Bound entangled states with secret key and their classical counterpart

Māris Ozols
UNIVERSITY OF CAMBRIDGE

Graeme Smith
John Smolin
IBM

February 6, 2014

A brief summary

Main result

A new construction of *bound entangled states with secret key*

Steps involved

1. Understand what is the classical analogue of this
2. Construct a probability distribution P_{ABE} that has the desired properties
3. Set $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$

A brief summary

Main result

A new construction of *bound entangled states with secret key*

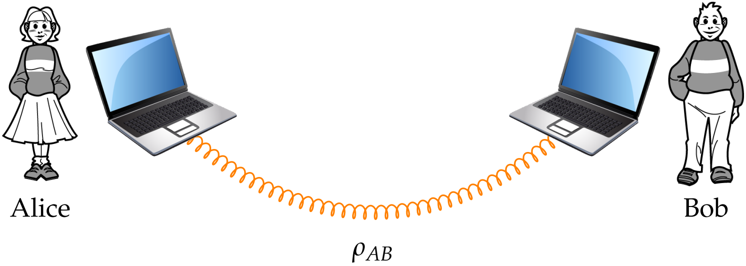
Steps involved

1. Understand what is the classical analogue of this
2. Construct a probability distribution P_{ABE} that has the desired properties
3. Set $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$

The significance of trash in cryptography

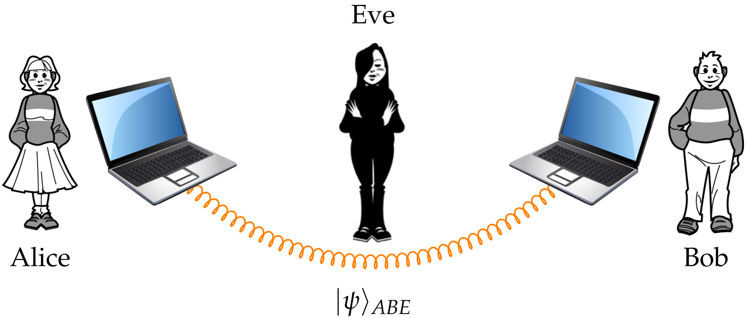
Shared entanglement and randomness

- Cryptographic and computational resource



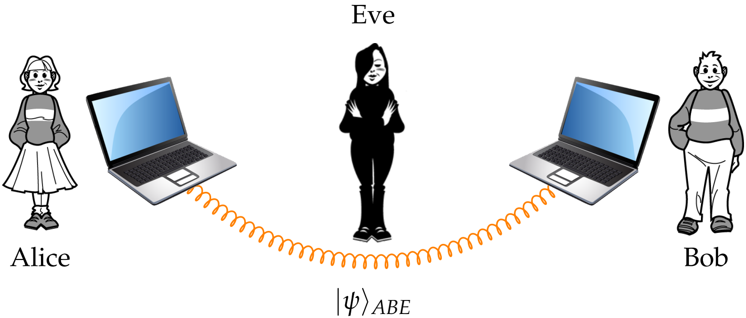
Shared entanglement and randomness

- Cryptographic and computational resource
- Joint state: $|\psi\rangle_{ABE}$ or P_{ABE}



Shared entanglement and randomness

- Cryptographic and computational resource
- Joint state: $|\psi\rangle_{ABE}$ or P_{ABE}
- When is such resource useful?



Perfect resources

When is P_{ABE} a perfect resource?

1. Identical for A and B
2. Uniformly random
3. Private from E

Perfect resources

When is P_{ABE} a perfect resource?

