Quantum Key Distribution Based on Arbitrarily Weak Distillable Entangled States

Karol Horodecki,[1] Debbie Leung,[2] Hoi-Kwong Lo,[3] and Jonathan Oppenheim[4]

[1]*Department of Mathematics Physics and Computer Science, University of Gdańsk, 80-952 Gdańsk, Poland*
[2]*Institute of Quantum Information, MSC 107-81, Caltech, Pasadena, California 91125, USA*
[3]*Department of Electrical and Computer Engineering, and Department of Physics, University of Toronto, Toronto, Ontario M5S 3G4, Canada*
[4]*Department of Applied Mathematics and Theoretical Physics, University of Cambridge, United Kingdom*

(Received 11 October 2005; published 21 February 2006)

States with private correlations but little or no distillable entanglement were recently reported. Here, we consider the secure distribution of such states, i.e., the situation when an adversary gives two parties such states and they have to verify privacy. We present a protocol which enables the parties to extract from such untrusted states an arbitrarily long and secure key, even though the amount of distillable entanglement of the untrusted states can be arbitrarily small.

DOI: 10.1103/PhysRevLett.96.070501 PACS numbers: 03.67.Dd, 03.67.Mn

Suppose Alice and Bob shared a maximally entangled state, say, an ebit $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Clearly, they can generate a private key directly by measuring their state in the Z basis, without any classical post processing. Are there other types of states with similar key-generating ability? Surprisingly, the answer is yes. Reference [1] gives a necessary and sufficient condition for a state to generate a key by a direct measurement in the computational basis—it must be some *twisted* version of a maximally entangled state called the *pbit* (private bit).

Now suppose Alice and Bob are unsure what state they are sharing. A striking feature of entanglement is that it can be verified and distilled [2]. Thus, Alice and Bob can first generate near-perfect ebits and then a private key. The best-known means to achieve quantum key distribution (QKD) via noisy, untrusted channels or states is distillation of ebits. It is then natural to try to go beyond this, by asking whether noisy and untrusted pbits can similarly be distilled or verified.

The distillation of pbits was consider in Refs. [1,3] when Alice and Bob know they share identical copies of some quantum states. However, can we achieve QKD with noisy or untrusted *pbits*? In this Letter, we provide a positive answer by the explicit construction of QKD protocols based on noisy pbits and by proving their unconditional security (against the most general attack allowed by quantum mechanics). The protocol essentially involves checking bit and phase errors, with phase errors being checked using a sublinear number of ebits. In the case when an adversary claims to give the parties copies of an ideal private key, which is always distillable, this sublinear number of ebits can be obtained by applying an initial distillation protocol on some of the key states. However, there are also states which approximate pbits, yet contain no distillable entanglement [1]. For these bound entangeld states [4], our protocol requires a sublinear amount of ebits as a resource.

We will begin with a review of known properties of pbits. We then introduce the protocol, and prove its security. The security proof we present relies on the composability of distillation protocols, and we provide a proof in the Ben-Or–Mayers model [5].

Private states, twisting, and their properties. Suppose Alice and Bob share a quantum state ρ_{AB} and the eavesdropper Eve has the purification (with her reduced density matrix denoted by ρ_E). We say that ρ_{AB} contains ideal security if and only if there is a local measurement taking it to some ideal ccq state

$$\rho_{\mathrm{ccq}}^{\mathrm{ideal}} = \sum_{i}^{d} \frac{1}{d} |ii\rangle\langle ii| \otimes \rho_E, \tag{1}$$

signifying that Alice and Bob each has a copy of the key i that is uncorrelated with Eve's quantum state (hence the term "ccq"). The class of states containing ideal security in this sense has been fully characterized in the following way:

Theorem 1.—[1,3] Any state $\rho_{ABA'B'}$ of a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'}$ with dimensions $d_A = d$, $d_B = d$, and arbitrary $d_{A'}$, $d_{B'}$, gives an ideal ccq state after measurement in the computational basis on the AB subsystem if and only if

$$\rho_{ABA'B'} = \frac{1}{d} \sum_{i,j=0}^{d-1} |ii\rangle\langle jj|_{AB} \otimes U_i \rho_{A'B'} U_j^{\dagger} \tag{2}$$

where $\rho_{A'B'}$ is an arbitrary state of the subsystem $A'B'$ and the U_i 's are arbitrary unitary transformations.

