Secure key distribution via pre- and postselected quantum states

Jeffrey Bub*

Philosophy Department, University of Maryland, College Park, Maryland 20742

(Received 9 September 2000; published 14 February 2001)

A quantum key distribution scheme whose security depends on the features of pre- and postselected quantum states is described.

DOI: 10.1103/PhysRevA.63.032309 PACS number(s): 03.67.Dd, 03.65.Ta

I. INTRODUCTION

A wide variety of quantum key distribution schemes have been proposed, following the original Bennett and Brassard protocol [1]. Ekert [2] has described a scheme in which two parties, Alice and Bob, create a shared random key by performing spin measurements on pairs of spin-$\frac{1}{2}$ particles in the singlet state. The particle pairs are emitted by a source towards Alice and Bob, who each measure spin along three different directions, chosen randomly and independently for each pair. After a sequence of measurements on an appropriate number of pairs, Alice and Bob announce the directions of their measurements publicly and divide the measurements into two groups: those in which they measured the spin in different directions, and those in which they measured the spin in the same direction. They publicly reveal the outcomes of the first group of measurements and use these to check that the singlet states have not been disturbed by an eavesdropper, Eve. Essentially, they calculate a correlation coefficient: any attempt by Eve to monitor the particles will disturb the singlet state and result in a correlation coefficient that is bounded by Bell's inequality and is hence distinguishable from the correlation coefficient for the singlet state. If Alice and Bob are satisfied that no eavesdropping has occurred, they use the second group of (oppositely correlated) measurement outcomes as the raw key.

The Ekert scheme solves the key distribution problem as well as the key storage problem, because there is no information in the singlets before Alice and Bob perform their measurements and communicate classically to establish the key. The scheme proposed here also involves entangled states, but the test for eavesdropping is different. Instead of a statistical test based on Bell's theorem, the test exploits conditional statements about measurement outcomes generated by pre- and postselected quantum states.

II. PRE- AND POSTSELECTED QUANTUM STATES

The peculiar features of pre- and postselected quantum states were first pointed out by Aharonov, Bergmann, and Lebowitz [3]. If (1) Alice prepares a system in a certain state $|\text{pre}\rangle$ at time t_1, (2) Bob measures some observable Q on the system at time t_2, and (3) Alice measures an observable of which $|\text{post}\rangle$ is an eigenstate at time t_3, and postselects for $|\text{post}\rangle$, then Alice can assign probabilities to the outcomes of Bob's Q measurement at t_2, conditional on the states $|\text{pre}\rangle$ and $|\text{post}\rangle$ at times t_1 and t_3, respectively, as follows [3,4]:

$$\text{prob}(q_k)=\frac{|\langle\text{pre}|P_k|\text{post}\rangle|^2}{\Sigma_i|\langle\text{pre}|P_i|\text{post}\rangle|^2}, \tag{1}$$

where P_i is the projection operator onto the ith eigenspace of Q. Notice that (1)—referred to as the ''ABL rule'' (Aharonov–Bergmann–Lebowitz rule) in the following—is time-symmetric, in the sense that the states $|\text{pre}\rangle$ and $|\text{post}\rangle$ can be interchanged.

If Q is unknown to Alice, she can use the ABL rule to assign probabilities to the outcomes of various hypothetical Q measurements. The interesting peculiarity of the ABL rule, by contrast with the usual Born rule for preselected states, is that it is possible—for an appropriate choice of observables $Q,Q',\ldots,$ and states $|\text{pre}\rangle$ and $|\text{post}\rangle$—to assign unit probability to the outcomes of a set of mutually *noncommuting* observables. That is, Alice can be in a position to assert a conjunction of conditional statements of the form: ''If Bob measured Q, then the outcome must have been q_i, with certainty, and if Bob measured Q', then the outcome must have been q'_j, with certainty...,'' where $Q,Q',\ldots$ are mutually noncommuting observables. Since Bob could only have measured at most one of these noncommuting observables, Alice's conditional information does not, of course, contradict quantum mechanics: she only knows the eigenvalue q_i of an observable Q if she knows that Bob in fact measured Q.

