Theoretical Computer Science 560 (2014) 7–11

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Quantum cryptography: Public key distribution and coin tossing ☆

Charles H. Bennett [a], Gilles Brassard [b]

[a] IBM Research, Yorktown Heights NY 10598, USA
[b] Département IRO, Université de Montréal, Montréal, QC, H3C 3J7 Canada

When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by use of a still subtler quantum phenomenon, the Einstein–Podolsky–Rosen paradox.

I. Introduction

Conventional cryptosystems such as ENIGMA, DES, or even RSA, are based on a mixture of guesswork and mathematics. Information theory shows that traditional secret-key cryptosystems cannot be totally secure unless the key, used once only, is at least as long as the cleartext. On the other hand, the theory of computational complexity is not yet well enough understood to prove the computational security of public-key cryptosystems.

In this paper we use a radically different foundation for cryptography, viz. the uncertainty principle of quantum physics. In conventional information theory and cryptography, it is taken for granted that digital communications in principle can always be passively monitored or copied, even by someone ignorant of their meaning. However, when information is encoded in non-orthogonal quantum states, such as single photons with polarization directions 0, 45, 90, and 135 degrees, one obtains a communications channel whose transmissions in principle cannot be read or copied reliably by an eavesdropper ignorant of certain key information used in forming the transmission. The eavesdropper cannot even gain partial information about such a transmission without altering it in a random and uncontrollable way likely to be detected by the channel's legitimate users.

Quantum coding was first described in [W], along with two applications: making money that is in principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. More recently [BBBW], quantum coding has been used in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Here we show that quantum coding by itself achieves one of the main advantages of public key cryptography by permitting secure distribution of random key information between parties who share no secret information initially, provided the parties have access, besides the quantum channel, to an ordinary channel susceptible to passive but not active eavesdropping. Even in the presence of active eavesdropping, the two parties can still distribute key securely if they share some secret information initially, provided the eavesdropping is not so active as to suppress communications completely. We also present a protocol for coin tossing by exchange of quantum messages. Except where

☆ This paper appeared originally on pages 175–179 of the Proceedings of the *International Conference on Computers, Systems and Signal Processing*, which took place in Bangalore (now Bengalūru) in December 1984. It appears now for the first time in an archival journal, exactly as it was in its original 1984 version, except for fresh typesetting abiding to *Theoretical Computer Science* style, the correction of about one dozen typographical mistakes, as well as updated email addresses, affiliations and bibliographic publication data. A scan of the original manuscript is available as supplementary online material.

E-mail addresses: chdbennett@gmail.com (C.H. Bennett), brassard@iro.umontreal.ca (G. Brassard).

http://dx.doi.org/10.1016/j.tcs.2014.05.025

otherwise noted the protocols are provably secure even against an opponent with superior technology and unlimited computing power, barring fundamental violations of accepted physical laws.

Offsetting these advantages is the practical disadvantage that quantum transmissions are necessarily very weak and cannot be amplified in transit. Moreover, quantum cryptography does not provide digital signatures, or applications such as certified mail or the ability to settle disputes before a judge.

II. Essential properties of polarized photons

Polarized light can be produced by sending an ordinary light beam through a polarizing apparatus such as a Polaroid filter or calcite crystal; the beam's polarization axis is determined by the orientation of the polarizing apparatus in which the beam originates. Generating single polarized photons is also possible, in principle by picking them out of a polarized beam, and in practice by a variation of an experiment [AGR] of Aspect et al.

Although polarization is a continuous variable, the uncertainty principle forbids measurements on any single photon from revealing more than one bit about its polarization. For example, if a light beam with polarization axis α is sent into a filter oriented at angle β, the individual photons behave dichotomously and probabilistically, being transmitted with probability $\cos^2(\alpha-\beta)$ and absorbed with the complementary probability $\sin^2(\alpha-\beta)$. The photons behave deterministically only when the two axes are parallel (certain transmission) or perpendicular (certain absorption).

If the two axes are not perpendicular, so that some photons are transmitted, one might hope to learn additional information about α by measuring the transmitted photons again with a polarizer oriented at some third angle; but this is to no avail, because the transmitted photons, in passing through the β polarizer, emerge with exactly β polarization, having lost all memory of their previous polarization α.

