II. Summary of multi-photon attacks I and II.** The multi-photon attacks I and II are briefly described in the main text. The table indicates for which parameters $S_{11\beta}$ of the probabilistic reporting strategies introduced in the main text the attacks apply and the main proposed countermeasures discussed in the main text. The value of $\beta$ runs over $\{0,1\}$.

| Reporting strategy | Definition | Brief description and comments | Considered before? | Subject to attack I? | Subject to attack II? | Known security guarantees for Bob |
|--------------------|------------|--------------------------------|--------------------|---------------------|----------------------|--------------------------------|
| I                  | $S_{00\beta} = S_{11\beta} = 0$, $S_{01\beta} = S_{10\beta} = 1$ | Bob only reports single clicks | Yes | Yes | No | None |
| II                 | $S_{00\beta} = 0$, $S_{01\beta} = 1$, $S_{10\beta} = 1$, $S_{11\beta} = 1$ | Bob reports single and double clicks | Yes (e.g. in Refs. \[14, 29\]) | No | Yes, if Bob’s detection efficiencies are different | Good security if Bob guarantees receiving only pulses with zero or one photons and having small dark count probabilities (see Lemma \[1\]) |
| III                | $S_{00\beta} = 0$, $S_{01\beta} = \frac{m_{\text{min}}}{\eta}$, $S_{10\beta} = \frac{m_{\text{min}}}{\eta}$, $S_{11\beta} \in [0,1]$ | Defined by \[8\] | No, case $S_{11\beta} > 0$ introduced here | Yes, if $S_{11\beta}$ is small enough | Yes, if $S_{11\beta}$ is large enough | See reporting strategy III |
| Symmetrization of losses | Ideally defined as special case of reporting strategy III with $S_{11\beta} = 0$, but precisely defined by \[6\] and \[7\] | It aims to symmetrize the detection probabilities of Bob’s detectors, but fails in general (see Theorem \[1\]) | Yes | No | See reporting strategy III |
| Trivial            | $S_{00\beta} = S$, $S_{01\beta} = S$, $S_{10\beta} = S$, $S_{11\beta} = S$, $S \in (0,1]$ | Bob reports all detection events with the same probability $S$; where normally $S = 1$, but we allow $S \in (0,1]$ | Yes, in ideal protocols without losses, for example | No | No | It is the only known reporting strategy that guarantees Bob perfect security against arbitrary multi-photon attacks (see Theorem \[1\]), but is not compatible with the correctness criteria \[2\] and \[3\] for common experimental setups (see details in Appendix \[A\]) |
| Probabilistic      | $S_{0c_1\beta} \in [0,1]$ for $(c_0, c_1) \in \{0,1\}^2$ | Includes as special cases the reporting strategies discussed above | No, the general case was introduced here | Yes, if $S_{11\beta}$ is small enough | Yes, if $S_{11\beta}$ is large enough | See previous reporting strategies |

**TABLE III. Summary of reporting strategies discussed in the main text and their relationships with multi-photon attacks I and II.** In the table, $S_{0c_1\beta}$ indicates that Bob sends Alice the message $m = 1$ with probability $S_{0c_1\beta}$ if the pulse received from her activates a detection event $(c_0, c_1) \in \{0,1\}^2$, or $m = 0$ otherwise, when he applies the measurement $B_\beta$, where $c_i = 1$ $(c_i = 0)$ indicates that the detector $D_i$ clicks (does not click), for $i \in \{0,1\}$ (see setup I illustrated in Fig. \[1\]). The value of $\beta$ runs over $\{0,1\}$. 

References: [14, 29, 13, 30, 60, 61, 60, 61].
Suppose that Alice sends Bob a pulse of photons. Thus, in practice Bob cannot guarantee that pulses with more than one photon do not enter his setup. Although the quantum states of the multi-photon pulses entering Bob’s setup with this countermeasure are out of Alice’s control, Bob must guarantee that Alice cannot exploit this imperfection to learn some information about \( \beta \). We believe this countermeasure deserves further investigation.

We conclude that implementations of theoretically unconditionally secure mistrustful cryptographic protocols need, at least, very careful analysis of practical possibilities for attacks of the type described. We hope our analyses of multi-photon and side-channel attacks will serve as cautionary examples and stimulate further investigations.

## II. METHODS

### A. Detection probabilities in multi-photon attacks

**Lemma 3.** Suppose that Alice sends Bob a pulse of \( k \) photons, each encoding a qubit state \( \rho_{\text{qubit}} \). That is, the state encoded by the pulse is \( \rho = \rho_{\text{qubit}}^\otimes k \). We define

\[
q_\beta = \langle \psi_{0\beta} | \rho_{\text{qubit}} | \psi_{0\beta} \rangle,
\]

for \( \beta \in \{0, 1\} \). Then

\[
P_{\text{det}}(0, 0|\beta, \rho, k) = (1 - d_{0\beta})(1 - d_{1\beta}) \left[ q_\beta (1 - \eta_{0\beta}) + (1 - q_\beta)(1 - \eta_{1\beta}) \right]^k,
\]

\[
P_{\text{det}}(0, 1|\beta, \rho, k) = (1 - d_{0\beta})(1 - q_\beta \eta_{0\beta})^k - (1 - d_{0\beta})(1 - d_{1\beta}) \left[ q_\beta (1 - \eta_{0\beta}) + (1 - q_\beta)(1 - \eta_{1\beta}) \right]^k,
\]

\[
P_{\text{det}}(1, 0|\beta, \rho, k) = (1 - d_{1\beta})(1 - (1 - q_\beta) \eta_{1\beta})^k - (1 - d_{0\beta})(1 - d_{1\beta}) \left[ q_\beta (1 - \eta_{0\beta}) + (1 - q_\beta)(1 - \eta_{1\beta}) \right]^k,
\]

\[
P_{\text{det}}(1, 1|\beta, \rho, k) = 1 + (1 - d_{0\beta})(1 - d_{1\beta}) \left[ q_\beta (1 - \eta_{0\beta}) + (1 - q_\beta)(1 - \eta_{1\beta}) \right]^k - (1 - d_{0\beta})(1 - q_\beta \eta_{0\beta})^k - (1 - d_{1\beta})(1 - (1 - q_\beta) \eta_{1\beta})^k,
\]

for \( \beta \in \{0, 1\} \) and \( k \in \{0, 1, 2 \ldots \} \). Now consider that Alice prepares a pulse of \( k \) photons with the probability distribution of a coherent source with average photon number \( \mu > 0 \), for \( k \in \{0, 1, 2 \ldots \} \). Then the probability \( P_{\text{det}}(c_0, c_1|\beta, \rho, \mu) \) of the detection event \( (c_0, c_1) \) is given by

\[
P_{\text{det}}^{cs}(0, 0|\beta, \rho, \mu) = (1 - d_{0\beta})(1 - d_{1\beta}) e^{-\mu \left[ q_{\beta} \eta_{0\beta} + (1 - q_{\beta}) \eta_{1\beta} \right]},
\]

\[
P_{\text{det}}^{cs}(0, 1|\beta, \rho, \mu) = (1 - d_{0\beta}) e^{-\mu q_{\beta} \eta_{0\beta}} - (1 - d_{0\beta})(1 - d_{1\beta}) e^{-\mu \left[ q_{\beta} \eta_{0\beta} + (1 - q_{\beta}) \eta_{1\beta} \right]},
\]

\[
P_{\text{det}}^{cs}(1, 0|\beta, \rho, \mu) = (1 - d_{1\beta}) e^{-\mu (1 - q_{\beta}) \eta_{1\beta}} - (1 - d_{0\beta})(1 - d_{1\beta}) e^{-\mu \left[ q_{\beta} \eta_{0\beta} + (1 - q_{\beta}) \eta_{1\beta} \right]},
\]

\[
P_{\text{det}}^{cs}(1, 1|\beta, \rho, \mu) = 1 + (1 - d_{0\beta})(1 - d_{1\beta}) e^{-\mu \left[ q_{\beta} \eta_{0\beta} + (1 - q_{\beta}) \eta_{1\beta} \right]} - (1 - d_{0\beta}) e^{-\mu q_{\beta} \eta_{0\beta}} - (1 - d_{1\beta}) e^{-\mu (1 - q_{\beta}) \eta_{1\beta}},
\]

for \( c_0, c_1, \beta \in \{0, 1\} \) and \( \mu > 0 \).

**Proof.** Let \( k_0 \) be the number of photons that go to detector \( D_0 \). The number of photons that go to detector \( D_1 \) is \( k_1 = k - k_0 \).

As previously stated, in our model, the dark counts and each photo-detection are independent random events. It
follows straightforwardly from (17) that:

\[ P_{\text{det}}(0, 0|\beta, \rho, k) = (1 - d_{0\beta})(1 - d_{1\beta}) \sum_{k_0=0}^{k} \left[ (k_{0}) (q_{\beta})^{k_0} (1 - q_{\beta})^{k-k_0} \times \right. \\
\left. \times (1 - \eta_{0\beta})^{k_0} (1 - \eta_{1\beta})^{k-k_0} \right], \]

\[ P_{\text{det}}(0, 1|\beta, \rho, k) = \sum_{k_0=0}^{k} \left\{ (k_{0}) (q_{\beta})^{k_0} (1 - q_{\beta})^{k-k_0} \times \right. \\
\left. \times \left[ (1 - d_{0\beta})(1 - \eta_{0\beta})^{k_0} (1 - (1 - \eta_{1\beta})^{k-k_0}) \right. \\
\left. + d_{1\beta}(1 - d_{0\beta})(1 - \eta_{0\beta})^{k_0} (1 - \eta_{1\beta})^{k-k_0} \right] \right\}, \]

\[ P_{\text{det}}(1, 0|\beta, \rho, k) = \sum_{k_0=0}^{k} \left\{ (k_{0}) (q_{\beta})^{k_0} (1 - q_{\beta})^{k-k_0} \times \right. \\
\left. \times \left[ (1 - (1 - \eta_{0\beta})^{k_0} (1 - (1 - \eta_{1\beta})^{k-k_0}) \right. \\
\left. + d_{0\beta}(1 - (1 - \eta_{0\beta})^{k_0} (1 - \eta_{1\beta})^{k-k_0}) \right. \\
\left. + d_{0\beta}d_{1\beta}(1 - \eta_{0\beta})^{k_0} (1 - \eta_{1\beta})^{k-k_0} \right] \right\}, \]

(20)

for \( \beta \in \{0, 1\} \) and \( k \in \{0, 1, 2, \ldots\} \). Using the binomial theorem, (18) follows straightforwardly from (20), as claimed.

Now we suppose that Alice generates photon pulses with a coherent source of average photon number \( \mu \). The probability that a pulse has \( k \) photons is \( p_k = e^{-\mu}\frac{\mu^k}{k!} \), hence, the probability \( P_{\text{det}}^{\text{cs}}(c_0, c_1|\beta, \rho, \mu) \) that, for a pulse, the detector \( D_0 \) clicks if \( c_0 = 1 \) (does not click if \( c_0 = 0 \)) and the detector \( D_1 \) clicks if \( c_1 = 1 \) (does not click if \( c_1 = 0 \)) is given by

\[ P_{\text{det}}^{\text{cs}}(c_0, c_1|\beta, \rho, \mu) = \sum_{k=0}^{\infty} p_k P_{\text{det}}(c_0, c_1|\beta, \rho, k) = \sum_{k=0}^{\infty} \frac{e^{-\mu}\mu^k}{k!} P_{\text{det}}(c_0, c_1|\beta, \rho, k), \]

(21)

for \( c_0, c_1, \beta \in \{0, 1\} \) and \( \mu > 0 \). Thus, from (20) and (21), and using \( e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} \) for \( x > 0 \), we obtain (19), as claimed.

B. Experiment

1. Experimental evaluation of the detection probabilities in a multi-photon attack

We experimentally evaluated the validity of the theoretical predictions for the detection probabilities given by (19), in Lemma 3. For this, Alice prepared the state with vertical polarization using a weak coherent photon source and varied the average photon number \( \mu \). This polarization corresponds to a qubit state \( \rho_{\text{qubit}} = |0\rangle \langle 0| \), which has Bloch vector along the \( z \) axis, given by \( \vec{r} = (0, 0, 1) \). That is, as above, each pulse encodes in the polarization a \( k \)-qubit state \( \rho = \rho_{\text{qubit}}^k \), where \( k \) has a probability distribution \( p_k = \frac{e^{-\mu}\mu^k}{k!} \), for \( k \in \{0, 1, 2, \ldots\} \). For \( c_0, c_1, \beta \in \{0, 1\} \), we fixed Bob’s measurement basis to \( B_\beta \) and computed the frequency of the detection events \((c_0, c_1)\) for a large number of pulses \( N = 4 \times 10^6 \), estimating in this way the detection probability \( P_{\text{det}}^{\text{cs}}(c_0, c_1|\beta, \rho, \mu) \). As above, Bob’s measurement bases \( B_0 \) and \( B_1 \) are the computational and Hadamard bases, respectively.

In practice, this was done as follows. Pulses of 1 \( \mu \)s with vertical polarization were generated by Alice at a repetition rate of 200 kHz for 20 s using two fibered amplitude modulators connected in series. An unbalanced coupler was then used for power calibration in order to fix the value of \( \mu \). The estimated uncertainty for the coupler’s splitting ratio is \( \pm 5 \% \), and the uncertainty on the power measurement is also \( \pm 5 \% \) from the relevant data sheet. Combining these uncertainties in quadrature, this gives a total uncertainty on \( \mu \) of \( \pm 7 \% \). One arm transmitted the signal, while the other was sent to a photodiode to calibrate the power. Bob’s measurement basis was selected using a half wave plate, with angle uncertainty of \( \pm 0.25^\circ \), hence contributing with \( \pm 0.5^\circ \) and \( \pm 1^\circ \) uncertainties in the physical polarization angle and in the Bloch sphere angle, respectively. The polarization was then projected using a fibered polarization beam splitter, and detected with two id230 free-running avalanche detectors, at Bob’s site (see Fig. 1).

In Fig. 3, we have plotted the obtained experimental estimates of \( P_{\text{det}}^{\text{cs}}(c_0, c_1|\beta, \rho, \mu) \), for \( c_0, c_1, \beta \in \{0, 1\} \) and for various values of \( \mu \). Fig. 4 also shows the plots for the theoretical predictions given by (19). In our theoretical predictions, we assume that \( d_{i\beta} = 0 \) and \( \eta_{i\beta} = \eta \in (0, 1) \), for \( i, \beta \in \{0, 1\} \). We measured a value of \( \eta = 0.12 \). Note that this value includes Bob’s detection efficiencies and the probability of loss in the quantum channel. Using the definition (17), we have that \( q_0 = \langle 0|\rho_{\text{qubit}}|0\rangle = \frac{1}{2}(1 + r_x) \) and \( q_1 = \langle +|\rho_{\text{qubit}}|+\rangle = \frac{1}{2}(1 + r_x) \), where \( r_x \) and \( r_z \) are the \( z \) and \( x \) components of the Bloch vector \( \vec{r} \), and where \( |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \). Thus, we have \( q_0 = 1 \) and \( q_1 = \frac{1}{2} \). By substituting these values in (19), we obtain
The uncertainty bars are so small that they are unnoticeable and lie within the corresponding markers.

FIG. 3. Detection probabilities. We plot the experimental estimates obtained for the detection probabilities $P_{\text{det}}(c_0,c_1|\beta,\rho,\mu)$, indicated with the labels “$P(01|c_0,c_1)$ exp”, and their theoretical predictions given by (22), indicated with the labels “$P(c_0,c_1)$ theo”, with $\eta = 0.12$, for various values of the average photon number $\mu$, for the qubit state $\rho_{\text{qubit}} = |0\rangle\langle 0|$, and for $c_0,c_1,\beta \in \{0,1\}$. The horizontal and vertical uncertainty bars are included. The vertical uncertainty bars are so small that they are unnoticeable and lie within the corresponding markers.

the plotted theoretical curves. These are given by

$$
\begin{align*}
P_{\text{det}}^{cs}(0,0|\beta,\rho,\mu) &= e^{-\mu\eta}, \\
P_{\text{det}}^{cs}(0,1|0,\rho,\mu) &= 0, \\
P_{\text{det}}^{cs}(1,0|0,\rho,\mu) &= 1 - e^{-\mu\eta}, \\
P_{\text{det}}^{cs}(1,1|0,\rho,\mu) &= 0, \\
P_{\text{det}}^{cs}(c,\bar{c}|1,\rho,\mu) &= e^{-\mu\frac{\bar{c}}{\beta}} - e^{-\mu\eta}, \\
P_{\text{det}}^{cs}(1,1|1,\rho,\mu) &= 1 + e^{-\mu\eta} - 2e^{-\mu\frac{\bar{c}}{\beta}},
\end{align*}
$$

(22)

for $\beta,\bar{c} \in \{0,1\}$. In Fig. 3 we observe a good agreement between the experimental estimates of the detection probabilities $P_{\text{det}}^{cs}(c_0,c_1|\beta,\rho,\mu)$ and the theoretical predictions given by (22), for $c_0,c_1,\beta \in \{0,1\}$. The slight disagreements observed for a few experimental points with the theoretical predictions of (22) are possibly explained by the uncertainties on some experimental quantities, like the detection efficiency and the measurement bases, for instance, in addition to the uncertainties on the average photon number $\mu$ given by the horizontal uncertainty bars.

2. Experimental simulation of multi-photon attack I

We illustrate a version of multi-photon attack I in which Alice sends Bob a photon pulse prepared with a coherent source, with average photon number $\mu >> 1$ chosen by Alice. We assume that Bob applies reporting strategy I, i.e. he only sets valid measurement outcomes, and sends Alice the message $m = 1$, for pulses that generate a click in only one of his detectors. We consider the case that $B_0$ and $B_1$ are the computational and Hadamard bases, respectively. Each photon in the pulse encodes a qubit state

$$
|\psi_{\text{m}}\rangle = \begin{cases} 
|0\rangle & \text{if } q_0 = 1 \text{ and } q_1 = \frac{1}{2}, \\
|1\rangle & \text{if } q_0 = 1 \text{ and } q_1 = \frac{1}{2}, \end{cases}
$$

in (17). If Bob sends Alice the message $m = 1$, Alice guesses that $\beta = 0$. If Bob sends $m = 0$, Alice guesses that $\beta = 1$. Thus, since we suppose that Bob generates $\beta$ randomly, Alice’s probability $P_{\text{guess}}^{cs}(\mu)$ to guess Bob’s bit $\beta$ in this attack is given by

$$
P_{\text{guess}}^{cs}(\mu) = \frac{1}{2} \left[ P_{\text{det}}^{cs}(1,0|0,\rho,\mu) + P_{\text{det}}^{cs}(0,1|0,\rho,\mu) \right]
+ P_{\text{det}}^{cs}(0,0|1,\rho,\mu) + P_{\text{det}}^{cs}(1,1|1,\rho,\mu),
$$

(23)

where $P_{\text{det}}^{cs}(c_0,c_1|\beta,\rho,\mu)$ is given by (19), for $c_0,c_1,\beta \in \{0,1\}$, and where $q_0 = 1$ and $q_1 = \frac{2}{3}$. In the simple case that $d_\beta = 0$ and $\eta_\beta = \eta \in (0,1)$, for $i,\beta \in \{0,1\}$, and $q_0 = 1$ and $q_1 = \frac{2}{3}$, (19) reduces to (22). Thus, from (22) and (23), we obtain (14).

We implemented an experimental simulation of the multi-photon attack described above. In our simulation, Alice and Bob use setup I illustrated in Fig. 1. Alice’s photon source is a coherent source with average photon number $\mu$. Bob measures the polarization of the pulse in
the basis $\mathcal{B}_0$ or in the basis $\mathcal{B}_1$, which are the horizontal-vertical polarization basis and the diagonal-diagonal basis (corresponding to polarization angle of $45^\circ$ and $-45^\circ$ from the horizontal axis towards the vertical axis), respectively. In the Bloch sphere, these are the computational and Hadamard bases, respectively.

Alice sets the value of $\mu$ and sends Bob photon pulses with the same polarization, in vertical polarization, corresponding to the qubits state $|0\rangle$. That is, each pulse encodes in the polarization a $k$-qubit state $\rho = \rho_{\text{qubit}}$, where $\rho_{\text{qubit}} = |0\rangle \langle 0|$, and where $k$ has a probability distribution $p_k = \frac{\epsilon}{e_k}$, for $k \in \{0,1,2,\ldots\}$. For $c_0, c_1, \beta \in \{0,1\}$, we fix Bob’s measurement basis to $\mathcal{B}_1$ and compute the frequency of the detection events $(c_0,c_1)$ for a large number of pulses $N$, estimating experimentally in this way the value of the detection probability $P_{\det}^{cs}(c_0,c_1|\beta,\rho,\mu)$. Alice’s probability $P_{\text{guess}}^{cs}(\mu)$ from (23) is used to guess Bob’s bit $\beta$ in the considered attack.

We have obtained the plotted experimental estimates of $P_{\text{guess}}^{cs}(\mu)$ for various values of $\mu$ in Fig. 2. In practice, the experimental data plotted in Fig. 4 corresponds to the same experimental data plotted in Fig. 3 but using (24). As follows from (29), computing $P_{\text{guess}}^{cs}(\mu)$ requires some probabilities $P_{\text{guess}}^{cs}(c_0,c_1|\beta,\rho,\mu)$ with both values of $\beta \in \{0,1\}$. Because in our experimental points the plots in Fig. 6 for different value of $\beta \in \{0,1\}$, the values of the average photon number are close but not exactly equal, we obtain each point in the experimental plot of Fig. 2 by taking $\mu$ as the average $\mu = \frac{\mu_i + \mu_j}{2}$, where $\mu_i$ is the value of the average photon number for the corresponding experimental point in the plot of Fig. 3 with $\beta = i$, for $i \in \{0,1\}$. As explained above, the experimental uncertainty for each value of $\mu_i$ is $7\%$, for $i \in \{0,1\}$. The uncertainty for each value of $\mu$ in the experimental plot of Fig. 2 is obtained by combining in quadrature the uncertainties for the corresponding values of $\mu_0$ and $\mu_1$ given in the experimental plots of Fig. 6. The theoretical prediction for $P_{\text{guess}}^{cs}(\mu)$ given by (4) is also shown in Fig. 2 for comparison with the experimental data. A good agreement between the experimental data and the theoretical prediction is observed. As mentioned for the plots of Fig. 6 the slight disagreements observed for a few experimental points in the plot of Fig. 2 with the theoretical predictions of (11) are expected due to the uncertainties on some experimental quantities, like the detection efficiency and the measurement bases, for example, in addition to the uncertainties on the average photon number $\mu$ given by the horizontal uncertainty bars.

C. Statistical Information

The number of photon pulses used for estimating the probabilities $P_{\text{det}}^{cs}(c_0,c_1|\beta,\rho,\mu)$ plotted in Fig. 8 and the probability $P_{\text{guess}}^{cs}(\mu)$ plotted in Fig. 2 for each value of the average photon number $\mu$ was $N = 4 \times 10^6$, for $c_0, c_1, \beta \in \{0,1\}$. The uncertainty for each experimental estimate of the probabilities $P_{\text{det}}^{cs}(c_0,c_1|\beta,\rho,\mu)$ plotted in Fig. 8 was taken as the standard error, given by

$$\Delta P = \sqrt{\frac{P(1-P)}{N}},$$

where $P$ is the obtained experimental estimate of the probability $P_{\text{det}}^{cs}(c_0,c_1|\beta,\rho,\mu)$, for $c_0, c_1, \beta \in \{0,1\}$ and for each value of $\mu$. The uncertainty for each experimental estimate of the probabilities $P_{\text{guess}}^{cs}(\mu)$ plotted in Fig. 2 was obtained using (23) and (24), combining in quadrature the uncertainties of the experimental estimates for the probabilities $P_{\text{det}}^{cs}(c_0,c_1|\beta,\rho,\mu)$ appearing in (23).

ACKNOWLEDGMENTS

M.B., A.C. and E.D. acknowledge financial support from the French National Research Agency (ANR) project quBIC. A.K. and D.P.G. acknowledge financial support from the UK Quantum Communications Hub grants no. EP/M013472/1 and EP/T001011/1. A.K. is partially supported by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation.

Author contributions

D.P.G. conceived the project. D.P.G. did the majority of the theoretical work, with input from A.K. M.B., A.C., E.D. and D.P.G. conceived the experiment. M.B. and A.C. constructed the experimental setup and took the experimental data. D.P.G. analysed the experimental data with input from M.B. and A.C. A.K. and D.P.G. wrote the manuscript with input from M.B., A.C. and E.D.

Appendix A: The trivial reporting strategy and the correctness properties

Lemma 4. Let Alice and Bob implement the practical protocol. Let $P_{\text{error}|c,c,\beta}$ be the probability that Bob obtains the wrong measurement outcome when he measures in the basis $\mathcal{B}_2$ of preparation by Alice and obtains a detection event $(c_0,c_1)$, for $c_0,c_1, \beta \in \{0,1\}$. If the photon pulse produces a detection event $(c,c)$, Bob assigns a random measurement outcome, which we assume gives a wrong outcome with some probability $P_{\text{error}|c,c,\beta}$ such that $\frac{1}{2} - \delta_{\text{error}}^{\text{equal}} \leq P_{\text{error}|c,c,\beta} \leq \frac{1}{2} + \delta_{\text{error}}^{\text{equal}}$, for a small $\delta_{\text{error}}^{\text{equal}} > 0$ and for $c, \beta \in \{0,1\}$. We assume that $P_{\text{error}|c,\beta} \leq \delta_{\text{error}}^{\text{diff}}$, for a small $\delta_{\text{error}}^{\text{diff}} > 0$ and for $c, \beta \in \{0,1\}$. Let $P_{\text{det}}^{cs}(c_0,c_1|\beta)$ be the probability that the pulse sent by Alice produces a detection event $(c_0,c_1)$ in Bob’s detectors when Bob measures in the basis $\mathcal{B}_3$, for $c_0,c_1, \beta \in \{0,1\}$.

