Quantum cloning bound and application to quantum key distribution

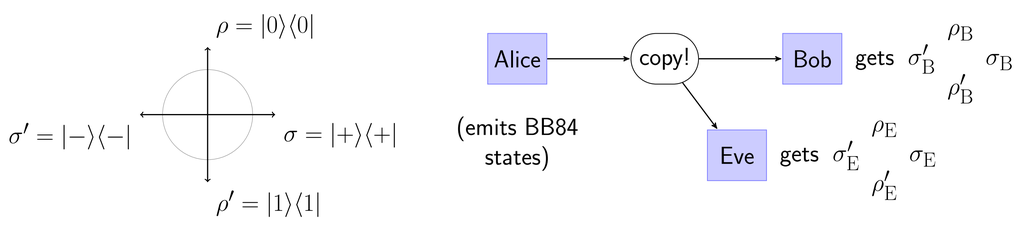
Erik Woodhead
Laboratoire d'Information Quantique, Université Libre de Bruxelles
Erik.Woodhead@ulb.ac.be

Intoduction: no-cloning

Background and preliminaries

The original intuition behind quantum key distribution was the no-cloning theorem, which implies that an eavesdropper can never perfectly clone arbitrary quantum states and will always introduce visible errors in any attempt to do so.

- The original proof of the no-cloning theorem considers almost exactly the scenario in the BB84 protocol:



If Eve attempts to clone in the computational (σ_z) basis, she will fail to copy the σ_x-basis states. If $|0\rangle_{\mathrm{A}} \mapsto |0\rangle_{\mathrm{B}}|0\rangle_{\mathrm{E}}$ and $|1\rangle_{\mathrm{A}} \mapsto |1\rangle_{\mathrm{B}}|1\rangle_{\mathrm{E}}$, then by linearity:

$$|\pm\rangle_{\mathrm{A}} \equiv \tfrac{1}{\sqrt{2}}\big(|0\rangle_{\mathrm{A}} \pm |1\rangle_{\mathrm{A}}\big) \mapsto \tfrac{1}{\sqrt{2}}\big(|0\rangle_{\mathrm{B}}|0\rangle_{\mathrm{E}} \pm |1\rangle_{\mathrm{B}}|1\rangle_{\mathrm{E}}\big)\,. \tag{1}$$

Bob's (and Eve's) reduced density operators are $\sigma_{\mathrm{B}} = \sigma'_{\mathrm{B}} = \frac{1}{2}\mathbb{1}$ – i.e. they are indistinguishable.

Conversely, if Eve clones in the x basis, the z-basis states become indistinguishable.

- A suggestive way to state this result is in terms of the trace distances between Bob's and Eve's reduced density operators:
  - If $D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}}) = 0$, in the worst case $D(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}}) = 1$. (Eve may perfectly distinguish the z-basis states.)
  - If $D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}}) = 1$, then $D(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}}) = 0$. (Eve has no ability distinguish the z-basis states.)

  (where: $D(\rho, \sigma) \equiv \frac{1}{2}\|\rho - \sigma\|_1$.)
- A generalisation for arbitrary unitary cloners was effectively derived by Fuchs *et al.* in 1997 [1]:

$$D(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}})^2 + D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}})^2 \leq 1\,, \tag{2}$$

which appeared as an intermediate result in their security proof of the BB84 protocol against individual attacks.

Results: outline

- We propose a strengthened version of (2), in which the trace distance is replace with the fidelity on Eve's side:

$$F(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}}) \geq D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}})\,. \tag{3}$$

(where: $F(\rho, \sigma) \equiv \|\sqrt{\rho}\sqrt{\sigma}\|_1$.)

(Proof idea: note that $D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}}) = \frac{1}{2}\mathrm{Tr}[(U_{\mathrm{B}} \otimes \mathbb{1}_{\mathrm{E}})X]$ where $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ for some Hermitian unitary U_{B}, note that $|0\rangle$ and $(U_{\mathrm{B}} \otimes \mathbb{1}_{\mathrm{E}})|1\rangle$ are purifications of ρ_{E} and ρ'_{E}, use Uhlmann's theorem.)

- We show that this cloning bound can be applied to a simple security proof of the BB84 protocol against collective attacks.
- Our results furthermore generalise to account for imperfections in Alice's box – ultimately to the case where Alice's box emits four arbitrary pure qubit states.

Illustration: simple key-rate derivation for BB84

The cloning bound (3) is useful because it applies to a straightforward security proof of BB84 against collective attacks:

- $D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}})$ is readily estimated by Alice and Bob in terms of the (x-basis) error rate δ_x:

$$D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}}) \geq |1 - 2\delta_x|\,. \tag{4}$$

(Helstrom bound.)

- The asymptotic secret key rate, secure against collective attacks, is readily bounded in terms of $F(\rho_{\mathrm{B}}, \rho'_{\mathrm{B}})$:

$$r \geq 1 - h\big(\tfrac{1}{2} + \tfrac{1}{2}F(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}})\big) - h(\delta_z)\,, \tag{5}$$

where $h(x) \equiv -x\log(x) - (1-x)\log(1-x)$, and δ_z is the z-basis error rate.

