A quantum cloning bound and application to quantum key distribution

Erik Woodhead[*]

Laboratoire d'Information Quantique, Université Libre de Bruxelles (ULB), 1050 Bruxelles, Belgium

2 August 2013

Quantum key distribution (QKD) was proposed nearly 30 years ago by Bennett and Brassard [1] as a way to generate and distribute cryptographic keys whose security is guaranteed by the laws of physics, and in particular inherent limitations of quantum physics, rather than assumed limitations of a potential adversary's computational power. Since that time, especially in the last 15 years or so, generic security proofs increasingly able to handle the realities of practical QKD implementations have been proposed.

The majority of recent generic security proofs have considered the entanglement-based variants of QKD protocols. Most experimental and commercially available QKD implementations, by contrast, are of the prepare-and-measure variety, and progress toward proving the unconditional security of prepare-and-measure QKD schemes has lagged somewhat behind the study of entanglement-based QKD. While certain prepare-and-measure protocols can equivalently be recast in the form of an entanglement-based scheme [2], this is normally limited to the somewhat idealised and artificial scenario where Alice's source states satisfy a condition of basis independence [3] (i.e. the average of the emitted source states is the same in the different bases used). Consequently, most results pertaining to entanglement-based QKD in practice do not carry over to realistic prepare-and-measure schemes, as the latter may suffer from *arbitrary* source flaws which deviate from the basis-independence criterion.

In our work, we provide a simple and intuitive information-theoretic security proof of the prepare-and-measure BB84 protocol which is able to handle the problem of arbitrary source and detector misalignments. Specifically, we derive an asymptotic secret keyrate, secure against collective attacks, for a BB84 implementation in which Alice's source is allowed to emit four given but arbitrary pure states and Bob's detector is left largely uncharacterised. A notable feature of our approach is its relatively direct treatment of the prepare-and-measure scenario, in that we never recast the BB84 protocol we study into an equivalent entanglement-based form and our security result is not explicitly derived based on the properties of entangled states. Instead, security is derived based on an appropriately characterised bound on an eavesdropper

[*] Erik.Woodhead@ulb.ac.be

(Eve)'s power to clone the source states emitted by Alice. Our approach can be seen as an evolution of Fuchs *et al.*'s original security proof of the BB84 protocol against individual attacks [4]. This idea of studying the prepare-and-measure BB84 variant directly was followed in some early security proofs against collective or general attacks [5, 6], but appears to have been largely abandoned since Shor and Preskill's analysis based on entanglement distillation [7].

The keyrate we derive is similar to a result previously derived by Marøy *et al.* in [8], itself an improvement over the bound predicted by the uncertainty relation [9, 10] in the special case of basis independence where a comparison may be made. However Marøy *et al.*'s result is limited to the asymptotic scenario (and is thus not a full unconditional security proof), and from a modern perspective the approach taken suffers certain drawbacks that may make generalisation difficult. Specifically, their security analysis is an evolution of a framework proposed by Koashi [11], which is unfortunately quite complicated and relies on a privacy amplification scheme defined by Koashi as an integral part of the security analysis. This is in contrast to recent information-theoretic security proofs of entanglement-based QKD, where the details of the post-processing step are decoupled from the rest of the security analysis. Given this state of affairs, a modern, information-theoretic foundation for the security of prepare-and-measure protocols is greatly desirable.

An outline of the scenario we consider and sketch of the security analysis now follows. We imagine Alice possesses a box which, depending on a choice of bit and "basis", emits one of four different quantum states which is then sent to Bob. We call the two "z-basis" states $|\alpha\rangle$ and $|\alpha'\rangle$ and the two "x-basis" states $|\beta\rangle$ and $|\beta'\rangle$, and we denote the corresponding density operators by $\rho = |\alpha\rangle\langle\alpha|$, $\rho' = |\alpha'\rangle\langle\alpha'|$, $\sigma = |\beta\rangle\langle\beta|$, and $\sigma' = |\beta'\rangle\langle\beta'|$. As a characterisation of the source states, we introduce a "basis overlap angle" θ defined such that

