THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

Experimental plug and play quantum coin flipping

Citation for published version:
Pappa, A, Jouguet, P, Lawson, T, Chailloux, A, Legré, M, Trinkler, P, Kerenidis, I & Diamanti, E 2014, 'Experimental plug and play quantum coin flipping' Nature Communications. DOI: 10.1038/ncomms4717

Digital Object Identifier (DOI):
10.1038/ncomms4717

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Nature Communications

Experimental plug&play quantum coin flipping

Anna Pappa,[1,2] Paul Jouguet,[1,3] Thomas Lawson,[1] André Chailloux,[2,4]
Matthieu Legré,[5] Patrick Trinkler,[5] Iordanis Kerenidis,[2,6] and Eleni Diamanti[1]

[1] *LTCI, CNRS - Télécom ParisTech, Paris, France*
[2] *LIAFA, CNRS - Université Paris Diderot 7, Paris, France*
[3] *SeQureNet, Paris, France*
[4] *CWI, Amsterdam, The Netherlands*
[5] *ID Quantique SA, Geneva, Switzerland*
[6] *Center for Quantum Technologies, National University of Singapore, Singapore*

(Dated: June 17, 2013)

Performing complex cryptographic tasks will be an essential element in future quantum communication networks. These tasks are based on a handful of fundamental primitives, such as coin flipping, where two distrustful parties wish to agree on a randomly generated bit. Although it is known that quantum versions of these primitives can offer information-theoretic security advantages with respect to classical protocols, a demonstration of such an advantage in a practical communication scenario has remained elusive. Here, we experimentally implement a quantum coin flipping protocol that performs strictly better than classically possible over a distance suitable for communication over metropolitan area optical networks. The implementation is based on a practical plug&play system, designed for quantum key distribution. We also show how to combine our protocol with coin flipping protocols that are almost perfectly secure against bounded adversaries, hence enhancing them with a level of information-theoretic security. Our results offer a powerful toolbox for future secure quantum communications.

Security is an imperative in all communication networks. Quantum communications hold the promise of achieving a security level that is impossible to reach by purely classical means. Indeed, information-theoretic security has been demonstrated for the cryptographic task of distributing a secret key between two trusted and collaborating communicating parties using systems exploiting quantum effects [1]. However, many advanced cryptographic schemes belong to a model where the two parties do not trust each other and hence cannot collaborate. One of the fundamental primitives in this setting is coin flipping, in which two spatially separated distrustful parties share a randomly generated bit, whose value must be unbiased [2]. It is known that, even when protocols are augmented with quantum communication, perfectly secure coin flipping, i.e., with a zero bias, is impossible without making some computational assumptions [3, 4]. A series of theoretical works, however, has demonstrated that the probability that an all-powerful malicious party can bias the coin, namely the cheating probability, can be strictly lower than 1 in the quantum setting, with an ultimate asymptotic bound of $1/\sqrt{2}$ [5–11]. Coin flipping therefore provides an ideal framework to demonstrate an advantage of quantum over classical communication, achieving unconditional security in a non-cooperative model that is crucial for cryptographic applications beyond key distribution.

To demonstrate such an advantage, we need to consider all imperfections that naturally appear in practical devices. For photonic systems, which constitute the chosen architecture for quantum communications, imperfections typically appear in the form of losses in the channel and measurement apparatus, and errors in the different implementation stages. Furthermore, systems suitable for long-distance communications over fiber-optic channels usually employ coherent light sources, thus becoming vulnerable to attacks exploiting the non-deterministic photon emission inherent in such sources [12].

Some of the aforementioned practical issues have been addressed in recent theoretical and experimental studies. An analysis of the problem of loss tolerance in current protocols provided an elegant solution [13], which however did not account for experimental noise and the presence of multiphoton pulses in coherent light source implementations. The cheating probability achieved by this protocol was slightly improved in subsequent work [14, 15]. To account for errors, the primitive of bit string generation was considered [16–18], but was later proven to be possible classically. In practice, after initial proof-of-principle demonstrations [19, 20], a recent implementation of the loss-tolerant protocol [21] used an entangled-photon source to eliminate the problem of multiphoton pulses. However, although in principle the cheating probability bound in the implemented protocol is independent of losses, no quantum advantage was demonstrated for a distance longer than a few meters. Finally, the closely related primitive of quantum bit commitment was experimentally demonstrated in a model where adversaries have access to an imperfect quantum memory [22]; however, the security of the protocol is entirely compromised against all-powerful adversaries.

Here, we provide a complete theoretical and experimental framework for the implementation of quantum coin flipping in practical communication scenarios. The protocol that we consider [23] takes all experimental imperfections into account. We show that our protocol can be combined with protocols that achieve almost perfect security, i.e., a bias asymptotically close to zero, against adversaries with bounded resources. More explicitly, if the adversary is bounded, then the protocol guarantees almost perfect security, while in the case of an all-powerful adversary, the protocol still guarantees a security level strictly higher than classically possible. Furthermore, we experimentally implement the protocol using a commercial plug&play system, designed for quantum key distribution [24, 25]. The key element of our implementation is that we take a realistic approach: to account for the unavoidable errors in the system and for coherent light source emission statistics, we allow for a non-zero but small probability of abort when both parties are honest, and accept the dependence of the cheating probability on communication loss thus departing from absolute loss tolerance [13, 21]. As a result, using an appropriate benchmark for classical coin flipping protocols [26], we can rigorously quantify the advantage offered by quantum communication as a function of distance, much in the way that the secret key fraction is calculated in practical quantum key distribution implementations [1]. We demonstrate a clear advantage for quantum coin flipping with information-theoretic security, at a communication distance suitable for metropolitan area network communications, with a system that can readily be deployed in such networks.