We will refer to a state of the form (2) as a "private state" or a "gamma state" or a "pdit" (and pbit when $d = 2$). Following the convention of [3], we will call subsystem AB the "key part" of the pdit and $A'B'$ its "shield" (Fig. 1).

Because of Theorem 1, the distillable key K_D of a quantum state σ can naturally be defined as the maximum ratio of the logarithm of the dimension d of the output pdit

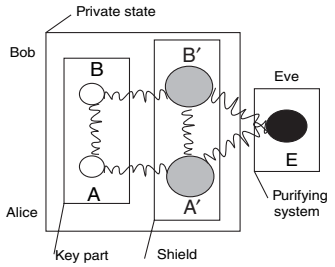

FIG. 1. A private state $\rho_{ABA'B'}$ with purifying system E. The key part (AB) after a complete von Neumann measurement gives an ideal key, which is secure due to the fact that Alice and Bob hold the shield part ($A'B'$).

to the number of copies of σ used, and the ratio is maximized over asymptotic $LOCC$ protocols [1,3].

Recall that any private state is a "twisted" maximally entangled state [1,3], with the twisting operation defined as

$$U^{(2)} = \sum_{ij} |ij\rangle\langle ij|_{AB} \otimes U^{\dagger}_{ijA'B'} \tag{3}$$

where $U_{ii} = U_i$ as defined in (2). Since twisting is reversible, we can see this in reverse: any pdit can be turned into a maximally entangled state on AB and some (global) ancillary state $\rho_{A'B'}$ on $A'B'$ by a certain twisting operation. More formally:

Observation 1.—Consider any private state $\rho_{ABA'B'}$ of the form (2) and the twisting defined as in (3). $U^{(2)}$ is called a "global untwisting"—it takes $\rho_{ABA'B'}$ in (2) into a state $P_+ \otimes \rho_{A'B'}$ called the basic pdit, where $P_+ = \sum_{ij=0}^{d-1} \frac{1}{d} |ii\rangle\langle jj|$ is a maximally entangled state on AB and $\rho_{A'B'}$ is the same as in (2). The same state change can also result from applying a "local untwisting" defined as

$$U^{(1)} = \sum_{i=0}^{d-1} |i\rangle\langle i|_B \otimes U^{\dagger}_{iiA'B'}. \tag{4}$$

Note that if Bob had access to A' he could transform a private state into a basic pdit using local untwisting (thus the name "local"). The global and local untwistings are, respectively, subscripted by (2) and (1) (labeling the number of control systems). Together with the obvious fact that exact teleportation of a system can be viewed as an identity map on it, we have the following observation:

Observation 2.—For any state $\rho_{ABA'B'}$, the composition of (i) teleportation of A' to Bob's side and (ii) local untwisting on $BB'A'$ commutes with measurement in the computational basis on AB.

A final property of pbits to review is as follows:

Proposition 1.—[6] For any private state ρ, $E_D(\rho) > 0$.

Remark.—This only holds for exact pbits, since one can approximate pbits with bound entangled states.

This concludes our summary for the known results on private states in the promise scenario in which Alice and Bob know that they share multiple copies of a certain state. We now switch to the general scenario. We will first describe our main protocol for QKD using noisy pbits, and then establish its unconditional security against the most general attack by Eve.

The main protocol, M. There are six major steps in the main protocol:

State distribution.—Alice and Bob request n copies of a certain private state $\gamma_{ABA'B'} \in B(C^d \otimes C^d \otimes C^{d_{A'}} \otimes C^{d_{B'}})$ given by (2). We consider the most general attack where the γ states are distributed by Eve. Therefore Alice and Bob may have an arbitrary joint state over all n systems. Without loss of generality, we take $d_{A'} \leq d_{B'}$ and assume compression has already been performed on subsystem A' to reduce its dimension.

Partial distillation.—Alice and Bob randomly choose k out of n systems and run a distillation protocol that would return $(m \times \log d_{A'}) + t$ [7] ebits if the input were indeed $\gamma^{\otimes k}$. Alice and Bob estimate the quality of $m \times \log d_{A'}$ of those untrusted ebits using the other t, say, using the Lo-Chau protocol [8]. Here, t is based on a quality parameter $0 < \epsilon < 1$, such that they abort the protocol with high probability if the fidelity between the untrusted and ideal ebits is less than $1 - \epsilon$.