Vaidman, Aharonov, and Albert [4] discuss a case of this sort, where the outcome of a measurement of any of the three spin components $\sigma_x,\sigma_y,\sigma_z$ of a spin-$\frac{1}{2}$ particle can be inferred from an appropriate pre-and postselection. Alice prepares the Bell state:

$$|\text{pre}\rangle=\frac{1}{\sqrt{2}}(|\uparrow_z\rangle_A|\uparrow_z\rangle_C+|\downarrow_z\rangle_A|\downarrow_z\rangle_C, \tag{2}$$

where $|\uparrow_z\rangle$ and $|\downarrow_z\rangle$ denote the σ_z eigenstates. Alice sends one of the particles—the channel particle, denoted by the subscript C—to Bob and keeps the ancilla, denoted by A. Bob measures either σ_x, or σ_y, or σ_z on the channel particle and returns the channel particle to Alice. Alice then measures an observable R on the pair of particles, where R has the eigenstates:

*Electronic address: jbub@carnap.umd.edu

TABLE I. σ_x, σ_y, σ_z measurement outcomes correlated with eigenvalues of R.

	σ_x	σ_y	σ_z
r_1	0	0	0
r_2	1	1	0
r_3	0	1	1
r_4	1	0	1

$$|r_1\rangle = \frac{1}{\sqrt{2}}|\uparrow_z\rangle|\uparrow_z\rangle + \frac{1}{2}(|\uparrow_z\rangle|\downarrow_z\rangle e^{i\pi/4} + |\downarrow_z\rangle|\uparrow_z\rangle e^{-i\pi/4}), \tag{3}$$

$$|r_2\rangle = \frac{1}{\sqrt{2}}|\uparrow_z\rangle|\uparrow_z\rangle - \frac{1}{2}(|\uparrow_z\rangle|\downarrow_z\rangle e^{i\pi/4} + |\downarrow_z\rangle|\uparrow_z\rangle e^{-i\pi/4}), \tag{4}$$

$$|r_3\rangle = \frac{1}{\sqrt{2}}|\downarrow_z\rangle|\downarrow_z\rangle + \frac{1}{2}(|\uparrow_z\rangle|\downarrow_z\rangle e^{i\pi/4} + |\downarrow_z\rangle|\uparrow_z\rangle e^{i\pi/4}), \tag{5}$$

$$|r_4\rangle = \frac{1}{\sqrt{2}}|\downarrow_z\rangle|\downarrow_z\rangle - \frac{1}{2}(|\uparrow_z\rangle|\downarrow_z\rangle e^{-i\pi/4} + |\downarrow_z\rangle|\uparrow_z\rangle e^{i\pi/4}). \tag{6}$$

Note that

$$|\mathrm{pre}\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle|\uparrow_z\rangle + |\downarrow_z\rangle|\downarrow_z\rangle \tag{7}$$

$$= \frac{1}{\sqrt{2}}(|\uparrow_x\rangle|\uparrow_x\rangle + |\downarrow_x\rangle|\downarrow_x\rangle \tag{8}$$

$$= \frac{1}{\sqrt{2}}(|\uparrow_y\rangle|\downarrow_y\rangle + |\downarrow_y\rangle|\uparrow_y\rangle \tag{9}$$

$$= \frac{1}{2}(|r_1\rangle + |r_2\rangle + |r_3\rangle + |r_4\rangle). \tag{10}$$

In Eqs. (8)–(10) and in the following, the subscripts A and C appearing in Eq. (2) are implicit in the tensor product notation. Equations (8)–(10) correspond to Eq. (2) of Ref. [4] or Eq. (54) of Ref. [5].