Results

Basic quantum coin flipping protocol. The protocol that we have analyzed and implemented is schematically shown as Protocol 1 (see [23] for a complete theoretical analysis). Alice sends to Bob a fixed number K of photon pulses in states $|\Phi_{\alpha_i,c_i}\rangle$, each of which is prepared independently following a random choice of basis α_i and bit c_i, with $i = 1, ..., K$, and a fixed protocol parameter y. Bob measures the K pulses by randomly selecting bases β_i, and replies with the position of the first successfully measured pulse j and a random bit b. Alice then reveals the basis and the bit used for that position: if the bases of the two parties agree, but the measurement output of Bob is not the same as Alice's bit, they abort. In all other cases, they agree that the coin value is $c_j \oplus b$.

Alice		**Bob**
choose $\{\alpha_i, c_i\}_1^K$		choose $\{\beta_i\}_1^K$
	$\xrightarrow{\lvert\Phi_{\alpha_i,c_i}\rangle}$	measure in basis $\{\beta_i\}_1^K$
	$\xleftarrow{j,b\in_R\{0,1\}}$	j: first measured pulse
	$\xrightarrow{c_j,\ \alpha_j}$	check
	Coin: $c_j \oplus b$	

Protocol 1. **Basic quantum coin flipping protocol.** The protocol consists of the following steps: (i) Alice sends to Bob K photon pulses. For $i = 1, ..., K$, she randomly chooses a basis $\alpha_i \in \{0,1\}$ and a bit $c_i \in \{0,1\}$, such that the state of the i-th pulse is $|\Phi_{\alpha_i,c_i}\rangle$, with $|\Phi_{\alpha_i,0}\rangle = \sqrt{y}|0\rangle + (-1)^{\alpha_i}\sqrt{1-y}|1\rangle$, $|\Phi_{\alpha_i,1}\rangle = \sqrt{1-y}|0\rangle - (-1)^{\alpha_i}\sqrt{y}|1\rangle$. (ii) For each pulse i, Bob randomly chooses β_i and measures in basis $\{|\Phi_{\beta_i,0}\rangle, |\Phi_{\beta_i,1}\rangle\}$. He sends j, the index of the first successfully measured pulse, and a random bit b to Alice. (iii) Alice replies by sending (α_j, c_j). If $\alpha_j = \beta_j$, Bob checks that his measurement outcome is indeed c_j, and if not he aborts. If he does not abort or if $\alpha_j \neq \beta_j$, the coin value is $c = c_j \oplus b$.

A crucial feature of the protocol is the assumption that the states are generated by an attenuated coherent light source, which is essential for a practical implementation, and not by a single-photon or entangled-photon source. Therefore, each pulse contains a number of photons that follows a Poisson distribution with mean photon number μ. The security analysis of the protocol [23] accounts for practical imperfections by introducing a probability to abort even when both parties are honest. This honest abort probability, denoted H, can be calculated as a function of all the experimental parameters, in particular the mean photon number per pulse μ, the number of protocol rounds K, the channel length, the detector quantum efficiency and dark count rate, and the error rate. Then, optimal cheating strategies for an all-powerful malicious party are devised for both Alice and Bob, leading to expressions for the maximal cheating probabilities, p_q^A and p_q^B, respectively. For our protocol, p_q^A is a function of y, while p_q^B depends on μ, K, and y [23]. Hence, for a given desired honest abort probability and specific experimental conditions, it is possible to minimize the cheating probabilities by finding optimal values for the protocol parameters μ and K. Additionally, the parameter y can be appropriately adjusted so that $p_q^A = p_q^B \equiv p_q$, which means that the protocol is fair.

This analysis allows us to evaluate the performance of the quantum coin flipping protocol, in terms of the maximal cheating probability attained for any given honest abort probability, for different communication distances. Furthermore, a security analysis allowing for a non-zero honest abort probability has also been performed for classical coin flipping protocols [26], providing the cheating probability bound $p_c = 1 - \sqrt{H/2}$, for $H < 1/2$, which is the honest abort probability region of practical interest. This can be used as a benchmark to assess quantitatively the advantage offered by the use of quantum resources for coin flipping.

Enhancing the security of protocols against bounded adversaries. Our basic quantum coin flipping protocol provides a cheating probability for an all-powerful adversary that is strictly lower than 1 for a wide range of realistic parameters. It therefore achieves an unconditional security level which is impossible classically. However, this level of security might not be useful for some applications; indeed, as we show later, the unbounded adversary can bias the coin with probability greater than 90%. We show that our protocol can be combined with protocols that achieve a bias asymptotically close to zero against bounded adversaries. As a result, such a combined protocol achieves an almost perfect security against bounded adversaries and, in addition, provides a level of security against unbounded adversaries that is strictly better than classically possible.