If the trivial reporting strategy (12) is implemented with $S = 1$ using a first class of experimental setups with
small probability of loss and high detection efficiencies, satisfying $P_{\text{det}}(c, c|\beta) \leq \delta^I_{\text{err}}$ for a small $\delta^I_{\text{err}} > 0$ and for $c, \beta \in \{0, 1\}$, then the condition (2) of the correctness property is satisfied for any $\delta_{\text{det}} \leq 1$, and the condition (3) of the correctness property is guaranteed if

$$
(\delta_{00}^I + \delta^I_{11}) \left( \frac{1}{2} + \frac{\delta_{\text{equal}}}{\delta_{\text{error}}} \right) + \frac{\delta_{\text{diff}}}{\delta_{\text{error}}} \leq \delta_{\text{error}}.
$$

(A1)

If a probabilistic reporting strategy (11) is implemented using a second class of experimental setups where Bob’s detection efficiencies are small and the probability of loss is high, satisfying that $P_{\text{det}}(0, 0|\beta) \geq 1 - \delta^I_{00}$, for a small $\delta^I_{00} > 0$ and for $\beta \in \{0, 1\}$, and the conditions (2) and (3) hold with

$$
\delta_{\text{det}} > \frac{\delta^I_{00}}{5(1 - \delta^I_{00})},
$$

(A2)

$$
\delta_{\text{error}} < \frac{1}{12} + \frac{\delta_{\text{equal}}}{\delta_{\text{error}}} \cdot \frac{6}{\delta_{\text{error}}},
$$

(A3)

then there exists $(c_0, c_1) \in \{(0, 1), (1, 0), (1, 1)\}$ and $\beta \in \{0, 1\}$ satisfying $S_{c_0 c_1 |\beta} > S_{00\beta}$, i.e. the reporting strategy is not the trivial one.

Proof. We consider the case of the first class of experimental setups following the trivial strategy (12) with $S = 1$. It follows straightforwardly from (12) and (13), since $S = 1$, that Bob’s probability to report Alice’s pulse as producing a measurement outcome is $P_{\text{det}} = 1$. Thus, the condition (2) is satisfied for any $\delta_{\text{det}} \leq 1$, as claimed. The probability of error $P_{\text{error}}$ is computed for the case in which Bob’s basis $B_{\beta}$ equals Alice’s basis and Bob reports the pulse as valid ($m = 1$). We consider the case $\beta = \beta'$. We have

$$
P_{\text{error}} = \sum_{c_0, c_1} S_{c_0 c_1 |\beta'} P_{\text{det}}(c_0, c_1|\beta') P_{\text{error}|c_0 c_1 |\beta'}
$$

$$
\geq \sum_{c_0, c_1} S_{c_0 c_1 |\beta'} P_{\text{det}}(c_0, c_1|\beta') P_{\text{error|00}}
$$

$$
= \frac{1}{1 + \sum_{c_0, c_1} S_{c_0 c_1 |\beta'} P_{\text{det}}(c_0, c_1|\beta')}
$$

$$
\geq \frac{1}{1 + \frac{\delta_{\text{equal}}}{\delta_{\text{error}}}}
$$

(A8)

We show from (A6) that

$$
P_{\text{error}} \geq \frac{1}{12} \frac{\delta_{\text{equal}}}{\delta_{\text{error}}}. \quad \text{(A7)}
$$

However, from (3) and (A3) we see that (A7) cannot hold. Thus, (A6) cannot hold either. Thus, (A5) holds.

We show (A7) from (A6). The probability of error $P_{\text{error}}$ is computed for the case in which Bob’s basis $B_{\beta}$ equals Alice’s basis and Bob reports the pulse as valid ($m = 1$). We consider the case $\beta = \beta'$. We have

$$
P_{\text{error}} \geq \frac{1}{12} \frac{\delta_{\text{equal}}}{\delta_{\text{error}}}. \quad \text{(A7)}
$$

We show from (A6) that

$$
P_{\text{error}} \geq \frac{1}{12} \frac{\delta_{\text{equal}}}{\delta_{\text{error}}}. \quad \text{(A7)}
$$

However, from (3) and (A3) we see that (A7) cannot hold. Thus, (A6) does not hold, as claimed.

We show from (A6) that

$$
P_{\text{error}} \geq \frac{1}{12} \frac{\delta_{\text{equal}}}{\delta_{\text{error}}}. \quad \text{(A7)}
$$

We show from (A6) that

$$
P_{\text{error}} \geq \frac{1}{12} \frac{\delta_{\text{equal}}}{\delta_{\text{error}}}. \quad \text{(A7)}
$$

We show from (A6) that

$$
P_{\text{error}} \geq \frac{1}{12} \frac{\delta_{\text{equal}}}{\delta_{\text{error}}}. \quad \text{(A7)}
$$

However, from (3) and (A3) we see that (A7) cannot hold. Thus, (A6) does not hold, as claimed.

We show from (A6) that

$$
P_{\text{error}} \geq \frac{1}{12} \frac{\delta_{\text{equal}}}{\delta_{\text{error}}}. \quad \text{(A7)}
$$

However, from (3) and (A3) we see that (A7) cannot hold. Thus, (A6) does not hold, as claimed.
We show (A10) from (A5) and (A9). We have
\[ P_{\text{det}} = \sum_{c_0, c_1, \beta} P(\beta) S_{c_0, c_1, \beta} P_{\text{det}}(c_0, c_1 | \beta) \]
\[ \leq \sum_{\beta} P(\beta) S_{00\beta} \sum_{c_0, c_1} P_{\text{det}}(c_0, c_1 | \beta) \]
\[ \leq \max_{\beta \in \{0,1\}} \{ S_{00\beta} \} \]
\[ < \frac{\delta_{00}^{|H|}}{5(1 - \delta_{00}^{|H|})}, \]  \hspace{1cm} (A11)
where \( c_0, c_1 \) and \( \beta \) run over \( \{0,1\} \), where in the second line we used (A9), in the third line we used that \( \sum_{c_0, c_1} P_{\text{det}}(c_0, c_1 | \beta) = 1 \) and \( \sum_{\beta} P(\beta) = 1 \), and in the last line we used (A5).

The second class of experimental setups includes implementations with weak coherent sources, for which \( P_{\text{det}}(0,0|\beta) \geq 1 - \delta_{00}^{|H|} \), for a small \( \delta_{00}^{|H|} > 0 \) and for \( \beta \in \{0,1\} \). For example, the experimental demonstrations of mistrustful quantum cryptography given by Refs. [13, 14, 50] used weak coherent sources with \( \mu \approx 0.05, 0.183, 0.005 \) respectively. For \( \mu = 0.05 \), the probability of a zero photon pulse is \( p_0 = e^{-\mu} \approx 0.95 \). Thus, due to losses in the quantum channel and Bob’s detection efficiencies being smaller than unity, we have \( \delta_{00}^{|H|} < 0.05 \) in this case. The condition (A2) is motivated by the fact that if \( P_{\text{det}}(0,0|\beta) \leq 1 - \delta_{00}^{|H|} \), then \( P_{\text{det}} \geq \delta_{\text{det}} \), where \( \delta_{\text{det}} \) is a suitable required lower bound for \( P_{\text{det}} \). Similarly, the experimental demonstrations of mistrustful quantum cryptography given by Refs. [13, 14, 60, 61] report the required upper bounds \( P_{\text{error}} < 0.05 \), \( P_{\text{error}} < 0.015 \), \( P_{\text{error}} < 0.046 \) and \( P_{\text{error}} < 0.01 \), respectively, in order to guarantee security against Bob. Thus, we see that in Refs. [13, 14, 60, 61], \( P_{\text{error}} < \frac{1}{4} \), and we have \( P_{\text{error}} < \delta_{\text{error}} \) satisfying (A3).

Appendix B: Security bounds

The following lemmas give upper bounds on the amount of information that Alice can obtain about \( \beta \) from Bob’s message \( m \). Lemma 5 provides a bound for an arbitrary reporting strategy by Bob. Together with Lemma 6, Lemmas 7 and 8 provide bounds when Bob follows reporting strategies II and III, respectively.

**Lemma 5.** Suppose that Alice sends Bob a pulse of \( k \) photons, encoding an arbitrary \( k \)-qubit state \( \rho \), which may be arbitrarily entangled and which may be entangled with an ancilla held by Alice. Suppose that Bob chooses the bit \( \beta \) with some probability

\[ P_{\text{basis}}(\beta) \leq \frac{1}{2} + \epsilon_{\text{basis}}, \]  \hspace{1cm} (B1)
for \( \beta \in \{0,1\} \) and for some \( \epsilon_{\text{basis}} \geq 0 \). Consider an arbitrary strategy by Bob to report the message \( m \in \{0,1\} \) to Alice. Then Alice’s probability \( P_{\text{guess}} \) to guess \( \beta \) from Bob’s message \( m \) satisfies

\[ P_{\text{guess}} \leq \left( \frac{1}{2} + \epsilon_{\text{basis}} \right) \left( 1 + |P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k)| \right). \]  \hspace{1cm} (B2)

**Proof.** Alice’s most general strategy to guess \( \beta \) from the message \( m \) is as follows. Alice guesses \( \beta = i \) with some probability \( P_{\text{Alice}}(i|m) \), when she receives the message \( m \), for \( i, m \in \{0,1\} \). Alice’s optimal strategy is a deterministic strategy. That is, one of the two following equations holds:

\[ P_{\text{Alice}}(i|m) = \delta_{i,m}, \]  \hspace{1cm} (B3)
\[ P_{\text{Alice}}(i|m) = \delta_{\bar{i},m}, \]  \hspace{1cm} (B4)
for \( i, m \in \{0,1\} \). Alice’s average probability to guess \( \beta \) is given by

\[ P_{\text{guess}} = \sum_{\beta=0}^{1} \sum_{m=0}^{1} P_{\text{basis}}(\beta) P_{\text{Alice}}(\beta|m) P_{\text{report}}(m|\beta, \rho, k). \]  \hspace{1cm} (B5)

If (B3) holds, it follows from (B1), (B3) and (B4) that

\[ P_{\text{guess}} \leq \left( \frac{1}{2} + \epsilon_{\text{basis}} \right) \sum_{\beta=0}^{1} P_{\text{report}}(\beta|\beta, \rho, k). \]  \hspace{1cm} (B6)

If (B4) holds, it follows from (B1), (B4) and (B5) that

\[ P_{\text{guess}} \leq \left( \frac{1}{2} + \epsilon_{\text{basis}} \right) \sum_{\beta=0}^{1} P_{\text{report}}(\beta|\beta, \rho, k). \]  \hspace{1cm} (B7)

Since

\[ P_{\text{report}}(\bar{m}|\beta, \rho, k) = 1 - P_{\text{report}}(m|\beta, \rho, k), \]  \hspace{1cm} (B8)
for \( \beta, m \in \{0,1\} \), we obtain that

\[ \sum_{\beta=0}^{1} P_{\text{report}}(\beta|\beta, \rho, k) = 1 + P_{\text{report}}(1|1, \rho, k) \]
\[ - P_{\text{report}}(1|0, \rho, k) \]
\[ \leq 1 + |P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k)|. \]  \hspace{1cm} (B9)

Similarly, from (B8), we obtain

\[ \sum_{\beta=0}^{1} P_{\text{report}}(\bar{\beta}|\beta, \rho, k) = 1 + P_{\text{report}}(1|0, \rho, k) \]
\[ - P_{\text{report}}(1|1, \rho, k) \]
\[ \leq 1 + |P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k)|. \]  \hspace{1cm} (B10)

Thus, from (B9), (B7), (B9) and (B10), the claimed result (B2) follows. \( \Box \)
Lemma 6. Let $\eta_{\text{low}}$ and $\eta_{\text{up}}$ be such that

$$0 < \eta_{\text{low}} \leq \eta_{i\beta} \leq \eta_{\text{up}} < 1,$$  \hspace{1cm} (B11)

for $i, \beta \in \{0, 1\}$. Let $0 \leq d_{i\beta} \leq \delta$, for $i, \beta \in \{0, 1\}$ and for some $0 \leq \delta < \frac{\eta_{\text{low}}}{2}$. We define

$$B_{\text{det}}^{\text{II}} = (1 - 2\delta)\left(\frac{\ln(1 - \eta_{\text{up}})}{\ln(1 - \eta_{\text{low}})} - 1\right)(1 - \eta_{\text{up}})B_{\text{exp}}^{\text{II}},$$ \hspace{1cm} (B12)

where

$$B_{\exp}^{\text{II}} = \frac{\ln\left((1 - 2\delta)\ln(1 - \eta_{\text{up}})/\ln(1 - \eta_{\text{low}})\right)}{\ln(1 - \eta_{\text{low}}) - \ln(1 - \eta_{\text{up}})}.$$ \hspace{1cm} (B13)

Suppose that Alice sends Bob a pulse of $k$ photons, encoding an arbitrary $k$-qubit state $\rho$, which may be arbitrarily entangled and which may be entangled with an ancilla held by Alice. Suppose also that Bob uses reporting strategy II. Then

$$|P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k)| \leq B_{\text{II}},$$ \hspace{1cm} (B14)

for $k \in \{0, 1, 2, \ldots\}$, where

$$B_{\text{II}} = \max\{2\delta, B_{\text{det}}^{\text{II}}\}.$$ \hspace{1cm} (B15)

Lemma 7. Let $\eta_{\text{min}}$ and $\eta_{\text{max}}$ be such that

$$\eta_{\text{min}} = \min_{i, \beta \in \{0, 1\}} \{\eta_{i\beta}\} > 0,$$

$$\eta_{\text{max}} = \max_{i, \beta \in \{0, 1\}} \{\eta_{i\beta}\} < 1.$$ \hspace{1cm} (B16)

Let $0 \leq d_{i\beta} \leq \delta$, for $i, \beta \in \{0, 1\}$ and for some $0 \leq \delta < \frac{1}{2}$. We define

$$B_{\text{det}}^{\text{III}} = 1 - \frac{\eta_{\text{min}}}{\eta_{\text{max}}} + (1 - 2\delta)\left(\frac{\ln(1 - \eta_{\text{max}})}{\ln(1 - \eta_{\text{min}})} - 1\right)(1 - \eta_{\text{max}})B_{\exp}^{\text{III}},$$ \hspace{1cm} (B17)

where

$$B_{\exp}^{\text{III}} = \frac{\ln\left((1 - 2\delta)\eta_{\text{max}}\ln(1 - \eta_{\text{max}})/\eta_{\text{min}}\ln(1 - \eta_{\text{min}})\right)}{\ln(1 - \eta_{\text{min}}) - \ln(1 - \eta_{\text{max}})}.$$ \hspace{1cm} (B18)

Suppose that Alice sends Bob a pulse of $k$ photons, encoding an arbitrary $k$-qubit state $\rho$, which may be arbitrarily entangled and which may be entangled with an ancilla held by Alice. Suppose also that Bob uses reporting strategy III with

$$\frac{\eta_{\text{min}}}{\eta_{\text{max}}} \leq S_{11\beta} \leq 1,$$ \hspace{1cm} (B19)

for $\beta \in \{0, 1\}$. Then

$$|P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k)| \leq B_{\text{III}},$$ \hspace{1cm} (B20)

for $k \in \{0, 1, 2, \ldots\}$, where

$$B_{\text{III}} = \max\{2\delta, B_{\text{det}}^{\text{III}}\}.$$ \hspace{1cm} (B21)

We note that the bounds $B_{\text{II}}$ and $B_{\text{III}}$ in Lemmas 6 and 7 respectively, tend to $2\delta$ if all the detection efficiencies tend to the same value $\eta$, as in this case we have $\eta_{\text{up}} \to \eta$, $\eta_{\text{low}} \to \eta$, $\eta_{\text{max}} \to \eta$ and $\eta_{\text{min}} \to \eta$. Additionally, if the dark count probabilities are zero then $\delta = 0$ and the bounds tend to zero in this case. This is expected. However, as we illustrate in Fig. 4 it is even for relatively close values of the detection efficiencies, the obtained bounds are not very small.

The proofs of Lemmas 6 and 7 use the following lemma.

Lemma 8. Suppose that Alice sends Bob a pulse of $k$ photons, encoding an arbitrary $k$-qubit state $\rho$, which may be arbitrarily entangled and which may be entangled with an ancilla held by Alice. Let $\eta_{\text{low}}$ and $\eta_{\text{up}}$ be such that

$$0 < \eta_{\text{low}} \leq \eta_{i\beta} \leq \eta_{\text{up}} < 1,$$ \hspace{1cm} (B22)

for $i, \beta \in \{0, 1\}$. Let $0 \leq d_{i\beta} \leq \delta$, for $i, \beta \in \{0, 1\}$, and

FIG. 4. Security bounds $B_{\text{II}}$ and $B_{\text{III}}$. We show plots for the bounds $B_{\text{II}}$ (top) and $B_{\text{III}}$ (bottom), defined by (B12) in Lemma 6 and by (B21) in Lemma 7 respectively. We consider the case $\delta = 10^{-5}$ in Lemmas 6 and 7. We also consider $\eta_{\text{low}} = \eta - \delta_{\text{eff}}$ and $\eta_{\text{up}} = \eta + \delta_{\text{eff}}$ in Lemma 6 and $\eta_{\text{min}} = \eta - \delta_{\text{eff}}$ and $\eta_{\text{max}} = \eta + \delta_{\text{eff}}$ in Lemma 7. We plot for five values of $\eta$ and for the range $\delta_{\text{eff}} \in [0, 0.01]$.

Let $0 \leq d_{i\beta} \leq \delta$, for $i, \beta \in \{0, 1\}$ and for some $0 \leq \delta < \frac{1}{2}$.
for some $0 \leq \delta < \frac{1}{2}$. Then

$$(1 - 2\delta)(1 - \eta_{up})^k \leq P_{det}(0, 0|\beta, \rho, k) \leq (1 - \eta_{low})^k, \quad (B23)$$

for $k \in \{0, 1, 2, \ldots\}$ and $\beta \in \{0, 1\}$.

**Proof.** Consider an arbitrary, and possibly entangled, $k$-qubit state $\rho$ encoded in a pulse of $k$ photons that Alice sends Bob, which may be in an arbitrary entangled state with an ancilla held by Alice. Let $P(k_0|\beta, \rho, k)$ be the probability that $k_0$ photons go to the detector $D_0$ and $k - k_0$ photons go to the detector $D_1$, when Bob measures in the basis $B_\beta$, for $\beta \in \{0, 1\}$, $k_0 \in \{0, 1, \ldots, k\}$ and $k \in \{0, 1, 2, \ldots\}$. It follows straightforwardly that

$$P_{det}(0, 0|\beta, \rho, k) = (1 - d_\beta)(1 - d_1\beta) \sum_{k_0=0}^{k} P(k_0|\beta, \rho, k) \times$$

$$\times [(1 - \eta_\beta)^{k_0}(1 - \eta_1\beta)^{k - k_0}]$$

$$\leq (1 - \eta_{low})^k \sum_{k_0=0}^{k} P(k_0|\beta, \rho, k)$$

$$= (1 - \eta_{low})^k, \quad (B24)$$

for any $k$-qubit state $\rho$, for $k \in \{0, 1, 2, \ldots\}$, and for $\beta \in \{0, 1\}$; where in the second line we used that $\eta_\beta \geq \eta_{low}$ and $d_\beta \geq 0$, for $i, \beta \in \{0, 1\}$; and in the third line we used that $\sum_{k_0=0}^{k} P(k_0|\beta, \rho, k) = 1$. Similarly, using that $\eta_\beta \leq \eta_{up}$ and $d_\beta \leq \delta$, it follows straightforwardly that

$$P_{det}(0, 0|\beta, \rho, k) \geq (1 - 2\delta)(1 - \eta_{up})^k, \quad (B25)$$

for any $k$-qubit state $\rho$, for $k \in \{0, 1, 2, \ldots\}$, and for $\beta \in \{0, 1\}$. Thus, from (B24) and (B25), we obtain (B23).

**Proof of Lemma 6** Consider an arbitrary, and possibly entangled, $k$-qubit state $\rho$ encoded in a pulse of $k$ photons that Alice sends Bob, which may be in an arbitrary entangled state with an ancilla held by Alice. In the reporting strategy II, the probability that Bob reports the entangled state with an ancilla held by Alice. In the re-

Proof.

Theorem 6. Consider an arbitrary, and possibly entangled, $k$-qubit state $\rho$ encoded in a pulse of $k$ photons that Alice sends Bob, which may be in an arbitrary entangled state with an ancilla held by Alice. In the re-

Proof.

We show below that if $\eta_{low} < \eta_{up}$ then

$$f(k) \leq f(B_{\exp}^{\II}), \quad (B32)$$

for $k \in \{0, 1, 2, \ldots\}$, where $B_{\exp}^{\II}$ is given by (B13). It follows straightforwardly from (B12), (B13) and (B29) that

$$f(B_{\exp}^{\II}) = B_{\det}^{\II}, \quad (B33)$$

where $B_{\det}^{\II}$ is given by (B12). Thus, (B27) follows from (B30) - (B33).

We assume that $\eta_{low} < \eta_{up}$ and show (B32). We define $k^* \in \mathbb{R}$ such that

$$f'(k^*) = 0. \quad (B34)$$

We show below that

$$k^* = B_{\exp}^{\II}. \quad (B35)$$

We also show that

$$f''(k^*) < 0. \quad (B36)$$

Thus, $f(k^*)$ is a maximum and

$$f(k) \leq f(k^*), \quad (B37)$$

for $k \in \{0, 1, 2, \ldots\}$. Therefore, (B32) follows from (B35) and (B37).

We show (B35). From (B29), we have

$$f'(k) = \ln(1 - \eta_{low})(1 - \eta_{low})^k - (1 - 2\delta)(1 - \eta_{up})(1 - \eta_{up})^k, \quad (B38)$$

for $k \in \mathbb{R}$. Thus, (B35) follows straightforwardly from (B13), (B24) and (B38).

We complete the proof by showing (B36). From (B38), we have

$$f''(k^*) = \left(\ln(1 - \eta_{low})\right)^2(1 - \eta_{low})^{k^*} - (1 - 2\delta)(1 - \eta_{up})\times\ln(1 - \eta_{low}) - \ln(1 - \eta_{up})\right) \times$$

$$\times (1 - 2\delta)(1 - \eta_{up})(1 - \eta_{up})^{k^*} < 0, \quad (B39)$$

where in the second line we used (B34) and (B38); and in the third line we used (B11), our assumption that $\eta_{low} < \eta_{up}$, and that $0 \leq \delta < \frac{1}{2}$.\qed
Proof of Lemma 7. From the definition of reporting strategy III, given by (8), and from (11), we have
\[
P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k) = \frac{\eta_{\min}}{\eta_{11}} P_{\text{det}}(0,1|1, \rho, k) + \frac{\eta_{\min}}{\eta_{01}} P_{\text{det}}(1,0|1, \rho, k)
+ S_{111} P_{\text{det}}(1,1,1|1, \rho, k) - \frac{\eta_{\min}}{\eta_{00}} P_{\text{det}}(1,0|0, \rho, k)
- \frac{\eta_{\min}}{\eta_{00}} S_{10} P_{\text{det}}(1,1,1|1, \rho, k).
\]

(B40)

From (B19) and (B40), we obtain
\[
P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k) 
\leq 1 - P_{\text{det}}(0,0|1, \rho, k) - \frac{\eta_{\min}}{\eta_{\max}} (1 - P_{\text{det}}(0,0|0, \rho, k)),
\]
and
\[
P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k) 
\geq \frac{\eta_{\min}}{\eta_{\max}} (1 - P_{\text{det}}(0,0|1, \rho, k)) - (1 - P_{\text{det}}(0,0|0, \rho, k)).
\]

(B41)

Thus, from (B41) and (B42), and from Lemma 8 we obtain
\[
|P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k)| = g(k),
\]
where we define
\[
g(k) \equiv 1 - \frac{\eta_{\min}}{\eta_{\max}} + \left| \frac{\eta_{\min}}{\eta_{\max}} (1 - \eta_{\min}) k - (1 - 2\delta)(1 - \eta_{\max}) k \right|,
\]
for \(k \in \mathbb{R}\). It follows from (B43) that
\[
|P_{\text{report}}(1|1, \rho, k) - P_{\text{report}}(1|0, \rho, k)| \leq g(k),
\]
for \(k \in \{0, 1, 2, \ldots\}\). If \(\eta_{\min} = \eta_{\max}\), it follows from (B16) and (B44), and from \(\delta \geq 0\), that
\[
g(k) \leq 2\delta,
\]
for \(k \in \{0, 1, 2, \ldots\}\). We show below that if \(\eta_{\min} < \eta_{\max}\) then
\[
g(k) \leq g(B_{\text{exp}}^{\text{III}}),
\]
for \(k \in \{0, 1, 2, \ldots\}\), where \(B_{\text{exp}}^{\text{III}}\) is given by (B18). It follows straightforwardly from (B17), (B18), and (B44) that
\[
g(B_{\text{exp}}^{\text{III}}) = B_{\text{det}}^{\text{III}},
\]
where \(B_{\text{det}}^{\text{III}}\) is given by (B20). Thus, the claimed bound (B50) follows from (B45) - (B48).

We assume that \(\eta_{\min} < \eta_{\max}\) and show (B51). We define \(\tilde{k} \in \mathbb{R}\) such that
\[
g'(\tilde{k}) = 0.
\]

We show below that
\[
\tilde{k} = B_{\text{exp}}^{\text{III}}.
\]
(B50)

We also show that
\[
g''(\tilde{k}) < 0.
\]
(B51)

Thus, \(g(\tilde{k})\) is a maximum and
\[
g(k) \leq g(\tilde{k}),
\]
(B52)
for \(k \in \{0, 1, 2, \ldots\}\). Therefore, (B17) follows from (B50) and (B52).

