Unconditional Privacy over Channels which Cannot Convey Quantum Information

K. Horodecki,[1,4] M. Horodecki,[2,4] P. Horodecki,[3,4] D. Leung,[5] and J. Oppenheim[6]

[1]*Department of Math, Physics, and Computer Science, University of Gdańsk, Gdańsk, Poland*
[2]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, Gdańsk, Poland*
[3]*Faculty of Applied Physics and Math, Technical University of Gdańsk, Gdańsk, Poland*
[4]*National Quantum Information Centre of Gdańsk, 81-824 Sopot, Poland*
[5]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L1N8, Canada*
[6]*Department of Applied Mathematics and Theoretical Physics, University of Cambridge, United Kingdom*

(Received 16 February 2007; published 17 March 2008)

Quantum cryptography enables one to verify that the state of the quantum system has not been tampered with and thus one can obtain privacy regardless of the power of the eavesdropper. All previous protocols relied on the ability to faithfully send quantum states or equivalently to share pure entanglement. Here we show this need not be the case—one can obtain verifiable privacy even through some channels which cannot be used to reliably send quantum states.

DOI: 10.1103/PhysRevLett.100.110502 PACS numbers: 03.67.Hk, 03.65.Ud, 03.67.Dd

Quantum mechanics allows for the distribution of a private key [1] whose security is assured by the laws of quantum mechanics. The ability to faithfully send arbitrary quantum states [2] or equivalently distill maximally entangled states [2–6] appeared to lay at the heart of obtaining privacy. All previous cryptographic schemes are qualitatively equivalent to each other and equivalent to distilling pure state entanglement. The first step in showing that this need not be the case was in [7] in the scenario where trusted states are given to the parties. There, we obtained the most general state which can produce a private key upon measurement. One can then recast all of quantum cryptography as a protocol which distills these *private states* under local operations and classical communication (LOCC). It was then shown that there exist private states which are not equivalent to pure entanglement. In fact, they can be produced from channels which have zero capacity [8,9]—the channels cannot be used to faithfully send quantum states, but they can produce states which are private. However, a key ingredient remained. For quantum key distribution (QKD) it is not enough for two parties to share private states; they must be able to verify this privacy. One imagines a scenario where the eavesdropper Eve actually gives the two parties the states, or the parties produce the states through a channel with which Eve can tamper. One must be able to verify that one indeed holds a private state and not something else.

Here, we provide a protocol which allows two parties (Alice and Bob) to verify that they possess private states using only LOCC. This works for all private states, even those created from zero-capacity channels, thus allowing us to obtain security over channels which cannot be used to send quantum information. The protocol is thus inequivalent to the original schemes. We previously [10] had introduced a protocol which worked over channels which could have arbitrary small capacity, but the protocol cannot be extended to the case where the capacity is strictly zero. Here, we will simply sketch the proof of security of our protocol. The technical details are contained in the Appendix of [11] as well as [12].

Let us recall that there are two scenarios for QKD. In entanglement based schemes, an adversary gives states to Alice and Bob and they distill pure entanglement in the form of the maximally entangled state $|\Phi_d\rangle := \frac{1}{\sqrt{d}} \times \sum_{i=1}^{d} |i\rangle_A |i\rangle_B$, where $\{|i\rangle\}$ is a computational basis for the local systems A and B possessed by Alice and Bob, respectively. They then verify that they indeed possess states very close to this form, and then measure in the computation basis to produce a secure key. One also has the so-called "prepare and measure" protocols, where Alice prepares a quantum state and sends it to Bob, who then measures it in some basis. They then examine the results to verify that the sent states were not overly tampered with, and then perform classical post-processing on the results to obtain a key. The two schemes are equivalent in the sense that current prepare-and-measure schemes can be reduced to protocols which rely on the distillation and verification of maximally entangled states as shown in [13]. In [7] it was shown that one could consider more general schemes based on the distillation of states of the form

$$\gamma_d^U = U(|\Phi_{dAB}\rangle\langle\Phi_{dAB}| \otimes \rho_{A'B'})U^\dagger \tag{1}$$

$$U = \sum_{ij}^{d} |ij\rangle\langle ij|_{AB} \otimes U_{ijA'B'} \tag{2}$$

and viewing any protocol as the distillation and verification of such private states. Here $\rho_{A'B'}$ is an arbitrary ancilla, the $U_{ijA'B'}$ are arbitrary unitaries on it, and U is called *twisting*.