Let us explain how we construct a combined protocol. We discern three stages, as in the commonly used protocols against bounded adversaries, including classical protocols employing one-way functions [27] and quantum protocols in the noisy quantum storage model [22, 28]. In the first stage (*commit*), which remains unchanged from the protocols against bounded adversaries, Alice and Bob exchange classical or quantum messages such that at the end of this stage each party has almost perfectly committed to one bit, S and T, respectively. In the second stage (*encrypt*), Alice and Bob encrypt their respective random bits using the committed values. In particular, Alice sends K pulses using the states $|\Phi_{\alpha_i,c_i\oplus S}\rangle$, for $i = 1, ..., K$, and Bob replies by sending $T \oplus b$ as well as j, the index of the first measured pulse, as in the basic protocol. In the third stage (*reveal*), Alice and Bob reveal (c_j, S) and (b, T), respectively, together with additional information depending on the underlying bounded adversary model and, if nobody aborts, the value of the coin is $c_j \oplus b$.

In Methods, we provide the combined protocols for two realistic models, one with computationally bounded adversaries and the other with adversaries with noisy quantum storage. In both cases, when the adversaries are bounded, we achieve the same, almost perfect, security as the original protocols; additionally, when the adversaries are unbounded, they still cannot cheat with a probability higher than the one provided by our basic quantum coin flipping protocol. Hence, the combined protocols offer the maximal possible security guarantees.

Experimental quantum coin flipping results. The basic quantum coin flipping protocol is tailored for a practical implementation using an attenuated coherent light source. We perform the experimental demonstra-

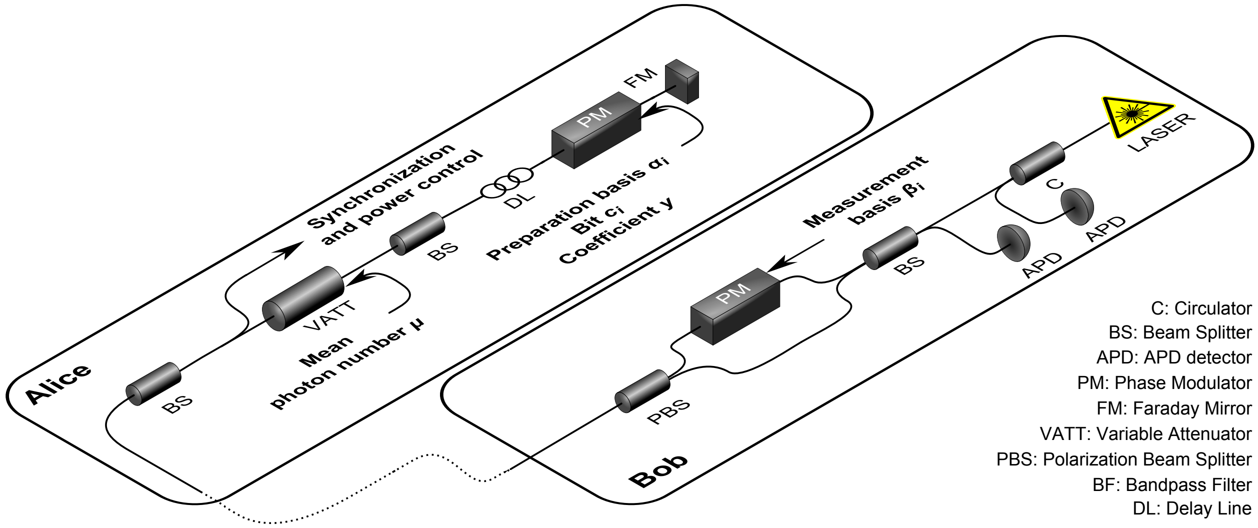

Figure 1. **Experimental setup of the quantum coin flipping plug&play system.** The laser source at Bob's setup emits photon pulses at a wavelength of 1550 nm and with an intensity of -13.5 dBm. These are separated at a 50/50 beamsplitter (BS) and then recombined at a polarization beam splitter (PBS), after having traveled through a short and a long arm, which contains a phase modulator and is appropriately arranged to transform horizontally polarized to vertically polarized states and vice versa. The pulses then travel to Alice through the communication channel, are reflected on a Faraday mirror, appropriately modulated and attenuated, and travel back to Bob orthogonally polarized. As a result, the pulses now take the other path at Bob's side and arrive simultaneously at the beamsplitter, where they interfere. Finally, they are detected by two InGaAs avalanche photodiode (APD) single-photon detectors. In our implementation, the quantum efficiency and dark count rate per detection gate of the detectors before and after the circulator, were 7.4% and 2×10^{-6}, and 7.7% and 6×10^{-6}, respectively. To implement the quantum coin flipping protocol, Alice chooses her basis and bit values by applying a suitable phase shift to the second pulse with her phase modulator. This modulator is also used to apply the state coefficient y. She also uses her variable attenuator to apply the required attenuation for a desired mean photon number per pulse μ. Bob chooses his measurement basis by applying an appropriate phase shift at the first pulse on its way back using his phase modulator. This interferometric setup compensates for all fluctuations in the channel. The two-way configuration demands particular care in the synchronization of the phase shift and attenuation signals, and the detection gates. This is achieved in practice by appropriate calibration procedures.

