Provably Secure Experimental Quantum Bit-String Generation

L. P. Lamoureux,[1] E. Brainis,[2] D. Amans,[2] J. Barrett,[1] and S. Massar[1]

[1]*Laboratoire d'Information Quantique and Quantum Information and Communication, CP 165, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium*

[2]*Optique et Acoustique, CP 194/5, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium*

(Received 12 July 2004; published 7 February 2005)

Coin tossing is a cryptographic task in which two parties who do not trust each other aim to generate a common random bit. Using classical communication this is impossible, but nontrivial coin tossing is possible using quantum communication. Here we consider the case when the parties do not want to toss a single coin, but many. This is called bit-string generation. We report the experimental generation of strings of coins which are provably more random than achievable using classical communication. The experiment is based on the "plug and play" scheme developed for quantum cryptography, and therefore well suited for long distance quantum communication.

DOI: 10.1103/PhysRevLett.94.050503 PACS numbers: 03.67.Dd, 03.67.Hk

Coin tossing is a cryptographic task, introduced by Blum [1], in which two parties who do not trust each another aim to generate a common random bit. Coin tossing is an important primitive that can be used in the design of other two-party protocols such as mental poker and mail certification and it could even form the basis of a scheme for bit commitment that is computationally secure against quantum attacks [2]. Classically, coin tossing is impossible without computational assumptions: at least one of the parties can in principle always cheat and fix the outcome. Using quantum communication, however, nontrivial coin tossing is possible [3–7]. In many applications, the parties do not want to generate a single coin, but many. This is called bit-string generation [8–10]. Here we report on an experimental implementation of bit-string generation based on the "plug and play" scheme developed for quantum key distribution in optical fibers at telecommunication wavelengths [11]. Using the theoretical analysis of [10] we are able to show that the bit strings generated in our experiment achieve a level of randomness impossible classically. This is the first demonstration of a fundamental new concept: namely, the possibility of generating random coins with an adversary who is limited only by the laws of physics.

The present work focuses on bit-string generation rather than the tossing of a single coin for two reasons. First it is shown in [10] that in principle arbitrarily high levels of randomness per bit can be obtained for bit-string generation whereas this is not the case for coin tossing [12,13]. Hence bit-string generation is more promising from the point of view of applications. Second, present experimental limitations (mainly detector noise and inefficiency) seem to preclude tossing a single coin with a level of randomness higher than what is possible classically. This difficulty is illustrated by another experiment which recently realized some aspects of coin tossing [14], but for which it was impossible to prove that a level of randomness impossible classically was achieved.

We begin by reviewing security conditions for the generation of n random bits. The outcome of the protocol is either a string of bits $\vec{x} \in \{0,1\}^n$ or one of the parties aborts, in which case we write $\vec{x} = \perp$. The protocol is *correct* if, when both parties are honest, the probability of aborting is small and all the coins are fair. Mathematically we express this as

$$\forall\, \vec{c} \in \{0,1\}^n, \quad \mathrm{P}(\vec{x}=\vec{c}) = (1-\delta_n)/2^n, \quad \mathrm{P}(\vec{x}=\perp) = \delta_n. \tag{1}$$

It is necessary to include the parameter δ_n because of experimental imperfections which induce a nonzero probability of the protocol aborting even if both parties are honest. In the protocol we use, δ_n decreases to zero exponentially fast with n and can be neglected.

We shall use two security conditions. The first, called the "average bias", describes the degree of randomness of individual bits of the string. Formally we define the upper bound $\bar{\epsilon}_{A(B)}$ on the average bias when Alice (Bob) is dishonest and the other party is honest as

$$\begin{aligned} &\forall\, S_A\ \forall\, \vec{c} \in \{0,1\}^n, \quad \frac{1}{n}\sum_{i=1}^{n} \mathrm{P}^{S_A H_B}(x_i = c_i) \le \frac{1}{2} + \bar{\epsilon}_A, \\ &\forall\, S_B\ \forall\, \vec{c} \in \{0,1\}^n, \quad \frac{1}{n}\sum_{i=1}^{n} \mathrm{P}^{H_A S_B}(x_i = c_i) \le \frac{1}{2} + \bar{\epsilon}_B, \end{aligned} \tag{2}$$

where we denote a general strategy of Alice (Bob) by S_A (S_B), and the honest strategy defined by the protocol as H_A (H_B). Classically, when $\delta_n = 0$, one has $\bar{\epsilon}_A + \bar{\epsilon}_B \ge 1/2$ [10]. (When $\delta_n \neq 0$ the classical bound becomes $\bar{\epsilon}_A + \bar{\epsilon}_B \ge 1/2 - 2\delta_n$.)