Random sampling, untwisting, phase-error estimation.—Upon passing the test, Alice and Bob will have $n - k$ systems and $m \times \log d_{A'}$ distilled ebits. They pick a random subset of m out of $n - k$ systems, and Alice teleports the m A' subsystems to Bob using the $m \times \log d_{A'}$ distilled ebits. To each teleported A' (together with his local corresponding system BB') Bob applies the local untwisting $U^{(1)}$ for γ, as in (4), to obtain m "untwisted" systems. On the m untwisted systems Alice and Bob measure σ_x on A and B and share the results to effect a measurement of $[\sigma_x \otimes \sigma_x]_{AB} \otimes I_{A'B'}$ and estimate the phase-flip error rate e_x.

Random sampling and bit-error estimation.—They pick another random subset of m out of $n - k - m$ systems and measure σ_z, share their results, and effectively measure $[\sigma_z \otimes \sigma_z]_{AB} \otimes I_{A'B'}$. This time, they obtain the bit-flip error rate e_z.

Raw-key generation.—If both e_x and e_z are reasonably small, Alice and Bob generate a raw key from the $n - k - 2m$ remaining systems by measuring $[\sigma_z \otimes \sigma_z]_{AB} \otimes I_{A'B'}$ on each of them. Otherwise, they abort the protocol.

Error correction and privacy amplification.—On the raw key, Alice and Bob perform the two-way Gottesman-Lo classical error correction and privacy amplification [9]—repeated concatenation of binary exclusive-OR operation (BXOR) and three-qubit phase code followed by one-way error correction or privacy amplification (EC or PA) procedure. □

We comment on some aspects of this protocol. First, Alice and Bob can perform any distillation protocol, even those assuming tensor power input state $\gamma^{\otimes k}$ (e.g., the "hashing" protocol of [10]). This is because having performed such protocol Alice and Bob subsequently check the quality of the distilled states. Second, we do not have to assume that the specific $\gamma_{ABA'B'}$ is distillable—instead, it is

guaranteed by proposition (1). Third, in the phase-error estimation, the local untwisting operation can be replaced by any global untwisting. While these two options are equivalent for perfect private states, they are generally different outside of the promise scenario. The global untwisting requires the extra teleportation of the A subsystem and thus the distillation of $m \times \log d$ additional ebits, but can give a higher rate than using local untwisting (e.g., as in case of the mixture of two orthogonal private states [11]).

Proof of unconditional security of main protocol. Before stating the proof, we discuss the ideas behind it. The unconditional security of M is by reduction to that of the Lo-Chau protocol [8] based on entanglement purification. This reduction is possible because private states are twisted maximally entangled states. Thus, the first step is to realize that, if Alice and Bob could (locally) untwist all n systems, Alice and Bob share some noisy maximally entangled states on the AB subsystems, and standard techniques [8,9,12] apply so that the scheme is secure. The second step is to realize that Alice and Bob do not need to untwist most of the systems, except for those used in phase-error estimation, and those are indeed untwisted in the main protocol M. This is because the untwisting is followed by the entanglement purification schemes and then measurements [8,9,12], a sequence of operations that can be replaced by measurements followed by classical postprocessing. But by observation 2, the measurements can be done before untwisting, which is then unnecessary. These replacements are security preserving, so that we obtain the desired security of the main protocol.

For clarity we will first assume Alice and Bob perform errorless teleportation and local untwisting, and then consider the case when these operations are only performed with certain fidelity.

(i) The case of ideal quantum operations.

Security of fully untwisted protocol M_1 from [9].—Let us first consider another protocol M_1 that differs from the main protocol only by an additional step of untwisting (teleporting A' and local untwisting) the $n-k-m$ systems before the measurements in bit-error estimation and raw-key generation. We now show that M_1 is unconditionally secure. Since Alice and Bob have performed all untwisting operations in M_1, they can trace out the $A'B'$ subsystems, which is equivalent to giving these subsystems to Eve and can only decrease security. Thus, without loss of generality, the input to M_1 can be taken to be 2-qubit noisy maximally entangled states, and results based on entanglement purification procedures are directly applicable. In particular, using Ref. [8], if the bit and phase-error rates are well estimated, the appropriate entanglement purification procedure will give a secure key. The *efficient* error estimation of Ref. [13] provides a good estimate of error rates that would have occurred if the rest of states were measured along the Bell basis. Thus, after estimating the error rates, Alice and Bob could apply an appropriate two-way distillation procedure and obtain a secure key by measuring in bit basis. Now, Ref. [9] also states that this can be done by first measuring in bit basis, and then performing EC or PA, which gives our M_1 protocol. Since the Gottesman-Lo procedure assures a secure key, we conclude that M_1 is unconditionally secure.