Alice can now assign values to the outcomes of Bob's spin measurements via the ABL rule, whether Bob measured σ_x, σ_y, or σ_z, based on the postselections $|r_1\rangle$, $|r_2\rangle$, $|r_3\rangle$, or $|r_4\rangle$, according to Table I (where 0 represents the outcome ↑ and 1 represents the outcome ↓) [4].

III. THE KEY DISTRIBUTION PROTOCOL

This case can be exploited to enable Alice and Bob to share a private random key in the following way: Alice prepares a certain number of copies (depending on the length of the key and the level of privacy desired) of the Bell state, Eq. (2). She sends the channel particles to Bob in sequence and keeps the ancillas. Bob measures σ_x or σ_z randomly on the channel particles and returns the particles, in sequence, to Alice. Alice then measures the observable R on the ancilla and channel pairs and divides the sequence into two subsequences: the subsequence S_{14} for which she obtained the outcomes r_1 or r_4, and the subsequence S_{23} for which she obtained the outcomes r_2 or r_3. The sequence of quantum operations can be implemented on a quantum circuit as in Fig. 1 [see Eq. (46) of Metzer [5]]. In the present paper, an ideal system without noise is assumed.

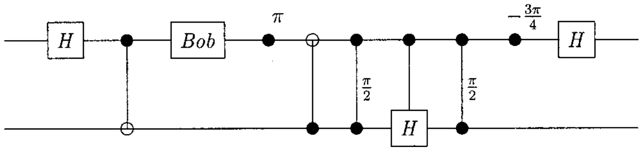

FIG. 1. Quantum circuit for key distribution protocol.

To check that the channel particles have not been monitored by Eve, Alice now publicly announces the indices of the subsequence S_{23}. As is evident from Table II, for this subsequence she can make conditional statements of the form: "For channel particle *i*, if σ_x was measured, the outcome was 1 (0), and if σ_z was measured, the outcome was 0 (1)," depending on whether the outcome of her R measurement was r_2 or r_3. She announces these statements publicly. If one of these statements, for some index *i*, does not agree with Bob's records, Eve must have monitored the ith channel particle. (Of course, agreement does not entail that the particle was *not* monitored.)

For suppose Eve measures a different spin component observable than Bob on a channel particle and Alice subsequently obtains one of the eigenvalues r_2 or r_3 when she measures R. Bob's measurement outcome, either 0 or 1, will be compatible with just one of these eigenvalues, assuming no intervention by Eve. But after Eve's measurement, both of these eigenvalues will be possible outcomes of Alice's measurement. So Alice's retrodictions of Bob's measurement outcomes for the subsequence S_{23} will not necessarily correspond to Bob's records. In fact, it is easy to see that if Eve measures σ_x or σ_z randomly on the channel particles, or if she measures a particular one of the observables σ_x, σ_y, or σ_z on the channel particles (the same observable on each particle), the probability of detection in the subsequence S_{23} is $\frac{3}{8}$.

In the subsequence S_{14}, the 0 and 1 outcomes of Bob's measurements correspond to the outcomes r_1 and r_4 of Alice's R measurements. If, following their public communica-

TABLE II. σ_x, σ_z measurement outcomes correlated with eigenvalues of R.

	σ_x	σ_z
r_1	0	0
r_2	1	0
r_3	0	1
r_4	1	1

tion about the subsequence S_{23}, Alice and Bob agree that there has been no monitoring of the channel particles by Eve, they use the subsequence S_{14} to define a shared raw key.

Note that even a single disagreement between Alice's retrodictions and Bob's records is sufficient to reveal that the channel particles have been monitored by Eve. This differs from the eavesdropping test in the Ekert protocol. Note also that Eve only has access to the channel particles, not the particle pairs. So no strategy is possible in which Eve replaces all the channel particles with her own particles and entangles the original channel particles, treated as a single system, with an ancilla by some unitary transformation, and then delays any measurements until after Alice and Bob have communicated publicly. There is no way that Eve can ensure agreement between Alice and Bob without having access to the particle pairs, or without information about Bob's measurements.