1. Identical for A and B
2. Uniformly random
3. Private from E

$$P_{ABE} = \mathrm{KEY}_{AB} \otimes \mathrm{TRASH}_E$$
$$\mathrm{KEY}_{AB} = \begin{cases} 0_A 0_B & \text{w.p. } 1/2 \\ 1_A 1_B & \text{w.p. } 1/2 \end{cases}$$

Perfect resources

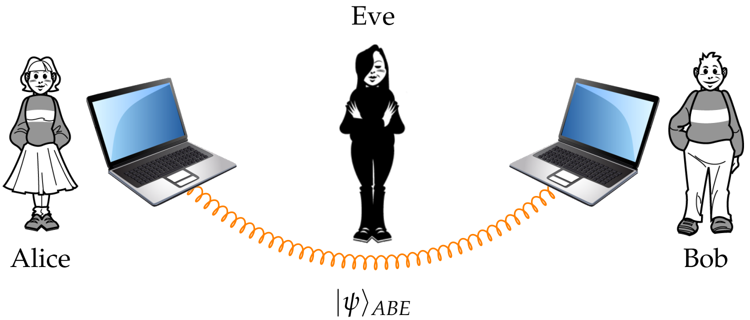
When is P_{ABE} a perfect resource?

1. Identical for A and B
2. Uniformly random
3. Private from E

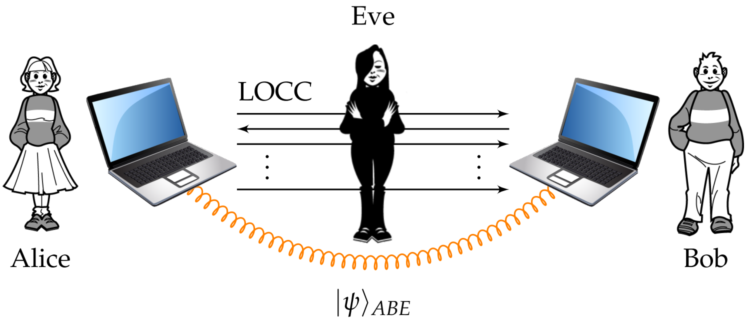
$$P_{ABE} = \mathrm{KEY}_{AB} \otimes \mathrm{TRASH}_E$$
$$\mathrm{KEY}_{AB} = \begin{cases} 0_A 0_B & \text{w.p. } 1/2 \\ 1_A 1_B & \text{w.p. } 1/2 \end{cases}$$

$$|\psi\rangle_{ABE} = |\mathrm{KEY}\rangle_{AB} \otimes |\mathrm{TRASH}\rangle_E$$
$$|\mathrm{KEY}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$$

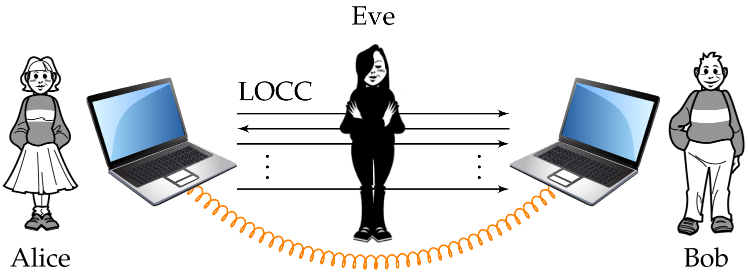
Distillation



Distillation

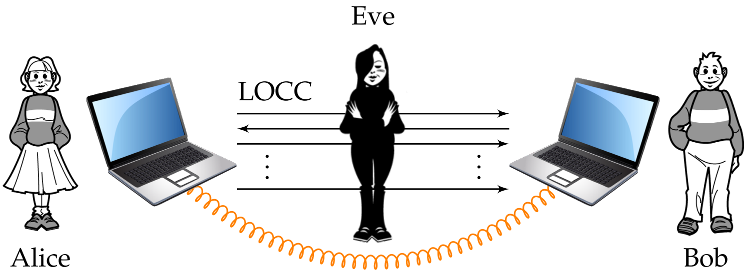


Distillation



$$|\mathrm{KEY}\rangle_{AB}^{\otimes k} \otimes |\mathrm{TRASH}\rangle_E$$

Distillation



$$|\mathrm{KEY}\rangle_{AB}^{\otimes k} \otimes |\mathrm{TRASH}\rangle_E$$

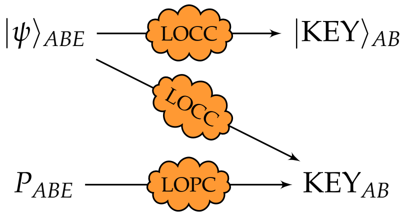
Entanglement distillation rate

$$D(|\psi\rangle_{ABE}) := \lim_{n\to\infty} \frac{1}{n}\Big(\#\text{ of } |\mathrm{KEY}\rangle_{AB} \text{ from } |\psi\rangle_{ABE}^{\otimes n} \text{ via LOCC}\Big)$$