We now give the protocol for verifying private states and prove its security. The protocol is a twisted version of verification schemes of $|\Phi_d\rangle$, and in the spirit of [13] we will prove security of our protocol by reducing it to security of the protocol due to Lo and Chau [5]. Let us recall that

the Lo-Chau protocol is as follows: (1) Alice can locally prepare n systems in the state $|\Phi_2\rangle$ and distribute Bob's share to him through an untrusted channel where Eve can attack all of Bob's share at once before it gets to him. After this step, they share the state ρ_0. (2) Perform tests (via public but authenticated discussion) on ρ_0 by randomly selecting m_x and m_z systems, and measuring $\sigma_z \otimes \sigma_z$ and $\sigma_x \otimes \sigma_x$ to estimate the bit ϵ_x and phase error rate ϵ_z, respectively. Here, the σ are the standard Pauli matrices. The error rates essentially tell us how far ρ_0 deviates from a maximally entangled state. (3) Based on the results of the test, the parties perform an appropriate entanglement purification protocol (EPP) to ρ_0 and output a state $\tilde{\gamma}$ which will be close to the maximally entangled state with high probability. One does not need to know the exact form of ρ_0, but only the error rates. (4) Generate a key by measuring $\tilde{\gamma}$ locally. The key can have varying size (depends on the error rate), and zero key length means "abort QKD."

The security of this protocol rests on the fact that the estimates ϵ_x, ϵ_z of the two error rates by random sampling will converge with high probability to their expectation values over the entire initial state ρ_0 thus ensuring that the final state $\tilde{\gamma}$ is close to maximally entangled. For small δ and $m_z < (\frac{2\delta^2}{1+2\delta^2})n$, we have, for example (see, e.g., [5,14]),

$$\Pr\left(|\epsilon_{zP} - \epsilon_z| \geq \delta\right) \leq 2e^{-m_z\delta^2/16}, \tag{3}$$

where ϵ_{zP} is the expectation value of the phase error rate. This result is from sampling theory and can be found as Prop. 1 in the Appendix of [11].

We now wish to modify this protocol so that we can use it to verify private states, which for the moment we take to be many copies of γ_2^U. In [7,15,16] examples of such states were given which result from zero-capacity channels, i.e., the channels cannot be used to faithfully send quantum states, but they can be used to share *bound entangled states* [17]. Bound entangled states are those which cannot be distilled into pure state entanglement, and thus cannot be used for teleportation (and hence have zero capacity). Since our protocol will work for such bound entangled states, it will work over such zero-capacity channels.

Since private states are twisted maximally entangled states, we could achieve verifiable privacy by *untwisting* the private state before each step of the protocol, so that we are just acting the above protocol on the maximally entangled state. We would thus need to modify the protocol as follows: ($2'$) Apply untwisting $U^{\otimes n\dagger}$ to ρ_0, then estimate ϵ_x and ϵ_z on the $(AB)^{\otimes n}$ systems as in the original step (2), and finally reapply $U^{\otimes n}$. ($3'$) Apply untwisting $U^{\otimes n\dagger}$, measure out a "raw key" in the computational basis of the remaining $n - m_x - m_z$ systems. ($4'$) Perform error correction and privacy amplification on the raw key via public discussion.

Such a protocol is unfeasible since U may be a global unitary and cannot be implemented by LOCC. However, it is secure, since if we were able to perform the twisting and untwisting, the only difference between this protocol and that of the Lo-Chau one is that classical privacy amplification [18] and error correction is used instead of an entanglement purification protocol (EPP). This does not affect security since it was shown [6,19] that there exist EPPs such that applying the EPP and measuring out a key can be securely converted to protocols where a key is first measured out and then we apply classical error correction and privacy amplification on the raw key to obtain a secure one. We now explain how to convert the above unfeasible protocol to a feasible one performed via LOCC.

First, in step ($2'$), for the $n - m_x - m_z$ which are not used for testing, the twisting and untwisting cancel and therefore do not need to be performed. Also, twisting and untwisting commutes with the measurement of bit errors via $\sigma_z \otimes \sigma_z$ and therefore cancel each other. Similarly, in step ($3'$), the measurement commutes with the untwisting, and therefore this untwisting is also unnecessary. Finally, for step ($2'$), untwisting the state, estimating the expected number of phase errors, and retwisting is equivalent to estimating the twisted phase error rate via the operator $\Sigma_x = U_{ABA'B'}(\sigma_x \otimes \sigma_x \otimes I_{A'B'})U^\dagger_{ABA'B'}$. Mercifully, our only remaining task is to find a way to estimate this error rate via LOCC, rather than via direct measuring of the global operator Γ_x.