We show (B50). From (B44), we have
\[
g'(k) = \frac{\eta_{\min}}{\eta_{\max}} \ln(1 - \eta_{\min})(1 - \eta_{\max}) k
- (1 - 2\delta) \ln(1 - \eta_{\max})(1 - \eta_{\max}) k,
\]
(B53)
for \(k \in \mathbb{R}\). Thus, (B50) follows straightforwardly from (B18), (B40) and (B53).

We complete the proof by showing (B51). From (B53), we have
\[
g''(\tilde{k}) = \frac{\eta_{\min}}{\eta_{\max}} \ln(1 - \eta_{\min})^2 (1 - \eta_{\min}) \tilde{k}
- (1 - 2\delta) \ln(1 - \eta_{\max})^2 (1 - \eta_{\max}) \tilde{k}
= (\ln(1 - \eta_{\min}) - \ln(1 - \eta_{\max})) \times
\times (1 - 2\delta) \ln(1 - \eta_{\max})(1 - \eta_{\max}) \tilde{k}
< 0,
\]
(B54)
where in the second line we used (B49) and (B53); and in the third line we used (B16), our assumption that \(\eta_{\min} < \eta_{\max}\), and that \(0 \leq \delta < \frac{1}{2}\). \(\square\)

Appendix C: Mistrustful quantum cryptography

In mistrustful cryptography, two or more parties who do not trust each other collaborate to implement a cryptographic task. Important cryptographic tasks in mistrustful cryptography are bit commitment, oblivious transfer, secure multi-party computation and coin flipping, for example. We say that a cryptographic protocol is \textit{unconditionally secure} if it is secure based only on the laws of physics, without imposing any technological limitations on the dishonest parties. There exist quantum and relativistic protocols in mistrustful cryptography that exploit the laws of quantum physics and relativity to guarantee security, respectively. For some tasks in mistrustful cryptography, there exists some impossibility results stating that some tasks in mistrustful cryptography cannot achieve unconditional security with quantum nonrelativistic protocols \cite{48, 50, 53}, or even with quantum relativistic protocols for other tasks \cite{56}. On the other hand, there are relativistic protocols that achieve unconditional security for some tasks \cite{12, 13, 17, 22, 24, 25, 53, 56, 62}. However, by imposing technological limitations on the dishonest parties, security
of some quantum nonrelativistic protocols can be guaranteed. For example, some tasks that cannot achieve unconditional security can be implemented securely in the noisy storage model \[58,59\] in which the dishonest parties can only store quantum states in noisy quantum memories with finite coherence times.

1. Quantum bit commitment

In bit commitment, Bob (the committing party) commits a secret bit \(b\) to Alice at a given time \(t_{\text{commit}}\). Bob chooses to unveil \(b\) to Alice at some time \(t_{\text{unveil}} > t_{\text{commit}}\). A bit commitment protocol must satisfy two security conditions. First, a bit commitment protocol is hiding if, when Bob follows the protocol and Alice deviates arbitrarily from the protocol, the probability that Alice guesses Bob’s bit \(b\) before Bob unveils satisfies \(P_{\text{guess}} \leq \frac{1}{2} + \epsilon_{\text{hiding}}\), for some \(\epsilon_{\text{hiding}} \geq 0\) that goes to zero as some security parameter goes to infinity. Second, a bit commitment protocol is binding if, when Alice follows the protocol and Bob deviates arbitrarily from the protocol, the probability \(p_i\) that Bob successfully unveils the bit \(b = i\) satisfies \(p_0 + p_1 \leq 1 + \epsilon_{\text{binding}}\), for \(i \in \{0,1\}\), and for some \(\epsilon_{\text{binding}} \geq 0\) that goes to zero as some security parameter goes to infinity. The hiding and binding properties are also called security against Alice and security against Bob, respectively, when Bob is the committing party.

Nonrelativistic quantum bit commitment cannot achieve unconditional security \[48,50\]. However, secure bit commitment can be achieved in the noisy storage model \[58,59\]. Nevertheless, there are relativistic classical \[9,10,15\] and quantum \[11,12,16,17\] bit commitment protocols that are unconditionally secure.

2. Quantum oblivious transfer

In a 1-out-of-2 oblivious transfer (OT) protocol \[71\], Alice inputs two strings of \(n\) bits, \(x_0\) and \(x_1\), initially secret from Bob. Bob inputs a bit \(b\), initially secret from Alice. At the end of the protocol, Bob outputs the string \(x_b\). Two security conditions must be fulfilled, called security against Alice and security against Bob. Security against Alice states that, if Bob follows the protocol and Alice deviates arbitrarily from the protocol, the probability that Alice guesses Bob’s input \(b\) satisfies \(P_{\text{Alice}} \leq \frac{1}{2} + \epsilon_{\text{Alice}}\), for some \(\epsilon_{\text{Alice}} \geq 0\) that goes to zero as some security parameter goes to infinity. Security against Bob states that, if Alice follows the protocol and Bob deviates arbitrarily from the protocol, Bob cannot learn both strings \(x_0\) and \(x_1\); this can be quantified by stating that the probability that Bob obtains both messages satisfies \(P_{\text{Bob}} \leq \epsilon_{\text{Bob}}\), for some \(\epsilon_{\text{Bob}} \geq 0\) that goes to zero as some security parameter goes to infinity.

1-out-of-\(m\) OT cannot be implemented with unconditional security in quantum cryptography \[53\]. This impossibility theorem holds even in the setting of relativistic quantum cryptography \[55\], although some relativistic variations of the task can be achieved with unconditional security \[22,24\]. However, 1-out-of-2 OT can be implemented securely in the noisy storage model \[58,59\].

3. Quantum coin flipping

In strong coin flipping, Bob and Alice, who are at distant locations, obtain a bit \(a\) that is random and which cannot be biased by neither of them. A strong coin flipping protocol must satisfy security against Alice and security against Bob. Security against Alice (Bob) states that if Alice (Bob) follows the protocol and Bob (Alice) deviates arbitrarily from the protocol, and Alice (Bob) obtains as outcome the bit \(a\) then it holds that \(P(a = i) \leq \frac{1}{2} + \epsilon\), for \(i \in \{0,1\}\), and for some \(\epsilon \geq 0\) that goes to zero as some security parameter goes to infinity.

Although there are relativistic protocols for strong coin flipping that are unconditionally secure \[27\], quantum nonrelativistic protocols for strong coin flipping cannot achieve unconditional security \[50\]. However there are quantum nonrelativistic protocols for strong coin flipping that unconditionally guarantee some level of security, in that the bias a dishonest party can give the coin is bounded below one \[51,52,72,74\].

Appendix D: Multi-photon attacks on experimental demonstrations of mistrustful cryptography protocols

Some of the quantum protocols discussed in the previous section offer unconditional security guarantees; others offer security based on technological assumptions. Over the past decade, they have been implemented in pioneering experimental demonstrations (e.g. \[13,14,30,60,61\]), often adapting quantum key distribution technology. Refs. \[60,61\] demonstrated quantum bit commitment and 1-out-of-2 quantum oblivious transfer in the noisy storage model. Ref. \[30\] demonstrated quantum coin flipping performing better than classical protocols over a distance of various kilometres, gaining three orders of magnitude in communication distance over previous experiments. Refs. \[13,14\] implemented quantum relativistic bit commitment protocols for the first time, showing that the protocol of Ref. \[12\] can be implemented in practice, over short and long range.

Two of us (E.D. and A.K.) have contributed to this work. Scientific honesty compels us to acknowledge that we did not appreciate all the obstacles to attaining provable and truly unconditional security in practical implementations of mistrustful quantum cryptographic protocols. In hindsight, we believe the implementations \[13,14,30,60,61\] may be best seen as proofs of principle. They show that some key technological challenges in implementing the protocols have been met and give
significant and valuable security guarantees based on assumptions about the parties’ behaviour and technology that are natural in some scenarios. However, more work appears to be required to deliver provably unconditional security. In particular, provable unconditional security against Alice (i.e. the sender of the quantum states, in our convention) requires implementing techniques countering the various side-channel and multi-photon attacks we have described and showing that her cheating probability can thus be made arbitrarily close to the ideal bound (which in most cases is zero).

Users and developers of mistrustful quantum cryptosystems may also need to consider whether some technological assumptions may be both necessary and sufficient in practical implementations, even for protocols that are theoretically unconditionally secure, given the difficulty in provably countering every possible side-channel attack.

We will discuss Refs. 13, 14, 30, 60, 61 separately below. We should first note that reanalysing previous implementations in the light of our attacks is not completely straightforward. Although the relevant papers are generally very clear and comprehensive, experimental details that at the time may not have seemed significant were not always given. For example, some of the experiments used off-the-shelf quantum key distribution equipment which may have been programmed either to discard double clicks or choose a random outcome. After discussing with colleagues, we understand it may not now be possible to say with certainty which option was used. This is unimportant for the future of the field. We believe we should note, though, when (what we now realise are) significant instructions are missing from the published reports, since future users trying to reproduce or improve on previous implementations may rely on these. Ref. 60 explicitly states that only single click detection events are reported by Bob as valid measurement outcomes, while Refs. 13, 30, 61 do not say whether multiple clicks are reported by Bob or not.

A related issue is the question of precisely how the symmetrization of losses technique was or might have been implemented. This technique was introduced by Ref. 60 and claimed to guarantee security against Alice by Refs. 13, 30, 60, 61. Indeed, as Lemma 2 states for the symmetrization of losses with setup I (see Fig. 1 of the main text) – as applied by Ref. 30, for example – security against Alice is guaranteed when she does not send multi-photon pulses, if Bob reduces the probability of assigning a measurement outcome due to a single click event \((c, \overline{c})\) by a suitable factor \(S_{\alpha \delta\beta}\), for \(c, \beta \in \{0, 1\}\). A similar result is shown by Lemma 3 below in a setup with four detectors (setup II, see Fig. 5), as implemented by Refs. 60, 61. However, the original symmetrization of losses technique 60 treats multiple clicks as invalid, and thus does not provide effective protection against multi-photon attack I. A natural defence against this attack is to report multiple clicks as valid measurement outcomes. However, one then needs to define an extension of the symmetrization of losses reporting strategy applicable to multiple click outcomes. A general extension of symmetrization of losses in setup I is what we have defined as reporting strategy III in \(\mathbf{5}\), where a double click is reported by Bob with some probability \(S_{11\delta\beta} \in [0, 1]\) when Bob measures in the basis \(B_\beta\), for \(\beta \in \{0, 1\}\). Theorem 1 then shows that multi-photon attack II applies if the detector efficiencies of Bob’s detectors are different and known by Alice. A countermeasure against this attack is to ensure Bob’s detectors have equal efficiency. This cannot be implemented perfectly. Lemma 4 guarantees that, if the efficiencies of Bob’s detectors are sufficiently close, then Alice can obtain little information about \(\beta\) if Bob applies reporting strategy III with the parameters of Lemma 4. However, as Fig. 4 illustrates, the efficiency differences need to be very small.

We should note that Ref. 13 implemented a slightly different version of symmetrization of losses with setup I which aimed not to symmetrize the detection efficiencies but to symmetrize Bob’s detection probabilities for both values of Bob’s measurement basis \(\beta \in \{0, 1\}\). This version of symmetrization of losses naturally incorporates double click events, which can be assigned a random measurement outcome. However, multi-photon attack II still applies.

We also note again that Ref. 14 discussed multi-photon attack I and implemented the countermeasure of reporting single and double clicks. Again, multi-photon attack II still applies.

Below we discuss variations of the multi-photon attacks I and II presented in the main text, as they apply to the protocols of Refs. 13, 14, 30, 60, 61. Because these protocols extend the task of private measurement of an unknown qubit state of the main text to a setting with \(N > 1\) photon pulses in different ways, we need to discuss the attacks separately for each protocol. A summary is given in Table 1 in the main text.

We note that, as indicated with a dash in Table 1, we have not found a clear application of the attack II to the protocol of Ref. 30. Furthermore, we have not investigated an application of this attack in setup II, introduced below (see Fig. 3), which is used in the protocols of Refs. 60, 61. The reason is that Bob’s detection probabilities as functions of the multi-photon states generated by Alice are much more complex to derive for setup II because Bob has four detectors in this case. Our analytic strategy should still apply, but we leave this for future work. The burden of proof, of course, lies on the other side. A full proof of security (within the given model) would require an explicit reporting strategy for setup II and a discussion of the information Alice can obtain from general multi-photon attacks against that strategy when Bob’s detector efficiencies are unequal and known to her.
1. Multi-photon attacks on the relativistic quantum bit commitment protocol of Ref. [13]

a. The relativistic quantum bit commitment protocol of Ref. [13]

Ref. [13] (co-authored by one of us) demonstrated the quantum relativistic bit commitment protocol of Ref. [12], using an extra stage of pre-processing to allow commitments to be made by the pre-agreed actions of parties separated by several thousand kilometres. We discuss here the application of multi-photon attacks on the protocol (as presented) and show that it does not guarantee hiding with unconditional security if the committer’s detectors have unequal efficiency and the committee becomes aware of the efficiencies. Ref. [13] takes Bob as the committing party. We follow this convention below.

The protocol of Ref. [13] is a relativistic quantum protocol. The attacks that we present below are implemented in the quantum stage of the protocol, which is nonrelativistic. For this reason, here we only need to discuss the quantum stage.

The nonrelativistic quantum stage of the protocol is as follows. Alice and Bob use setup I discussed in the main text and illustrated in Fig. 1. Alice’s photon source is a weak coherent source with small average photon number $\mu$. Alice sends Bob $N$ photon pulses, each encoding in the polarization a qubit state chosen randomly from the set $S = \{\ket{0}, \ket{1}, \ket{+}, \ket{-}\}$, where $B_0 = \{\ket{0}, \ket{1}\}$ and $B_1 = \{\ket{+}, \ket{-}\}$ are two qubit orthogonal bases. Ref. [13] considers the particular case that $B_0$ and $B_1$ are the computational and Hadamard bases, respectively. Bob chooses a random bit $\beta$. Immediately after their reception, Bob measures each of the $N$ photon pulses in the qubit orthogonal basis $B_\beta$. In order to deal with losses in the quantum channel, for each pulse sent by Alice, Bob sends Alice a message $m = 1$ if the pulse produced a valid measurement outcome and $m = 0$ otherwise. Bob chooses the committed bit $b$ and sends the message $c = \beta \oplus b$ to Alice.

Ref. [13] implemented the following version of the symmetrization of losses strategy. Bob tests his system by implementing the protocol agreed with Alice, with the agreed experimental parameters. Then, Bob computes the ratio $R = n_\beta N$, where $n_\beta$ is the number of pulses producing valid measurement outcomes when Bob measures all pulses in the basis $B_\beta$, for $\beta \in \{0, 1\}$. Then, when implementing the protocol with Alice, Bob performs the following actions. If $R \leq 1$, when a pulse produces a click, Bob sets $m = 1$ and assigns a valid measurement outcome with probability $R$ if $\beta = 1$, or with unit probability if $\beta = 0$. On the other hand, if $R > 1$, when a pulse produces a click, Bob sets $m = 1$ and assigns a valid measurement outcome with probability $\frac{1}{R}$ if $\beta = 0$, or with unit probability if $\beta = 1$. This effectively makes Bob’s detection probabilities for the cases $\beta = 0$ and $\beta = 1$ equal when both parties follow the protocol. We note that Ref. [13] does not explicitly say whether this procedure applies only to single clicks, or to single and double clicks, although we understand that double clicks were probably counted.

However, we need to consider cheating strategies available to Alice. We make some simplifying assumptions (which if anything reduce the power of cheating attacks) to illustrate these. We assume that $B_0$ and $B_1$ are the computational and Hadamard bases, respectively, as in Ref. [13]. We assume that Bob uses the single photon threshold detectors $D_0$ and $D_1$ to register outcomes associated with the states $\ket{0}$ ($\ket{+}$) and $\ket{1}$ ($\ket{-}$) if $\beta = 0$ ($\beta = 1$). We assume that $\eta_{\beta} = \eta_{i} \in (0, 1)$, for $i, \beta \in \{0, 1\}$. Since Bob cannot guarantee his detector to have exactly the same efficiencies, we assume that $\eta_0 \neq \eta_1$. Without loss of generality, we assume that $1 > \eta_0 > \eta_1 > 0$. We also assume that Alice’s preparation devices and Bob’s measurement devices are perfectly aligned. Thus, random BB84 states are prepared exactly by Alice. Bob randomly chooses $\beta \in \{0, 1\}$ and measures all pulses exactly in the basis $B_\beta$, where $B_0$ and $B_1$ are exactly the computational and Hadamard bases, respectively. We note from these assumptions that, due to symmetry, the detection probabilities when Bob measures in the basis $B_0$ are the same as the detection probabilities when Bob measures in the basis $B_1$. Thus, for large $N$, the ratio $R$ obtained by Bob in his symmetrization of losses strategies is very close to unity. We assume here that $R = 1$.

b. Multi-photon attack I

Suppose that Bob only assign valid measurement outcomes to pulses that produce a click in only one of his detectors. Furthermore, we assume that Bob applies the symmetrization of losses strategies described above. As discussed in the main text, Alice can implement multi-photon attack I and gain information about Bob’s measurement basis $B_\beta$. To illustrate this, consider a setup in which Alice’s polarization preparation devices and Bob’s polarizers are precisely aligned. Alice can send a pulse with a large number of photons $k$ in the same polarization state chosen from $S$: for example, $\rho = (\ket{0}\bra{0})^\otimes k$. If Bob measures the pulse in the basis $B_0$ then the detection event $(c_0, c_1) = (1, 0)$ occurs with high probability, giving $m = 1$ with unit probability if $R \leq 1$, or with probability $\frac{1}{R}$ if $R > 1$. If Bob measures in the basis $B_1$ then the detection event $(c_0, c_1) = (1, 1)$ occurs with high probability, giving $m = 0$. Thus, given $m$, Alice can learn $\beta$ with high probability. Note that this attack applies whether or not $\eta_0 = \eta_1$.

In practice, Alice and Bob’s devices cannot be perfectly precise. However, Alice can still learn significant information about Bob’s bit $\beta$ from the message $m$ with an appropriate choice of $k$. In particular, Alice can send Bob photon pulses prepared with a coherent source with average photon number $\mu >> 1$ and guess Bob’s bit $\beta$ with probability close to unity, as our experimental simu-
luation shows (see Fig. 2 of the main text). Furthermore, Alice can increase her probability to guess $\beta$ by sending Bob various pulses with a large number of photons.

Partial countermeasures that Bob can apply against these attacks are the following. First, Bob can use reporting strategy II and assign a random outcome when a double click is obtained; or he can use reporting strategy III with the parameters of Lemma 7. Lemma 1 shows reporting strategy II is perfectly effective if Bob’s detectors have exactly equal efficiencies. Lemmas 6 and 7 guarantee that, if the efficiencies of Bob’s detectors are sufficiently close, then Alice can obtain little information about $\beta$ if Bob applies reporting strategy II or III, with the parameters of Lemma 6 or 7 respectively. However, as Fig. 4 illustrates, the efficiency differences need to be very small. Second, Bob can abort the protocol if a fraction of pulses greater than $r_{\text{double}}^{\text{max}} \in (0,1)$, previously agreed with Alice, produces double clicks.

c. Multi-photon attack II

As noted above, multi-photon attack I would apply if Bob discarded double clicks as invalid measurements. We thus assume that Bob sends Alice the message $m = 1$ for each pulse sent by Alice that produces a click in at least one of his detectors. We also assume that Bob applies the countermeasure against multi-photon attacks in which he aborts if he observes a ratio of double click events higher than a maximum value $r_{\text{double}}^{\text{max}} \in (0,1)$ agreed with Alice. We present a multi-photon attack by Alice that for certain parameters allows Alice to guess Bob’s bit $\beta$ with probability approaching unity as the number of pulses $N$ of the protocol increases.

Alice generates two nonempty and nonintersecting subsets of $[N]$, $\Omega_{\text{protocol}}$ and $\Omega_{\text{attack}}$, satisfying $\Omega_{\text{protocol}} \cup \Omega_{\text{attack}} = [N]$. Let $a = \frac{\Omega_{\text{protocol}}}{N}$. It follows that $|\Omega_{\text{attack}}| = aN$ and $|\Omega_{\text{protocol}}| = (1-a)N$, with $a \in (0,1)$. Alice sends Bob $N$ photon pulses. The polarization degrees of freedom of each of the pulses with labels from the set $\Omega_{\text{protocol}}$ are prepared by Alice in a quantum state as established in the protocol agreed with Bob. Each of the pulses with labels from the set $\Omega_{\text{attack}}$ is prepared by Alice in $k^*$ photons, encoding in the polarization a quantum state $\rho$. Let $P_{\text{protocol}}(1|\beta)$ and $P_{\text{attack}}(1|\beta)$ be the probabilities that a pulse with label from the sets $\Omega_{\text{protocol}}$ and $\Omega_{\text{attack}}$ activates a detection in at least one of the two detectors, respectively, i.e that Bob sends Alice the message $m = 1$ for that pulse, when Bob measures the pulses in the basis $\mathcal{B}_B$, for $\beta \in \{0,1\}$.

Alice chooses $k^*$, $\rho$ and $a$ in such a way that: 1) the probability that there are more than $N_r^{\text{max}}$ double, double clicks in Bob’s detectors is negligible; and 2) it holds that

$$g_1(a, \rho, k^*) > g_0(a, \rho, k^*) > 0,$$  \hfill (D1)

where

$$g_\beta(a, \rho, k^*) = aP_{\text{attack}}(1|\beta) + (1-a)P_{\text{protocol}}(1|\beta),$$  \hfill (D2)

for $\beta \in \{0,1\}$. Let $Z_\beta$ denote the random variable corresponding to the number of pulses producing that at least one of the two of Bob’s detectors click when Bob measures in the basis $\mathcal{B}_B$, and let $E(Z_\beta)$ denote its expectation value, for $\beta \in \{0,1\}$. We have that

$$E(Z_\beta) = N g_\beta(a, \rho, k^*),$$  \hfill (D3)

for $\beta \in \{0,1\}$. Thus, from (D1) and (D3), we have

$$E(Z_1) > E(Z_0).$$  \hfill (D4)

Alice defines a parameter $\delta \in (0,1)$ satisfying

$$E(Z_0)(1 + \delta) = E(Z_1)(1 - \delta) = G_N.$$  \hfill (D5)

If the number of events $Z$ reported by Bob to give at least one click, i.e. for which Bob sends the message $m = 1$ to Alice, is smaller than $G_N$, Alice guesses that Bob measured in the basis $\mathcal{B}_0$, otherwise Alice guesses that Bob measured in the basis $\mathcal{B}_1$. It follows that Alice’s average probability to guess Bob’s bit $\beta$ in this attack is given by

$$P_{\text{guess}} = \frac{1}{2} \left[ \text{Prob}[Z_0 < E(Z_0)(1 + \delta)] \right]$$

$$+ \frac{1}{2} \left[ \text{Prob}[Z_1 \geq E(Z_1)(1 - \delta)] \right]$$

$$= 1 - \frac{1}{2} \left[ \text{Prob}[Z_0 \geq E(Z_0)(1 + \delta)] \right]$$

$$- \frac{1}{2} \left[ \text{Prob}[Z_1 < E(Z_1)(1 - \delta)] \right]$$

$$\geq 1 - \frac{1}{2} \left[ e^{-N g_\beta(a, \rho, k^*)^2} + e^{-N g_0(a, \rho, k^*)^2} \right],$$  \hfill (D6)

where in the last line we used (D3) and two Chernoff bounds (23). Thus, since $g_\beta(a, \rho, k^*) > 0$ for $\beta \in \{0,1\}$, we see from (D6) that $P_{\text{guess}}$ approaches unity with increasing $N$.

A possible countermeasure by Bob against this type of attack is to measure suitable statistical properties of the pulses sent by Alice. For example, Bob may modify his setup by adding more beam splitters and single photon detectors. In this way, Bob can measure the number of pulses producing clicks across different combinations of his detectors. If Bob observes statistics that deviate considerably from the statistics expected in the protocol agreed with Alice, Bob may abort the protocol.

d. Example of multi-photon attack II: a double-photon attack

Suppose Bob reports double clicks, i.e. sends the message $m = 1$ to Alice and randomly chooses the outcome.
We present an attack by Alice in which the photon statistics of the pulses that she sends to Bob correspond to those agreed for her weak coherent source. Thus, there is no way in which Bob can know that Alice is cheating.

We illustrate the attack on an implementation with parameters \( N = 2 \times 10^7, \eta_0 = 0.12, \eta_1 = 0.08, d_0 = d_1 = 10^{-5} \) and a weak coherent source with average photon number \( \mu = 0.05 \). The values \( \eta_0 = 0.12 \) and \( \eta_1 = 0.08 \) are consistent with uncertainty values for the detection efficiencies of 0.02, which is a common value. We show that Alice can guess Bob’s bit \( \beta \) with failure probability smaller than 0.035. Our example shows that Alice could in principle undetectably exploit the difference of Bob’s detector efficiencies due to their experimental uncertainty to guess Bob’s input \( \beta \) with high probability, for some values of the experimental parameters.

Note that the actual experimental parameters reported in Ref. \([12]\) are different: \( N = 2.2 \times 10^6, \eta \approx 0.06 \) and \( \mu = 0.05 \). The values of \( d_0, d_1 \) and the uncertainties of Bob’s detection efficiencies were not reported by Ref. \([13]\). Even if we assume the above values for \( d_0 \) and \( d_1 \) and uncertainties of the detection efficiencies not greater than 0.02, we have not shown the attack discussed allows Alice to guess \( \beta \) with probability close to unity in the experiment actually implemented. What our illustration shows is that reproducing the implementation with modestly different and plausible parameters leads to an unnoticed insecurity.