More distillation rates

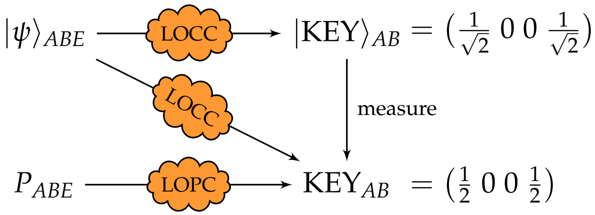
- $D(|\psi\rangle_{ABE})$ – entanglement distillation rate
- $K(P_{ABE})$ – key distillation rate

More distillation rates



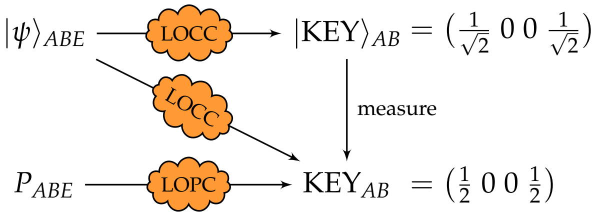
- $D(|\psi\rangle_{ABE})$ – entanglement distillation rate
- $K(P_{ABE})$ – key distillation rate
- $K(|\psi\rangle_{ABE})$ – key distillation rate

More distillation rates



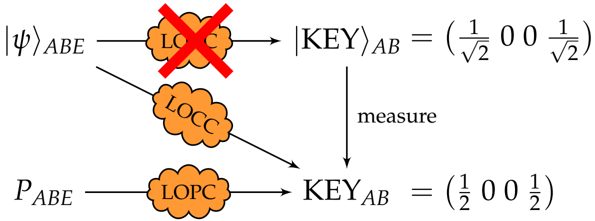
- $D(|\psi\rangle_{ABE})$ – entanglement distillation rate
- $K(P_{ABE})$ – key distillation rate
- $K(|\psi\rangle_{ABE})$ – key distillation rate

More distillation rates



- $D(|\psi\rangle_{ABE})$ – entanglement distillation rate
- $K(P_{ABE})$ – key distillation rate
- $K(|\psi\rangle_{ABE})$ – key distillation rate
- $K(|\psi\rangle_{ABE}) \geq D(|\psi\rangle_{ABE})$

More distillation rates

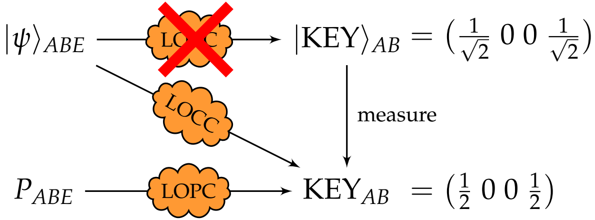


- $D(|\psi\rangle_{ABE})$ – entanglement distillation rate
- $K(P_{ABE})$ – key distillation rate
- $K(|\psi\rangle_{ABE})$ – key distillation rate
- $K(|\psi\rangle_{ABE}) \geq D(|\psi\rangle_{ABE})$

Bound entanglement

$|\psi\rangle_{ABE}$ is entangled
but $D(|\psi\rangle_{ABE}) = 0$

More distillation rates

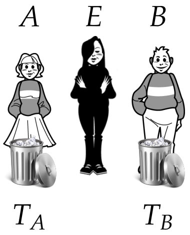


- $D(|\psi\rangle_{ABE})$ – entanglement distillation rate
- $K(P_{ABE})$ – key distillation rate
- $K(|\psi\rangle_{ABE})$ – key distillation rate
- $K(|\psi\rangle_{ABE}) \geq D(|\psi\rangle_{ABE})$

Bound entanglement
$|\psi\rangle_{ABE}$ is entangled
but $D(|\psi\rangle_{ABE}) = 0$