The second security condition measures the degree of randomness of the string taken as a whole. We define $H_{A(B)}$ as the entropy of the string if Alice (Bob) is dishonest and the other party is honest. In [10], bounds on the entropy are derived for our protocol assuming general cheating. However the corresponding classical bound is not known, although it is conjectured in [10] to be of the form $H_A + H_B \leq n + o(n)$. We refer to [10] for a more detailed discussion of security conditions and for formal definitions of $H_{A(B)}$.

The protocol we shall use, inspired by that of [8,10] is as follows. Choose a security parameter $0 < \kappa < 1$. (1) For $i = 1$ to n. (2) Alice chooses a random bit a_i. If $a_i = 0$, she prepares a coherent state of the electromagnetic field with amplitude α: $\psi_0 = |\alpha\rangle$. If $a_i = 1$, she prepares a coherent state with amplitude $-\alpha$: $\psi_1 = |-\alpha\rangle$. She sends the coherent state ψ_{a_i} to Bob. After receiving the quantum state from Alice, Bob chooses a random bit b_i. Bob tells Alice the value of b_i. (3) After learning the value of b_i, Alice reveals the value of a_i to Bob. (4) Bob now verifies whether the state Alice sent him is indeed the coherent state $|(-1)^{a_i}\alpha\rangle$. He does this by using a local oscillator (LO) to carry out the displacement $\mathcal{D}[-(-1)^{a_i}\alpha]$. If Alice was honest, the displaced state should be the vacuum state. Bob checks that this is the case by sending the state onto a single photon detector. If the detector clicks, Bob sets $k_i = 1$. If the detector does not click, Bob sets $k_i = 0$. (5) Next i. (6) If $\frac{1}{n}\sum_i k_i > \kappa$, Bob aborts. Otherwise the output of the protocol is the bit string $x_i = (a_i + b_i) \bmod 2$.

When Bob is dishonest his best strategy is to measure the state sent to him by Alice as soon as he receives it [i.e., before carrying out step (3) above]. One easily shows, see [10], that

$$\bar{\epsilon}_B \leq \frac{\sin\theta}{2}, \quad \text{where } \cos\theta = |\langle\psi_0|\psi_1\rangle| = e^{-2|\alpha|^2}. \quad (3)$$

If Alice is dishonest she may not send Bob the state ψ_{a_i} but an arbitrary state ρ. In general she may prepare an entangled state, keeping half of it and sending the other half to Bob. Furthermore, she may correlate and even entangle her strategy over different runs. In [10], however, it is shown that strategies correlated over different runs cannot help Alice for large n. A bound on $\bar{\epsilon}_A$ is proven that depends on the average value of the fidelity $f_i = \langle\psi_{a_i}|\rho|\psi_{a_i}\rangle$, as estimated by Bob. Since the probability that Bob's detector clicks (assuming his detector is perfect) is related to the fidelity by $P(k_i = 1) \geq 1 - f_i$, the result of [10] then implies that, assuming large n, the bias if Alice is dishonest is bounded by $\bar{\epsilon}_A \leq \mathcal{F}(\kappa)$, where $\mathcal{F}(x) = \frac{\sqrt{x}}{\sqrt{2}\sin^2\theta} + \frac{x}{\sin^2\theta}$. Below we show how this relation must be modified to take into account imperfections in Bob's measuring apparatus.

Note that due to such imperfections, Bob's detector may click even if Alice is honest. Alice and Bob should choose κ such that it is larger than the expected number of clicks if both parties are honest. When this is the case, the probability δ_n that the protocol aborts if both parties are honest decreases exponentially fast to zero and the protocol is correct.