tion using the commercial system Clavis2 of IDQuantique [24], which is designed for quantum key distribution (QKD). The experimental setup is shown in Fig. 1. This so-called plug&play system relies on an autocompensating interferometric setup, which guarantees excellent system stability. A two-way approach is employed: light pulses at 1550 nm are sent from Bob to Alice, who uses a phase modulator to encode her information. The pulses are then reflected by a Faraday mirror and attenuated to the desired level before being sent back to Bob. Finally, Bob chooses a measurement basis with his phase modulator and registers the detection events using two single-photon detectors. When the BB84 QKD protocol [29] is implemented by the plug&play system, the states prepared by Alice and measured by Bob correspond to the states $|\Phi_{\alpha_i,c_i}\rangle$ used in our quantum coin flipping protocol, with $y = 1/2$. Hence, the quantum transmission stage of the QKD protocol is identical to that of the quantum coin flipping protocol with the exception that, in the latter, y should be appropriately modified to guarantee the fairness of the implemented protocol. In practice, this parameter is set using the control signal that drives Alice's phase modulator, which is also used to encode Alice's basis and bit information.

Let us now describe the experimental procedure. We perform quantum coin flipping experiments for two channel lengths, namely 15 and 25 km. In Table I we provide typical values of the experimental parameters used in the implementations. For each channel length, Alice sets the average photon number per pulse μ with the variable attenuator shown in Fig. 1, using a previously established calibration relationship. It is important to note that typical uses of the Clavis2 for QKD employ significantly higher μ values, hence our implementation required operating the system in previously untested parameter regimes, and appropriately adjusting the calibration and synchronization procedures.

The quantum transmission part of the protocol is subsequently implemented, leading to a set of data containing the preparation and measurement basis choices of Alice and Bob, respectively, and the measurement outcomes of Bob, similarly to the raw key data obtained in quantum key distribution experiments. Based on this

	15 km		25 km	
Coefficient y	0.88		0.85	
μ ($\times 10^{-3}$)	2.8 $\pm$0.1	**2.1 $\pm$ 0.1**	5.1$\pm$ 0.1	**4 $\pm$ 0.1**
Protocol rounds K	65700	**95700**	88900	**120000**
Cheating probability	0.909 $\pm$ 0.001	**0.907 $\pm$ 0.001**	0.933 $\pm$ 0.002	**0.929 $\pm$ 0.002**

Table I. **Experimental parameter values for honest abort probability $H = 1\%$.** The parameters correspond to a fair protocol, for which the cheating probabilities for a malicious Alice or Bob are the same. This is ensured by the choice of the coefficient y. To perform an experiment for a specific value of the average photon number per pulse μ, Alice applies a control signal to her variable attenuator, according to a previously established calibration relationship. The difference between the value of μ expected by this relationship given the known experimental conditions in the path from Bob's laser to Alice's attenuator, and the value of μ deduced from the actual detection events and the conditions in the path between Alice's output and Bob's detectors, gives rise to the reported uncertainty in this value. For a given channel length, the number of required rounds, and hence the protocol runtime, decreases for higher μ values, at the expense of slightly higher cheating probabilities. The size of the detection event data used to calculate the rounds K required to obtain the specific honest abort probability is sufficiently large (typically 3×10^5) to ensure that the finite-size effects in our implementation are negligible. For the specific system parameters, the cheating probability can then be computed using the security analysis of the basic quantum coin flipping protocol. The highlighted parameters correspond to the values shown in Fig. 2.

data, we calculate the number of protocol rounds K that are required to achieve a desired honest abort probability. The detection events registered by Bob, in conjunction with the known experimental conditions in the path between Alice and Bob, can be used to determine the actual average photon number per pulse μ that is exiting Alice's system. In practice, we find that this value is slightly different from the one estimated by the variable attenuator calibration relationship. This difference is at the origin of the uncertainty in the values of μ shown in Table I.

The described experimental procedure is performed using several values of μ for each channel length, and then choosing the number of rounds K to attain the desired honest abort probability. Based on these sets of parameters, we derive the cheating probabilities of a malicious Alice and Bob, p_q^A and p_q^B, respectively, using the security analysis of the basic quantum coin flipping protocol. This allows us to find, for both channel lengths, the sets of values for μ, K and y that minimize the cheating probability and at the same time make the protocol fair ($p_q^A = p_q^B \equiv p_q$). Note that for simplicity, the y values of our experimental data have been chosen independently of the honest abort probability value; in practice, slight modifications of these values might be required to achieve a perfectly fair protocol for each specific honest abort probability. The optimized experimental parameters for an honest abort probability $H = 1\%$ are highlighted in Table I.

In Fig. 2 we show the cheating probability calculated from our experimental data for 15 and 25 km, as a function of the honest abort probability. For each value of the honest abort probability, the number of rounds K and mean photon number per pulse μ has been optimized as explained previously. The uncertainty in the estimation of μ is illustrated by the shaded areas in the plot. To quantify the advantage offered by quantum communication, we use the classical cheating probability bound, p_c [26]. We can see that the cheating probability is strictly lower than classically possible for both distances, and for practical values of honest abort probabilities.