(Proof idea: apply Devetak-Winter bound $r \geq H(Z \mid \mathrm{E}) - H(Z \mid Z')$, replace ρ_{E}, ρ'_{E} with purifications $|\Psi\rangle$, $|\Phi\rangle$ such that $|\langle\Psi|\Phi\rangle| = F(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}})$ in evaluation of $H(Z \mid \mathrm{E})$.)

- Applying (3) and (4) to (5), we immediately recover the Shor-Preskill bound:

$$r \geq 1 - h(\delta_x) - h(\delta_z)\,. \tag{6}$$

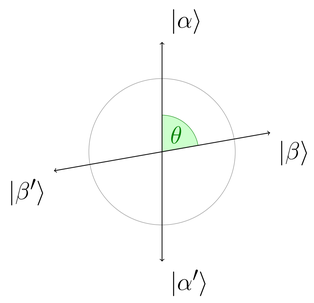
It is worth noting that this result is (mostly) device-independent on Bob's side – this comes from the use of the Helstrom bound above.

State imprecisions on Alice's side

In a realistic setting, no physical source can prepare BB84 states with perfect precision. Thus one must be able to handle a source emitting states that deviate slightly from ideal BB84 states. This is one issue practical security proofs must account for.

In these cases, the cloning bound (3) no longer applies and must be generalised.

Arbitrary source states



- We call the source states $\{|\alpha\rangle, |\alpha'\rangle\}$ ("z basis") and $\{|\beta\rangle, |\beta'\rangle\}$ ("x basis").
- We define a "basis overlap angle" θ by

$$\sqrt{1 + |\sin(\theta)|} = \tfrac{1}{2}\big|\langle\alpha|\beta\rangle + \langle\alpha'|\beta\rangle + \langle\alpha|\beta'\rangle - \langle\alpha'|\beta'\rangle\big|\,. \tag{7}$$

- in the case of orthogonal qubit bases, θ coincides with the angle on the Bloch sphere (see figure left).

One can show that

$$F(\rho_{\mathrm{E}}, \rho'_{\mathrm{E}}) \geq f_\theta\big(D(\sigma_{\mathrm{B}}, \sigma'_{\mathrm{B}})\big) \tag{8}$$

with $f_\theta(D) \equiv |\sin(\theta)|D - |\cos(\theta)|\sqrt{1 - D^2}$.

The key-rate bound becomes

$$r \geq 1 - h\big(\tfrac{1}{2} + \tfrac{1}{2}f_\theta(|1 - 2\delta_x|)\big) - h(\delta_z)\,. \tag{9}$$

Qubit source and detector

- Key-rate bound can be improved somewhat for arbitrary qubit states.
- Bound can be further improved if Bob's detector is assumed two-dimensional.

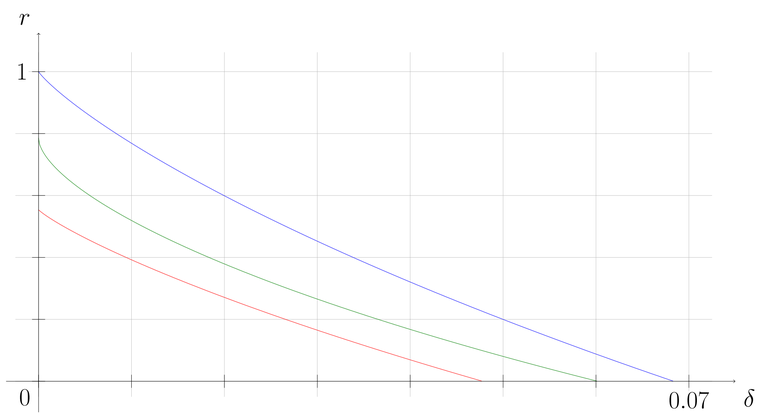
Fidelity bounds are of the form $F^Z_{\mathrm{E}} \geq g_\alpha \circ f^{(2)}_\varphi\big(D^Z_{\mathrm{B}}, D^X_{\mathrm{B}}\big)$. ($\alpha, \varphi$: parameters characterising source.)

Relation to existing results

The key rate (9) is ...

- similar to a key rate derived by Marøy *et al.* [2], and
- an improvement over the key rate predicted by the uncertainty relation [3] (where a comparison can be made).

A comparison of key rates for $\theta = 1.2\,\mathrm{rad}$, corresponding to a deviation of around $21°$, and with symmetric errors ($\delta_x = \delta_z \equiv \delta$) is illustrated on the figure below (for an orthogonal qubit basis source).



Above: 1) key rate derived from the uncertainty relation, 2) equation (9), and 3) improved key rate bound if Bob's Hilbert space is restricted to $\dim = 2$. The threshold error rates are $\delta_0 \approx 4.78\,\%$, $6.02\,\%$, and $6.84\,\%$.

References

[1] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163–1172 (1997).
[2] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).
[3] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

Article ref: E. W., Phys. Rev. A **88**, 012331 (2013).