Our experimental setup, depicted in Fig. 1, is based on the plug and play system developed for long distance quantum key distribution [11]. The advantage of the plug and play system is that it constitutes an all-fiber (standard SMF-28), automatically balanced interferometer, and hence is well suited to long distance quantum communication. However the plug and play system has a number of specific features which must be carefully taken into account.

Bob to Alice and Bob's cheating.—Each round of the protocol begins with Bob producing a short (20 ns) intense (25 mW) laser pulse at $\lambda = 1.55$ μm. The pulse is split in two by the 50/50 coupler C_1. The two pulses acquire a relative time delay of 100 ns and then impinge with orthogonal polarization on a polarizing beam splitter (PBS) whereupon they are sent to Alice. Between C_1 and the PBS, along the long path, are an attenuator, a 99/1 coupler C_2, and a phase modulator. The role of these elements will be explained later. The relative attenuation of the two pulses is $A \simeq 45$ dB. The first pulse to reach Alice is intense and contains $N_0 \simeq 10^9$ photons. This pulse will play the role of LO. The second pulse to reach Alice is attenuated and contains AN_0 photons. The second pulse will play the role of signal.

Upon receiving the pulses, Alice measures the intensity of the signal pulse (using the 80/20 coupler C_3 and a classical detector D_{cl}) and attenuates both pulses. The

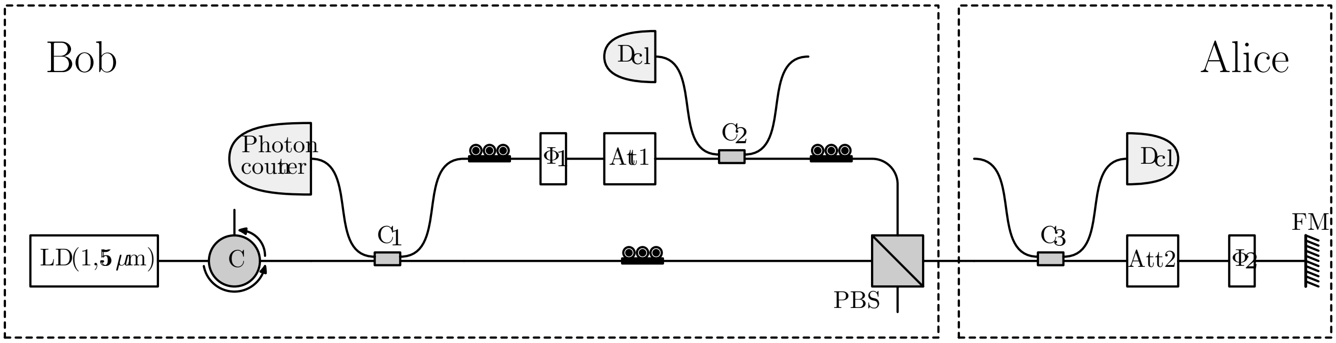

FIG. 1. Optical setup. LD: laser diode; C_i ($i = 1, 2, 3$): coupler; Att: attenuator, Φ: phase modulator; FM: Faraday mirror; D_{cl}: classical detector.

two pulses are reflected by the Faraday mirror and travel back to Bob. The total attenuation at Alice's site is $A' \simeq 50$ dB. Thus the two pulses now contain $A'N_0$ and $AA'N_0$ photons, respectively. In particular the signal pulse now contains only a few photons ($AA'N_0 = |\alpha|^2 = O(1)$). Alice also adds a phase $\phi_A = a_i\pi$ to the signal pulse, thereby encoding the value of her bit a_i.

The fact that Bob provides Alice with the signal state seems to provide him with some simple cheating strategies. For instance he could provide Alice with a signal state that is squeezed in phase in order to decrease the overlap between $|\psi_0\rangle$ and $|\psi_1\rangle$. This apparently allows him to discriminate much better $|\psi_0\rangle$ from $|\psi_1\rangle$ and hence the value of a_i. The role of the attenuation is to prevent this kind of cheating. Indeed under strong attenuation any quantum state tends towards a mixture of coherent states.