To obtain further insight into our results, we define a gain function, as follows:

$$G = p_c - p_q,$$

where p_c and p_q are the classical cheating probability bound and the quantum cheating probability value derived from our experimental data, respectively. If the experimental data yields a positive G for a certain honest abort probability, this means that these results cannot be obtained by any purely classical means. We can then use the gain as a figure of merit to assess the performance of our quantum coin flipping implementation in a secure communication scenario. In Fig. 3, we show the gain as a function of distance, for a fixed honest abort probability $H = 1\%$. The channel length of 25 km is close to the cut-off distance for which a positive gain can be obtained, however this range is sufficient for many applications requiring communication over metropolitan area networks. Note that, contrary to quantum key distribution, here no classical error-correction process can be implemented since Alice and Bob do not trust each other, which results in an inherent limitation to the attainable communication distance. Using better single-photon detectors [30], with lower dark count rates, for instance, would extend the communication distance of our protocol.

Finally, in our implementation, the classical steps of the coin flipping protocol following the quantum transmission are not performed in real time. However, it is clear that the coin flipping rate will be dominated by the time that it takes for K pulses to travel from

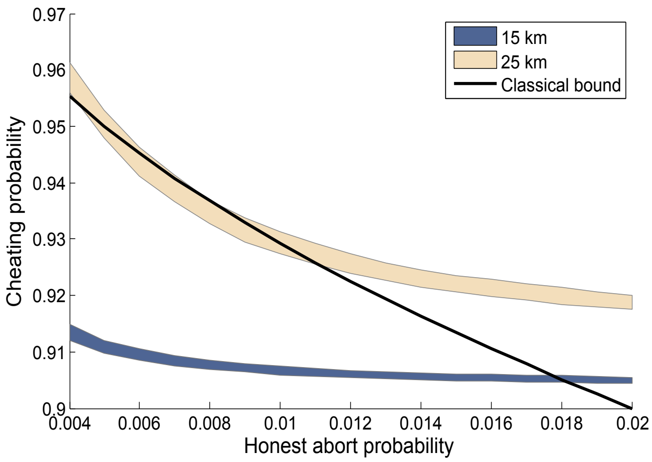

Figure 2. **Cheating probability as a function of honest abort probability for channel lengths of 15 and 25 km.** The cheating probability for each honest abort probability value is calculated from the experimental data using the security analysis of the basic quantum coin flipping protocol. The values correspond to a fair protocol. The shaded areas are derived from the uncertainty in the estimation of the average photon number per pulse exiting Alice's setup. The solid line represents the cheating probability bound for classical coin flipping protocols. For both channel lengths, quantum communication leads to lower cheating probability values than is classically possible, for a range of practical honest abort probabilities.

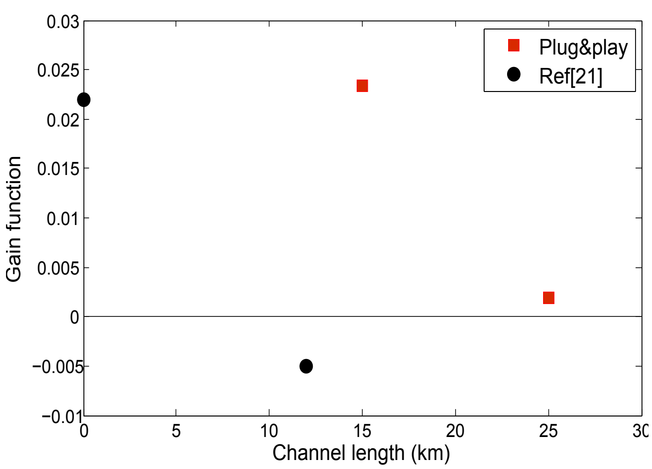

Figure 3. **Gain as a function of channel length.** The gain function is calculated as the difference between the classical and quantum cheating probability, and illustrates the advantage offered by the use of quantum communication for coin flipping. The red squares correspond to the cheating probabilities achieved by our plug&play implementation for 15 and 25 km, for a fixed honest abort probability of 1%. A positive gain is obtained for both distances. For comparison, previous experimental results based on an entangled-photon source implementation of a loss-tolerant quantum coin flipping protocol [21] are also shown (blue circles): a positive gain is obtained only for a very short distance (10 m), with an honest abort probability of 1.8%.

Alice to Bob. For a laser pulse repetition rate of 10 MHz, this corresponds roughly to a few tens of coin flips per second. As we can see in Table I, if Alice increases the average photon per pulse exiting her system, the required number of protocol rounds reduces, which also reduces the runtime for the protocol, but this comes at the expense of a slightly higher cheating probability. Hence, in a real communication scenario of two distrustful parties wishing to agree on a coin value using the plug&play system, the parties would be given a choice of gain values for a range of honest abort probabilities given their communication distance and the desired communication rate. This parameter choice will have an effect on the security only in the case of an unbounded adversary, since in the bounded models the bias achieved by our combined protocols is asymptotically close to zero.