Another way one might hope to learn more than one bit from a single photon would be not to measure it directly, but rather somehow amplify it into a clone of identically polarized photons, then perform measurements on these; but this hope is also vain, because such cloning can be shown to be inconsistent with the foundations of quantum mechanics [WZ].

Formally, quantum mechanics represents the internal state of a quantum system (e.g. the polarization of a photon) as a vector ψ of unit length in a linear space H over the field of complex numbers (Hilbert space). The inner product of two vectors $\langle\phi \mid \psi\rangle$ is defined as $\sum_j \phi_j^* \psi_j$, where * indicates complex conjugation. The dimensionality of the Hilbert space depends on the system, being larger (or even infinite) for more complicated systems. Each physical measurement M that might be performed on the system corresponds to a resolution of its Hilbert space into orthogonal subspaces, one for each possible outcome of the measurement. The number of possible outcomes is thus limited to the dimensionality d of the Hilbert space, the most complete measurements being those that resolve the Hilbert space into d 1-dimensional subspaces.

Let M_k represent the projection operator onto the kth subspace of measurement M, so that the identity operator on H can be represented as a sum of projections: $I = M_1 + M_2 + \ldots$. When a system in state ψ is subjected to measurement M, its behavior is in general probabilistic: outcome k occurs with a probability equal to $|M_k\psi|^2$, the square of the length of the state vector's projection into subspace M_k. After the measurement, the system is left in a new state $M_k\psi/|M_k\psi|$, which is the normalized unit vector in the direction of the old state vector's projection into subspace M_k. The measurement thus has a deterministic outcome, and leaves the state vector unmodified, only in the exceptional case that the initial state vector happens to lie entirely in one of the orthogonal subspaces characterizing the measurement.

The Hilbert space for a single polarized photon is 2-dimensional; thus the state of a photon may be completely described as a linear combination of, for example, the two unit vectors $r_1 = (1, 0)$ and $r_2 = (0, 1)$, representing respectively horizontal and vertical polarization. In particular, a photon polarized at angle α to the horizontal is described by the state vector $(\cos\alpha, \sin\alpha)$. When subjected to a measurement of vertical-vs.-horizontal polarization, such a photon in effect chooses to become horizontal with probability $\cos^2\alpha$ and vertical with probability $\sin^2\alpha$. The two orthogonal vectors r_1 and r_2 thus exemplify the resolution of a 2-dimensional Hilbert space into 2 orthogonal 1-dimensional subspaces; henceforth r_1 and r_2 will be said to comprise the 'rectilinear' basis for the Hilbert space.

An alternative basis for the same Hilbert space is provided by the two 'diagonal' basis vectors $d_1 = (0.707, 0.707)$, representing a 45-degree photon, and $d_2 = (0.707, -0.707)$, representing a 135-degree photon. Two bases (e.g. rectilinear and diagonal) are said to be 'conjugate' [W] if each vector of one basis has equal-length projections onto all vectors of the other basis: this means that a system prepared in a specific state of one basis will behave entirely randomly, and lose all its stored information, when subjected to a measurement corresponding to the other basis. Owing to the complex nature of its coefficients, the two-dimensional Hilbert space also admits a third basis conjugate to both the rectilinear and diagonal bases, comprising the two so-called 'circular' polarizations $c_1 = (0.707, 0.707i)$ and $c_2 = (0.707i, 0.707)$; but the rectilinear and diagonal bases are all that will be needed for the cryptographic applications in this paper.

The Hilbert space for a compound system is constructed by taking the tensor product of the Hilbert spaces of its components; thus the state of a pair of photons is characterized by a unit vector in the 4-dimensional Hilbert space spanned by the orthogonal basis vectors r_1r_1, r_1r_2, r_2r_1, and r_2r_2. This formalism entails that the state of a compound system is not generally expressible as the cartesian product of the states of its parts: e.g. the Einstein–Podolsky–Rosen state of two photons, $0.7071(r_1r_2 - r_2r_1)$, to be discussed later, is not equivalent to any product of one-photon states.