Private bound entanglement
$|\psi\rangle_{ABE}$ is bound entangled
but $K(|\psi\rangle_{ABE}) > 0$ [HHHO05]

Entanglement vs classical key

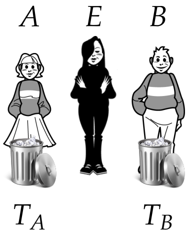


Compare

$$|\Psi_1\rangle := \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB}\Big) \otimes |\varphi\rangle_{T_A T_B} \otimes |\phi\rangle_E$$

$$|\Psi_2\rangle := \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB}|\varphi\rangle_{T_A T_B} + |11\rangle_{AB}|\varphi^{\perp}\rangle_{T_A T_B}\Big) \otimes |\phi\rangle_E$$

Entanglement vs classical key



Compare

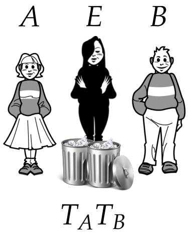
$$|\Psi_1\rangle := \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB}\Big) \otimes |\varphi\rangle_{T_A T_B} \otimes |\phi\rangle_E$$

$$|\Psi_2\rangle := \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB}|\varphi\rangle_{T_A T_B} + |11\rangle_{AB}|\varphi^{\perp}\rangle_{T_A T_B}\Big) \otimes |\phi\rangle_E$$

Observe

- If T_A and T_B are discarded, $|\Psi_1\rangle$ contains a quantum $|\text{KEY}\rangle$ whereas $|\Psi_2\rangle$ contains only a classical KEY

Entanglement vs classical key



Compare

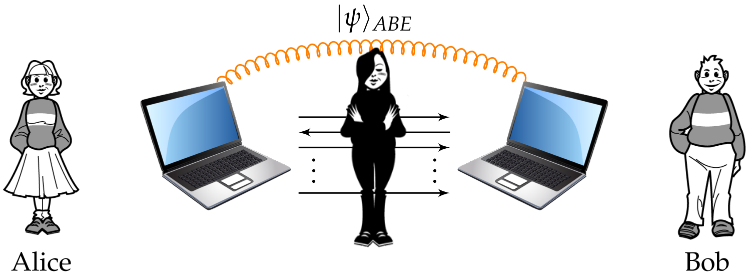
$$|\Psi_1\rangle := \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB}\Big) \otimes |\varphi\rangle_{T_A T_B} \otimes |\phi\rangle_E$$

$$|\Psi_2\rangle := \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB}|\varphi\rangle_{T_A T_B} + |11\rangle_{AB}|\varphi^{\perp}\rangle_{T_A T_B}\Big) \otimes |\phi\rangle_E$$

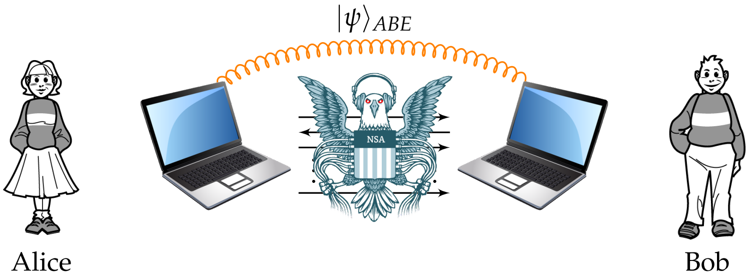
Observe

- If T_A and T_B are discarded, $|\Psi_1\rangle$ contains a quantum $|\text{KEY}\rangle$ whereas $|\Psi_2\rangle$ contains only a classical KEY
- Quantum $|\text{KEY}\rangle$ is immune against Eve accessing T_A and T_B (due to monogamy of entanglement)

Distillation with remanent devices



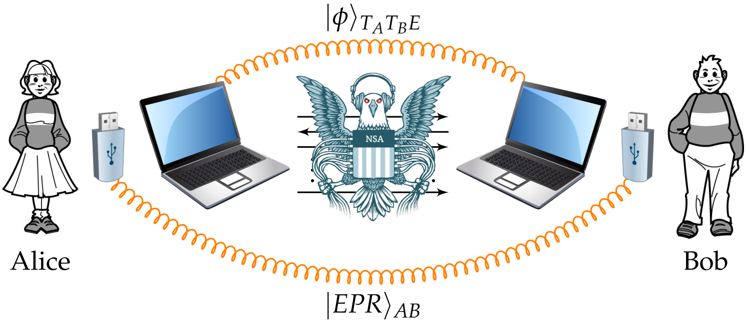
Distillation with remanent devices



Extra assumption

- At the end of the protocol Eve confiscates both devices; she can recover all information that was erased
- Alice and Bob can keep *only* the key