Security of main protocol M from that of M_1.—Recall that M and M_1 only differ in the additional untwisting on the systems used in the bit-error estimation and the raw-key generation steps. We now show that the extra untwisting is unnecessary for the security of M_1. Observation 2 tells us that untwisting commutes with measurement in the computation basis. Hence it cannot change measurement outcomes obtained in the bit-error estimation step and the raw-key generation steps, and thus the values of the estimated bit-error rate and the raw key. It follows that untwisting of these $n-k-m$ systems does not effect the value of the final key and it is unnecessary. Thus M differs from M_1 only by omitting the necessary untwisting, and its security follows from that of M_1. This ends the proof of unconditional security of the main protocol in case of ideal operations of teleportation and untwisting.

(ii) The case of imperfect quantum operations.—We now consider the case when Alice and Bob share the maximally entangled state and can perform teleportation and local untwisting only up to some confidence level. In other word, we assume that

$$\|\sigma - P_+\|_{\mathrm{tr}} < \epsilon, \tag{5}$$

$$\forall_\rho \ \|\Lambda_{\mathrm{te}}^{\mathrm{noisy}}(\rho) - \Lambda_{\mathrm{te}}^{\mathrm{ideal}}(\rho)\| \le \epsilon_1, \tag{6}$$

$$\forall_\rho \ \|\Lambda_{\mathrm{untw}}^{\mathrm{noisy}}(\rho) - \Lambda_{\mathrm{untw}}^{\mathrm{ideal}}(\rho)\| \le \epsilon_2, \tag{7}$$

where, as before, P_+ is the projector onto a maximally entangled state, σ is the state produced by imperfect distillation, $\Lambda_{\mathrm{te}}^{\mathrm{ideal}}$ denotes perfect teleportation of A' and $\Lambda_{\mathrm{te}}^{\mathrm{noisy}}$ the actual transformation accomplished by Alice and Bob. ϵ, ϵ_1, ϵ_2, are exponential decaying functions in n. Similar notation holds for the local untwisting operation in (7). We have assumed negligible errors in other operations.

Note that the estimate of the bit-error rate is unaffected by the above errors (5)–(7). Now, we show that if the erroneous operations have bounded errors as described above, the probability is small that they observe a phase-error rate e_x' different from what they would have obtained (e_x) using ideal operations. This can be proved directly or by using a general composability result [5].

In essence, the composability result [5] guarantees the following in the Ben-Or–Mayers model: Consider a protocol π that uses a certain ideal resource κ and achieves security quantified by a *security parameter* ϵ_π (this quantifies the level of insecurity, but we will not go into the definition). Suppose there is a subprotocol κ' providing the resource κ with security parameter $\epsilon_{\kappa'}$. Then, the protocol π' that uses κ' (instead of κ) will have security parameter $\epsilon_{\pi'} \le \epsilon_\pi + \epsilon_{\kappa'}$.

Thus, without loss of generality, we can analyze a variation of the main protocol that uses ideal ebits instead of σ

obtained from imperfect distillation. If this new protocol is secure, so is the original one (up to a degradation of ϵ in the security parameter). In particular, Eve could have jointly attacked the imperfect distillation procedure and subsequent steps in the main protocol, and the composability result still applies in the Ben-Or–Mayers model. It then remains to consider imperfect operations (6) and (7).

Let ρ_{in} be the state of the n systems distributed in the first step of the main protocol, $\rho_{\text{out}} = \Lambda_{\text{untw}}^{\text{noisy}}(\Lambda_{\text{te}}^{\text{noisy}}(\rho_{\text{in}}))$, and $U^{(1)}$ be the ideal local untwisting defined by γ. By the invariance of norm under unitary rotation and by the triangle inequality we obtain

$$\|U^{(1)}\rho_{\text{in}}U^{(1)\dagger} - \rho_{\text{out}}\|_{\text{tr}} \leq \epsilon_1 + \epsilon_2. \tag{8}$$

The same procedure consisting of measurements and classical postprocessing is then applied to $U^{(1)}\rho_{\text{in}}U^{(1)\dagger}$ in the ideal case, and to ρ_{out} in Alice and Bob's imperfect protocol, leading to the ideal and actual phase-error estimates e_x and e_x'. Since the trace norm can only decrease under this procedure, the trace distance between the distribution of e_x and e_x' is at most $\epsilon_1 + \epsilon_2$, as we have set out to prove. This ends the proof of unconditional security of the most general version of the main protocol.