$$\sqrt{1 + |\sin(\theta)|} = \tfrac{1}{2}\big|\langle\alpha|\beta\rangle + \langle\alpha'|\beta\rangle + \langle\alpha|\beta'\rangle - \langle\alpha'|\beta'\rangle\big| \tag{1}$$

wherever the RHS is greater than 1. Following Eve's unitary attack, these states are contained in some Hilbert space $\mathcal{H}_{\mathrm{A}} \subset \mathcal{H}_{\mathrm{B}} \otimes \mathcal{H}_{\mathrm{E}}$, where $\mathcal{H}_{\mathrm{B}}$ and $\mathcal{H}_{\mathrm{E}}$ respectively denote the Hilbert spaces accessible to Bob and Eve. Upon reception of the states emitted by Alice, Bob performs one of two binary-outcome measurements in order to compute his version of the raw key. Alice and Bob then sacrifice a subset of their results in order to estimate the z- and x-basis bit error rates δ_z and δ_x, and if these are not too high, extract a secret key by error correction and privacy amplification. We consider the common variant of BB84 in which only the z-basis results are used to generate the final key.

In the context of our approach, the x-basis bit-error rate serves to bound the distinguishability between the parts of the x-basis source states accessible to Bob, measured in terms of the trace distance. Specifically, via the Helstrom bound, we have

$$D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}}) \geq |1 - 2\delta_x|\,, \tag{2}$$

where $D(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1$, $\|\cdot\|_1$ denotes the trace norm, and subscripts indicate partial tracing in the usual way (e.g. $\sigma_{\mathrm{B}} = \mathrm{Tr}_{\mathrm{E}}[\sigma]$).

To bound the keyrate, we apply the Devetak-Winter bound [12], which provides a lower bound on the asymptotic keyrate that can be securely extracted by one-way post-processing against collective attacks. The result is a bound on the keyrate given in terms of the fidelity between the parts of the z-basis states accessible to Eve:

$$r \geq 1 - h\big(\tfrac{1}{2} + \tfrac{1}{2}F(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}})\big) - h(\delta_z)\,, \tag{3}$$

where $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$ and $h(x) = -x \log(x) - (1-x) \log(1-x)$ denotes the binary entropy function. The security analysis is then completed by a bound on $F(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}})$ given $D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}})$. Any such bound can be considered a fundamental limit on an eavesdropper's ability to clone states allowed by quantum physics, and in general will depend on a characterisation of the source states. Given the basis overlap angle θ introduced in (1), we show that

$$F(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}}) \geq f_\theta\big(D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}})\big) \,, \tag{4}$$

with the function f_θ defined by $f_\theta(v) = \max\big(\lvert\sin(\theta)\rvert v - \lvert\cos(\theta)\rvert\sqrt{1-v^2}, 0\big)$. A keyrate bound is then obtained simply by substituting (2) and (4) into (3). The result is

$$r \geq 1 - h\big[\tfrac{1}{2} + \tfrac{1}{2} f_\theta\big(\lvert 1 - 2\delta_x \rvert\big)\big] - h(\delta_z) \,. \tag{5}$$

The derivations of Eqs. (3) and (4) are straightforward and given in [13], where we also give an improved result in the special case of a qubit source. If we additionally assume Bob's measurements are two-dimensional, the results is further improved to the point that, in the absence of detected errors, we certify an asymptotic keyrate of 1.

References

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 11 (IEEE, New York, 1984) pp. 175–179.

[2] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[3] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[4] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

[5] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, Algorithmica **34**, 372 (2002).

[6] D. Mayers, J. ACM **48**, 351 (2001).

[7] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[8] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).

[9] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).

[10] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[11] M. Koashi, New J. Phys. **11**, 045018 (2009).

[12] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).

[13] E. Woodhead, Phys. Rev. A **88**, 012331 (2013).