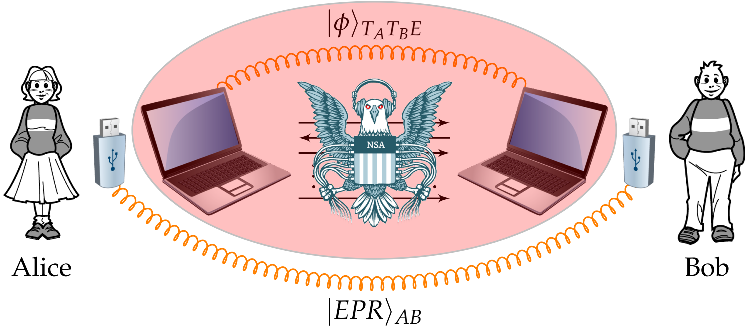
Distillation with remanent devices



Extra assumption

- At the end of the protocol Eve confiscates both devices; she can recover all information that was erased
- Alice and Bob can keep *only* the key

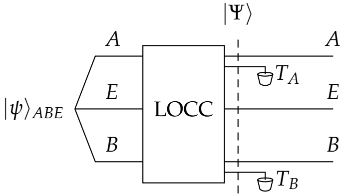
Distillation with remanent devices



Extra assumption

- At the end of the protocol Eve confiscates both devices; she can recover all information that was erased
- Alice and Bob can keep *only* the key

Quantum distillation



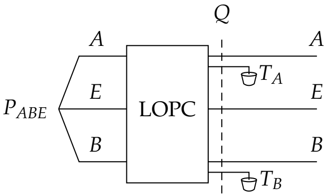
$$\frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB}\Big) \otimes |\varphi\rangle_{T_A T_B} \otimes |\phi\rangle_E$$

entangled key

$$\frac{1}{\sqrt{2}}\Big(|00\rangle_{AB}|\varphi\rangle_{T_A T_B} + |11\rangle_{AB}|\varphi^{\perp}\rangle_{T_A T_B}\Big) \otimes |\phi\rangle_E$$

classical key

Classical distillation



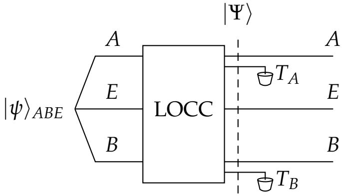
$$\frac{1}{2}\Big(00_{AB} + 11_{AB}\Big) \otimes \varphi_{T_A T_B} \otimes \phi_E$$

classical key?

$$\frac{1}{2}\Big(00_{AB} \otimes \varphi_{T_A T_B} + 11_{AB} \otimes \varphi^{\perp}_{T_A T_B}\Big) \otimes \phi_E$$

classical key?

Quantum distillation



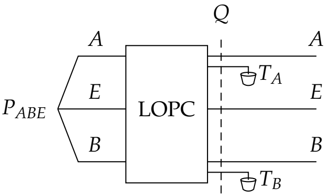
$$\frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB}\Big) \otimes |\varphi\rangle_{T_A T_B} \otimes |\phi\rangle_E$$

entangled key

$$\frac{1}{\sqrt{2}}\Big(|00\rangle_{AB}|\varphi\rangle_{T_A T_B} + |11\rangle_{AB}|\varphi^{\perp}\rangle_{T_A T_B}\Big) \otimes |\phi\rangle_E$$

classical key

Classical distillation



$$\frac{1}{2}\Big(00_{AB} + 11_{AB}\Big) \otimes \varphi_{T_A T_B} \otimes \phi_E$$

classical key?

