UNIVERSITY OF COPENHAGEN
DEPARTMENT OF MATHEMATICAL SCIENCES

Random private quantum states

Matthias Christandl, Roberto Ferrara, Cécilia Lancien, ArXiV: 1801.02861

The study of properties of randomly chosen quantum states has in recent years led to many insights into quantum entanglement. In this work, we study private quantum states from this point of view. Private quantum states are bipartite quantum states characterised by the property that carrying out a simple local measurement yields a secret bit. This feature is shared by the maximally entangled pair of quantum bits, yet private quantum states are more general and can in their most extreme form be almost bound entangled. In this work, we study the entanglement properties of random private quantum states and show that they are hardly distinguishable from separable states and thus have low repeatable key, despite containing one bit of key. The technical tools we develop are centred around the concept of locally restricted measurements and include a new operator ordering, bounds on norms under tensoring with entangled states and continuity bounds for relative entropy measures.

QMATH Centre for the Mathematics of Quantum Theory
VILLUM FONDEN
DANMARKS FRIE FORSKNINGSFOND INDEPENDENT RESEARCH FUND DENMARK
cnrs
erc
FNSNF
JOHN TEMPLETON FOUNDATION

Motivation

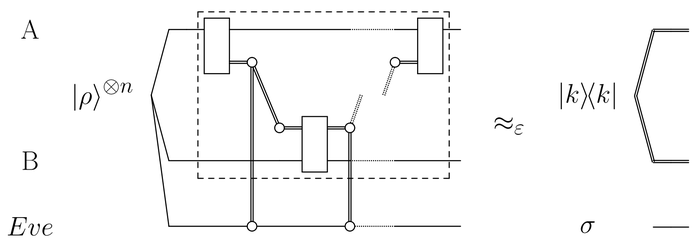
Distillable Key vs. a QKD protocol

- A given Quantum Key Distribution (QKD) protocol accepts any *unknown* input state and extracts an amount of key from it (maybe zero).
- The distillable key $K(\rho)$ is an optimization over the amount of key that any protocols can extract from the *known* input state ρ.

The error estimation step in a QKD protocol can be thought as going from an unknown input to a known input. $K(\rho)$ is a theoretical upper bound on the key that can be extracted after that step (and is independent of the protocol).

Distillable Key - Tripartite Formalism

Local Operations and Classical Communication with wiretap channel and output a classical uniform secret key:

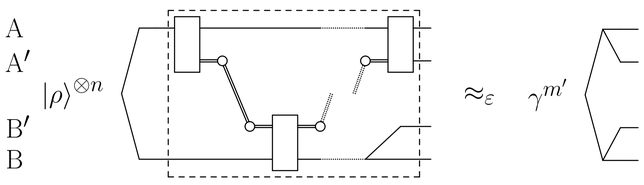


where $|k\rangle\langle k|$ are m bits of key (uniformly random). The resulting rate of key distillation is $\frac{m}{n}$ which is then optimized over all possible protocols:

$$K(\rho) \coloneqq \lim_{\varepsilon\to 0}\lim_{n\to\infty}\sup\frac{m}{n}$$

Distillable Key - Bipartite Formalism [1]

Local Operations and Classical Communication with output a private state:



where $\gamma^{m'}$ are the class of states called *private states* (see next).

- Easier to relate to other (bipartite) entanglement measures
- Gives the same rate:

$$K(\rho) = \lim_{\varepsilon\to 0}\lim_{n\to\infty}\sup\frac{m'}{n}$$

Eve holds the purification at all times:

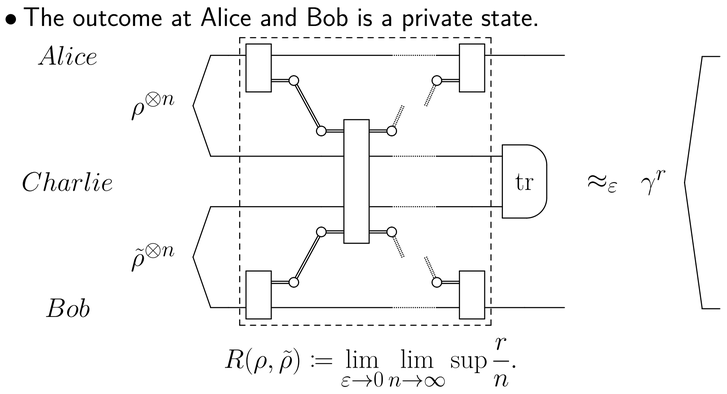
- Tracing something sends it to Eve.
- To recover the tripartite formalism, recover Eve via the purification and trace A' and B'.

(...maybe a few technicalities got swept under the rug.)