Discussion. We have rigorously demonstrated a significant advantage of quantum over classical communication with information-theoretic security guarantees using the fundamental cryptographic primitive of coin flipping. Furthermore, we have demonstrated this advantage using a commercial plug&play system, which does not require any entangled-photon or quantum memory resources, over distances suitable for metropolitan area communication networks. This greatly enlarges the scope of unconditionally secure quantum cryptography, in particular to the case where the parties do not trust each other.

Additionally, by combining our quantum coin flipping protocol with protocols secure against bounded adversaries we enhance them with a level of information-theoretic security. It is interesting to note that our protocol is based on a bit commitment scheme, augmented only by an additional classical message from Bob to Alice between the *commit* and *reveal* stages. This means that our combined coin flipping protocols can also be viewed as commitment schemes where both parties commit some value to each other. Hence, our security analysis can be extended in a straightforward way to hold for bit commitment in the computational models that we have considered. In the same way, our implementation indeed performs plug&play quantum bit commitment.

As in practical quantum key distribution, our implementation of quantum coin flipping may be vulnerable to side-channel attacks. The power control setup placed at the entrance of Alice's system as a countermeasure for the so-called Trojan horse attacks [31] can also be used, incidentally, to counter a possible attack where Bob sends strong light pulses to Alice, which lead to an increased average photon number per pulse and consequently to a greater cheating probability. Identifying other potential side-channel attacks and devising appropriate countermeasures is of great importance, as for all practical quantum cryptographic systems.

Methods

Combined quantum coin flipping protocols. We show how to combine the basic quantum coin flipping protocol with protocols that achieve almost perfect security against adversaries that possess limited resources. We consider, in particular, computationally bounded adversaries and adversaries with noisy quantum storage.

The computationally bounded protocol, shown as Protocol 2, uses an injective one-way function f, upon which Alice and Bob have previously agreed [27]. In the *commit* stage of the protocol, Alice and Bob choose random strings, x_A and x_B, respectively, and commit to the bits $h(x_A)$ and $h(x_B)$ by exchanging $f(x_A)$ and $f(x_B)$, where h is a hardcore predicate of f. Hardcore predicates make it impossible to guess the value $h(x)$ from $f(x)$ with probability greater than one half. A good example of a hardcore predicate function is the parity of the bits in a string, since it can be proven [27] that given the parity and the image of the string, it is not feasible to guess the string itself. Moreover, since f is an injective one-way function, by sending the values $f(x)$, neither of the two parties can lie about the value of their chosen string and thus change the value $h(x)$. Hence, at the end of this stage Alice and Bob have almost perfectly committed to $h(x_A)$ and $h(x_B)$. In the *encrypt* stage, for $i = 1, ..., K$, Alice randomly selects α_i and c_i and sends the K quantum states $|\Phi_{\alpha_i, c_i \oplus h(x_A)}\rangle$ to Bob, prepared in the same way as in the basic protocol. Bob performs a measurement in the randomly selected bases $\{|\Phi_{\beta_i,0}\rangle, |\Phi_{\beta_i,1}\rangle\}$, and replies with the position j of the first successfully measured pulse and a random bit b encrypted as $b \oplus h(x_B)$. Finally, in the *reveal* stage, Alice and Bob reveal their strings and check that they are consistent with the function outputs exchanged during the *commit* phase. They also exchange their chosen bit and Bob aborts only if $\alpha_j = \beta_j$ and his measurement outcome does not agree with c_j. If he does not abort, then the value of the coin is $c_j \oplus b$. Note that the *encrypt* stage and the first step of the *reveal* stage correspond to our basic quantum coin flipping protocol, slightly modified to fit the underlying computationally bounded model.

Concerning the security analysis, if Alice is computationally bounded, then she cannot guess the value $h(x_B)$ with probability greater than one half, which means that Bob's bit b is perfectly hidden from her when Bob sends $b \oplus h(x_B)$. Therefore, the protocol remains almost perfectly secure against Alice. If Bob is computationally bounded, then the bits c_j are perfectly hidden as $c_j \oplus h(x_A)$, hence the protocol remains almost perfectly secure against Bob. If, on the other hand, the parties are unbounded, they can perfectly compute the hardcore predicates and the security of the protocol becomes exactly the same as the security of our basic coin flipping protocol.

Alice		**Bob**
choose x_A	$\xrightarrow{f(x_A)}$	choose x_B
	$\xleftarrow{f(x_B)}$	
choose $\{\alpha_i, c_i\}_1^K$	$\xrightarrow{\lvert\Phi_{\alpha_i, c_i \oplus h(x_A)}\rangle}$	measure in $\{\beta_i\}_1^K$
	$\xleftarrow{j,\ b \oplus h(x_B)}$	j: first measured pulse, $b \in_R \{0,1\}$
	$\xrightarrow{x_A,\ c_j,\ \alpha_j}$	
	$\xleftarrow{x_B,\ b}$	
	Coin: $c_j \oplus b$	

Protocol 2. **Computationally-bounded quantum coin flipping**.