As discussed in the main text, we assume that Alice knows which of her prepared pulses have two photons. Alice prepares the states perfectly. We assume that Alice prepares in the state \( |0\rangle \) with probability close to unity in at least one of the two Bob’s detectors if \( i = 1 \), and that it does not activate any detection if \( i = 0 \), when Bob measures in the basis \( B_\beta \), for \( \beta \in \{0,1\} \). We compute \( P_\beta(i) \) for \( i, \beta \in \{0,1\} \) below and show that \( P_0(1) > P_1(1) > 0 \) for \( \eta_0 > \eta_1 \). Thus, we have \( E(N_{0}^{\text{rep},0}) > E(N_{0}^{\text{rep},1}) \), where

\[
E(N_{0}^{\text{rep},\beta}) = N e^{-\mu \bar{N}_\beta(1)/8} \tag{D7}
\]

is the expectation value of the random variable \( N_{0}^{\text{rep},\beta} \), for \( \beta \in \{0,1\} \). Therefore, since \( P_0(1) > P_1(1) > 0 \), we can find numbers \( \delta > 0 \) and \( G \) such that

\[
E(N_{0}^{\text{rep},0})(1 + \delta) = E(N_{0}^{\text{rep},0})(1 - \delta) = G. \tag{D8}
\]

It is straightforward to obtain that

\[
\delta = \frac{P_0(1) - P_1(1)}{P_0(1) + P_1(1)}, \tag{D9}
\]

\[
G = \frac{N e^{-\mu \bar{N}_0(1)/8} P_0(1) P_1(1)}{4(P_0(1) + P_1(1))}. \tag{D10}
\]

Alice’s guessing strategy is as follows. Bob measures in the basis \( B_\beta \) and Alice knows the value of \( N_{0}^{\text{rep},\beta} \), for some \( \beta \in \{0,1\} \). But Alice does not know the value of \( \beta \), which she is trying to guess. To clarify this issue, let us denote \( N_{0}^{\text{rep}} = N_{0}^{\text{rep},\beta} \). Alice computes the value of \( N_{0}^{\text{rep}} \) from the pulses for which Bob reported \( m = 1 \). If \( N_{0}^{\text{rep}} \leq G \), Alice guesses \( \beta = 1 \), otherwise she guesses \( \beta = 0 \). As we show below, from \([DS]\) and from Chernoff bounds, Alice’s probability of failure \( P_{\text{fail}} \) in guessing \( \beta \) is very small for \( N \) large enough.

We compute an upper bound on Alice’s probability of failure \( P_{\text{fail}} \). From \([D9]\), and since we show below that \( P_0(1) > P_1(1) > 0 \) from \( \eta_0 > \eta_1 \), we have \( 0 < \delta < 1 \). It follows that

\[
P_{\text{fail}} = \frac{1}{2} \left( \text{Prob}(N_{0}^{\text{rep},0} \leq G) + \text{Prob}(N_{0}^{\text{rep},1} > G) \right)
< \frac{1}{2} \left( e^{-\frac{E(N_{0}^{\text{rep},0}) \bar{N}_0^2}{2}} + e^{-\frac{E(N_{0}^{\text{rep},1}) \bar{N}_0^2}{2}} \right)
= \frac{1}{2} \left( e^{-\frac{N e^{-\mu \bar{N}_0(1)^2/8}}{4\delta}} + e^{-\frac{N e^{-\mu \bar{N}_0(1)^2/8}}{4\delta}} \right), \tag{D11}
\]

where in the first line we used the definition of Alice’s guessing strategy; in the second line we used \([D8]\), \( 0 < \delta < 1 \) and Chernoff bounds \([22]\); and in the last line we used \([D7]\). Thus, we see from \([D11]\) that Alice’s probability of failure can be negligible for \( N \) large enough.
It is important to note that Bob's reported detection frequencies are the same for both cases: 1) when he measures all the received pulses in the computational basis ($\beta = 0$), and 2) when he measures all the received pulses in the Hadamard basis ($\beta = 1$). This is easy to see by noting the following. First, Alice prepares BB84 states randomly. Second, Bob's detection probabilities for pulses prepared by Alice in the state $|0\rangle$ ($|1\rangle$) and measured by Alice in a basis $B_\beta$ are the same for pulses prepared by Alice in the state $|+\rangle$ ($|-\rangle$) and measured by Bob in a basis $B_\bar{\beta}$ and vice versa. Thus, in the symmetrization of losses strategy implemented by Bob he gets the ratio $R$ very close to unity, for large $N$. We conclude from this attack that the symmetrization of losses strategy does not guarantee to Bob that Alice cannot obtain information about her choice of basis $b$. It follows that the experimental demonstration of bit commitment of Ref. [12] is not hiding; hence, it is not unconditionally secure.

We compute $P_0(1)$ and $P_1(1)$ and we show that $P_0(1) > P_1(1) > 0$, for $\eta_0 > \eta_1 > 0$. Both photons of a two-photon pulse prepared by Alice in the state $|0\rangle$ go to the detector $D_0$ when Bob measures in the computational basis (i.e. when $\beta = 0$). Thus, we have

$$P_0(1) = 1 - \left(1 - d_0\right)\left(1 - d_1\right)\left(1 - \eta_0\right)^2,$$

where $d_i$ the probability of a dark count by the detector $D_i$, for $i \in \{0, 1\}$. On the other hand, when Bob measures in the Hadamard basis (i.e. when $\beta = 1$), each photon goes to the detector $D_i$ with probability $\frac{1}{2}$. Thus, we have

$$P_1(1) = 1 - \frac{\left(1 - d_0\right)\left(1 - d_1\right)}{4}\left[(1 - \eta_0)^2 + (1 - \eta_1)^2 \right]$$

$$+ 2(1 - \eta_0)(1 - \eta_1).$$

Note that (D12) and (D13) follow straightforwardly from Lemma 3 of the main text. It follows from (D12) and (D13) that $P_0(1) > P_1(1) > 0$, for $\eta_0 > \eta_1 > 0$.

We compute an example of Alice's probability of failure $P_{\text{fail}}$ in this attack. We consider the parameters $d_0 = d_1 = 10^{-5}$, $\mu = 0.05$, $\eta_0 = 0.12$, $\eta_1 = 0.08$, $N = 2 \times 10^7$. These are reasonable experimental parameters. For example, $\mu = 0.05$, $N = 2.2 \times 10^6$ and values of $\eta$ around 0.06 are reported by Ref. [13]. We note that our chosen value for $N$ is roughly only ten times the value chosen in Ref. [13]. Although Ref. [13] does not report this, uncertainties in detection efficiency of 0.02 or higher are usual; hence, values $\eta_0 = 0.12$ and $\eta_1 = 0.08$ are reasonable. Moreover, a reasonable experimental value for the dark count rate is 1000/s, which for a standard gate width value of 10 ns gives a dark count probability of $10^{-5}$. From (D9), (D12), and (D13), we obtain $P_0(1) = 0.2256$, $P_1(1) = 0.1900$, $\delta = 0.0857$. Thus, from (D11), we obtain $P_{\text{fail}} < 0.035$.

The previous attack can straightforwardly be extended in various ways. For example, Alice may try to guess Bob's measurement choice $\beta \in \{0, 1\}$ from pulses for which Bob reported $m = 1$ that Alice prepared in some particular state $|\psi\rangle$ from the BB84 set with some particular number of photons $k$, or with number of photons in some range, for example with $k \geq 2$. More generally, the idea of the previous attack is that Alice follows the protocol agreed with Bob, but still is able to exploit the fact that Bob's detectors have different detection efficiencies $\eta_0 \neq \eta_1$, and that she has some knowledge about $\eta_0$ and $\eta_1$.

In the previous attack and extensions discussed above, Alice follows the protocol agreed with Bob, i.e. she prepares BB84 states randomly with a weak coherent source set to a small average photon number $\mu$ previously agreed with Bob. This guarantees to Alice that Bob cannot detect her cheating, because Alice is following the agreed protocol. In more general attacks, Alice may deviate from the agreed protocol in various ways. For example, she may prepare BB84 states with a probability distribution different to random, or she may prepare more general states, she could prepare some photon pulses with different average photon number, she could use different photon sources, etc. However, all these variations from the agreed protocol may be detected in principle by Bob. Bob could, for example, apply some specific quantum measurements in a subset of the received pulses and verify that the detection probabilities and the outcome probabilities correspond to the expected values in the agreed protocol.

We note that the previous attack exploits the fact that the probability that Bob reports the detection of a pulse is different for different measurement basis. A partial countermeasure against this attack, or extensions, consists in implementing a nontrivial probabilistic reporting strategy, discussed in the main text, with appropriate values of the reporting probabilities $S_{c_0,c_1,\beta}$, for $c_0,c_1,\beta \in \{0,1\}$. However, as shown in Theorem 4 of the main text, for any nontrivial probabilistic reporting strategy applied by Bob, Alice can obtain some information about Bob's chosen bit $\beta$. Thus, this countermeasure cannot be perfectly effective.

\begin{enumerate}
\item[\textbf{e.}] Extending the bounds of Lemmas 6 and 7
\end{enumerate}

We recall that in Ref. [13] Bob applies a particular form of the symmetrization of losses as reporting strategy, in which the goal is to symmetrize his detection probabilities for his both choices $\beta \in \{0,1\}$ of measurement bases. However, below we deduce an upper bound on the probability that Alice can guess Bob's bit $\beta$ when Bob applies either the reporting strategy II or the reporting strategy III, with the parameters of Lemmas 6 and 7, respectively.

The bounds of Lemmas 6 and 7 apply to the bit commitment protocol of Ref. [13] when Alice implements a multi-photon attack consisting in a single photon pulse and Bob applies reporting strategy II or III, respectively. Thus, Lemma 6 implies an upper bound on Alice's probability to guess Bob's bit $\beta$ with a multi-photon attack.
of a single pulse. Alice can extend her attack by sending various multi-photon pulses. In principle, the $N$ pulses that Alice sends Bob in the protocol can be chosen by Alice as multi-photon pulses with appropriately chosen photon numbers $k$. Lemmas [5] and [6] or [5] and [7] can be used to deduce an upper bound on Alice's probability $P_{\text{guess}}$ to guess $\beta$ for this more general case, when Bob applies reporting strategy II or III, respectively.

Let us assume for now that Bob applies an arbitrary reporting strategy. For $i \in [N]$, let $k_i$ be the number of photons encoded in the polarization degrees of freedom of the $i$th pulse. We define $B_i$ as a number satisfying

$$\left| P_{\text{report}}(1|1, \rho_i, k_i) - P_{\text{report}}(1|0, \rho_i, k_i) \right| \leq B_i,$$

(D14)

for the reporting strategy applied by Bob, and for any quantum state $\rho_i$ of $k_i$ qubits encoded in the $k_i$ photons of the $i$th pulse, which may be entangled among the $k_i$ qubits, and which may also be entangled with any other quantum systems. For example, if Bob applies the reporting strategy II with the parameters of Lemma [6] then $B_i$ can be given by the bound $B_{\text{II}}$ of Lemma [6] which is valid for any $k_i \in \{0, 1, 2, \ldots\}$. If Bob applies the reporting strategy III with the parameters of Lemma [7] then $B_i$ can be given by the bound $B_{\text{III}}$ of Lemma [7] which is valid for any $k_i \in \{0, 1, 2, \ldots\}$. Furthermore, if Bob applies the reporting strategy III with the parameters of Lemma [2] and $k_i \in \{0, 1\}$ then $B_i$ can be given by the bound $B_{\text{II}}^{k_i}$ of Lemma [2]. We show below that

$$P_{\text{guess}} \leq \frac{1}{2} + \frac{1}{2} \sum_{i=1}^{N} B_i,$$

(D15)

for any multi-photon attack by Alice.

If Bob applies the reporting strategy II with the parameters of Lemma [6] then we have from (D15) and from Lemma [6] that

$$P_{\text{guess}} \leq \frac{1}{2} + \frac{NB_{\text{II}}}{2},$$

(D16)

for any multi-photon attack by Alice. However, as illustrated in Fig. [4] the bound $B_{\text{II}}$ of Lemma [6] is not very small even for relatively close values for the detection efficiencies. Since $N$ is usually required to be large in order to guarantee security against Bob – for example, $N = 2.2 \times 10^6$ in the protocol of Ref. [13] – the upper bound on $P_{\text{guess}}$ given by (D16) is not smaller than unity for any practical case.

It seems that our bounds would be more useful if Bob applies the reporting strategy III instead. Suppose that Bob applies reporting strategy III with the parameters of Lemma [4]. From the $N$ pulses that Alice sends Bob, let $N_{\text{empty}}$, $N_{\text{single}}$ and $N_{\text{mult}}$ be the number of pulses with zero photons, with one photon, and with more than one photon, respectively. Suppose that Bob can guarantee with probability at least $1 - \epsilon$ that

$$N_{\text{empty}} \geq (1 - \delta_{\text{empty}})N,$$

(D17)

$$N_{\text{mult}} \leq \delta_{\text{mult}} N,$$

(D18)

where

$$0 \leq \delta_{\text{mult}} \leq \delta_{\text{empty}} \leq 1,$$

(D19)

for some $0 \leq \epsilon << 1$. Bob could guarantee this by aborting if the number of pulses not producing any click is below a threshold, or if the number of double clicks is above a threshold, for instance. These thresholds must be chosen carefully so that the probability that Bob aborts is negligible if Alice and Bob follow the agreed protocol.

Since, from Lemmas [2] and [7] we have $B_{\text{III}}^0 \leq B_{\text{III}}^1 \leq B_{\text{III}}$ for $\delta$ small enough, it follows from (D15), from (D17) – (D19), and from Lemmas [2] and [7] that

$$P_{\text{guess}} \leq \epsilon + (1 - \epsilon) \left[ \frac{1}{2} + \frac{N}{2} \left( (1 - \delta_{\text{empty}})B_{\text{III}}^0 + (\delta_{\text{empty}} - \delta_{\text{mult}})B_{\text{III}}^1 + \delta_{\text{mult}}B_{\text{III}} \right) \right].$$

(D20)

Bob can always guarantee (D17) and (D19) with $\delta_{\text{empty}} = 1$ and any $\delta_{\text{mult}} \in [0, 1]$. In this case, if (D18) is also satisfied, then (D20) reduces to

$$P_{\text{guess}} \leq \epsilon + (1 - \epsilon) \left[ \frac{1}{2} + \frac{N}{2} \left( (1 - \delta_{\text{mult}})B_{\text{III}}^1 + \delta_{\text{mult}}B_{\text{III}} \right) \right].$$

(D21)

We see from Lemma [2] that $B_{\text{III}} \leq 11\delta + 3\delta^2$. Thus if the dark count probabilities are small enough; more precisely, if $N\delta << 1$, then the bound (D21) can guarantee $P_{\text{guess}} - \frac{1}{2} << \frac{1}{2}$ if $\epsilon << 1$ and $N\delta_{\text{mult}}B_{\text{III}} << 1$.

The bound (D21) seems promising in protocols agreed by Alice and Bob where the fraction of pulses with more than one photon is small enough. For example, if in the protocol agreed with Bob, Alice has a source of pairs of entangled photons in which she measures one of the photons and sends the other one to Bob, with transmissions considered valid if Alice obtains a measurement outcome, the probability that a pulse has more than one photon is very small. Thus, Bob expects that the fraction of pulses with more than one photon is small, if Alice follows the agreed protocol.

The bound (D21) with $\delta_{\text{empty}} << 1$ seems promising in protocols agreed by Alice and Bob where the fraction of pulses with more than one photon is small enough and the fraction of empty pulses is large enough. For example, if in the protocol agreed by Alice and Bob Alice uses a weak coherent source with small average photon number $\mu$, the probability that a pulse is empty is $p_0 = e^{-\mu} \approx 1$, and the probability that a pulse has more than one photon is $p_{\text{mult}} = 1 - (1 + \mu)e^{-\mu} << 1$. Thus, Bob expects that the the fraction of empty pulses is large and the fraction of pulses with more than one photon is small, if Alice and Bob follow the agreed protocol.

If useful partial security can indeed be attained with current technology by (for example) these methods, it would be worth exploring whether greater security can
be attained by extending the bit commitment protocols. Suppose for example that one can implement a bit commitment protocol with a guarantee that $P_{\text{guess}} < \frac{1}{2} + \epsilon_{\text{hiding}}$ and $p_0 + p_1 < 1 + \epsilon_{\text{binding}}$, where $\epsilon_{\text{hiding}} \ll \frac{1}{2}$ and $\epsilon_{\text{binding}}$ is very small. This guarantee may be conditional on some assumptions, for example that Alice only uses photonic sources, with no side-channel attacks. One could then, for example, consider a new protocol with $M$ iterations of the above as sub-protocols in which Bob commits to bits $z_1, \ldots, z_M$. The new protocol then commits Bob to the XOR bit $z = z_1 \oplus \cdots \oplus z_M$. If Alice carries out only the attacks we have described separately on each iteration, she obtains incomplete information about each $z_i$. Hence, by the piling-up lemma \[78\], her information about the committed bit $z$ tends to zero as $M$ gets large. However, whether Alice has more powerful attacks (under the given assumptions) needs to be analysed, as does the dependence of $\epsilon_{\text{binding}}$ on $M$.

We leave as open problems to investigate whether the bounds \[D20\] and \[D21\] can provide useful security in practice and (if so) whether variant protocols offer further practical security advantages. Similar comments apply to other implementations of bit commitment schemes discussed below.

We show \[D15\]. In an arbitrary multi-photon attack, Alice encodes a quantum state $\rho$ in the $N$ photon pulses that Alice sends Bob. Each pulse has an arbitrary number of photons chosen by Alice. The state $\rho$ is an arbitrary entangled state among all the qubits encoded by the polarization degrees of freedom of the photons in the $N$ pulses, which can also be entangled with an ancilla held by Alice.

Bob sends Alice a message $m = (m_1, \ldots, m_N) \in \{0,1\}^N$ indicating that the $j$th pulse produced a valid measurement outcome if $m_j = 1$, or otherwise if $m_j = 0$, for $j \in [N]$. Let $P(m|\beta)$ be the probability that Bob sends the message $m \in \{0,1\}^N$ when he measures in the basis $B_\beta$, and let $P_\beta$ denote the probability distribution for $m \in \{0,1\}^N$ given $\beta$, for $\beta \in \{0,1\}$. The probability $P_{\text{guess}}$ that Alice guesses Bob’s bit $\beta$ satisfies

$$P_{\text{guess}} \leq \frac{1}{2} + \frac{1}{2} \|P_0 - P_1\|$$

$$= \frac{1}{2} + \frac{1}{4} \sum_m |P(m|0) - P(m|1)|,$$

(D22)

where $\|P_0 - P_1\|$ is the variational distance between the probability distributions $P_0$ and $P_1$, where in the second line we used the definition of the variational distance, and where $m$ runs over $\{0,1\}^N$.

We show below that

$$\sum_m |P(m|0) - P(m|1)| \leq 2 \sum_i B_i.$$

(D23)

Thus, from \[D22\] and \[D23\] we obtain the bound \[D15\].

Let $m_0 = 1$. We have

$$P(m|\beta) = \prod_{i=1}^N P_i(m_i|m_0m_1 \cdots m_{i-1} \beta),$$

(D24)

where $P_i(j_i|j_0j_1 \cdots j_{i-1} b)$ is the probability that $m_i = j_i$ given that $m_t = j_t$ and that $\beta = b$, for $(j_0, \ldots, j_N) \in \{0,1\}^N + 1$, $b \in \{0,1\}$, $l \in \{0,1, \ldots, i - 1\}$ and $i \in [N]$. From \[D23\] and \[D24\] we see that \[D23\] follows from

$$2 \sum_{i=1}^N B_i \geq \sum_m \prod_{i=1}^N P_i(m_i|m_0m_1 \cdots m_{i-1}0)$$

$$- \prod_{i=1}^N P_i(m_i|m_0m_1 \cdots m_{i-1}1).$$

(D25)

We show \[D26\]. Let $\rho_i(j_1 \ldots j_i - 1 b)$ be the quantum state encoded in the $k_i$ qubits of photon-polarization in the $i$th pulse when $m_i = j_i$ and $\beta = b$, for $l \in \{1,2, \ldots, i - 1\}$, $b \in \{0,1\}$ and $i \in [N]$. We see that

$$P_i(m_i|m_0m_1 \cdots m_{i-1} \beta) = P_{\text{report}}(m_i|\beta, \rho_i(m_1 \cdots m_{i-1} \beta), k_i).$$

(D26)

Thus, from \[D14\], we have

$$|P_i(1|m_0m_1 \cdots m_{i-1}1) - P_i(1|m_0m_1 \cdots m_{i-1}0)| \leq B_i,$$

(D27)

for $i \in [N]$.

We show \[D26\] by induction. We first show \[D26\] for the case $N = 1$. We have,

$$\sum_{m_1=0}^1 |P_1(m_1|m_01) - P_1(m_1|m_00)|$$

$$= 2|P_1(1|m_01) - P_1(1|m_00)|$$

$$\leq 2B_1,$$

(D28)

as claimed, where in the first line we used that $P_1(1|m_00) = 1 - P_1(0|m_00)$ for $\beta \in \{0,1\}$, and in the second line we used \[D27\] for the case $i = N = 1$.

Now we assume that \[D26\] holds for the case $N = M \in \mathbb{N}$. We show that \[D26\] holds for the case $N = M + 1$. To simplify notation we take $m \in \{0,1\}^{M+1}$, $y = (m_0, m_1, \ldots, m_N)$ and $x = m_{N+1}$. Using a telescoping
sum, we have

\[
W = \sum_{x} \sum_{y} \left| P_{M+1}(x|y1) - P_{M+1}(x|y0) \right| \times \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}0) \times \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}1) + \left( \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}1) - \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}0) \right) \times P_{M+1}(x|y1) \\
= \sum_{y} \left| (P_{M+1}(0|y1) - P_{M+1}(0|y0)) \times \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}0) \times \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}1) + \left( \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}1) - \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}0) \right) \times P_{M+1}(0|y1) \right| \\
+ \sum_{y} \left| (P_{M+1}(1|y1) - P_{M+1}(1|y0)) \times \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}0) \times \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}1) + \left( \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}1) - \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}0) \right) \times P_{M+1}(1|y1) \right|
\]

where \( C_y = \max \{ C_y^{-1,-1}, C_y^{-1,1}, C_y^{1,-1}, C_y^{1,1} \} \), and where

\[
C^{a,a'}_y = a \left( \left( \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}1) - \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}0) \right) \times P_{M+1}(0|y1) \right) + a' \left( \left( \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}1) - \prod_{i=1}^{M} P_i(y_i|y_0y_1 \cdots y_{i-1}0) \right) \times P_{M+1}(1|y1) \right),
\]

for \( a, a' \in \{0, 1\} \). Using that \( P_{M+1}(0|y\beta) + P_{M+1}(1|y\beta) = 1 \), for all \( y \) and \( \beta \in \{0, 1\} \), we obtain from (D30) that

\[
C^{a,a}_y \leq \sum_{y} C_y,
\]

(D29)
for all \( y \) and for \( a \in \{-1, 1\} \). Similarly, we obtain

\[
C_y^{a,-a} = 2a(P_{M+1}(0|y1) - P_{M+1}(0|y0)) \times \\
\times \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-10) \\
+ a(2P_{M+1}(0|y1) - 1) \times \\
\times \left( \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-11) \\
- \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-10) \right) \\
\leq 2|P_{M+1}(0|y1) - P_{M+1}(0|y0)| \times \\
\times \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-10) \\
+ |2P_{M+1}(0|y1) - 1| \times \\
\times \left| \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-11) \\
- \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-10) \right| \\
\leq 2|P_{M+1}(0|y1) - P_{M+1}(0|y0)| \times \\
\times \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-10) \\
+ \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-11) \\
- \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-10) \right|, \tag{D32}
\]

and \( \text{D27} \), we have

\[
W \leq \sum_{y} \left[ 2|P_{M+1}(0|y1) - P_{M+1}(0|y0)| \times \\
\times \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-10) \\
+ \sum_{y} \left| \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-11) \\
- \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-10) \right| \right] \\
\leq 2B_{M+1} \sum_{y} \prod_{i=1}^{M} P_i(y_i|y_0 y_1 \cdots y_i-10) + 2 \sum_{i=1}^{M} B_i \\
= 2B_{M+1} \sum_{y} P(y|0) + 2 \sum_{i=1}^{M} B_i \\
= 2 \sum_{i=1}^{M+1} B_i, \tag{D33}
\]

as claimed, where in the second line we used \( \text{D27} \) with \( i = M + 1 \) and that \( |P_{M+1}(0|y1) - P_{M+1}(0|y0)| = |P_{M+1}(1|y1) - P_{M+1}(1|y0)| \), and the assumption that \( \text{D25} \) holds for the case \( N = M \); where in the third line we used \( \text{D24} \); and where in the last line we used \( \sum_{y} P(y|0) = 1 \).

2. Multi-photon attacks on the relativistic
quantum bit commitment protocol of Ref. \[14\]

Ref. \[14\] demonstrated Kent’s \[12\] quantum relativistic
protocol for bit commitment. We show below that there are multi-photon attacks that apply to the protocol of Ref. \[14\], which imply that this protocol is not perfectly hiding.

In the notation of Ref. \[14\], Alice is the committer. However, we follow our usual convention, taking Bob to be the committer.

The protocol of Ref. \[14\] is a relativistic quantum protocol. The attacks discussed below are implemented in the quantum stage of the protocol, which is nonrelativistic. For this reason, here we only need to discuss the quantum stage.

The nonrelativistic quantum stage of the protocol of Ref. \[14\] is equivalent to the quantum stage of the protocol of Ref. \[13\], discussed in section \[13a\]. Alice and Bob use setup I discussed in the main text and illustrated in Fig. 1 of the main text. Alice’s photon source is a weak coherent source with small average photon number \( \mu \). Alice sends Bob \( N \) photon pulses, each encoding in the polarization a qubit state chosen randomly from the BB84 set. Bob chooses a random bit \( \beta \). Immediately after their reception, Bob measures each of the \( N \) photon pulses in the qubit orthogonal basis \( B_\beta \), where \( B_0 \)
and $B_1$ are the computational and Hadamard bases, respectively. In order to deal with losses in the quantum channel, for each pulse sent by Alice, Bob sends Alice a message $m = 1$ if the pulse produced a valid measurement outcome and $m = 0$ otherwise.