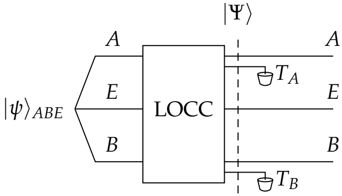
$$\frac{1}{2}\Big(00_{AB} \otimes \varphi_{T_A T_B} + 11_{AB} \otimes \varphi^{\perp}_{T_A T_B}\Big) \otimes \phi_E$$

classical key?

Private randomness

- There are two types of private randomness!

Quantum distillation



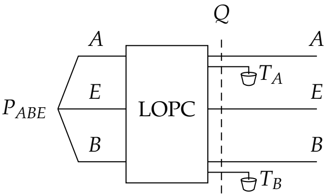
$$\frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB}\Big) \otimes |\varphi\rangle_{T_A T_B} \otimes |\phi\rangle_E$$

entangled key

$$\frac{1}{\sqrt{2}}\Big(|00\rangle_{AB}|\varphi\rangle_{T_A T_B} + |11\rangle_{AB}|\varphi^{\perp}\rangle_{T_A T_B}\Big) \otimes |\phi\rangle_E$$

classical key

Classical distillation



$$\frac{1}{2}\Big(00_{AB} + 11_{AB}\Big) \otimes \varphi_{T_A T_B} \otimes \phi_E$$

classical key?

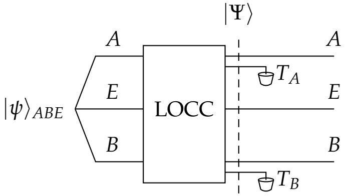
$$\frac{1}{2}\Big(00_{AB} \otimes \varphi_{T_A T_B} + 11_{AB} \otimes \varphi^{\perp}_{T_A T_B}\Big) \otimes \phi_E$$

classical key?

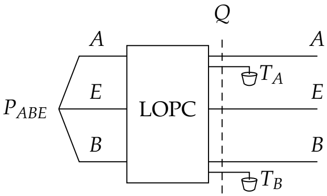
Private randomness

- There are two types of private randomness!
- Classical analog of entanglement [CP02] is private randomness that is distilled on remanent devices

Quantum distillation



Classical distillation



$$\frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB}\Big) \otimes |\varphi\rangle_{T_A T_B} \otimes |\phi\rangle_E$$

entangled key

$$\frac{1}{2}\Big(00_{AB} + 11_{AB}\Big) \otimes \varphi_{T_A T_B} \otimes \phi_E$$

~~classical key?~~

$$\frac{1}{\sqrt{2}}\Big(|00\rangle_{AB}|\varphi\rangle_{T_A T_B} + |11\rangle_{AB}|\varphi^{\perp}\rangle_{T_A T_B}\Big) \otimes |\phi\rangle_E$$

classical key

$$\frac{1}{2}\Big(00_{AB} \otimes \varphi_{T_A T_B} + 11_{AB} \otimes \varphi^{\perp}_{T_A T_B}\Big) \otimes \phi_E$$

classical key?