Distillable Key - Repeater Station [4]

With private states it is easy to define a key distillation rate with a single repeater station in the middle:

- Protocols are tripartite LOCC with Charlie.
- Charlie is untrusted ⇒ remaining systems go to Eve (trace)
- The outcome at Alice and Bob is a private state.



$$R(\rho,\tilde\rho) \coloneqq \lim_{\varepsilon\to 0}\lim_{n\to\infty}\sup\frac{r}{n}.$$

For upper bounds a single station is without loss of generality, because more stations can only reduce the rate.

Bounded memory repeater station

To simulate a station that can only act on N copies at the time, we just force Charlie to trace all his systems every N copies. No restriction is imposed on Alice and Bob. This gives the lower rate $R^N(\rho,\tilde\rho)$

Private states

Without loss of generality a private state containing one bit of key ($m = 1$) looks like this[1, 6]:

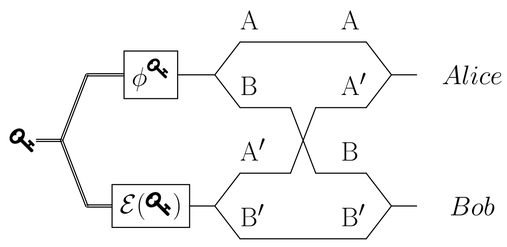
$$\gamma = \frac{1}{2}\cdot\phi_+\otimes\varrho^+ + \frac{1}{2}\cdot\phi_-\otimes\varrho^-$$

- $\sigma_\pm$ are orthogonal states of $\mathrm{A}'\mathrm{B}'$, with $|\mathrm{A}'| = |\mathrm{B}'| = d$.
- $\phi_\pm$ are the Bell state of AB (with $|\mathrm{A}| = |\mathrm{B}| = 2^m = 1$):

$$|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

- $\pm \simeq_{\mathbf{Q}_\pm}$, i.e. the mixture uses as much randomness as the key

Basically:



Random construction

Construct $\varrho^\pm$ as follows

- Split the d^2 dimensional Hilbert space $A'B'$ in half, name these projectors P^+ and P^-
- Pick a unitary U uniformly at random according to the Haar measure
- Define the uniform mixtures

$$\varrho^\pm = U\left(\frac{P^\pm}{\operatorname{tr} P^\pm}\right)U^\dagger$$

In the limit $d\to\infty$, $\rho^\pm$ stay PPT-distinguishable (distinguishable under PPT operations, PPT="Positive under Partial Trasposition"), but become SEP-indistinguishable (indistinguishable under separable operations). This is due to the relative growth of the sets of PPT and separable states with respect to the set of all states. [5]

Result: γ is PPT-distinguishable but SEP-indistinguishable from its flipped version $\overline{\gamma}$

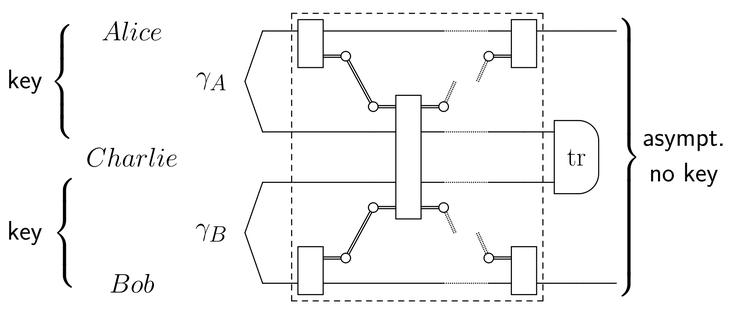
$$\overline{\gamma} = \frac{1}{2}\cdot\phi_+\otimes\varrho^- + \frac{1}{2}\cdot\phi_-\otimes\varrho^+$$

Intuition

In principle the additional maximally entangled states could aid the measurement. Notice that this is not the same as having the maximally entangled state in product. Still, even in that case, the growing size of the systems $A'B'$ makes the help of a bit of entanglement irrelevant.

Random construction: Not repeatable

Below consider a bounded memory repeater station that can only act on one copy at the time.
Using the above properties in an appropriate way we can show that with high probability the key of these random private states cannot be repeated.
While similar results have been shown before [4, 6], these are the first states to be far from the set of PPT states.



Remark: when the goal is distilling maximally entangled states, the PPT condition is the only known criterion to prove that the resulting rate is zero.