The key distribution protocol as outlined above solves the key distribution problem but not the key storage problem. If Bob actually makes the random choices, measures σ_x or σ_z, and records definite outcomes for the spin measurements before Alice measures R, as required by the protocol, Bob's measurement records—stored as classical information—could in principle be copied by Eve without detection. In that case, Eve would know the raw key (which is contained in this information), following the public communication between Alice and Bob to verify the integrity of the quantum communication channel.

To solve the key storage problem, the protocol is modified in the following way: Instead of actually making the random choice for each channel particle, measuring one of the spin observables, and recording the outcome of the measurement, Bob keeps the random choices and the spin measurements ''at the quantum level'' until after Alice announces the indices of the subsequence S_{23} of her R measurements. To do this, Bob enlarges the Hilbert space by entangling the quantum state of the channel particle via a unitary transformation with the states of two ancilla particles that he introduces. One particle is associated with a Hilbert space spanned by two eigenstates, $|c_{\sigma(x)}\rangle$ and $|c_{\sigma(z)}\rangle$, of a choice observable C. The other particle is associated with a Hilbert space spanned by two eigenstates, $|p_{\uparrow}\rangle$ and $|p_{\downarrow}\rangle$, of a pointer observable P. (See Ref. [6], footnote *t*, or Ref. [7] for details of how to implement the unitary transformation on the enlarged Hilbert space.)

On the modified protocol (assuming the ability to store entangled states indefinitely), Alice and Bob share a large number of copies of an entangled four-particle state. When they wish to establish a random key of a certain length, Alice measures R on an appropriate number of particle pairs in her possession and announces the indices of the subsequence S_{23}. Before Alice announces the indices of the subsequence S_{23}, neither Alice nor Bob have stored any classical information. So there is nothing for Eve to copy. After Alice announces the indices of the subsequence S_{23}, Bob measures the observables D and P on his ancillas with these indices and announces the eigenvalue $|p_{\uparrow}\rangle$ or $|p_{\downarrow}\rangle$ as the outcome of his $\sigma(x)$ or $\sigma(z)$ measurement, depending on the eigenvalue of D. If Alice and Bob decide that there has been no eavesdropping by Eve, Bob measures D and P on his ancillas in the subsequence S_{14}. It is easy to see that the ABL rule applies in this case, just as it applies in the case where Bob actually makes the random choice and actually records definite outcomes of his $\sigma(x)$ or $\sigma(z)$ measurements before Alice measures R. (In fact, if the two cases were not equivalent for Alice—if Alice could tell from her R measurements whether Bob had actually made the random choice and actually performed the spin measurements, or had merely implemented these actions ''at the quantum level''—the difference could be exploited to signal superluminally.)

There are clearly other possible ways of exploiting this case to implement a secure key distribution protocol (involving all three spin component observables, for example), but the principle is similar. It would seem worthwhile to consider whether other applications of pre- and postselection might be applied as a tool in quantum cryptology.

ACKNOWLEDGMENTS

This work was partially supported by the University of Maryland General Research Board. Illuminating discussions with Gilles Brassard, Lev Vaidman, and especially Adrian Kent are acknowledged.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] Y. Aharanov, P. G. Bergmann, and J. L. Lebowitz, in *Quantum Theory and Measurement*, edited by J. A. Wheeler and W. H. Zurek (Princeton University Press, Princeton, 1983), pp. 680–686.

[4] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).

[5] S. Metzger, e-print quant-ph/0006115.

[6] H.-K. Lo, in *Introduction to Quantum Computation and Information*, edited by H.-K. Lo, S. Popescu, and T. Spiller (World Scientific, Singapore, 1998), pp. 76–119.

[7] J. Bub, Found. Phys. (to be published), e-print quant-ph/007090.