We note that in the protocol of Ref. 14, there are two setups equivalent to setup I (see Fig. 1 of the main text) that work in parallel. For this reason Bob has four detectors in that protocol. Despite this difference with the setup of Ref. 13, the analyses of section D.1 apply to the protocol of Ref. 14 too, because Alice may simply apply parallel attacks on both setups, or she can choose to apply attacks in only one of the setups.

Differently to the protocol of Ref. 13, in the protocol of Ref. 14, Bob’s committed bit is $\beta$. In the multi-photon attacks discussed in section D.1, for the protocol of Ref. 13, Alice tries to guess Bob’s bit $\beta$. Thus, as discussed below, some of the attacks of section D.1 apply to the protocol of Ref. 14.

Unlike Ref. 13, Ref. 14 does not implement the symmetrization of losses strategy. Instead, Ref. 14 applies the countermeasure in which Bob reports a valid measurement outcome, i.e. sets $m = 1$, for each pulse for which at least one detector clicks. Thus, multi-photon attack I does not apply.

However, the versions of the multi-photon attack II discussed in sections D.1c and D.1d apply to the protocol of Ref. 14. This is because it cannot be guaranteed that Bob’s detection efficiencies are exactly equal. In the actual experiment, the measured values for Bob’s detection efficiencies were 50.4±1.1%, 50.4±0.4%, 52.4±1.0% and 50.2±1.1% [3]. However, Ref. 14 also makes the important point that Bob could include calibrated attenuators in front of his detectors to make their detection efficiencies equal, in order to defend against attacks exploiting unequal detector efficiencies. As far as we are aware, this is the first discussion of this valuable countermeasure (albeit not in the context of the specific attacks we consider here). We note, though, that even if this countermeasure were implemented, experimental uncertainties would remain. There is no way to guarantee that Bob’s detector efficiencies are exactly equal for a given frequency, nor that they are precisely frequency-independent or that Alice uses precisely the stipulated frequency.

The upper bound on Alice’s probability to guess Bob’s bit $\beta$ derived in section D.1c assumes that Bob sets $m = 1$ for pulses producing a click in at least one of Bob’s detectors and that Bob’s detector efficiencies are not exactly equal. Thus, this bound also applies to the protocol of Ref. 14. However, this particular bound does not appear strong enough to provide any security guarantee for the parameters of Ref. 14. It would also be very interesting to explore whether practical security could be attained by a combination of the use of attenuators and other methods, using the results of section D.1c. For example, Alice could be required to use a single photon source, and Bob could test a subset of the received pulses to ensure that the number of multi-photon pulses is suitably small.

3. A multi-photon attack on the quantum coin-flipping protocol of Ref. 30

Ref. 30 demonstrated a nonrelativistic quantum strong coin-flipping protocol and argued that the implementation guaranteed with information theoretic security an upper bound $p_c$ on the probability that an all-powerful malicious party can bias the coin. This bound depends on various experimental parameters, including the honest abort probability and the distance between Bob and Alice, and is strictly smaller than unity for some parameter values (see Figure 2 of Ref. 30, for example).

Ref. 30 does not say whether a double detection event is registered as a measurement outcome, and if so, how it is registered. Assuming that Bob only assigns single clicks as valid measurement outcomes, we discuss below how a version of the multi-photon attack I discussed in the main text applies to the protocol of Ref. 30, where Alice succeeds in setting the outcome of the coin flip with probability very close to unity.

As discussed below, if Bob reports single and double clicks as valid measurement outcomes, he can only reduce Alice’s success probability in this attack to a value slightly below $\frac{2}{3}$. It is not clear whether Ref. 30 obtained an upper bound on the probability $P_{\text{Alice}}$ that dishonest Alice can bias the coin flip that is below $\frac{2}{3}$ for any values of the possible experimental parameters, which would imply that this attack implies violation of the bound. In particular, Figure 2 of Ref. 30 suggests that the smallest value for this bound demonstrated experimentally was approximately 0.91, achieved for a communication distance of 15 km. Nevertheless, Equation (1) in the Supplementary Information of Ref. 30 states that $P_{\text{Alice}} \leq \frac{3}{4} + \frac{1}{2} \sqrt{y(1-y)}$, where the parameter $y$ satisfies $y \in (\frac{1}{2},1)$. There exist $y \in (\frac{1}{2},1)$ for which $\frac{3}{4} + \frac{1}{2} \sqrt{y(1-y)} < \frac{2}{3}$. Thus, if any parameter $y$ from the range $(\frac{1}{2},1)$ can be obtained in principle experimentally then our attack implies a violation of the security bound derived in Ref. 30.

The quantum strong coin-flipping protocol of Ref. 30 is the following. First, Alice sends to Bob $N$ photon pulses prepared in states $|\Phi_{\alpha_i,\gamma_i}\rangle$, encoding the bit $\gamma_i$ in a basis labelled by the bit $\alpha_i$, and their labels $i$, for $i \in [N] = \{1,\ldots,N\}$ and for a predetermined integer $N$. The states are given by $|\Phi_{\alpha_i,0}\rangle = \sqrt{\gamma_0}|0\rangle + (-1)^{\alpha_i}\sqrt{1-\gamma_0}|1\rangle$ and $|\Phi_{\alpha_i,1}\rangle = \sqrt{1-\gamma_0}|0\rangle - (-1)^{\alpha_i}\sqrt{\gamma_0}|1\rangle$, for $\alpha_i \in \{0,1\}$, for some predetermined parameter $y \in (\frac{1}{2},1)$. We note that $B_{\alpha_i} = \{|\Phi_{\alpha_i,r}\rangle\}_{r=0}^1$ forms an orthonormal basis, for $\alpha_i \in \{0,1\}$. Second, Bob measures the $i$th pulse in the basis $B_{\beta_i}$, where the bit $\beta_i$ is chosen randomly by Bob, and obtains some bit outcome
o_i or does not register any measurement outcome, for \( i \in [N] \). We note that due to losses and detection efficiencies smaller than unity, not all pulses produce a detection in Bob’s detectors, i.e. Bob does not obtain a measurement outcome for all \( i \in [N] \). Let \( j \in [N] \) be the first pulse for which Bob registers a measurement outcome, which is a bit \( o_j \). Third, Bob generates a random bit \( b \) and communicates \( b \) to Alice. Fourth, Alice communicates \( a_i \) and \( \gamma_i \) to Bob. Fifth, Bob checks whether \( a_i = \beta_j \), in which case Bob aborts if and only if \( o_j \neq \gamma_j \). If \( a_i \neq \beta_j \), Bob does not abort. If Bob does not abort then Bob and Alice agree that the outcome of the coin flip is \( a = \gamma_j \oplus b \), i.e. the XOR of the bit \( b \) given by Bob and the bit \( \gamma_j \) given by Alice. Ref. \([30]\) implemented the technique of symmetrization of losses presented in Ref. \([60]\) and discussed in the main text.

In the attack we describe below, we assume that in the protocol of Ref. \([30]\) double clicks are not assigned as valid measurement outcomes by Bob and that the symmetrization of losses technique is implemented as described in the main text. Thus, we assume that Bob assigns a valid measurement outcome to the detection event \((c, c)\) with some probability \( S_{c\bar{c}b} > 0 \) when he measured a pulse in the basis \( B_b \), in such a way that \( S_{c\bar{c}b} \) satisfies the conditions of Lemma \(2 \) in the main text, for \( c, \beta \in \{0, 1\} \). Let \( S_{\text{min}} = \min\{S_{c\bar{c}b}\}_{c, \beta \in \{0, 1\}} \). In particular, it is stated by Ref. \([30]\) that there was not any important deviation between the frequencies of detection events for the two measurement bases applied by Bob. However, Ref. \([30]\) reports a ratio of approximately 0.68 in the number of detections observed by Bob in his two detectors, giving a value of \( S_{\text{min}} = 0.68 \). Thus, in the protocol implemented with Alice, Bob assigned valid measurement outcomes to detection events of his detector with higher number of detections with a probability of 0.68, and to detection events of his detector with lower number of detections with unit probability.

The protocol uses a slight variation of setup I given in the main text (see Fig. \(1 \) of the main text). The experimental setup of Ref. \([30]\) consists in a plug and play system with a two-way approach: light pulses of 1550 nm are sent from Bob to Alice, and Alice uses a phase modulator to prepare the qubit states. The pulses are then reflected using a Faraday mirror and attenuated to the desired average photon number before being sent back to Bob. Finally, Bob uses a phase modulator to choose his measurement basis and register the detection events using two threshold single photon detectors. In practice, we can suppose that the experimental setup is equivalent to setup I given in Fig. \(1 \) of the main text.

\( b. \) Multi-photon attack I

In order to present an attack to the quantum coin flipping protocol above, we first make some observations. As in the experimental demonstration of Ref. \([30]\), we assume that Bob uses threshold single photon detectors for registering the outcome of his measurement. A measurement by Bob uses two single photon detectors \( D_0 \) and \( D_1 \). An outcome \( o_i \) corresponds to a detector \( D_i \) registering a detection, for \( D_i \in \{0, 1\} \).

Assuming that Bob only assigns valid measurement outcomes to detection events in which only one of his detectors click and that he applies the symmetrization of losses technique as described above, we present a version of the multi-photon attack I presented in the main text to the protocol of Ref. \([30]\). We assume that Bob is honest and that Alice is cheating. Alice chooses a set \( \Omega \subseteq [N] \) with \( M \) elements, for some positive integer \( M < N \). For \( i \notin \Omega \), Alice does not send any pulses to Bob. For \( i \in \Omega \), Alice sends a pulse with \( k \) photons in the state \( |\Phi_{\alpha_i, \gamma_i}\rangle \), where the bits \( \alpha_i \) and \( \gamma_i \) are chosen randomly by Alice. Alice chooses her desired coin flip outcome \( a \). Bob sends the index \( j \in [N] \) and the bit \( b \) to Alice. Let \( \tilde{\alpha}_j \) and \( \tilde{\gamma}_j \) be the bits that Alice sends Bob, indicating her supposed chosen basis and encoded bit, respectively. Alice sets \( \tilde{\gamma}_j = b \oplus a \). If \( \tilde{\gamma}_j = \gamma_j \) then Alice sets \( \tilde{\alpha}_j = \alpha_j \), otherwise she sets \( \tilde{\alpha}_j = \alpha_j \oplus 1 \). Alice sends \( \tilde{\alpha}_j \) and \( \tilde{\gamma}_j \) to Bob.

We show that this attack allows Alice to succeed with very high probability. First, we note that if Bob does not abort and if he assigns at least one measurement outcome, the outcome of the coin flip is \( \tilde{\gamma}_j \oplus b \), which equals the bit \( a \) chosen by Alice. It remains to be shown that the probability that Bob aborts or that he does not assign any measurement outcome is negligible. In order to illustrate the attack more easily, consider an ideal situation in which there are not dark counts at Bob’s detectors, Alice’s state preparations are perfect and Bob’s measurement outcomes do not have errors. Let us also consider the limit \( k \to \infty \), i.e. Alice prepares pulses with an infinite number of photons. Thus, we see that Bob can only register detection events at his detectors for pulses with labels from the set \( \Omega \). For \( i \in \Omega \), if \( \beta_i \neq \alpha_i \), i.e. if Bob measures in a basis different to the one of preparation by Alice, then an infinite number of photons go to the detector \( D_0 \) and an infinite number of photons go to the detector \( D_1 \); hence, both detectors register a detection, and Bob does not assign a measurement outcome to the pulse with label \( i \). On the other hand, for \( i \notin \Omega \), if \( \beta_i = \alpha_i \), i.e. if Bob measures in the basis of preparation by Alice, then all photons go to the detector \( D_{\gamma_i} \); hence, the detector \( D_{\gamma_i} \) registers a detection, and Bob assigns the measurement outcome \( o_i = \gamma_i \) with a probability greater or equal than \( S_{\text{min}} \). Thus, the first pulse for which Bob registers a measurement outcome, which has label \( j \), satisfies \( j \in \Omega \), \( \beta_j = \alpha_j \) and \( o_j = \gamma_j \). The probability for this to hold is the probability that Bob chooses \( \beta_i = \alpha_i \) and Bob assigns the detector click as a valid measurement outcome for at least one \( i \in \Omega \), which is easily seen to be greater or equal than \( 1 - \left( 1 - \frac{S_{\text{min}}}{2} \right)^M \).

Therefore, we see that in the case that \( \tilde{\gamma}_j = \gamma_j \), Alice reports \( \tilde{\alpha}_j = \alpha_j \oplus 1 = \beta_j \oplus 1 \) and \( \tilde{\gamma}_j = \gamma_j \oplus 1 = \alpha_j \oplus 1 \);
hence, Bob does not abort, as in this case $\beta_j = \tilde{\alpha}_j \oplus 1$. We see that Bob does not abort in any case, and Alice succeeds in her cheating strategy if Bob chooses $\beta_i = \alpha_i$ and Bob assigns the detector click as a valid measurement outcome for at least one $i \in \Omega$, which occurs with probability greater or equal than $1 - \left(1 - \frac{S_{\text{min}}}{M}\right)^M$. Thus, since $S_{\text{min}} > 0$, for $M$ large enough, Alice can make his cheating probability arbitrarily close to unity.

In practice, Alice cannot send pulses with infinite number of photons, the state preparation and measurements will have some errors, Bob’s detectors have nonzero dark count probabilities. However, it is easy to see that an adaptation of the attack discussed above can be applied in a realistic scenario. For example, given the parameters of the protocol agreed by Alice and Bob, Alice can simulate Bob’s detection probabilities and choose the set $\Omega$ to lie within the first few pulses, and pulses with labels not from the set $\Omega$ can be chosen by Alice to have specific average number of photons, in such a way that Bob’s detection probabilities are very close to what is expected in the agreed protocol. In practice, $N$ is chosen very large, for example $N$ is of the order of $10^{10}$ in the experimental demonstration of Ref. [30]. Thus, Bob can choose $M$ to be large but small compared to $N$, for example, $M = 40$, which gives $(1 - \frac{S_{\text{min}}}{M})^M = 6 	imes 10^{-8}$, for the value $S_{\text{min}} = 0.68$ reported by Ref. [30]. Alice cannot set the number of photons $k$ of the dishonest pulses to be infinite, but she can set the average photon number to a value $\mu >> 1$ with a coherent source, as in the attack that we have simulated experimentally and discussed in the main text, for example.

c. Partial countermeasures and more general attacks

Bob can apply a partial countermeasure against this attack by assigning a random measurement outcome to detection events in which both of his detectors register a detection. It is straightforward to see that in the ideal attack we discussed above with $M = 1$ and assuming there is no symmetrization of losses (i.e. that $S_{\text{min}} = 1$), with this partial countermeasure, Bob aborts with probability $\frac{1}{2}$, corresponding to the case $\beta_j = \alpha_j \oplus 1 = \tilde{\alpha}_j$, $\gamma_j = b \oplus a \oplus 1 = \tilde{\gamma}_j \oplus 1$ and $\alpha_j = \gamma_j = \tilde{\gamma}_j \oplus 1$. Thus, in this case, assuming that symmetrization of losses is implemented, the probability that Bob does not abort and assigns a valid measurement outcome is equal or greater than $\frac{1}{2} S_{\text{min}}$. Thus, in situations where $S_{\text{min}}$ is close to unity, Alice can succeed with this attack with probability close to $\frac{1}{2}$. It does not help Alice in this case to set $M >> 1$, as in this case it is not difficult to see that the probability that Bob aborts is equal or greater than $1 - \left(1 - \frac{S_{\text{min}}}{2M}\right)^M$, which approaches unity as $M$ increases.

In the attacks discussed above Alice does not send any pulses for $i \notin \Omega$. But this could be easily discovered by Bob if $M = |\Omega|$ is small, as for the case $M = 1$. Alice can refine her attacks by sending pulses with the statistics of the protocol agreed with Bob for $i \notin \Omega$ and to define $\Omega = \{1, 2, \ldots, M\}$, i.e to let $\Omega$ correspond to the first $M$ pulses. The attacks presented above apply straightforwardly in this case and the lower bounds on Alice’s probabilities to succeed in these attacks derived above hold in this case too.

In addition to reporting single and double clicks, a possible extra countermeasure by Bob to apply against the previous attacks is to choose the index $j$ randomly from the set $[N]$, instead of choosing $j$ as the index of the first successfully measured pulse, as in the protocol of Ref. [60]. In this way, Alice cannot effectively choose a small set $\Omega$ for her dishonest multi-photon pulses that guarantees with high probability that $j \in \Omega$. On the other hand if Alice chooses a large set $\Omega$ then Bob aborts with high probability, as discussed above.

Broadly, what the previous attack illustrates is that, because Alice has the ability to prepare pulses with many photons and because Bob’s single photon detectors are threshold detectors, the probabilities of Bob’s measurement outcomes are not in general proportional to $\langle \Phi_{a, \gamma_i} | \rho | \Phi_{a, \gamma_i} \rangle$, for photon pulses prepared by Alice to encode a qubit state $\rho$ in each photon, contrary to the assumption made in the security proof of Ref. [60].

4. A multi-photon attack on the quantum bit commitment protocol of Ref. [60]

a. The quantum bit commitment protocol of Ref. [60]

Ref. [60] demonstrated quantum bit commitment in the noisy storage model. Below, we present an attack to this protocol and show that it is insecure: we show that it is not hiding.

In the protocol of Ref. [60] Alice is the committer. Although this notation is different to the one introduced in section [C] we follow this notation here because it is consistent with an extension of setup I, which we introduce below. The protocol of Ref. [60] includes a subroutine that uses a setup different to the setup I described in the main text. We call this setup II (see Fig. 5).

In setup II, Alice has a source of pair of entangled photons. For each pair generated by Alice, she sends a photon to Bob and she measures the other photon randomly in one of two qubit orthogonal bases, $B_0$ and $B_1$. Bob also measures his photon randomly in the bases $B_0$ and $B_1$. Without loss of generality we suppose that $B_0$ = $\{ |0\rangle, |1\rangle \}$ is the computational basis and $B_1$ = $\{ |+\rangle, |\rangle \}$ is a qubit orthogonal basis where the Bloch vector of the qubit state $|+\rangle$ has an angle $\theta \in [0, \pi]$ from the $x$ axis towards the $z$ axis in the Bloch sphere. At each site, the random measurement is implemented with a 50 : 50 beam splitter, followed by two polarizing beam splitters and four single photon detectors. The quantum channel between the 50 : 50 beam splitter and one of the polarizing beam splitters contains a wave plate that rotates the polarization an angle $\frac{\pi}{2} - \theta$ from the $z$ axis towards the $x$ axis
FIG. 5. Setup II. Alice’s setup consists in a source of entangled photon pairs, a 50:50 beam splitter, a half-wave plate, two polarizing beam splitters and four threshold single photon detectors $D_0$, $D_1$, $D_+$ and $D_-$. Bob’s setup consists in a 50:50 beam splitter, a wave plate, two polarizing beam splitters ($PBS_{01}$ and $PBS_{+-}$) and four threshold single photon detectors $D_0$, $D_1$, $D_+$ and $D_-$. 

in the Bloch sphere. Thus, one of the polarizing beam splitters measures the received photon pulse in the basis $B_0$ and the other one measures the received photon pulse in the basis $B_1$. In particular, Bob’s polarizing beam splitters $PBS_{01}$ and $PBS_{+-}$ implement qubit measurements in the bases $B_0$ and $B_1$, respectively. The case $\theta = 0$ corresponds to $B_0$ and $B_1$ being the computational and Hadamard bases, respectively, which is the particular case considered in Ref. [60].

Alice and Bob have each four single photon detectors, each one corresponding to one of the four generated states. Let $D_0$, $D_1$, $D_+$ and $D_-$ be Bob’s detectors corresponding to the states $|0\rangle$, $|1\rangle$, $|\bar{+}\rangle$ and $|\bar{-}\rangle$, respectively. The detectors are threshold detectors, i.e., they cannot distinguish the number of photons producing a detection.

Let $0 \leq d_i < 1$ and $\eta_i \in (0, 1)$ be the dark count probability and the detection efficiency of Bob’s detector $D_i$, respectively, which we assume are known by Alice, for $i \in \{0, 1, +, -\}$. Let $\eta_{\min} = \min\{\eta_0, \eta_1, \eta_+, \eta_-\}$.

It is explicitly stated in Ref. [60] that only detection events where a single detector clicks are considered as valid measurement outcomes. Thus, in a valid round a pair of photon pulses generated by Alice produces a single click in one of Alice’s detectors and a single click in one of Bob’s detectors. In order to deal with losses in the quantum channel, for each photon pulse sent by Alice, Bob sends a message $m = 1$ to Alice indicating that a single click in one of his detectors is produced or a message $m = 0$ indicating the opposite. The symmetrization of losses technique is applied by Bob. More precisely, the following reporting strategy is applied by Bob in Ref. [60].

**Definition 1** (Symmetrization of losses in setup II (SLLII)). Bob tests his setup by preparing and measuring states as in the protocol agreed with Alice, a large number of times $N$ in parallel. Then, for $i \in \{0, 1, +, -\}$, Bob computes the frequency $F_i$ of detection events in which only the detector $D_i$ clicks, which provides a good estimate of the corresponding probability $P_i$ if $NF_i \gg 1$. Bob then computes numbers $S_i \in (0, 1]$ satisfying

\[ S_i F_i = F_{\min}, \]  

for $i \in \{0, 1, +, -\}$, where $F_{\min} = \min\{F_0, F_1, F_+, F_-\}$. Bob sends Alice the message $m = 1$ and assigns a valid measurement outcome corresponding to the detector $D_i$ with a probability $S_i$ if only the detector $D_i$ clicks, for $i \in \{0, 1, +, -\}$.

Similarly to Lemma 2 of the main text, the following lemma shows that the SLLII reporting strategy guarantees to Bob that Alice cannot obtain any information about Bob’s assigned measurement basis $B_\beta$ if Alice’s pulse does not have more than one photon and $d_i = 0$, for $\beta \in \{0, 1\}$, for arbitrary $\eta_i \in (0, 1)$ and for $i \in \{0, 1, +, -\}$. Furthermore, it guarantees that Alice cannot obtain much information about $\beta$ if Alice’s pulse does not have more than one photon and $0 < d_i \leq \delta$, for $0 < \delta << 1$ and $i \in \{0, 1, +, -\}$.

**Lemma 9.** Consider setup II illustrated in Fig. 5. Let $d_i \leq \delta$, for some $0 \leq \delta < 1$ and for $i \in \{0, 1, +, -\}$. Suppose that Alice sends Bob a single photon pulse ($k = 1$) in arbitrary qubit state $\rho$ or that she does not send him any photons ($k = 0$). Suppose that Bob applies the SLLII reporting strategy with

\[ S_i = \frac{\eta_{\min}}{\eta_i}, \]  

for $i \in \{0, 1, +, -\}$. Then

\[ |P_{\text{report}}(1, 1|\rho, k) - P_{\text{report}}(1, 0|\rho, k)| \leq 6\delta, \]  

for $k \in \{0, 1\}$, where $P_{\text{report}}(1, \beta|\rho, k)$ is the probability that Bob reports the message $m = 1$ to Alice and assigns a measurement in the basis $B_\beta$, for $\beta \in \{0, 1\}$.

Note that we have slightly changed the notation $P_{\text{report}}(1, \beta|\rho, k)$ used for setup I to $P_{\text{report}}(1, \beta|\rho, k)$ for setup II. This is because in setup I Bob chooses the measurement basis by appropriately setting the wave plate. However, in setup II, the assigned measurement basis is not chosen by Bob; it is an outcome, which depends on the detectors that are activated.

The proof of Lemma 9 uses Lemma 10 given below. Thus, it is presented below.

As stated in Ref. [60], it is a necessary condition for security against Alice that she cannot learn any information about the measurement bases obtained by Bob. It is claimed by Ref. [60] that the SLLII reporting strategy guarantees this condition. Below we show that this claim is wrong: that Alice can obtain a lot of information about Bob’s measurement bases.

**b. Multi-photon attack I**

We describe a version of multi-photon attack I that applies in setup II. The attack works equally well if Bob’s
setup is the same as in setup II, independently of whether Alice’s photon source is a source of pairs of entangled photons or not. What matters is that Alice sends Bob photon pulses and that Bob measures randomly in one of two bases, $\mathcal{B}_0$ and $\mathcal{B}_1$, using Bob’s setup of four threshold single photon detectors illustrated in Fig. [5].

**Definition 2** (Multi-photon attack I in setup II (MPAI)). Suppose that Alice and Bob use setup II, illustrated in Fig. [5]. Alice prepares a dishonest pulse of $k$ photons encoding a $k$-qubit state $\rho$ in the polarization degrees of freedom, for some nonnegative integer $k$ chosen by Alice. The quantum state $\rho$ is chosen by Alice and can be an arbitrary entangled state, which can also be entangled with an ancilla held by Alice. When specified, we will consider the particular case $\rho = \rho^{\otimes k}_{\text{qubit}}$ in which the dishonest pulse consist in $k$ photons, each of them encoding the qubit state $\rho_{\text{qubit}}$ with Bloch vector $\vec{r} = (r_x, r_y, r_z)$. Let $P_{\text{report}}(1, \beta | \rho, k)$ be the probability that Bob reports the message $m = 1$ to Alice and that Bob assigns a valid measurement outcome in the basis $\mathcal{B}_\beta$, for $\beta \in \{0, 1\}$. We assume that Alice knows the value of $P_{\text{report}}(1, \beta | \rho, k)$, for $\beta \in \{0, 1\}$. If $P_{\text{report}}(1, 0 | \rho, k) \geq P_{\text{report}}(1, 1 | \rho, k)$, and if Bob reports to Alice the message $m = 1$, Alice guesses that Bob’s obtained basis is $\mathcal{B}_0$. On the other hand, if $P_{\text{report}}(1, 1 | \rho, k) > P_{\text{report}}(1, 0 | \rho, k)$, and if Bob reports to Alice the message $m = 1$, Alice guesses that Bob’s obtained basis is $\mathcal{B}_1$. Thus, the probability that Alice guesses Bob’s obtained basis $\mathcal{B}_\beta$ for the dishonest pulse is given by

$$P_{\text{guess}} = \frac{\max_{\beta \in \{0, 1\}} \{P_{\text{report}}(1, \beta | \rho, k)\}}{P_{\text{report}}(1, 0 | \rho, k) + P_{\text{report}}(1, 1 | \rho, k)}.$$  \hfill (D37)

We note that we must condition on Bob assigning a measurement outcome, either in the basis $\mathcal{B}_0$ or in the basis $\mathcal{B}_1$. We show in Lemma [11] below that $P_{\text{report}}(1, 0 | \rho, k) \neq P_{\text{report}}(1, 1 | \rho, k)$ for a range of parameters. Thus, it follows from (D37) that $P_{\text{guess}} > \frac{1}{2}$. We also show that for a range of parameters it holds that $P_{\text{guess}} \to 1$ if $k \to \infty$. Thus, Alice can guess Bob’s assigned measurement basis for the dishonest pulse with great probability, which violates security against Alice.