Technicalities - Local measures

Definitions

Let X be an operator, ρ,σ states and $\mathbf{L}$ a set of channels, then:

$$\|X\|_{\mathbf{L}} \coloneqq \sup_{\Lambda\in\mathbf{L}}\|\Lambda(X)\|_1\,,$$
$$D_{\mathbf{L}}(\varrho\|\varsigma) \coloneqq \sup_{\Lambda\in\mathbf{L}} D(\Lambda(\varrho)\|\Lambda(\varsigma))$$

which were defined in[2, 3] for measurements. If $\mathcal{K}$ is a set of states

$$: \|\varrho-\mathcal{K}\|_{\mathbf{L}} \coloneqq \inf_{\varsigma\in\mathcal{K}}\|\varrho-\varsigma\|_{\mathbf{L}}$$
$$D_{\mathbf{L}}(\varrho\|\mathcal{K}) \coloneqq \inf_{\varsigma\in\mathcal{K}} D_{\mathbf{L}}(\varrho\|\varsigma).$$

Private states vs their shield

For any private state such that $\frac{1}{2}(\varrho^+ + \varrho^-)$ is separable:

$$\|\gamma-\mathcal{S}\|_{\mathbf{SEP}(\mathrm{AA}':\mathrm{BB}')} \le \frac{3}{2}\|\varrho^+-\varrho^-\|_{\mathbf{SEP}(\mathrm{A}':\mathrm{B}')}$$
$$\|\gamma-\mathcal{S}\|_{\mathbf{PPT}(\mathrm{AA}':\mathrm{BB}')} \ge \frac{1}{2}\|\varrho^+-\varrho^-\|_{\mathbf{PPT}(\mathrm{A}':\mathrm{B}')}.$$

where $\mathcal{S}\equiv\mathcal{S}(\mathrm{AA}':\mathrm{BB}')$ are the separable states and $\mathbf{PPT}/\mathbf{SEP}(\mathrm{C}:\mathrm{D})$ are the PPT/separable measurements on systems C and D.

Random private states

With high probability in our construction:

$$\|\gamma-\mathcal{S}\|_{\mathbf{SEP}(\mathrm{AA}':\mathrm{BB}')} \le \frac{C}{\sqrt{d}}$$
$$\|\gamma-\mathcal{S}\|_{\mathbf{PPT}(\mathrm{AA}':\mathrm{BB}')} \ge c$$

where $C, c > 0$ are universal constants. Using the asymptotic continuity of $D_{\mathbf{L}}$ and the Pinsker inequality this translates to:

$$D_{\mathbf{SEP}(\mathrm{AA}':\mathrm{BB}')}(\gamma\|\mathcal{S}) \le \frac{C'\log d}{\sqrt{d}}$$
$$D_{\mathbf{PPT}(\mathrm{AA}':\mathrm{BB}')}(\gamma\|\mathcal{S}) \ge c'.$$

Single copy repeater station

$$R^1_D(\varrho,\tilde\varrho) \le D_{\mathbf{SEP}(\mathrm{C}\tilde{\mathrm{C}}:\mathbb{AB})}(\varrho\otimes\tilde\varrho\|\mathcal{S}).$$

where $\mathcal{S}\equiv\mathcal{S}(\mathrm{A}':\mathrm{C}:\tilde{\mathrm{C}}:\mathrm{B}')$ and $\mathbf{SEP}(\mathrm{C}\tilde{\mathrm{C}}:\mathbb{AB})$ are partial separable measurements: $\mathrm{C}\tilde{\mathrm{C}}$ are measured at the end of the protocol, but AB can stay quantum.
Let γ_A on $\mathrm{AA}'\mathrm{CC}'$ and γ_B on $\tilde{\mathrm{C}}\tilde{\mathrm{C}}'\mathrm{BB}'$ be two random private states, and let $d_A \coloneqq |\mathrm{A}'| = |\mathrm{C}'|$ and $d_B \coloneqq |\mathrm{B}'| = |\tilde{\mathrm{C}}'|$. Then, with high probability

$$R^1_D(\gamma_A,\gamma_B) \le C\varepsilon(d_A,d_B)\log d_B$$

where $\varepsilon(d_A,d_B) \coloneqq \min\left(1/\sqrt{d_B},\, d_B/\sqrt{d_A}\right)$.
Interesting limit: $0 \ll d_2\log d_2 \ll \sqrt{d_1}$.

References

[1] **K. Horodecki**, **M. Horodecki**, **P. Horodecki**, **J. Oppenheim**, *PRL* **94**, 160502 (2005), arXiv:quant-ph/0309110. .

[2] **W. Matthews**, **S. Wehner**, **A. Winter** *Commun. Math. Phys.* **291**, 813 (2009) arXiv:0810.2327. .

[3] **M. Piani**, *PRL* **103**, 160504 (2009), arXiv:0904.2705. .

[4] **S. Bäuml**, **M. Christandl**, **K. Horodecki**, **A. Winter**, *Nature Communications* **6**, 6908 (2014), arXiv:1402.5927. .

[5] **G. Aubrun**, **C. Lancien**, *Quant. Inf. Proc.* **15**, 512 (2014) arXiv:1406.1959. .

[6] **M. Christandl**, **R. Ferrara**, *PRL* **119**, 220506 (2017) arXiv:1609.04696. .