To show this we describe the state by its generalized Wigner function $W(q, p, s)$. We recall that $W(s = -1)$ is the Q function which is always positive, $W(s = 0)$ is the Wigner function, and $W(s = +1)$ is the P function. If the P function is positive, then the state is a mixture of coherent states. Under attenuation by A we have (see [15]): $W^{\text{out}}(q, p, s) = \frac{1}{A}W^{\text{in}}(\frac{q}{\sqrt{A}}, \frac{p}{\sqrt{A}}, \frac{s+A-1}{A})$ which implies that $W^{\text{out}}(s = (1-2)A)$ is positive. This expresses the fact that for $A \to 0$ one tends towards a positive P function. This result can be made more quantitative by supposing that after attenuation we add a small amount of Gaussian noise with mean number of chaotic photons n. This affects the W function as $W^{\text{out}}(q, p, s) = W^{\text{in}}(q, p, s - 2n)$. Thus attenuation followed by addition of chaotic photons yields the transformation $W^{\text{out}}(q, p, s) = \frac{1}{A}W^{\text{in}}(\frac{q}{\sqrt{A}}, \frac{p}{\sqrt{A}}, \frac{s-2n+A-1}{A})$ and, in particular, if $n = A$ we have $W^{\text{out}}(q, p, s = +1) = \frac{1}{A}W^{\text{in}}(\frac{q}{\sqrt{A}}, \frac{p}{\sqrt{A}}, s = -1)$, i.e., the output P function is positive since it is given in terms of the input Q function. Thus after strong attenuation, say $A = 10^{-3}$, a quantum state is very well approximated by a mixture of coherent states since a very small amount of Gaussian noise with mean number of chaotic photons $n = 10^{-3}$ transforms the state into a mixture of coherent states.

Another simple cheating strategy is for Bob to increase the intensity of the signal state since it is then much easier for him to estimate the phase ϕ_A. The role of the classical intensity measurement is to ensure that the signal state Alice sends back is not too intense. In fact it is impossible for Bob to exploit the fact that he provides Alice with the light pulse which will become the signal state, since by measuring the intensity of the pulse Bob sends her and then attenuating it, Alice ensures that she sends back to Bob a coherent state of known intensity.

Note that the classical intensity measurement of Alice will be affected by noise because AN_0 is close to the sensitivity limit of Alice's detector. We circumvent this technical problem by letting Alice carry out statistical tests on the n intensity measurements (one for each round of the protocol). More precisely she checks whether the distribution of measured intensities is consistent with the Gaussian distribution she expects from instrumental noise. If it is she has a precise estimate of $|\alpha|^2$, and hence of $\overline{\epsilon}_B$ through Eq. (3). If it is not she aborts.

From Alice to Bob and Alice's cheating.—Upon receiving the two pulses from Alice, Bob uses coupler C_2 to measure the intensity of the LO, attenuates it by A, and adds a phase $e^{i\phi_B}$, with $\phi_B = a_i\pi$. Note that by measuring the intensity of the LO state provided by Alice and then attenuating it, Bob ensures that the LO he uses is a coherent state (or a mixture of coherent states) of known intensity $|\beta|^2$. (The argument is exactly the same as that given above in the case of Alice.)

Let us consider the two states that interfere at coupler C_1. On the one hand there is the LO which as we have just argued is a coherent state of known intensity $|\beta|^2$. On the other hand there is the signal state. The signal state travels through the PBS where it gets attenuated by A_0. It then interferes with the LO at coupler C_1. This coupler has transmission and reflection coefficients T and R (both are approximately 50%). Finally one of the outputs of the coupler is sent to a single photon detector (id Quantique) with efficiency η. In our experiment $A_0T = 4.3$ dB and $\eta = 10.5\%$. We can therefore model the whole of Bob's detection system by the scheme depicted in Fig. 2. It is composed of the LO (a coherent state of amplitude β), the signal state Ψ, the attenuator A_0, a beam splitter with transmission, and reflection coefficients T and R. The imperfect detector is modeled by an attenuation of η followed by a perfect detector.