The MPAII attack can be easily extended as follows. Let $N$ be the number of photon pulses that Alice sends Bob in the predetermined protocol. Alice chooses a subset $\Omega$ of labels for these $N$ pulses and prepares a dishonest pulse as in the MPAII attack if its label belongs to $\Omega$. For each pulse with label from the set $\Omega$, Alice measures the measurement basis assigned by Bob as in the MPAII attack.

Let $P_{\text{det}}(c_0, c_1, c_+, c_- | \rho, k)$ be the probability that the detector $D_0$ clicks if $c_0 = 1$ and does not click if $c_0 = 0$, that the detector $D_1$ clicks if $c_1 = 1$ and does not click if $c_1 = 0$, that the detector $D_+$ clicks if $c_+ = 1$ and does not click if $c_+ = 0$, and that the detector $D_-$ clicks if $c_- = 1$ and does not click if $c_- = 0$, for $c_0, c_1, c_+, c_- \in \{0, 1\}$, when Alice sends Bob a photon pulse of $k$ photons encoding the $k$-qubit state $\rho$ in the polarization degrees of freedom.

In order to present Lemma [11] we first need to introduce the following lemma.

**Lemma 10.** Consider Alice’s MPAII attack, which uses setup II illustrated in Fig. [5] in the particular case $\rho = \rho^{\otimes k}_{\text{qubit}}$ for some qubit state $\rho_{\text{qubit}}$ with Bloch vector $\vec{r} = (r_x, r_y, r_z)$. Suppose that Bob uses the SLM reporting strategy, with $S_i = \frac{\cos \eta_i}{\sin \eta_i}$, for $i \in \{0, 1, +, -\}$. The probability $P_{\text{report}}(1, \beta | \rho, k)$ that Bob sends the message $m = 1$ to Alice and assigns a measurement outcome in the basis $\mathcal{B}_\beta$, for $\beta \in \{0, 1\}$, is given by

$$P_{\text{report}}(1, 0 | \rho, k) = S_0 P_0 + S_1 P_1,$$
$$P_{\text{report}}(1, 1 | \rho, k) = S_+ P_+ + S_- P_-.$$  \hfill (D38)

where

$$P_0 = (1 - d_1)(1 - d_+)(1 - d_-) \left[ 1 - \frac{1}{2} \left( \eta_1 + (1 - \theta) \eta_0 \right) + \eta_0 (\eta_0 - \eta_1) + \eta_+ (\eta_+ - \eta_-) \right]^k,$$
$$P_+ = (1 - d_0)(1 - d_+)(1 - d_-) \left[ 1 - \frac{1}{2} \left( \eta_1 + q_0 (\eta_0 - \eta_1) + (1 - q_+ \eta_-) \right)^k \right.$$
$$\left. + (1 - q_+ \eta_-) \right] - (1 - d_1) \left[ 1 - \frac{1}{2} \left( \eta_1 + \eta_+ \right) + q_0 (\eta_0 - \eta_1) + \eta_+ (\eta_+ - \eta_-) \right]^k,$$
$$P_- = (1 - d_0)(1 - d_+)(1 - d_-) \left[ 1 - \frac{1}{2} \left( \eta_1 + q_0 (\eta_0 - \eta_1) \right) + q_+ \eta_+ \right]^k$$
$$\left. - (1 - d_+) \left[ 1 - \frac{1}{2} \left( \eta_1 + \eta_- \right) + q_0 (\eta_0 - \eta_1) + \eta_+ (\eta_+ - \eta_-) \right]^k \right),$$  \hfill (D39)

and where

$$q_0 = \frac{1}{2} (1 + r_z),$$
$$q_+ = \frac{1}{2} (1 + r_x \cos \theta + r_z \sin \theta).$$  \hfill (D40)

We note that we do not lose generality by considering that $\mathcal{B}_0$ is the computational basis and $\mathcal{B}_1$ is a qubit
orthogonal basis in the $x - z$ plane in the Bloch sphere. This is because any pair of qubit orthogonal bases $B_0$ and $B_1$ define a plane in the Bloch sphere. Without loss of generality we can take this plane to be the $x - z$ plane. Then, without loss of generality we can also suppose that $B_0$ is the basis along the $z$ axis, i.e. the computational basis.

Proof of Lemma 10. Consider Bob’s setup in Fig. 5. In the considered MPAII attack, Alice sends Bob a pulse of $k$ photons, where each photon encodes the qubit state $\rho_{\text{qubit}}$, for some nonnegative integer $k$. That is, $\rho = \rho_{\text{qubit}}^k$. Let $k_01$ be the number of photons that are transmitted through the 50:50 beam splitter towards the polarizing beam splitter PBS$_{01}$ and let $k_{-} = k - k_01$ be the number of photons that are reflected from the 50:50 beam splitter towards the polarizing beam splitter PBS$_{-}$, for $k_01 \in \{0, 1, \ldots, k\}$. Let $k_0$ and $k_1 = k_0 - k_01$ be the number of photons that go towards the detectors D$_0$ and D$_1$, respectively, for $k_0 \in \{0, 1, \ldots, k_01\}$. Let $k_-$ and $k_{+} = k - k_01 - k_+$ be the number of photons that go towards the detectors D$_+$ and D$_-$, respectively, for $k_{+} \in \{0, 1, \ldots, k - k_01\}$.

The probabilities that a photon is transmitted through the 50:50 beam splitter towards the polarizing beam splitter PBS$_{01}$ and reflected from the 50:50 beam splitter towards the polarizing beam splitter PBS$_{-}$ are both $\frac{1}{2}$. We note that we do not lose generality by supposing that the 50:50 beam splitter has transmission and reflection probabilities exactly equal to $\frac{1}{2}$. If these probabilities were different, these values could be absorbed in the efficiencies of the detectors, leaving the equivalent transmission and reflection probabilities of the 50:50 beam splitter effectively equal to $\frac{1}{2}$. The probabilities that a photon directed towards the polarizing beam splitter PBS$_{01}$ goes to the detectors D$_0$ and D$_1$ are $q_0 = \langle 0 | \rho_{\text{qubit}} | 0 \rangle = \frac{1}{2} (1 + r_z)$ and $q_1 = 1 - q_0$, respectively, where $r_z$ is the $z$ component of the Bloch vector $\vec{r}$ of the qubit state $\rho$. The probabilities that a photon directed towards the polarizing beam splitter PBS$_{-}$ goes to the detectors D$_+$ and D$_-$ are $q_+ = \langle + | \rho_{\text{qubit}} | + \rangle = \frac{1}{2} (1 + r_x \cos \theta + r_y \sin \theta)$ and $q_- = 1 - q_+$, respectively, where $r_x$ is the $x$ component of the Bloch vector $\vec{r}$ of the qubit state $\rho_{\text{qubit}}$ and where $\theta$ is the angle from the $x$ axis towards the $z$ axis of the Bloch vector $\vec{r}$ in the Bloch sphere.

Let $P_0(0 | \rho_{kk01} k_0 k_+)$ and $P_1(1 | \rho_{kk01} k_0 k_+)$ be the probabilities that the detector D$_i$ does not click and clicks, respectively, given the values of $\rho$, $k$, $k_01$, $k_0$ and $k_+$, for $i \in \{0, 1, +, -\}$. Let $P(k_01 k_0 k_+ | \rho, k)$ be the probability of the values $k_01$, $k_0$ and $k_+$, given $\rho$ and $k$. We have that

$$P_{\text{det}}(c_0 c_1 c_{\text{--}} | \rho, k) = \sum_{k_{01}=0}^{k} \sum_{k_0=0}^{k_{01}} \sum_{k_+=0}^{k-k_{01}} [P(k_01 k_0 k_+ | \rho, k) P_0(0 | \rho_{kk01} k_0 k_+) \times \times P_1(1 | \rho_{kk01} k_0 k_+) P_+ (c_+ | \rho_{kk01} k_0 k_+) \times \times P_{\text{--}}(c_{\text{--}} | \rho_{kk01} k_0 k_+)],$$

(D41)

for $c_0, c_1, c_+, c_{\text{--}} \in \{0, 1\}$, where

$$P(k_01 k_0 k_+ | \rho, k) = \frac{k}{k_{01}} \frac{k_{01}}{k_0} \frac{(k - k_{01})}{k_+} \left(\frac{1}{2}\right)^k \times \times (q_0)^{k_0} (1 - q_0)^{k_01 - k_0} (q_+)^{k_+} \times \times (1 - q_+)^{k - k_01 - k_+},$$

for $i \in \{0, 1, +, -\}$. Let $P_i$ be the probability that only the detector D$_i$ clicks, for $i \in \{0, 1, +, -\}$. We have that

$$P_0 = P_{\text{det}}(1000 | \rho, k),$$

$$P_1 = P_{\text{det}}(0100 | \rho, k),$$

$$P_+ = P_{\text{det}}(0010 | \rho, k),$$

$$P_{\text{--}} = P_{\text{det}}(0001 | \rho, k).$$

(D43)

The probability $P_{\text{report}}(1, 0 | \rho, k)$ that Bob sends the message $m = 1$ to Alice and assigns a measurement outcome in the basis $B_0$ is the probability that Bob assigns a measurement outcome corresponding to the state $|0\rangle$ (detector D$_0$) plus the probability that Bob assigns a measurement outcome corresponding to the state $|1\rangle$ (detector D$_1$). Similarly, the probability $P_{\text{report}}(1, 1 | \rho, k)$ that Bob sends the message $m = 1$ to Alice and assigns a measurement outcome in the basis $B_1$ is the probability that Bob assigns a measurement outcome corresponding to the state $|+\rangle$ (detector D$_+$) plus the probability that Bob assigns a measurement outcome corresponding to the state $|-\rangle$ (detector D$_-$. Since in the SLII reporting strategy used by Bob, Bob assigns a measurement outcome to the detector D$_i$ with probability $S_i$ if only the detector D$_i$ clicks then we have that $P_{\text{report}}(1, 0 | \rho, k)$ and $P_{\text{report}}(1, 1 | \rho, k)$ are given by (D38). Finally, from (D41) - (D38), it follows straightforwardly using the binomial theorem that $P_i$ is given by (D39), for $i \in \{0, 1, +, -\}$, as claimed.

The following lemma states Alice’s guessing probability in the MPAII attack when Bob uses the SLII reporting strategy, given some specific experimental parameters.

Lemma 11. Suppose that Alice applies the MPAII attack with $\rho = \rho_{\text{qubit}}^k$ and that Bob uses the SLII reporting strategy with $S_i = \frac{n_{\text{min}}}{n_i}$, for some qubit state $\rho_{\text{qubit}}$. 
for some nonnegative integer \( k \), and for \( i \in \{0, 1, +, -\} \). Consider the following parameters: \( \rho_{\text{qubit}} = |0\rangle\langle 0|, \theta = 0, 0 < d_i = d << 1 \) and \( \eta_i = \eta \in (0, 1) \), for \( i \in \{0, 1, +, -\} \). We assume that Alice knows these values. Alice computes the probability \( P_{\text{report}}(1, \beta|\rho, k) \) that Bob sends the message \( m = 1 \) to Alice and assigns a measurement outcome in the basis \( \mathcal{B}_\beta \), for \( \beta \in \{0, 1\} \). Then \( S_i = 1 \), for \( i \in \{0, 1, +, -\} \) and

\[
P_{\text{report}}(1, 0|\rho, k) = P_0 + P_1, \quad P_{\text{report}}(1, 1|\rho, k) = P_+ + P_-, \tag{D44}
\]

where

\[
P_0 = (1 - d)^3 \left[ (1 - \frac{\eta}{2})^k - (1 - d)(1 - \eta)^k \right] ,
\]

\[
P_1 = d(1 - d)^3(1 - \eta)^k ,
\]

\[
P_+ = P_- = (1 - d)^3 \left[ (1 - \frac{3\eta}{4})^k - (1 - d)(1 - \eta)^k \right] , \tag{D45}
\]

for any nonnegative integer \( k \). It also holds that \( P_{\text{report}}(1, 0|\rho, k) = P_{\text{report}}(1, 1|\rho, k) \) if \( k \in \{0, 1\} \) and that \( P_{\text{report}}(1, 0|\rho, k) > P_{\text{report}}(1, 1|\rho, k) \) if \( k \geq 2 \). Alice guesses that Bob assigns a measurement outcome in the basis \( \mathcal{B}_\beta \) if Bob sends her the message \( m = 1 \). Alice’s probability to guess the measurement basis assigned by Bob is given by

\[
P_{\text{guess}} = \frac{P_{\text{report}}(1, 0|\rho, k)}{P_{\text{report}}(1, 0|\rho, k) + P_{\text{report}}(1, 1|\rho, k)} , \tag{D46}
\]

which satisfies \( P_{\text{guess}} = \frac{1}{2} \) if \( k \in \{0, 1\} \), \( P_{\text{guess}} > \frac{1}{2} \) if \( k \geq 2 \) and \( P_{\text{guess}} \to 1 \) as \( k \to \infty \).

**Proof.** Since \( \eta_i = \eta \in (0, 1) \) and \( S_i = \frac{q_0}{q_+} \), we see from Bob’s\textsuperscript{SLII} reporting strategy that \( S_i = 1 \), for \( i \in \{0, 1, +, -\} \). Since in Alice’s\textsuperscript{MPAI} considered attack, \( \rho = \rho_{\text{qubit}} \otimes \mathbf{r}^\dagger \) with \( \rho_{\text{qubit}} = |0\rangle\langle 0| \), the Bloch vector \( \mathbf{r}^\dagger \) of the qubit state \( \rho_{\text{qubit}} \) is \( \mathbf{r}^\dagger = (0, 0, 1) \). From this, and since \( \theta = 0 \), we have \( q_0 = 1 \) and \( q_+ = \frac{3}{4} \) in Equation (D40) of Lemma 10. By substituting \( q_0 = 1 \), \( q_+ = \frac{3}{4} \), \( S_i = 1 \), \( d_i = d \) and \( \eta_i = \eta \) in Equations (D38) and (D39) of Lemma 10, it is straightforward to obtain (D44) and (D45).

It is easy to see from (D44) and (D45) that \( P_{\text{report}}(1, 0|\rho, k) = P_{\text{report}}(1, 1|\rho, k) \) if \( k \in \{0, 1\} \). To see that \( P_{\text{report}}(1, 0|\rho, k) > P_{\text{report}}(1, 1|\rho, k) \) if \( k \geq 2 \), we note from (D44) and (D45) that

\[
P_{\text{report}}(1, 0|\rho, k) - P_{\text{report}}(1, 1|\rho, k) = (1 - d)^3 f(k), \tag{D47}
\]

where

\[
f(k) = \left( 1 - \frac{\eta}{2} \right)^k + (1 - \eta)^k - 2 \left( 1 - \frac{3\eta}{4} \right)^k , \tag{D48}
\]

for any nonnegative integer \( k \). The function \( g(x) = x^k \) is convex for \( x > 0 \) and \( k \geq 2 \), since \( g''(x) = k(k-1)x^{k-2} > 0 \) for \( x > 0 \) and \( k \geq 2 \). Thus, we have

\[
f(k) = 2 \left[ \left( 1 - \frac{\eta}{2} \right)^k + \frac{1}{2} (1 - \eta)^k - \left( 1 - \frac{3\eta}{4} \right)^k \right] > 2 \left[ \left( 1 - \frac{\eta}{2} \right)^k + \frac{1}{2} (1 - \eta)^k - \left( 1 - \frac{3\eta}{4} \right)^k \right] = 2 \left[ \left( 1 - \frac{3\eta}{4} \right)^k - (1 - \frac{3\eta}{4})^k \right] = 0 , \tag{D49}
\]

for \( k \geq 2 \), where in the second line we used that \( \eta \in (0, 1) \) and that the function \( g(x) = x^k \) is convex for \( x > 0 \) and \( k \geq 2 \). Thus, from (D47) – (D49), we see that \( P_{\text{report}}(1, 0|\rho, k) > P_{\text{report}}(1, 1|\rho, k) \) if \( k \geq 2 \). It follows from (D40) that \( P_{\text{guess}} > \frac{1}{2} \) if \( k \geq 2 \), as claimed.

Now we show that \( P_{\text{guess}} \to 1 \) if \( k \to \infty \). It follows from (D44) – (D46) that

\[
P_{\text{guess}} = 1 - \frac{P_+ - P_-}{P_0 + P_1 + P_+ + P_-} = 1 - \frac{2 \left( 1 - \frac{\eta}{2} \right)^k + (1 - 4(1 - d))(1 - \eta)^k + 2 \left( 1 - \frac{3\eta}{4} \right)^k}{2 \left[ 1 - (1 - d)(1 - \eta)^k \right]} = 1 - \frac{2 + \left( 1 - \frac{\eta}{2} \right)^k + (1 - 4(1 - d))(1 - \eta)^k}{\left( 1 - \frac{\eta}{2} \right)^k} \tag{D50}
\]

We see that \( \left( 1 - \frac{\eta}{2} \right)^k \to \infty \) as \( k \to \infty \) and \( \left( 1 - \frac{\eta}{2} \right)^k \to 0 \) as \( k \to \infty \). Thus, we see from (D50) that \( P_{\text{guess}} \to 1 \) as \( k \to \infty \), as claimed. \( \square \)

It is important to interpret correctly the value of \( P_{\text{guess}} \) in Lemma 11. As explained above this probability is conditioned on Bob setting \( m = 1 \), i.e. on Bob assigning a valid measurement outcome in any of the two bases. Thus, although \( P_{\text{guess}} \) can be very close to unity for \( k \) large enough, this does not mean that Alice’s dishonest pulse allows her to guess Bob’s assigned measurement basis with great probability. In fact, it is easy to see from Equations (D44) and (D45) that \( P_{\text{report}}(1, 0|\rho, k) + P_{\text{report}}(1, 1|\rho, k) \to 0 \) as \( k \to \infty \). This means that the probability that Bob assigns \( m = 1 \) is very small if \( k \) is large. However, Alice can implement the generalization of the\textsuperscript{MPAI} attack described above in which Alice sends Bob various dishonest pulses. In the extreme case that each of the \( N \) pulses that Alice sends Bob is a dishonest pulse with large number of photons \( k \), for a small fraction of the pulses Bob will send Alice the message \( m = 1 \). But for each of these pulses, the probability that Alice guesses the measurement basis assigned by Bob is very close to unity.

A possible countermeasure by Bob against the\textsuperscript{MPAI} attack is that Bob aborts if a fraction \( f < \delta_{\text{report}} \) of the
FIG. 6. Alice’s guessing probability. We plot Alice’s guessing probability $P_{\text{guess}}$ in the MPAII attack when Bob uses the SLII reporting strategy, with the parameters of Lemma 11, as a function of the number of photons $k$, for $k \in \{0, 1, \ldots, 150\}$. We consider the case $d = 10^{-5}$ and consider five different values for the detection efficiencies $\eta$.

pulses sent by Alice produces the value $m = 1$, for some predetermined $\delta_{\text{report}} \in (0, 1)$. Investigating this countermeasure in detail is left as an open problem. However, neither this nor other countermeasures were proposed in Ref. [60]. We must then conclude that the protocol of Ref. [60] is insecure.

In Fig. 6 we plot Alice’s guessing probability $P_{\text{guess}}$ in the MPAII attack when Bob uses the SLII reporting strategy, with the parameters of Lemma 11 as a function of the number of photons $k$ of Alice’s dishonest pulse. We consider the case that Bob’s dark count probabilities are $d = 10^{-5}$ and consider various values for the efficiencies $\eta \in (0, 1)$ of Bob’s detectors.

c. Proof of Lemma 10

Proof. We can suppose that Alice implements the MPAII attack in the particular case $k \in \{0, 1\}$, that Alice sends Bob an empty pulse if $k = 0$, and that $\rho = \rho_{\text{qubit}}$ is a qubit state with Bloch vector $\vec{r} = (r_x, r_y, r_z)$ if $k = 1$. Thus, the probability $P_{\text{report}}(1, \beta|\rho, k)$ that Bob sets $m = 1$ and assigns a valid measurement outcome in the basis $B_\beta$ is given by Eq. (D38) of Lemma 10 for $\beta, k \in \{0, 1\}$.

We consider the case $k = 0$. From Eqs. (D38) – (D40) we have

where in the second line we used that $0 < \eta_{\text{min}} \leq \eta_i$ and $0 \leq d_i \leq d < 1$, for $i \in \{0, 1, +, -\}$.

We consider the case $k = 1$. From Eqs. (D38) – (D40)
of Lemma [10], we have

\[
\left| P_{\text{report}}(1,0|\rho,k) - P_{\text{report}}(1,1|\rho,k) \right| \\
= \eta_{\min} \left[ (1 - d_1)(1 - d_-)(1 - d_0)(1 - \eta_0) \right. \\
\quad + \left. \frac{(1 - d_0)(1 - d_+)(1 - d_-)q_0\eta_0}{\eta_0} \right] \\
\quad + \frac{(1 - d_0)(1 - d_1)(1 - d_-)q_+\eta_-}{\eta_-} \\
\quad - \frac{(1 - d_0)(1 - d_1)(1 - d_-)q_+\eta_+}{\eta_+} \\
\quad + \left[ \frac{d_0(1 - d_1)(1 - d_+)(1 - d_-)}{\eta_0} \right. \\
\quad + \frac{d_1(1 - d_0)(1 - d_+)(1 - d_-)}{\eta_1} \right] \\
\quad - \frac{d_+ (1 - d_0)(1 - d_1)(1 - d_-)}{\eta_+} \\
\quad - \frac{d_- (1 - d_0)(1 - d_1)(1 - d_-)}{\eta_-} \\
\quad \times [1 - \frac{1}{2} (q_0\eta_0 + (1 - q_0)\eta_1) \\
\quad + q_+\eta_+ + (1 - q_+\eta_-)] \right] \\
\leq 1 - (1 - \delta)^2 (2 - 2\delta) + 2\delta \\
= 6\delta - 5\delta^2 + 2\delta^3 \\
\leq 6\delta,\quad (D52)
\]

where in the third line we used that \( 0 \leq d_i \leq \delta < 1, \)
\( 0 \leq \eta_0 \leq 1, \) \( 0 \leq q_+ \leq 1 \) \( 0 < \eta_{\min} \leq \eta_i < 1, \) for
\( i \in \{0,1,+,-\}; \) and in the last line we used that \( \delta^3 \leq \delta^2 \) since
\( 0 \leq \delta < 1. \)

The claimed result [D30] follows from [D51] and [D52].

\[\text{d. Reporting single and double clicks}\]

As in setup I discussed in the main text, a better reporting strategy in setup II is that Bob sets \( m = 1 \) if one or two detectors click. More precisely, we consider the following reporting strategy.

**Definition 3** (Reporting single and double clicks with setup II (RSDCI)). Bob sends Alice the message \( m = 1 \) if at least one detector from the pair \( D_0, D_1 (D_+, D_-) \) clicks and none detector from the pair \( D_+, D_- (D_0, D_1) \) click. If only the detector \( D_\beta \) clicks, Bob sets \( m = 1 \) and assigns the measurement outcome corresponding to the detector \( D_\beta, i \in \{0,1,+,-\}. \) If \( D_0 \) and \( D_1 \) click, but \( D_+ \) and \( D_- \) do not click, Bob sets \( m = 1 \) and randomly assigns a measurement outcome corresponding to the detector \( D_0 \) and \( D_1. \) Similarly, if \( D_+ \) and \( D_- \) click, but \( D_0 \) and \( D_1 \) do not click, Bob sets \( m = 1 \) and randomly assigns a measurement outcome corresponding to the detector \( D_+ \) and \( D_- \). In all other cases Bob sets \( m = 0. \)

We see that with this reporting strategy, Bob assigns a measurement outcome in the basis \( B_0 \) with unit probability if at least one of the detectors \( D_0 \) and \( D_1 \) click and none of the detectors \( D_+ \) and \( D_- \) click. Similarly, Bob assigns a measurement outcome in the basis \( B_1 \) with unit probability if at least one of the detectors \( D_+ \) and \( D_- \) click and none of the detectors \( D_0 \) and \( D_1 \) click.