Distilling entanglement versus distilling unconditionally secure key. We will comment now on the distilled or distillable entanglement in the context of our main protocol. We denote $K_D^{u,M}(\gamma)$ as the amount of key obtained in main protocol (M) when Alice and Bob demand n copies of pdit γ given that the joint state passes error estimation step. We consider also the amount of entanglement *distilled* in that protocol denoted as $E_D^M(\gamma)$.

Distilled entanglement versus distilled secure key.—For the main protocol one has for any pdit γ: $E_D^M(\gamma) \approx 0$. This comes from the sublinear sample size $s = o(\log d \log n)$ needed to estimate the phase-error rate in the efficient protocol of Lo, Chau, and Ardehali [13]. Thus the amount of distilled entanglement per input copy approaches zero with increasing n. On the other hand the value of $K_D^{u,M}(\gamma) = c$ is nonzero by definition.

Distillable entanglement versus distilled secure key.—We now compare the distillable entanglement of pdit γ with the distillable unconditionally secure key. Below we give an example of the states showing $K_D^{u,M}(\gamma)$ can be *arbitrarily* greater than $E_D(\gamma)$. It is based on the same state for which one has $K_D(\gamma) > E_D(\gamma)$ [1,3].

Example.—Consider the pbit $\gamma_0 \in B(C^2 \otimes C^2 \otimes C^d \otimes C^d)$ of the form [1]:

$$\gamma_0 = p|\psi_+\rangle\langle\psi_+| \otimes \rho_s + (1-p)|\psi_-\rangle\langle\psi_-| \otimes \rho_a \tag{9}$$

where $p = \frac{1}{2}(1 + \frac{1}{d})$ and $\rho_{s/a}$ are normalized projectors onto symmetric/antisymmetric subspace. One has for this state $E_D(\gamma_0) \leq \log(1 + \frac{1}{d})$ [1]. This leads to the conclusion that there are states for which the gap between distillable entanglement and distillable unconditionally secure key is arbitrarily high:

$$K_D^{u,M}(\gamma_0^{\otimes \log d}) \geq c \log d \underset{d}{\rightarrow} \infty, \tag{10}$$

$$E_D(\gamma_0^{\otimes \log d}) \leq \log d \log\left(1 + \frac{1}{d}\right) \underset{d}{\rightarrow} 0, \tag{11}$$

where in the second inequality we have used additivity of log-negativity measure, which is an upper bound on distillable entanglement [14].

In summary, we introduce protocols for QKD based on noisy pbits, which are a generalization of singlets. We have found that one can still distill a key in the adversary model even when the distillable entanglement is made arbitrarily small. Notice that pbits are the most general type of states that can give a secure key. Therefore, our work generalizes QKD to the most general type of initial states.

A question which arises is whether a truly prepare-and-measure scheme exists which does not use the teleportation step. One could then extract a verifiable secure key from bound entangled states (which have strictly zero distillable entanglement). A protocol for doing this using quantum tomography was given in Ref. [1]; however, a security proof was not given. Such a proof will be the subject of a future publication. Finally, we note that in the case of *noisy* pbits, the untwisting operation in our protocol is not known to be optimal (nor proven suboptimal).

We thank Matthias Christandl, Daniel Gottesman, Michał and Pawel Horodecki, and Andreas Winter for valuable discussions, and the Newton Institute for their hospitality while this research was conducted. We acknowledge the support of EU Grants RESQ (IST-2001-37559), QUPRODIS (IST-2001-38877), and PROSECCO (IST-2001-39227); Grant No. PBZ-MIN-008/P03/2003; NSF Grant No. EIA-0086038, the Tolman Foundation, the Croucher Foundation, NSERC, the CRC Program, CFI, OIT, PREA, and CIPI.

[1] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[2] C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[3] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, quant-ph/0506189.
[4] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[5] M. Ben-Or and D. Mayers, quant-ph/0409062.
[6] P. Horodecki and R. Augusiak (to be published).
[7] The logarithm is taken to be base 2 in this Letter.
[8] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[9] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[10] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
[11] K. Horodecki *et al.*, quant-ph/0506203.
[12] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[13] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[14] G. Vidal and R. Werner, Phys. Rev. A **65**, 032314 (2002).