Let us denote by α the amplitude of the coherent state that would give rise to destructive interference at the single photon detector. It satisfies $\alpha\sqrt{A_0T} + i\beta\sqrt{R} = 0$. When $a_i = 0$, the state Alice should send if she is honest is the coherent state $|\alpha\rangle$. (If $a_i = 1$ she should send the state $|-\alpha\rangle$; by using the phase modulator Bob can cancel this phase.) But if Alice is dishonest she will send another state $|\Psi\rangle$. We expand $|\Psi\rangle$ in the basis of displaced Fock states $|\Psi\rangle = D_a(\alpha)\sum_n c_n|n\rangle$ where $D_a(\alpha)$ is the displacement operator acting on mode a, ie., $D_a(\alpha)aD_a(\alpha)^\dagger = a - \alpha$, and $|n\rangle = (a^\dagger)^n/\sqrt{n!}|0\rangle$ are the Fock states. The fidelity of the state sent by Alice is thus $f = |\langle\alpha|\Psi\rangle|^2 = |c_0|^2$.

We model the effect of the attenuation by the transformation $a \to \sqrt{A_0}a' + \sqrt{1-A_0}e_1$ where e_1 is a mode of the environment; the effect of the BS by the transforma-

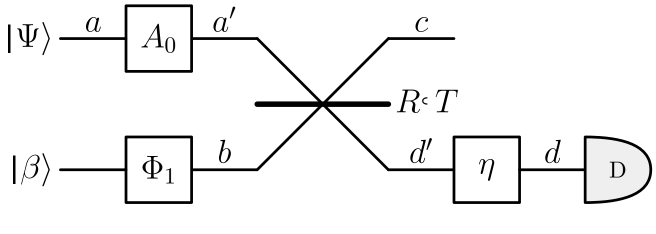

FIG. 2. Optical setup equivalent to Bob's measurement, including its imperfections.

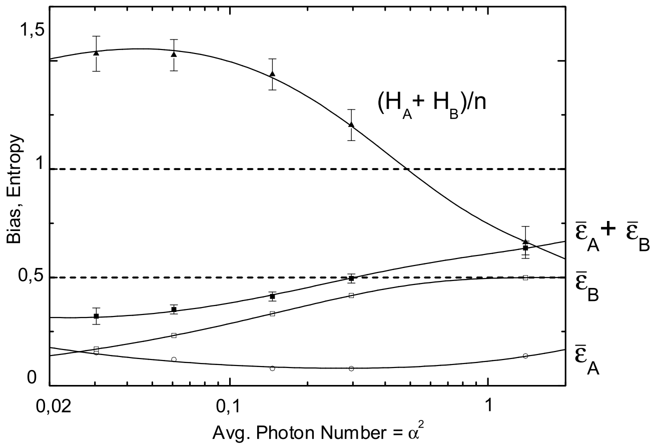

FIG. 3. Measured bounds on average bias and on entropy of bit strings for different values of the average photon number α^2. Open squares: bounds on $\bar{\epsilon}_B$ obtained using Eq. (3); open circles: bounds on $\bar{\epsilon}_A$ obtained using Eq. (5); filled squares: bounds on $\bar{\epsilon}_A + \bar{\epsilon}_B$. Classically the sum is always greater than 1/2. The bit strings are clearly more random than is allowed by the best classical protocol. The same expressions which give bounds on $\bar{\epsilon}_A$, $\bar{\epsilon}_B$ also give lower bounds on the entropies $H_{A(B)}$ of the bit string if Alice (Bob) is dishonest (see [10]). Filled triangles: bounds on the entropy per bit $(H_A + H_B)/n$. It is conjectured in [10] that for any classical protocol $(H_A + H_B)/n$ is bounded by 1 for large n. The experimental points are clearly above this bound. The error bars for $\bar{\epsilon}_A + \bar{\epsilon}_B$ and $(H_A + H_B)/n$ describe systematic errors arising from incorrect calibration of detector efficiency η and incorrect estimation of α^2. The plotted curves are theoretical predictions based on the observed optical visibility of 96.5%. For $\bar{\epsilon}_B$ the curve is given by Eq. (3) and for $\bar{\epsilon}_A$ it is given by Eq. (5) using the fact that, for small α^2, $(\kappa - \kappa_{\rm dark})/A_0T\eta \simeq (1 - V)\alpha^2/2$.