As the following lemma shows, if Bob applies the RSDCI reporting strategy, with Bob’s detectors having exactly equal efficiencies and their dark count probabilities being independent of his measurement basis, Alice cannot learn any information about \( \beta \) from the message \( m. \)

**Lemma 12.** Consider setup II of Fig. 3 in which Bob uses the RSDCI reporting strategy. Suppose that Alice sends Bob a dishonest pulse of \( k \) photons, for some nonnegative integer \( k \) chosen by Alice. Let \( \rho \) be an arbitrary quantum entangled state of the \( k \) qubits encoded in the polarization of the \( k \) photons, which is an arbitrary entangled state with an ancilla held by Alice, and which is chosen by Alice. Let \( P_{\text{report}}(1,\beta|\rho,k) \) be the probability that Bob sends the message \( m = 1 \) to Alice and assigns a valid measurement outcome in the basis \( B_\beta, \) for \( \beta \in \{0,1\}. \) Suppose that \( \eta_0 = \eta_1 \in (0,1) \) and \( \eta_+ = \eta_- \in (0,1), \) for \( i \in \{0,1,+,-\}. \) Then

\[
P_{\text{report}}(1,0|\rho,k) = (1 - d_0)(1 - d_-)(1 - \eta_0)^k \\
- (1 - d_0)(1 - d_1)(1 - d_+)(1 - d_-) \left(1 - \frac{\eta_0 + \eta_+}{2}\right)^k,
\]

\[
P_{\text{report}}(1,1|\rho,k) = (1 - d_0)(1 - d_1)(1 - \eta_0)^k \\
- (1 - d_0)(1 - d_1)(1 - d_+)(1 - d_-) \left(1 - \frac{\eta_0 + \eta_+}{2}\right)^k,
\]

for any quantum state \( \rho \) of \( k \) qubits, for any nonnegative integer \( k, \) and for any qubit orthogonal bases \( B_0 \) and \( B_1. \)
Corollary 1. In Lemma 12, if \((1 - d_0)(1 - d_1) = (1 - d_0)(1 - d_1)\) and \(\eta_i = \eta_i\), for \(i \in \{0, 1, +, -\}\), then \(P_{\text{report}}(1, 0|\rho, k) = P_{\text{report}}(1, 1|\rho, k)\), for any quantum state \(\rho\) of \(k\) qubits and for any nonnegative integer \(k\) chosen by Alice, and for any qubit orthogonal bases \(B_0\) and \(B_1\). Thus, Alice cannot obtain any information about Bob’s assigned measurement basis in this case.

Exactly equal detection efficiencies cannot be guaranteed in practice. However, as discussed in the main text, attenuators can be used to make the detector efficiencies approximately equal. Furthermore, Bob can effectively make his detectors to have approximately equal dark count probabilities by simulating dark counts in the detectors with lower dark count probabilities so that they approximate the dark count probability of the detector with highest dark count probability.

Proof of Lemma 12. The probability that Bob sets \(m = 1\) and assigns a measurement outcome in the basis \(B_0\) is the probability that he assigns a valid measurement outcome to the state corresponding to the detector \(D_0\) plus the probability that he assigns a valid measurement outcome to the state corresponding to the detector \(D_1\). Similarly, the probability that Bob sets \(m = 1\) and assigns a measurement outcome in the basis \(B_1\) is the probability that he assigns a valid measurement outcome to the state corresponding to the detector \(D_+\) plus the probability that he assigns a valid measurement outcome to the state corresponding to the detector \(D_-\). Thus, it follows from Bob’s RSDDCII reporting strategy that

\[
P_{\text{report}}(1, 0|\rho, k) = P_{\text{det}}(1000|\rho, k) + P_{\text{det}}(0100|\rho, k) + P_{\text{det}}(1001|\rho, k),
\]

\[
P_{\text{report}}(1, 1|\rho, k) = P_{\text{det}}(0010|\rho, k) + P_{\text{det}}(0001|\rho, k) + P_{\text{det}}(0011|\rho, k).
\]

(D54)

Consider Bob’s setup in Fig. 5. Alice sends Bob a pulse of \(k\) photons, encoding a \(k\)-qubit state \(\rho\) in the polarization degrees of freedom, for some nonnegative integer \(k\). Let \(k_0\) be the number of photons that are transmitted through the 50:50 beam splitter towards the polarizing beam splitter PBS01 and let \(k_+ = k - k_0\) be the number of photons that are reflected from the 50:50 beam splitter towards the polarizing beam splitter PBS1-, for \(k_0 \in \{0, 1, \ldots, k\}\). Let \(k_0\) and \(k_1 = k_0 - k_0\) be the number of photons that are reflected from the detectors \(D_0\) and \(D_1\), respectively, for \(k_0 \in \{0, 1, \ldots, k_0\}\). Let \(k_+\) and \(k_- = k - k_0 - k_+\) be the number of photons that go towards the detectors \(D_+\) and \(D_-\), respectively, for \(k_+ \in \{0, 1, \ldots, k - k_0\}\).

The probabilities that a photon is transmitted through the 50:50 beam splitter towards the polarizing beam splitter PBS01 and reflected from the 50:50 beam splitter towards the polarizing beam splitter PBS1- are both \(\frac{1}{2}\). We note that we do not lose generality by considering that the 50:50 beam splitter has transmission and reflection probabilities exactly equal to \(\frac{1}{2}\). If these probabilities were different, these values could be absorbed in the efficiencies of the detectors, leaving the equivalent transmission and reflection probabilities of the 50:50 beam splitter effectively equal to \(\frac{1}{2}\).

Let \(P(k_0, k_0'k_1'k_+|\rho, k)\) be the probability of the values \(k_0, k_0'\) and \(k_+\), given \(\rho\) and \(k\). We have that

\[
P(k_0, k_0'k_1'k_+|\rho, k) = \left(\frac{1}{2}\right)^k \left(k \choose k_0\right) P(k_0, k_1'k_+|\rho, k),
\]

where \(P(k_0, k_1'k_+|\rho, k)\) is given by the Born rule and satisfies

\[
\sum_{k_0=0}^{k} \sum_{k_0'=0}^{k-k_0} P(k_0, k_0'k_1'k_+|\rho, k) = 1,
\]

for any \(k_0 \in \{0, 1, \ldots, k\}\), for any \(-\)qubit state \(\rho\) and for any nonnegative integer \(k\).

Let \(P_{\text{det}}(c_0, c_1, c_2, c_3|k_0, k_0', k_+, k)\) be the probability of the detection event \((c_0, c_1, c_2, c_3)\), given the values \(k_0, k_0'\) and \(k_+\), which is independent of \(\rho\), for \(c_0, c_1, c_2, c_3 \in \{0, 1\}\). We have that

\[
P_{\text{det}}(c_0, c_1, c_2, c_3|k_0, k_0', k_+, k) = \sum_{k_0=0}^{k} \sum_{k_0'=0}^{k-k_0} \left[P_{\text{det}}(c_0, c_1, c_2, c_3|k_0, k_0', k_+, k) \times P(k_0, k_0'k_+|\rho, k)\right],
\]

and that

\[
P_{\text{det}}(c_0, c_1, c_2, c_3|k_0, k_0', k_+, k) = P_0(c_0|k_0)P_1(c_1|k_0, k_0')P_+(c_+|k_+, k)P_-(c_-|k_0, k_+, k),
\]

where \(P_i(c_i|k_i)\) is the probability that the detector \(D_i\) clicks if \(c_i = 1\) and does not click if \(c_i = 0\), given the value of \(k_i\), which satisfies

\[
P_i(0|k_i) = (1 - d_i)(1 - \eta_i)\eta_i^{k_i},
\]

\[
P_i(1|k_i) = 1 - P_i(0|k_i),
\]

for \(i \in \{0, 1, +, -\}\), \(c_0, c_1, c_2, c_3 \in \{0, 1\}\), any \(-\)qubit state \(\rho\) and any nonnegative integer \(k\); where we recall that \(k_1 = k_0 - k_0'\) and \(k_- = k - k_0 - k_+\).
From (D51), (D52), (D54), (D55), and (D56), we have

\[ P_{\text{report}}(1, 0|\rho, k) \]

\[ = \sum_{k_{01}=0}^{k} \sum_{k_{0}+0}^{k-k_{01}} \sum \left( \frac{1}{2} \right) \left( k \begin{array}{c} \binom{k}{k_{01}} \end{array} \right) P(k_{0}k_{+}|k_{01}, \rho, k) \times \]

\[ \left[ (1 - P_{0}(0|k_{0})P_{1}(0|k_{01}, k_{0})) \times \right. \]

\[ \left. \times P_{-}(0|k_{+})P_{-}(0|k_{01}, k_{+}, k) \right] \]

\[ = \left( \frac{1}{2} \right) \left[ \frac{k_{+}}{k_{01}} \right] \sum \left( \frac{1}{2} \right) \left( k \begin{array}{c} \binom{k}{k_{01}} \end{array} \right) P(k_{0}k_{+}|k_{01}, \rho, k) \times \]

\[ \left[ (1 - d_{+})(1 - d_{-})(1 - \eta_{+})^{k-k_{01}} \right. \]

\[ - (1 - d_{0})(1 - d_{1})(1 - d_{+})(1 - d_{-}) \times \]

\[ \left. \times (1 - \eta_{0})^{k_{01}}(1 - \eta_{+})^{k-k_{01}} \right] \]

\[ = (1 - d_{+})(1 - d_{-}) \left( 1 - \frac{\eta_{+}}{2} \right)^{k} \]

\[ -(1 - d_{0})(1 - d_{1})(1 - d_{+})(1 - d_{-}) \left( 1 - \frac{\eta_{0} + \eta_{+}}{2} \right)^{k}, \]  

(D60)

where in the second line we used (D59), \( \eta_{+} = \eta_{-} \) and \( \eta_{0} = \eta_{1} \), in the third line we used (D56), and in the last line we used the Binomial theorem. Similarly, from (D54), (D55), (D57), (D58), and (D59), we have

\[ P_{\text{report}}(1, 1|\rho, k) \]

\[ = \sum_{k_{01}=0}^{k} \sum_{k_{0}+0}^{k-k_{01}} \sum \left( \frac{1}{2} \right) \left( k \begin{array}{c} \binom{k}{k_{01}} \end{array} \right) P(k_{0}k_{+}|k_{01}, \rho, k) \times \]

\[ \left[ (1 - P_{+}(0|k_{+})P_{-}(0|k_{01}, k_{+}, k)) \times \right. \]

\[ \left. \times P_{0}(0|k_{0})P_{1}(0|k_{01}, k_{0}) \right] \]

\[ = \left( \frac{1}{2} \right) \left[ \frac{k_{+}}{k_{01}} \right] \sum \left( \frac{1}{2} \right) \left( k \begin{array}{c} \binom{k}{k_{01}} \end{array} \right) P(k_{0}k_{+}|k_{01}, \rho, k) \times \]

\[ \left[ (1 - d_{0})(1 - d_{1})(1 - \eta_{0})^{k_{01}} \right. \]

\[ - (1 - d_{0})(1 - d_{1})(1 - d_{+})(1 - d_{-}) \times \]

\[ \left. \times (1 - \eta_{0})^{k_{01}}(1 - \eta_{+})^{k-k_{01}} \right] \]

\[ = (1 - d_{0})(1 - d_{1})(1 - d_{+})(1 - d_{-}) \left( 1 - \frac{\eta_{0} + \eta_{+}}{2} \right)^{k}, \]  

(D61)

where in the second line we used (D59), \( \eta_{+} = \eta_{-} \) and \( \eta_{0} = \eta_{1} \), in the third line we used (D56), and in the last line we used the Binomial theorem. Thus, the claimed result (D53) follows from (D60) and (D61).

\[ \square \]

5. A multi-photon attack on the quantum oblivious transfer protocol of Ref. [61]

Ref. [61] demonstrated quantum 1-out-of-2 oblivious transfer in the noisy storage model. The protocol of Ref. [61] uses setup II, which is illustrated in Fig. 5. A subroutine of this protocol is equivalent to the subroutine discussed in section (D4) and implemented in the protocol of Ref. [61]. The [SLII] reporting strategy is used by Bob, as it is claimed by Ref. [61] that this guarantees security against Alice. However, Ref. [61] does not say whether Bob only reports single clicks as valid measurement outcomes, or whether Bob reports multiple clicks as valid measurement outcomes. If Bob only reports single clicks as valid measurement outcomes, then the multi-photon attack I in setup II [MPAII] attack) and the results presented in section (D4) apply too. In particular, as illustrated in Fig. 6 and discussed in section (D4) Alice can guess Bob’s measurement bases with high probability by implementing the [MPAII] attack with a large number of photons \( k \).
Appendix E: Proofs of Lemmas 1 and 2 and Theorem 1

Lemma 1. Suppose that \( \eta_{i,\beta} = \eta \) and \( d_{i,\beta} = d_{i} \), for \( i, \beta \in \{0, 1\} \). If Bob uses reporting strategy II, then for an arbitrary quantum state \( \rho \) encoded in a pulse of \( k \) photons that Alice sends Bob, and for arbitrary qubit orthogonal bases \( B_{0} \) and \( B_{1} \), it holds that
\[
P_{\text{report}}(1|\beta, \rho, k) = 1 - (1 - d_{0})(1 - d_{1})(1 - \eta)^{k}, \quad (E1)
\]
for \( \beta \in \{0, 1\} \) and \( k \in \{0, 1, 2, \ldots\} \).

Proof. By definition, if Bob follows reporting strategy II then
\[
P_{\text{report}}(1|\beta, \rho, k) = 1 - P_{\text{det}}(0, 0|\beta, \rho, k), \quad (E2)
\]
for \( \beta \in \{0, 1\} \) and \( k \in \{0, 1, 2, \ldots\} \). Let \( k_{0} \) be the number of photons that go to detector \( D_{0} \). The number of photons that go to detector \( D_{1} \) is \( k = k - k_{0} \). The probability \( P(k_{0}|\beta, \rho) \) that \( k_{0} \) photons go to \( D_{0} \) and \( k - k_{0} \) photons go to \( D_{1} \) depends both on the quantum state \( \rho \) and on the quantum measurement \( B_{\beta} \) implemented by Bob, via the Born rule. As previously stated, in our model, the dark counts and each photo-detection are independent random events. We define \( P_{i}(0|\rho, k_{0}) \) to be the probability that \( D_{i} \) does not click, which is independent of whether \( D_{1} \) clicks, and which is independent of Bob’s measurement basis \( B_{\beta} \), for \( i, \beta \in \{0, 1\} \). We have
\[
P_{i}(0|\rho, k_{0}) = \begin{cases} (1 - d_{0})(1 - \eta)^{k_{0}}, & \text{if } i = 0, \\ (1 - d_{1})(1 - \eta)^{k - k_{0}}, & \text{if } i = 1. \end{cases} \quad (E3)
\]
for \( k_{0} \in \{0, 1, \ldots, k\} \) and \( k \in \{0, 1, 2, \ldots\} \). Thus, for a \( k \)-photon pulse, the probability \( P_{i}(0, 0|\beta, \rho, k) \) that no detector clicks when Bob measures in the basis \( B_{\beta} \) is given by
\[
P_{\text{det}}(0, 0|\beta, \rho, k) = \sum_{k_{0}=0}^{k} P(k_{0}|\beta, \rho) P_{i}(0|\rho, k_{0}) P_{i}(0|\rho, k_{0}) = \sum_{k_{0}=0}^{k} P(k_{0}|\beta, \rho) (1 - d_{0})(1 - d_{1}) \times \times (1 - \eta)^{k_{0}}(1 - \eta)^{k - k_{0}} = \sum_{k_{0}=0}^{k} P(k_{0}|\beta, \rho)(1 - d_{0})(1 - d_{1})(1 - \eta)^{k} = (1 - d_{0})(1 - d_{1})(1 - \eta)^{k}, \quad (E4)
\]
for \( \beta \in \{0, 1\} \), where in the second line we used \( [\text{X}] \), in the third line we used the assumption that \( \eta_{0} = \eta_{1} = \eta \), and in last line we used \( \sum_{k_{0}=0}^{k} P(k_{0}|\beta, \rho) = 1, \) for \( \beta \in \{0, 1\} \). Thus, \( [\text{X}] \) follows from \( [\text{E2}] \) and \( [\text{E4}] \).

Lemma 2. Let \( d_{i,\beta} \leq \delta \), for some \( 0 \leq \delta < 1 \) and for \( i, \beta \in \{0, 1\} \). Consider the practical protocol with \( p_{0} + p_{1} = 1 \) in which Alice sends Bob a single photon pulse \( (k = 1) \) in arbitrary qubit state \( \rho \) or an empty pulse \( (k = 0) \). Suppose that Bob applies reporting strategy III. Then
\[
|P_{\text{report}}(1|1, \rho) - P_{\text{report}}(1|0, \rho)| \leq B_{III}^{0}, \quad (E5)
\]
for \( k \in \{0, 1\} \), where
\[
B_{III}^{0} = 2\delta, \quad B_{III} = 6\delta + 2\delta^{2} + S_{III}^{\text{max}}(5\delta + \delta^{2}), \quad (E6)
\]
and where \( S_{III}^{\text{max}} = \max\{S_{110}, S_{111}\} \).

Proof. If Alice sends Bob a pulse of \( k \) photons encoding a state \( \rho \) and Bob measures in the basis \( B_{\beta} \), the probability that Bob reports the message \( m = 1 \) to Alice is given by
\[
P_{\text{report}}(1|\beta, \rho, k) = \sum_{c_{0}=0}^{1} \sum_{c_{1}=0}^{1} S_{c_{0}, c_{1}|\beta} P_{\text{det}}(c_{0}, c_{1}|\beta, \rho, k), \quad (E7)
\]
for \( \beta \in \{0, 1\} \) and \( k \in \{0, 1, 2, \ldots\} \). From \( [\text{X}] \) in the main text and from \( [\text{E7}] \), we have
\[
P_{\text{report}}(1|\beta, \rho, k) = \eta_{\min} \left( \frac{P_{\text{det}}(0, 1|\beta, \rho, k)}{\eta_{\beta}} + \frac{P_{\text{det}}(1, 0|\beta, \rho, k)}{\eta_{\beta}} \right) + S_{11|\beta} P_{\text{det}}(1, 1|\beta, \rho, k), \quad (E8)
\]
for \( \beta \in \{0, 1\} \) and \( k \in \{0, 1, 2, \ldots\} \). We consider the case \( k = 0 \). From \( [\text{E8}] \) and from Lemma 3 in the main text, we have
\[
P_{\text{report}}(1|\beta, \rho, 0) = \eta_{\min} \left( \frac{(1 - d_{0,\beta})d_{1,\beta}}{\eta_{\beta}} + \frac{(1 - d_{1,\beta})d_{0,\beta}}{\eta_{\beta}} \right) + S_{11|\beta} d_{0,\beta} d_{1,\beta}, \quad (E9)
\]
for \( \beta \in \{0, 1\} \). Since \( 0 < \eta_{\min} \leq \eta_{\beta}, 0 \leq d_{i,\beta} \leq \delta < 1 \) and \( S_{11|\beta} \leq \eta_{\beta} \), for \( i, \beta \in \{0, 1\} \), it follows straightforwardly from \( [\text{E9}] \) that
\[
|P_{\text{report}}(1|1, \rho, 0) - P_{\text{report}}(1|0, \rho, 0)| \leq 2\delta. \quad (E10)
\]
We consider the case \( k = 1 \). From \( [\text{E8}] \) and from Lemma 3 in the main text, we have
\[
P_{\text{report}}(1|\beta, \rho, 1) = \eta_{\min} \left( \frac{\eta_{\beta}(1 - q_{\beta}) - d_{0,\beta}(1 - q_{\beta}d_{\eta_{\beta}})}{\eta_{\beta}} + (d_{0,\beta} + d_{1,\beta} - d_{0,\beta}d_{\eta_{\beta}})(q_{\beta}(1 - \eta_{\beta})) + (1 - q_{\beta})(1 - \eta_{\beta}) \right) + S_{11|\beta} \left[ 1 + (1 - d_{0,\beta})(1 - d_{1,\beta})(q_{\beta}(1 - \eta_{\beta})) + (1 - q_{\beta})(1 - \eta_{\beta}) \right] - (d_{0,\beta} - q_{\beta}d_{\eta_{\beta}}) \right), \quad (E11)
\]
for $\beta \in \{0,1\}$. Since $0 < \eta_{\min} \leq \eta_{i\beta}, 0 \leq d_{i\beta} \leq \delta < 1$ and $0 \leq S_{i\beta} \leq S_{i\beta}^{\max}$, for $i, \beta \in \{0,1\}$, it follows straightforwardly from (E11) that

$$P_{\text{report}}(1|1, \rho, 1) - P_{\text{report}}(1|0, \rho, 1) \leq 6\delta + 2\delta^2 + S_{i\beta}^{\max}(5\delta + \delta^2). \tag{E12}$$

Thus, from (E10), (E14) and (E12), the claimed result (E15) follows. \hfill \Box

Theorem 1. Suppose that

$$d_{i\beta} = 0, \tag{E13}$$
$$\eta_{i\beta} = \eta_i \in (0, 1), \tag{E14}$$
$$\eta_0 \neq \eta_i, \tag{E15}$$

for $i, \beta \in \{0,1\}$, and $B_0$ and $B_1$ are arbitrary distinct qubit orthogonal bases. If Alice sends Bob a pulse of $k$ photons encoding a state $\rho$, with $k \in \{0,1,2\}$ chosen by Alice and unknown to Bob, then the only probabilistic reporting strategy that guarantees to Bob that Alice cannot obtain any information about $\beta$ from his message $m$ is the trivial strategy (E12).

Proof. We first show Theorem 1 analytically for the case that $B_0$ and $B_1$ are the computational and Hadamard bases, respectively, with $|\psi_0\rangle = |0\rangle, |\psi_10\rangle = |1\rangle, |\psi_01\rangle = |+\rangle$ and $|\psi_{11}\rangle = |--\rangle$. We then show Theorem 1 numerically for the case that $B_0$ and $B_1$ are arbitrary distinct qubit orthogonal bases.

1. Analytical proof for the case that $B_0$ and $B_1$ are the computational and Hadamard bases, respectively.

We consider the case that $B_0$ and $B_1$ are the computational and Hadamard bases, respectively. Alice does not obtain any information about $\beta$ from Bob’s message $m$ if and only if

$$P_{\text{report}}(1|1, \rho, k) = P_{\text{report}}(1|0, \rho, k), \tag{E16}$$

for any $k$-qubit state $\rho$ and for $k \in \{0,1,2\}$.

We first note that if (E12) of the main text holds then, from (E13) of the main text, (E16) holds too, for any $k$-qubit state $\rho$ and for any $k \in \{0,1,2,\ldots\}$. Thus, Alice does not obtain any information about $\beta$ from Bob’s message $m$ in this case.

Now we show that Bob is guaranteed that Alice cannot obtain any information about $\beta$ from his message $m$ only if (E12) of the main text holds. From (E11) of the main text and (E16), it follows that

$$\sum_{i=0}^{1} \sum_{j=0}^{1} (S_{ij}1P_{\text{det}}(i, j|1, \rho, k) - S_{ij}0P_{\text{det}}(i, j|0, \rho, k)) = 0, \tag{E17}$$

for any $k$-qubit state $\rho$ encoded in a pulse of $k$ photons, and for $k \in \{0,1,2\}$.

From (E17), we establish a set of eight linear equations, by considering the case $k = 0$, the case $k = 1$ with $\rho \in \{\{0\}\{0\}, \{1\}\{1\}, \{+\}\{+\}, \{--\}\{--\}\}$, and the case $k = 2$ with $\rho \in \{(00)(00), \{11\}(11), \{+\}++\}$. Considering the state $\rho = |--\|--\$ does not give any extra information. It does not simplify the proof either. As we show below, the only solution for this set of equations is given by (E12) of the main text.

From (E18) of the main text, (E13), (E14) and (E17), we obtain in the case $k = 0$ that

$$S_{0001} = S_{000}. \tag{E18}$$

In the case $k = 1$ with $\rho = |00\rangle\langle 00|$, we obtain from (E17) of the main text that $q_0 = |00\rangle\langle 00|^2 = 1$ and $q_1 = |++\rangle\langle ++|^2 = 1\frac{1}{4}$. Thus, from (E18) of the main text, (E13), (E14) and (E17), we obtain

$$\frac{1}{1} - \frac{(\eta_0 + \eta_1)}{2} \bigg) S_{0001} + \frac{\eta_0}{2} S_{101} + \frac{\eta_1}{2} \bigg) S_{111} - (1 - \eta_0) S_{000} - \eta_0 S_{100} = 0. \tag{E19}$$

In the case $k = 1$ with $\rho = |11\rangle\langle 11|$, we obtain from (E17) of the main text that $q_0 = |[11]\rangle\langle 11|^2 = 1\frac{1}{4}$ and $q_1 = |[+\]++|^2 = 1\frac{1}{4}$. Thus, from (E18) of the main text, (E13), (E14) and (E17), we obtain

$$(1 - \eta_0) S_{0001} + \eta_0 S_{101} - \bigg) S_{000} - \eta_0 S_{100} = 0. \tag{E20}$$

In the case $k = 1$ with $\rho = |0\rangle\langle 0|$, we obtain from (E17) of the main text that $q_0 = |[0]\rangle\langle 0|^2 = 1\frac{1}{4}$ and $q_1 = |[+\]++|^2 = 1\frac{1}{4}$. Thus, from (E18) of the main text, (E13), (E14) and (E17), we obtain

$$(1 - \eta_0) S_{0001} + \eta_0 S_{101} - \bigg) S_{111} - (1 - \eta_0) S_{000} - \eta_0 S_{100} = 0. \tag{E21}$$

In the case $k = 2$ with $\rho = |00\rangle\langle 00|$, we obtain from (E17) of the main text that $q_0 = |[00]\rangle\langle 00|^2 = 1\frac{1}{4}$ and $q_1 = |[+\]++|^2 = 1\frac{1}{4}$. Thus, from (E18) of the main text, (E13), (E14) and (E17), we obtain

$$\frac{1}{1} - \frac{(\eta_0 + \eta_1)}{2} \bigg) S_{0001} + \bigg) S_{101} + \frac{\eta_1}{2} \bigg) S_{111} - (1 - \eta_0)^2 S_{000} - (1 - \eta_0^2) S_{100} = 0. \tag{E22}$$

In the case $k = 2$ with $\rho = |11\rangle\langle 11|$, we obtain from (E17) of the main text that $q_0 = |[11]\rangle\langle 11|^2 = 1\frac{1}{4}$ and $q_1 = |[+\]++|^2 = 1\frac{1}{4}$. Thus, from (E18) of the main text, (E13), (E14) and (E17), we obtain

$$\bigg) S_{0001} + \bigg) S_{101} + (1 - \eta_0^2) S_{111} - (1 - \eta_0)^2 S_{000} - (1 - \eta_0^2) S_{100} = 0. \tag{E23}$$
In the case \( k = 2 \) with \( \rho = |++\> + |++\>, \) we obtain from (17) of the main text that \( q_0 = |0\> + |1\> \) and \( q_1 = |+\> + |+\> \). Thus, from (18) of the main text, (E18), (E14) and (E17), we obtain

\[
(1 - \eta_0)^2 S_{001} + (1 - (1 - \eta_0)^2) S_{101} - \left( 1 - \frac{\eta_0 + \eta_1}{2} \right)^2 S_{000} - \left( 1 - \frac{\eta_0 + \eta_1}{2} \right)^2 S_{010} - \frac{\eta_0 \eta_1}{2} S_{110} \]

\[
- \left( 1 - \frac{\eta_0 + \eta_1}{2} \right)^2 S_{100} = 0. \quad (E24)
\]

In the case \( k = 2 \) with \( \rho = |11\> + |11\>, \) we obtain from (17) of the main text that \( q_0 = |0\> + |1\> \) and \( q_1 = |+\> + |+\> \). Thus, from (18) of the main text, (E18), (E14) and (E17), we obtain

\[
(1 - \eta_0)^2 S_{001} + \left( 1 - \frac{\eta_0 + \eta_1}{2} \right)^2 S_{011} + \left( 1 - \frac{\eta_0 + \eta_1}{2} \right)^2 S_{101} + \frac{\eta_0 \eta_1}{2} S_{111} - (1 - \eta_0)^2 S_{000} - (1 - (1 - \eta_0)^2) S_{010} = 0. \quad (E25)
\]

We solve the system of equations (E18) – (E25) in two parts. First, we solve the system of equations (E18) – (E22). Then, using the obtained solutions, we solve the remaining system of equations (E24) – (E25).