In the noisy storage protocol [22], shown as Protocol 3, the parties first agree on an error-correcting code. This is followed by a *prepare* stage, where Alice sends to Bob $2n$ quantum states, which are the states used in the basic protocol, with $y = 1/2$. Bob measures the states using randomly chosen bases $\{\hat{b}_i\}_1^{2n}$. At the end of this procedure, Alice has a string containing the bits used to construct the states, namely $X^{2n} = X_1^n X_2^n$, and Bob has a string containing his measurement results, namely $\tilde{X}^{2n} = \tilde{X}_1^n \tilde{X}_2^n$. If the choices of the states and the measurement bases are uniformly random, then the strings agree on approximately half of the positions.

The parties then perform the main coin flipping protocol. In the *commit* stage, Alice and Bob commit to bits $D_A = \mathrm{Ext}(X_1^n, r)$ and $D_B = \mathrm{Ext}(\tilde{X}_2^n, \tilde{r})$, respectively, where $\mathrm{Ext} : \{0,1\}^n \otimes R \to \{0,1\}$ is a family of 2-universal hash functions, and $(r, \tilde{r})$ are strings chosen by Alice and Bob in order to randomly pick a hash function from this family. To this end, they first calculate the syndromes $w = Syn(X_1^n)$ and $\tilde{w} = Syn(\tilde{X}_2^n)$ based on the chosen error-correcting code, and commit to the extractor function values by exchanging the syndromes and half of the bases' values they used in the measurements. In the *encrypt* stage, Alice encrypts her bit choices c_j by sending K states $|\Phi_{\alpha_j, c_j \oplus D_A}\rangle$, prepared as in the basic protocol. Bob chooses randomly β_j and measures in $\{|\Phi_{\beta_j,0}\rangle, |\Phi_{\beta_j,1}\rangle\}$. He then encrypts a bit b by sending $b \oplus D_B$ to Alice, together with the index m of the first successfully measured pulse. Finally, in the *reveal* stage, Alice and Bob reveal their string and bit values and check that for the positions with the same bases, X_2^n coincides with $\tilde{X}_2^n$ and X_1^n coincides with $\tilde{X}_1^n$, respectively. They also check that the syndromes and extractor outputs correspond to the received strings. If the measurement outcome for the first measured pulse agrees with the revealed bit for the same choice of bases or if the bases are different, they agree on the coin, otherwise they abort. Again, the *encrypt* stage and the first step of the *reveal* stage correspond to the basic quantum coin flipping protocol.

Alice		**Bob**
choose $\{b_i, x_i\}_1^{2n}$	$\xrightarrow{\lvert\Phi_{b_i,x_i}\rangle}$	measure in $\{\hat{b}_i\}_1^{2n}$
String:		String:
$X^{2n} = X_1^n X_2^n$		$\tilde{X}^{2n} = \tilde{X}_1^n \tilde{X}_2^n$
$\lvert X_1^n\rvert = \lvert X_1^n\rvert = n,$		$\lvert\tilde{X}_1^n\rvert = \lvert\tilde{X}_1^n\rvert = n$
	Wait time Δt	
$w = Syn(X_1^n),$		$\tilde{w} = Syn(\tilde{X}_2^n),$
string r		string $\tilde{r}$
$D_A = Ext(X_1^n, r)$	$\xrightarrow{\{b_i\}_1^{n/2},\ w,\ r}$	$D_B = Ext(\tilde{X}_2^n, \tilde{r})$
	$\xleftarrow{\{\tilde{b}_i\}_{n/2+1}^n,\ \tilde{w},\ \tilde{r}}$	
choose $\{\alpha_j, c_j\}_1^K$	$\xrightarrow{\lvert\Phi_{\alpha_j, c_j \oplus D_A}\rangle}$	measure in $\{\beta_j\}_1^K$
	$\xleftarrow{D_B \oplus b,\ m}$	m: 1st measured pulse
	$\xrightarrow{X_1^n, c_m}$	
	$\xleftarrow{\tilde{X}_2^n,\ b}$	
check:		check:
$Syn(\tilde{X}_2^n) = \tilde{w}$		$Syn(X_1^n) = w$
$Ext(\tilde{X}_2^n, \tilde{r}) = D_B$		$Ext(X_1^n, r) = D_A$
	Coin: $c_m \oplus b$	

Protocol 3. **Noisy storage quantum coin flipping.**

The noisy storage limitation together with the waiting time Δt that is imposed on the parties, forces them to measure any quantum state they might have wanted to keep unmeasured in order to improve their cheating strategy. Bob is forced to measure the states sent by Alice and Alice is forced to measure whatever entangled share she may have kept when sending the states to Bob.

Concerning the security analysis, if Alice has noisy storage, then she cannot guess the value D_B with probability greater than one half, hence Bob's bit b is perfectly hidden from her when Bob sends $b \oplus D_B$. Therefore, the protocol remains almost perfectly secure against Alice. If Bob has noisy storage, then again the bits c_j are perfectly hidden as $c_j \oplus D_A$ and the protocol remains almost perfectly secure against Bob. If, on the other hand, the parties have perfect memory, they can perfectly compute the values D_A and D_B and the security of the protocol reduces exactly to the security of our basic quantum coin flipping protocol.