tions $a' \to \sqrt{T}d' - i\sqrt{R}c$, $b \to \sqrt{T}c - i\sqrt{R}d'$; and the effect of the detector inefficiency by $d' \to \sqrt{\eta}d + \sqrt{1-\eta}e_2$ where e_2 is another mode of the environment (the modes a, a', b, c, d', d are all described in the figure). One then finds that the state just before entering the single photon detector is $D_c(\gamma)\sum_n \frac{c_n}{\sqrt{n!}}[\sqrt{A_0T\eta}d^\dagger + i\sqrt{A_0R}c^\dagger + \sqrt{1-A_0}e_1^\dagger + \sqrt{(1-\eta)TA_0}e_2^\dagger]^n|0\rangle$ where $\gamma = \beta\sqrt{T} + i\alpha\sqrt{A_0R}$. From this one easily computes that the probability that the detector does not register a single click is

$$P(\text{no click}) = \sum_{n=0}^{\infty} |c_n|^2(1 - A_0T\eta)^n. \qquad (4)$$

The probability of registering a click is thus bounded by $P(\text{click}) \geq (1 - |c_0|^2)A_0T\eta$. Thus the number of clicks on Bob's detector divided by $A_0T\eta$ gives a bound on the fidelity $|c_0|^2$.

A final inefficiency that must be taken into account is that Bob's detector will have a nonzero dark count rate $\kappa_{\rm dark} = 9 \times 10^{-4}$. Putting all this together we deduce the bound on the average bias if Alice is dishonest:

$$\bar{\epsilon}_A \leq \mathcal{F}\left(\frac{\kappa - \kappa_{\rm dark}}{A_0T\eta}\right) \qquad (5)$$

Note that this bound on $\bar{\epsilon}_A$ is given entirely by parameters which can be measured by Bob.

Using this protocol, and taking into account experimental imperfections as described below, a typical run of our experiment generates 10^7 coins. Some results for different values of $|\alpha|^2$ are presented in Fig. 3. For instance when $|\alpha|^2 = 0.03$, we obtained $\bar{\epsilon}_A + \bar{\epsilon}_B = 0.32 \pm 0.04$, which is significantly better than the classical bound $\bar{\epsilon}_A + \bar{\epsilon}_B \geq 1/2$.

An important property of this protocol and of its experimental implementation is that we do not have to make any hypothesis about the Hilbert space Alice or Bob use if they are dishonest—for instance, it is not necessary to restrict them to the single photon subspace—nor do we have to make any hypothesis about the kind of technology they can use if they are dishonest. Thus the randomness of the bit string when one of the parties is dishonest is guaranteed by the laws of physics.

The authors thank Jaromír Fiurášek for helpful discussions. They acknowledge financial support from the Action de Recherche Concertée de la Communauté Française de Belgique, from the IUAP program of the Belgian Federal Governement under grant no. V-18 and from the European Union through project RESQ IST-2001-37559.

[1] M. Blum in *Advances in Cryptology: A Report on CRYPTO 81*, edited by A. Gersho (Department of Electrical and Computer Engineering, University of California, Santa Barbara, CA, 1981), p. 11.
[2] A. Kent, Phys. Rev. A **68**, 012312 (2003).
[3] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2002).
[4] R. W. Spekkens and T. Rudolph, Phys. Rev. Lett. **89**, 227901 (2002).
[5] A. Ambainis, *Proceedings of STOC'01*, p. 134, (quant-ph/0204022).
[6] A. Ambainis, quant-ph/0204063.
[7] C. Mochon, quant-ph/0403193.
[8] J. Barrett and S. Massar, Phys. Rev. A **69**, 022322 (2004).
[9] A. Kent, in *Quantum Communication, Measurement and Computing (QCMC'02)* (edited by J. Shapiro and O. Hirota) (Rinton Press, Paramus, 2003).
[10] J. Barrett and S. Massar, Phys. Rev. A **70**, 052310 (2004).
[11] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34**, 2116 (1998).
[12] H.-K. Lo and H. F. Chau, Physica D (Amsterdam) **120**, 177 (1998).
[13] A. Yu. Kitaev, *Lecture delivered at QIP 2003*, MSRI, Berkeley, CA, 2002 (unpublished); see http://www.msri.org/publications/video/index05.html.
[14] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, Phys. Rev. Lett. **94**, 040501 (2005).
[15] Ulf Leonhardt, *Measuring the Quantum State of Light*, (Cambridge University Press, Cambridge, 1997).