To do this, we will first decompose Σ_x in terms of products of observables which can be locally measured. We then show that this estimation of the observable in terms of these product observables is a good estimation. As will be explained shortly, this involves adapting the quantum de Finetti theorem [20] and a Chernoff-like bound. (A possible alternative route could be based on the results of [21].) We write

$$\Sigma_x = \sum_{j_a, j_b = 1}^{t} s_{j_a j_b} O_{j_a AA'} \otimes O_{j_b BB'}, \tag{4}$$

where $\{O_j\}_{j=1}^t$ is a basis (trace-orthonormal) for Hermitian operators acting on AA' and BB', and $t = d^2d'$, d' the dimension of $A'B'$. Alice and Bob can now estimate the average value of Σ_x by dividing the m_z samples into t^2 groups, and then based on public discussion they estimate $O_{j_a AA'} \otimes O_{j_b BB'}$ on the ith test system. Then they sum these estimates over $i = 1, \ldots, m_z/t^2$ with the coefficients given by Eq. (4).

The outcome of this LOCC estimation procedure will result in giving some empirical value for the average of Σ_x, which we call $\langle \Sigma^{\text{ind}} \rangle_{\text{emp}}$.

We want to see if $\langle \Sigma^{\text{ind}} \rangle_{\text{emp}}$ is close to the average $\langle \Sigma \rangle_{\text{emp}}$ that would have been obtained via hypothetical direct global measurement of Σ_x on the rest of the systems (as does the measurement on sample performed in the unfeasible yet secure modified Lo-Chau protocol).

Indeed, $\langle\Sigma^{\text{ind}}\rangle_{\text{emp}}$ will be close to $\langle\Sigma\rangle_{\text{emp}}$ if the entire m_z sample systems are in a joint tensor-power state $\rho_0^{\otimes n}$, and if the number of systems we test is large enough. This follows from Eq. (4) and the fact that for tensor-power states, we may regard each measurement as an independent event. We can then use the Chernoff bound which states that a random sample of k independent measurements of an operator O on state $\rho^{\otimes n}$ will converge exponentially fast in k to its average value $\langle O\rangle = \mathrm{Tr}(O\rho)$. More precisely, the probability that $|\langle O\rangle_{\text{emp}} - \langle O\rangle| \geq \delta$ decays as $\sim e^{-Ck\delta^2}$ for C a positive constant. In this case we know that the estimate of each of the t^2 local measurements will converge exponentially fast to $\mathrm{Tr}(\rho_0 O_j)$ as we increase the number of tested systems $k = m_z/t^2$.

However, in our current problem, Alice and Bob share ρ_0 which is *not* a tensor-power state, and each measurement cannot be considered to be an independent event. Fortunately, there is a sense in which a random sampling of m_z systems is close to tensor power. First, permutation symmetry can be imposed on the protocol (since we can choose a random sample in any order), and second, since the estimation involves only a small portion (m_z) of the entire n systems, the exponential quantum DeFinetti theorem [20] states that the measured (reduced) state is close to a mixture of "almost-tensor-power states". This is captured by Theorem 2 of the Appendix of [11]. We can now apply a Chernoff-like bound to these almost-tensor-power states. The exact analysis involves many adaptations of the results in [20] and is given in the Appendix of [11] as Theorem 1.

The result has consequences beyond the current considerations. Essentially, any realizations of an observable (i.e., a decomposition of the operator in terms of others), is a good one, in the sense that performing a one kind of measurement on m out of n systems via one realization will yield average values which are well correlated with the values obtained by performing another realization of the measurement on the remaining $n - m$ systems. This is captured in Theorem 3 of the Appendix of [11]. We can apply this to the current case to show that the probability that $|\langle\Sigma^{\text{ind}}\rangle_{\text{emp}} - \langle\Sigma\rangle_{\text{emp}}| > \delta$ can be made small. This says that the estimated twisted phase errors through measuring a sample via LOCC is correlated with the result we would obtain if we made an ideal measurement of twisted phase errors on the rest of system. Thus in terms of security, the only difference between the modified protocol, and that of Lo and Chau, is that instead of Eq. (3) governing the accuracy of the phase error estimate, we have through Theorem 3