We solve the system of equations (E18) – (E22). We first eliminate the variable \( S_{001} \) by substituting (E18) in (E19) – (E22). We obtain

\[
\frac{\eta_0 - \eta_1}{2} S_{000} + \frac{\eta_0}{2} S_{101} + \frac{\eta_1}{2} S_{011} - \eta_0 S_{100} = 0, \quad (E26)
\]

\[
\frac{\eta_0 - \eta_1}{2} S_{000} + \frac{\eta_0}{2} S_{101} + \frac{\eta_1}{2} S_{011} - \eta_1 S_{100} = 0, \quad (E27)
\]

\[
\frac{\eta_0 - \eta_1}{2} S_{000} + \eta_0 S_{101} - \frac{\eta_0}{2} S_{011} - \eta_1 S_{100} = 0, \quad (E28)
\]

\[
\frac{\eta_0 - \eta_1}{2} S_{000} + \eta_0 S_{101} - \frac{\eta_1}{2} S_{011} - \eta_0 S_{100} = 0. \quad (E29)
\]

We use (E26) to eliminate \( S_{000} \) in (E27) – (E29). Adding (E26) to (E27) and (E28), and subtracting (E26) from (E29), and rearranging terms, we obtain respectively

\[
\eta_1 S_{011} + \eta_0 S_{101} - \eta_0 S_{010} - \eta_1 S_{100} = 0, \quad (E30)
\]

\[
\eta_1 S_{011} + 3\eta_0 S_{101} - \eta_0 S_{010} - 3\eta_1 S_{100} = 0, \quad (E31)
\]

\[
\eta_0 S_{010} - \eta_1 S_{101} - \eta_1 S_{100} = 0, \quad (E32)
\]

Subtracting (E30) from (E31), or from (E32), and rearranging terms, we obtain

\[
S_{101} = S_{100}. \quad (E33)
\]

From (E30) and (E33) we obtain

\[
S_{011} = S_{010}. \quad (E34)
\]

From (E26), (E33) and (E34), we obtain

\[
(\eta_0 - \eta_1) S_{000} + \eta_1 S_{010} - \eta_0 S_{100} = 0. \quad (E35)
\]

Thus, the solutions to the system of equations (E18) – (E22) consist in (E18) and (E33) – (E35).

Now we use the obtained solutions, (E18), and (E33) – (E35), to solve the remaining system of equations (E23) – (E25). Substituting (E18), (E33) and (E34) in (E23), and multiplying by four, we obtain

\[
((2 - \eta_0 + \eta_1)^2 - 4(1 - \eta_0)^2) S_{000}
\]

\[+(1 - \eta_0)^2 - 4(1 - \eta_0) S_{000} + 2\eta_0 \eta_1 S_{111}
\]

\[+(2 - \eta_0)^2 - 4(1 - (1 - \eta_0)^2) S_{100} = 0. \quad (E36)
\]

Substituting (E18) and (E33) in (E24), and multiplying by four, we obtain

\[
(4 - (1 - \eta_0)^2) S_{000} + (4 - (1 - \eta_0)^2 - (2 - \eta_0)^2 - (2 - (\eta_0 + \eta_1))^2) S_{100}
\]

\[-(2 - \eta_0)^2 - 4(1 - \eta_0)^2) S_{100} = 0 \quad (E37)
\]

Substituting (E18), (E33) and (E34) in (E25), and multiplying by four, we obtain

\[
((2 - \eta_0 + \eta_1)^2 - 4(1 - \eta_1)^2) S_{000}
\]

\[+(2 - \eta_0)^2 - 4(1 - \eta_0)^2 - 4(1 - \eta_0)^2) S_{010}
\]

\[+(2 - \eta_0)^2 - 4(1 - \eta_0)^2) S_{100} = 0. \quad (E38)
\]

Thus, now we have a system of four equations, (E35) – (E38), with five variables, \( S_{000}, S_{100}, S_{010}, S_{110} \) and \( S_{111} \). By subtracting (E36) from (E38), we eliminate \( S_{111} \), and we obtain

\[
4((1 - \eta_0)^2 - (1 - \eta_1)^2) S_{000} - 4(1 - (1 - \eta_1)^2) S_{100} + 4(1 - (1 - \eta_1)^2) S_{100} = 0. \quad (E39)
\]

Thus, now we have a system of three equations, (E35), (E37) and (E39), with four variables, \( S_{000}, S_{100}, S_{010} \) and \( S_{110} \). We use (E35) to eliminate \( S_{010} \) from (E37) and (E39). We multiply (E35) by \(-(2 - \eta_1)^2 - 2(\eta_0 + \eta_1)^2) / \eta_1 \) and subtract from (E37), and we arrange terms to obtain

\[
(\eta_1 - \eta_0) S_{000} + (\eta_0 - 3\eta_1) S_{100} + 2\eta_1 S_{110} = 0. \quad (E40)
\]

We multiply (E35) by \(-4(1 - (1 - \eta_1)^2) / \eta_1 \) and subtract from (E39), and we arrange terms to obtain

\[
(\eta_1 - \eta_0) S_{000} - S_{110} = 0. \quad (E41)
\]

Thus, from (E15) and (E41), we get

\[
S_{000} = S_{110}. \quad (E42)
\]

We substitute (E42) in (E10) and obtain

\[
S_{100} = S_{110}. \quad (E43)
\]

Since \( \eta_1 > 0 \), from (E35) and (E42), we obtain

\[
S_{100} = S_{110}. \quad (E44)
\]
Since $\eta_0 > 0$ and $\eta_1 > 0$, it is straightforward to obtain from (E30), (E32) and (E44) that

$$S_{111} = S_{100}. \quad (E45)$$

Thus, from (E18), (E33), (E34) and (E42) – (E45), we obtain the claimed result (12) of the main text.

We note from (E31) that if $\eta_0 = \eta_1$ then (E42) does not follow. In this case, from (E14), (E18) and (E33) – (E37), it follows straightforwardly that $S_{001} = S_{000}$ and $S_{001|\beta} = S$ for $(c_0, c_1) \in \{(0, 1), (1, 0), (1, 1)\}$, $\beta \in \{0, 1\}$ and any $S_{000}, S \in \{0, 1\}$.

2. Computational proof for the case that $B_0$ and $B_1$ are arbitrary distinct qubit orthogonal bases

a. Obtaining a system of linear equations

We suppose that

$$d_{i\beta} = 0, \quad (E46)$$

$$\eta_{i\beta} = \eta_1 \in (0, 1), \quad (E47)$$

$$\eta_0 \not= \eta_1, \quad (E48)$$

for $i, \beta \in \{0, 1\}$, and $B_0$ and $B_1$ are arbitrary qubit orthogonal bases. Below we show numerically that if Alice sends Bob a pulse of $k$ photons encoding a state $\rho$, with $k \in \{0, 1, 2\}$ chosen by Alice and unknown to Bob, then the only probabilistic reporting strategy that guarantees to Bob that Alice cannot obtain any information about $\beta$ from his message $m$ is the trivial strategy (12) of the main text.

The bases $B_0$ and $B_1$ define a plane in the Bloch sphere. Without loss of generality, this plane can be taken as the $x \times z$ plane, and $B_0$ can be taken as the computational basis, with $|\psi_00\rangle = |0\rangle$ and $|\psi_10\rangle = |1\rangle$. Thus, in general, the states of the basis $B_1$ are given by

$$|\psi_01\rangle = \cos(a)|0\rangle + \sin(a)|1\rangle,$$

$$|\psi_{11}\rangle = \sin(a)|0\rangle - \cos(a)|1\rangle, \quad (E49)$$

where $a = \frac{\pi}{4} - \frac{\theta}{2}$ is half the angle in the Bloch sphere between the states $|\psi_{00}\rangle$ and $|\psi_{01}\rangle$, and $\theta$ is the angle in the Bloch sphere between the states $|\psi_{01}\rangle$ and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, for $\theta \in [0, \frac{\pi}{4}]$ and $a \in (0, \frac{\pi}{4}]$.

We proceed as in the analytical proof of Theorem 1. From the condition that Alice cannot obtain any information about Bob’s message $m$, we obtain a set of eight linear equations. We solve these equations numerically with a Mathematica program, provided as supplementary material, and we obtain that the only solution corresponds to the trivial strategy (12) of the main text.

Alice does not obtain any information about $\beta$ from Bob’s message $m$ if and only if

$$P_{\text{report}}(1|1, \rho, k) = P_{\text{report}}(1|0, \rho, k), \quad (E50)$$

for any $k$-qubit state $\rho$ and for $k \in \{0, 1, 2\}$.

We note that if (12) of the main text holds then, from (13) of the main text, (E50) holds too, for any $k$-qubit state $\rho$ and for any $k \in \{0, 1, 2, \ldots\}$. Thus, Alice does not obtain any information about $\beta$ from Bob’s message $m$ in this case.

Now we show, numerically, that Bob is guaranteed that Alice cannot obtain any information about $\beta$ from his message $m$ only if (12) of the main text holds. From (11) of the main text and (E50), it follows that

$$\sum_{c_0=0}^1 \sum_{c_1=0}^1 [S_{c_0c_11}P_{\text{det}}(c_0, c_1|1, \rho, k) - S_{c_0c_10}P_{\text{det}}(c_0, c_1|0, \rho, k)] = 0, \quad (E51)$$

for any $k$-qubit state $\rho$ encoded in a pulse of $k$ photons, and for $k \in \{0, 1, 2\}$.

From (E51), we establish a set of eight linear equations, by considering the case $k = 0$, the case $k = 1$ with $\rho \in \{(0, 0), |01\rangle, \langle 0|0\rangle, \langle 0|1\rangle, \langle 0|1\rangle\}$, and the case $k = 2$ with $\rho \in \{(00, 00), |01\rangle, |11\rangle, |0\rangle_1, |0\rangle_0, |1\rangle_0\}$. As we show below, the only solution for this set of equations is (12) of the main text.

From (13) of the main text, (E46), (E47) and (E51), we obtain in the case $k = 0$ that

$$S_{001} = S_{000}. \quad (E52)$$

In the case $k = 1$ with $\rho = |00\rangle, |0\rangle$, we obtain from (17) of the main text that $\eta_0 = |00\rangle, |0\rangle = 1$ and $\eta_1 = |00\rangle, |0\rangle = 1 - \cos^2(a)$. Thus, from (18) of the main text, (E46), (E47) and (E51), we obtain

$$[1 - \eta_0 \cos^2(a) - \eta_1 (1 - \cos^2(a))] S_{001} + \eta_0 \cos^2(a) S_{011}$$

$$+ \eta_1 (1 - \cos^2(a)) S_{011} - (1 - \eta_0) S_{000} - \eta_0 S_{0000} = 0. \quad (E53)$$

In the case $k = 1$ with $\rho = |00\rangle, |0\rangle$, we obtain from (17) of the main text that $\eta_0 = |00\rangle, |0\rangle = 0$ and $\eta_1 = |00\rangle, |0\rangle = \sin^2(a) = 1 - \cos^2(a)$. We express $\sin^2(a)$ in terms of $\cos^2(a)$, as this makes the numerical calculation by the Mathematica program easier. Thus, from (18) of the main text, (E46), (E47) and (E51), we obtain

$$[1 - \eta_0 (1 - \cos^2(a)) - \eta_1 \cos^2(a)] S_{001}$$

$$+ \eta_0 (1 - \cos^2(a)) S_{011} + \eta_1 \cos^2(a) S_{011} - (1 - \eta_1) S_{000} - \eta_1 S_{010} = 0. \quad (E54)$$

In the case $k = 1$ with $\rho = |0\rangle, |0\rangle$, we obtain from (17) of the main text that $\eta_0 = |0\rangle, |0\rangle = 0$ and $\eta_1 = |0\rangle, |0\rangle = 1$. Thus, from (18) of the main text, (E46), (E47) and (E51), we obtain

$$(1 - \eta_0) S_{001} + \eta_0 S_{011} - \eta_1 (1 - \cos^2(a)) S_{010} - \eta_0 \cos^2(a) S_{010}$$

$$- \eta_0 \cos^2(a) S_{010} - (1 - \eta_0) S_{000} - \eta_0 S_{0000} = 0. \quad (E55)$$
In the case $k = 1$ with $\rho = |\psi_{11}\rangle\langle\psi_{11}|$, we obtain from (17) of the main text that $q_0 = |\langle 0 | \psi_{11} \rangle|^2 = 1 - \cos^2(a)$ and $q_1 = |\langle \psi_{01} | \psi_{11} \rangle|^2 = 0$. Thus, from (18) of the main text, (E46), (E47) and (E51), we obtain
\[
(1 - \eta_1)S_{001} + \eta_1 S_{111} - \eta_1 \cos^2(a)S_{010} - \eta_0 \eta_1 \cos^2(a)S_{000} - \eta_0 (1 - \cos^2(a)) S_{100} = 0. \tag{E56}
\]
In the case $k = 2$ with $\rho = |00\rangle\langle 00|$, we obtain from (17) of the main text that $q_0 = |\langle 00 \rangle|^2 = 1$ and $q_1 = |\langle \psi_{01} \rangle|^2 = \cos^2(a)$. Thus, from (18) of the main text, (E46), (E47) and (E51), we obtain
\[
\left[ 1 - \eta_0 \cos^2(a) - \eta_1 (1 - \cos^2(a)) \right]^2 S_{001} + \left[ (1 - \eta_0 \cos^2(a))^2 - \left[ (1 - \eta_0 \cos^2(a) - \eta_1 (1 - \cos^2(a))) \right]^2 \right] S_{011} + \left[ (1 - \eta_1 \cos^2(a))^2 - \left[ (1 - \eta_0 \cos^2(a) - \eta_1 (1 - \cos^2(a))) \right]^2 \right] S_{101} + 2\eta_0 \eta_1 \cos^2(a)(1 - \cos^2(a))S_{111} - (1 - \eta_0)^2 S_{000} - (1 - (1 - \eta_0)^2) S_{100} = 0. \tag{E57}
\]
In the case $k = 2$ with $\rho = |\psi_{01}\rangle\langle\psi_{01}|$ we obtain from (17) of the main text that $q_0 = |\langle 0 | \psi_{01} \rangle|^2 = \cos^2(a)$ and $q_1 = |\langle \psi_{01} | \psi_{01} \rangle|^2 = 1$. Thus, from (18) of the main text, (E46), (E47) and (E51), we obtain
\[
(1 - \eta_0)^2 S_{000} + (1 - (1 - \eta_0)^2) S_{101} - \left[ 1 - \eta_0 \cos^2(a) - \eta_1 (1 - \cos^2(a)) \right]^2 S_{000} - \left[ (1 - \eta_0 \cos^2(a))^2 - \left[ (1 - \eta_0 \cos^2(a) - \eta_1 (1 - \cos^2(a))) \right]^2 \right] S_{011} - 2\eta_0 \eta_1 \cos^2(a)(1 - \cos^2(a))S_{1110} - \left[ (1 - \eta_1 \cos^2(a))^2 - \left[ (1 - \eta_0 \cos^2(a) - \eta_1 (1 - \cos^2(a))) \right]^2 \right] S_{100} = 0. \tag{E58}
\]
In the case $k = 2$ with $\rho = |11\rangle\langle 11|$, we obtain from (17) of the main text that $q_0 = |\langle 01 \rangle|^2 = 0$ and $q_1 = |\langle \psi_{01} | \psi_{11} \rangle|^2 = 1 - \cos^2(a)$. Thus, from (18) of the main text, (E46), (E47) and (E51), we obtain
\[
\left[ 1 - \eta_0 (1 - \cos^2(a)) - \eta_1 \cos^2(a) \right]^2 S_{001} + \left[ (1 - \eta_0 (1 - \cos^2(a)))^2 - \left[ (1 - \eta_0 (1 - \cos^2(a)) - \eta_1 \cos^2(a)) \right]^2 \right] S_{011} + \left[ (1 - \eta_1 \cos^2(a))^2 - \left[ (1 - \eta_0 (1 - \cos^2(a)) - \eta_1 \cos^2(a)) \right]^2 \right] S_{101} + 2\eta_0 \eta_1 \cos^2(a)(1 - \cos^2(a))S_{111} - (1 - \eta_1)^2 S_{000} - (1 - (1 - \eta_1)^2) S_{100} = 0. \tag{E59}
\]
\[b. \quad \text{Solving numerically the system of linear equations}\]

We solve numerically the system of linear equations given by (E52) – (E59), using a Mathematica program, which we attach as supplementary material. We use the code ‘Reduce’, with the system of equations (E52) – (E59). The program gives us output various solutions to the system of equations, according to different values of $\eta_0$, $\eta_1$ and $\cos^2(a)$, also output by the program. In particular, in the last line, when simplified, the program outputs the conditions $\eta_0 \neq 0$, $\eta_1 \neq 0$, $\eta_0 \neq 1$ and $\cos^2(a) \neq 1$, and the solution corresponding to the trivial probabilistic reporting strategy (12) of the main text, as claimed.

Furthermore, in the penultimate line, when simplified, the program outputs the conditions $\eta_0 = \eta_1 \neq 0$ and $\cos^2(a) \neq 1$, and the solution $S_{001} = S_{000}$ and $S_{c_1 \in \beta} = S_{c_0 \in \beta}$ for $(c_0, c_1) \in \{(0, 1), (1, 0), (1, 1)\}$ and any $S_{000}$, $S$, which is the solution that we got in the proof of Theorem 1 under the conditions $\eta_0 = \eta_1 \neq 0$ for the particular case in which $B_0$ and $B_1$ are the computational and Hadamard bases. The program also outputs, in the eight line, when simplified, the conditions $\cos^2(a) = 1$, $\eta_0 \neq 0$ and $\eta_1 \neq 0$, and the solution $S_{c_0 \in \{0, 1\}} = S_{c_0 \in \beta}$ for $(c_0, c_1) \neq (1, 1)$, which is straightforward to deduce analytically, and which corresponds to the case $B_0 = B_1$.

The output lines can be seen in the Mathematica program, which we attach as supplementary material. In the program, we use the variables ‘NO’ and ‘NL’ instead of ‘$\eta_0’ and ‘$\eta_1’, and ‘S_{c_0 \in \beta}’ instead of ‘S_{c_0 \in \beta}’, respectively, for $c_0, c_1, \beta \in \{0, 1\}$.

[1] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A 73, 022320 (2006)

[2] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems. Phys. Rev. A 74, 022313 (2006)
[3] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A 78, 042333 (2008).

[4] C. F. Fung, K. Tanaki, B. Qi, H. Lo, and X. Ma, Security proof of quantum key distribution with detection efficiency mismatch, Quantum Inf. Comput. 9, 131 (2009).

[5] V. Makarov, Controlling passively quenched single photon detectors by bright light, New J. Phys. 11, 065003 (2009).

[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nature Photon. 4, 686–689 (2010).

[7] S. Sajeeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, and A. Pappa, A randomized protocol for signing contracts, Phys. Rev. A 91, 032326 (2015).

[8] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, Attacks on practical quantum key distribution systems (and how to prevent them), Contemporary Physics 57, 366 (2016).

[9] A. Kent, Unconditionally secure bit commitment, Phys. Rev. Lett. 83, 1447 (1999).

[10] A. Kent, Secure classical bit commitment using fixed capacity communication channels, J. Cryptology 18, 313 (2005).

[11] A. Kent, Unconditionally secure bit commitment with flying qudits, New J. Phys. 13, 113015 (2011).

[12] A. Kent, Unconditionally secure bit commitment by transmitting measurement outcomes, Phys. Rev. Lett. 109, 130501 (2012).

[13] T. Lunghi, J. Kaniowski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, Experimental bit commitment based on quantum communication and special relativity, Phys. Rev. Lett. 111, 180504 (2013).

[14] Y. Liu, Y. Cao, M. Curty, S.-K. Liao, J. Wang, K. Cui, Y.-H. Li, Z.-H. Lin, Q.-C. Sun, D.-D. Li, H.-F. Zhang, Y. Zhao, T.-Y. Chen, C.-Z. Peng, Q. Zhang, A. Cabello, and J.-W. Pan, Unconditionally securely bit commitment, Phys. Rev. Lett. 112, 010504 (2014).

[15] T. Lunghi, J. Kaniowski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden, Practical relativistic bit commitment, Phys. Rev. Lett. 115, 030502 (2015).

[16] E. Adlam and A. Kent, Deterministic relativistic quantum bit commitment, Int. J. Quantum Inf. 13, 1550029 (2015).

[17] E. Adlam and A. Kent, Device-independent relativistic quantum bit commitment, Phys. Rev. A 92, 022315 (2015).

[18] E. Verbanis, A. Martin, R. Houlmann, G. Boso, F. Bussières, and H. Zbinden, 24-hour relativistic bit commitment, Phys. Rev. Lett. 117, 140506 (2016).

[19] M. O. Rabin, How To exchange Secrets with Oblivious Transfers, Tech. Rep. (Aiken Computation Lab, Harvard University, 1981).

[20] S. Even, O. Goldreich, and A. Lempel, A randomized protocol for signing contracts, Commun. ACM 28, 637 (1985).

[21] C. Crépeau, Equivalence between two flavours of oblivious transfers, in Advances in Cryptology — CRYPTO ’87, edited by C. Pomerance (Springer Berlin Heidelberg, Berlin, Heidelberg, 1988) pp. 350–354.

[22] D. Pitalúa-García, Spacetime-constrained oblivious transfer, Phys. Rev. A 93, 062346 (2016).

[23] D. Pitalúa-García and I. Kerenidis, Practical and unconditionally secure spacetime-constrained oblivious transfer, Phys. Rev. A 98, 032327 (2018).

[24] D. Pitalúa-García, One-out-of-m spacetime-constrained oblivious transfer, Phys. Rev. A 100, 012302 (2019).

[25] R. Amiri, R. Stárek, M. Micuda, L. Mista, M. Dusek, P. Wallden, and E. Andersson, Imperfect 1-out-of-2 quantum oblivious transfer: bounds, a protocol, and its experimental implementation (2020), preprint at http://arxiv.org/abs/2007.04712.

[26] M. Blum, Coin flipping by telephone a protocol for solving impossible problems, SIGACT News 15, 23–27 (1983).

[27] A. Kent, Coin tossing is strictly weaker than bit commitment, Phys. Rev. Lett. 83, 5382 (1999).

[28] C. Moehring, Quantum weak coin flipping with arbitrarily small bias (2007), preprint at http://arxiv.org/abs/0711.4114.

[29] G. Berlin, G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, Experimental loss-tolerant quantum coin flipping, Nat. Commun. 2, 561 (2011).

[30] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, Experimental plug and play quantum coin flipping, Nat. Commun. 5, 3717 (2014).

[31] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis, and L. Magnin, A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias, SIAM J. Comput. 45, 633 (2016).

[32] M. Bozzo, U. Chabaud, I. Kerenidis, and E. Diamanti, Quantum weak coin flipping with a single photon, Phys. Rev. A 102, 022414 (2020).

[33] A. C. Yao, Protocols for secure computations, in 23rd Annual Symposium on Foundations of Computer Science, 1982. SFCS ’82 1982. pp. 160–164.

[34] A. Kent, W. J. Munro, and T. P. Spiller, Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints, Phys. Rev. A 84, 012326 (2011).

[35] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, Position-based quantum cryptography: Impossibility and constructions, SIAM J. Comput. 43, 150 (2014).

[36] A. Kent, Quantum tagging for tags containing secret classical data, Phys. Rev. A 84, 022335 (2011).

[37] P. Wallden, V. Dumjko, A. Kent, and E. Andersson, Quantum digital signatures with quantum-key-distribution components, Phys. Rev. A 91, 042304 (2015).

[38] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Secure quantum signatures using insecure quantum channels, Phys. Rev. A 93, 032325 (2016).

[39] S. Wiesner, Conjugate coding, ACM Sigact News 15, 78 (1983).

[40] D. Gavinsky, Quantum money with classical verification, in 2012 IEEE 27th Conference on Computational Complexity (2012) pp. 42–52.

[41] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac, Unforgeable noise-tolerant quantum tokens,