Acknowledgments

This research was supported by the French National Research Agency, through CRYQ (ANR-09-JCJC-0067) and HIPERCOM (2011-CHRI-006) projects, by the European Union through the project Q-CERT (FP7-PEOPLE-2009-IAPP), and by the City of Paris through the CiQWii project. ID Quantique work was supported by the European Union project SIQS. A.P. and T.L. acknowledge support from Digiteo. P.J. acknowledges support from the ANRT (Agence Nationale de la Recherche et de la Technologie). A.P., P.J., T.L., and E.D. thank the ID Quantique team for their hospitality during their visits to Geneva.

[1] Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).

[2] Blum, M. Coin flipping by telephone: a protocol for solving impossible problems. In *Advances in Cryptology; a Report on CRYPTO'81*, vol. 82, 11–15 (Santa Barbara, California, USA, 1981).

[3] Lo, H.-K. & Chau, H. F. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D* **120,** 177–187 (1998).

[4] Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **78,** 3414–3417 (1997).

[5] Aharonov, D., Ta-Shma, A., Vazirani, U. & Yao, A. Quantum bit escrow. In *STOC 2000, The 32nd Annual ACM Symposium on Theory of Computing, Portland, OR, USA*, 705–714 (ACM, New York, USA, 2000).

[6] Spekkens, R. & Rudolph, T. Quantum protocol for cheat-sensitive weak coin flipping. *Phys. Rev. Lett.* **89,** 1–4 (2002).

[7] Kitaev, A. Lecture delivered at the *Annual Quantum Information Processing Workshop (QIP 2003), MSRI, Berkeley, CA, 1317 Dec 2002.*

[8] Nayak, A. & Shor, P. Bit-commitment-based quantum coin flipping. *Phys. Rev. A* **67,** 012304 (2003).

[9] Ambainis, A. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.* **68,** 398–416 (2004).

[10] Colbeck, R. An entanglement-based protocol for strong coin tossing with bias 1/4. *Phys. Lett. A* **362,** 390–392 (2007).

[11] Chailloux, A. & Kerenidis, I. Optimal quantum strong coin flipping. In *Proceedings of the 50th Annual Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta* (IEEE Computer Society, 2009).

[12] Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85,** 1330–1333 (2000).

[13] Berlin, G., Brassard, G., Bussières, F. & Godbout, N. Loss-tolerant quantum coin flipping. *Phys. Rev. A* **80,**

062321 (2009).
[14] Chailloux, A. Improved loss-tolerant quantum coin flipping. Presented at the *10th Asian Quantum Information Processing Conference, Tokyo, Japan* (August 2010).
[15] Aharon, N., Massar, S. & Silman, J. A family of loss-tolerant quantum coin flipping protocols. *Phys. Rev. A* **82,** 052307 (2010).
[16] Kent, A. Large n quantum cryptography. In *Proceedings of the 6th International Conference on Quantum Communication, Measurement and Computing, QCMC02, 2002* (Rinton Press Inc, 2003).
[17] Barrett, J. & Massar, S. Quantum coin tossing and bit-string generation in the presence of noise. *Phys. Rev. A* **69,** 022322 (2004).
[18] Lamoureux, L. P., Brainis, E., Amans, D., Barrett, J. & Massar, S. Provably secure experimental quantum bit-string generation. *Phys. Rev. Lett.* **94,** 050503 (2005).
[19] Molina-Terriza, G., Vaziri, A., Ursin, R. & Zeilinger, A. Experimental quantum coin tossing. *Phys. Rev. Lett.* **94,** 040501 (2005).
[20] Ngyuen, A. T., Frison, J., Huy, K. P. & Massar, S. Experimental quantum tossing of a single coin. *New J. Phys.* **10,** 083087 (2008).
[21] Berlin, G. *et al.* Experimental loss-tolerant quantum coin flipping. *Nat. Commun.* **2,** 561 (2011).
[22] Ying, N. N. H., Joshi, S. K., Ming, C. C., Kurtsiefer, C. & Wehner, S. Experimental implementation of bit commitment in the noisy storage model. *Nat. Commun.* **3,** 1326 (2012).
[23] Pappa, A., Chailloux, A., Diamanti, E. & Kerenidis, I. Practical quantum coin flipping. *Phys. Rev. A* **84,** 052305 (2011).
[24] http://www.idquantique.com.
[25] Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. & Zbinden, H. Quantum key distribution over 67 km with a plug&play system. *New J. Phys.* **4,** 41 (2002).
[26] Hänggi, E. & Wüllschleger, J. Tight bounds for classical and quantum coin flipping. In *Proceedings of the 8th Theory of Cryptography Conference, TCC 2001, Providence, RI, USA, March 28-30, 2011*, Lecture Notes in Computer Science, Vol. 6597 (Springer, 2011).
[27] Goldreich, O. *Foundations of Cryptography, Volume I, Basic Tools* (Cambridge University Press, 2003).
[28] Wehner, S., Schaffner, C. & Terhal, B. Cryptography from noisy storage. *Phys. Rev. Lett.* **100,** 220502 (2008).
[29] Bennett, C. H. & Brassard, G. in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India,* 175–179 (IEEE, New York, 1984).
[30] Natarajan, C. M., Tanner, M. G. & Hadfield, R. H. Superconducting nanowire single-photon detectors: physics and applications. *Superconductor Science and Technology* **25,** 063001 (2012).
[31] Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73,** 022320 (2006).