$$\Pr(|\langle\Sigma^{\text{ind}}\rangle_{\text{emp}}^{(m)} - \langle\Sigma\rangle_{\text{emp}}^{(n-m_z)}| > \delta) \leq 2e^{-[(n-m_z)(r+1)/2n] + (1/2)d^4 d'^2 \ln(n-m_z)} + (t^2+1)2^{-[(\delta^2/36t^2d^2d') - H(rt^2/m_z)](m_z/t^2) + d'd^2 \log[(m_z/2t^2)+1]} + 2e^{-(m_z\delta^2/144d'd^2)}, \quad (5)$$

where the three expressions in the upper bound come from the exponential quantum DeFinetti theorem, the Chernoff bound, and random sampling theory and r is some natural number we will take to be $\geq d^4 d'^2 \ln n$. The superscripts for the empirical values of Σ_x refer to $\langle\Sigma^{\text{ind}}\rangle_{\text{emp}}$ being measured using m systems while $\langle\Sigma\rangle_{\text{emp}}$ is measured on the remaining $n - m_z$.

This then proves security of the scheme, since the only significant change from the unfeasible protocol is the method for estimating phase errors. The calculation of security in terms of composable security parameters for QKD [22] is given in [12].

We now touch on several issues which arise. The protocol we have given, as with all entanglement based protocols, relies on keeping the quantum state ρ_0 from decohering, and is therefore not currently practical. However, it can be converted to a prepare-and-measure protocol where Alice prepares a state, sends it down a channel (which might have zero quantum capacity), and then Bob measures the state right away. The conversion adapts well known techniques and is contained in [12] along with an example.

Here we considered verification of tensor powers of private states with $d = 2$. It is straightforward to extend this to the verification of private states of any dimension, and states where the twisting is close to tensor power. It is not clear whether one can extend this to private states which are not tensor power such as a single γ_d; as of yet we do not have a no-go theorem. This is quite different from verification of pure state entanglement where the maximally entangled state of any dimension can be written as $|\Phi_2\rangle^{\otimes n}$ and we are thus always trying to verify something close to tensor power.

Here, we considered a twisted version of the Lo-Chau scheme, but we could have just as well considered twisted versions of other parameter estimation schemes. Indeed our protocol is not optimal in its use of resources and it may be interesting to improve it. Some potential avenues were noted in [12]. A tomographic verification scheme was suggested originally in [7], and it may be interesting to explore its efficiency. It is simpler in the sense that one could just discard some states, and be left with almost-tensor-product states as in [20].

Finally, we have demonstrated conceptually that quantum key distribution is not equivalent to the ability to send quantum information. However, we only know of a few channels which have the property of offering security without allowing quantum communication. It would be very interesting to find other examples, and perhaps even more interesting to know whether there are any bound entangled states which cannot produce a secure key.

We thank Daniel Gottesman and Hoi-Kwong Lo for valuable discussions. We acknowledge support from EU Grants No. QAP IST-015848 and No. IP SCALA 015714. J. O. also acknowledges the Royal Society and D. L. is supported by the CRC, CRC-CFI, ORF, CIAR, NSERC, MITACS, and ARO. K. H. acknowledges the support of the Foundation for Polish Science.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Computer Society Press, New York, 1984), pp. 175–179.
[2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[3] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[6] G. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[7] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[8] P. Horodecki, M. Horodecki, and R. Horodecki, J. Mod. Opt. **47**, 347 (2000).
[9] D. DiVincenzo, T. Mor, P. Shor, J. Smolin, and B. Terhal, Commun. Math. Phys. **238**, 379 (2003).
[10] K. Horodecki, D. Leung, H.-K. Lo, and J. Oppenheim, Phys. Rev. Lett. **96**, 070501 (2006).
[11] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, arXiv:quant-ph/0702077.
[12] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, arXiv:quant-ph/0608195.
[13] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[14] R. Renner and R. Koenig, *Proceedings of TCC 2005, LNCS* (Springer, New York, 2005), Vol. 3378.
[15] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, arXiv:quant-ph/0506189.
[16] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, arXiv:quant-ph/0506203.
[17] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[18] C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[19] P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[20] R. Renner, Ph.D. thesis, ETH, 2005.
[21] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[22] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, arXiv:quant-ph/0409078.