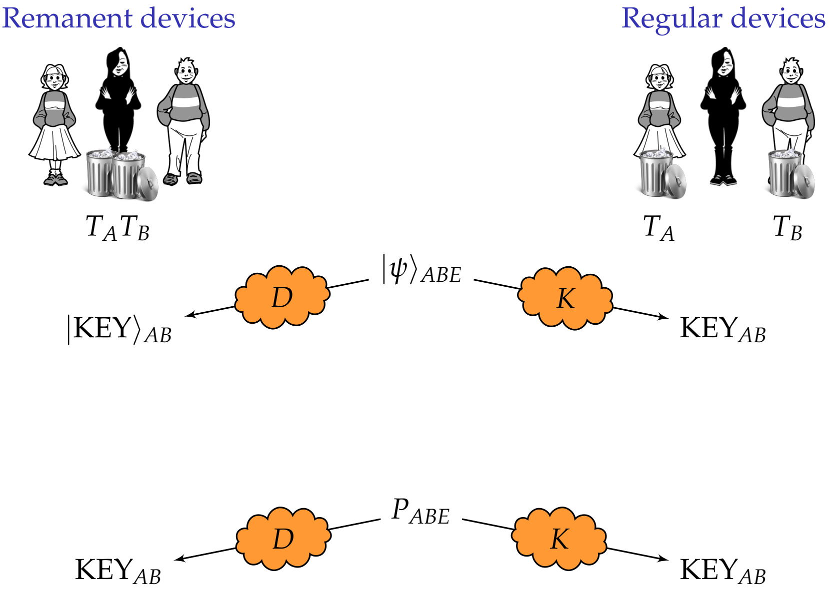
Private randomness

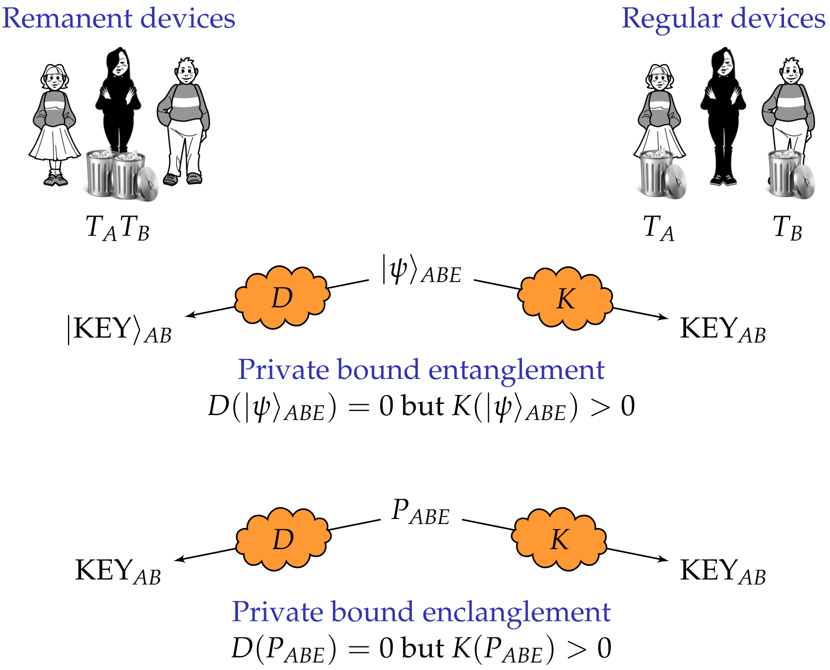
- There are two types of private randomness!
- Classical analog of entanglement [CP02] is private randomness that is distilled on remanent devices
- This resource needs a new name…

cl[assical] *en*[t]*anglement*

=

enclanglement


Remanent devices
Regular devices
$T_A T_B$
T_A
T_B
$|\psi\rangle_{ABE}$
D
K
$|\mathrm{KEY}\rangle_{AB}$
KEY_{AB}
P_{ABE}
D
K
KEY_{AB}
KEY_{AB}


Remanent devices
Regular devices
$T_A T_B$
T_A
T_B
$|\psi\rangle_{ABE}$
D
K
$|\mathrm{KEY}\rangle_{AB}$
KEY_{AB}
Private bound entanglement
$D(|\psi\rangle_{ABE}) = 0$ but $K(|\psi\rangle_{ABE}) > 0$
P_{ABE}
D
K
KEY_{AB}
KEY_{AB}
Private bound enclanglement
$D(P_{ABE}) = 0$ but $K(P_{ABE}) > 0$

Main results

Theorem 1

If $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$ is quantical then

- $D(\psi_{ABE}) \geq D(P_{ABE})$ and
- $K(\psi_{ABE}) \geq K(P_{ABE})$

Theorem 2

There exist quantical distributions P_{ABE} with $D(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$

Main results

Theorem 1

If $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$ is quantical then

- $D(\psi_{ABE}) \geq D(P_{ABE})$ and
- $K(\psi_{ABE}) \geq K(P_{ABE})$

Theorem 2

There exist quantical distributions P_{ABE} with
$D(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$

Corollaries

1. New construction of private bound entanglement
2. Noise helps in one-way classical key distillation

quant[um]

+

[class]*ical*

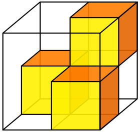
=

quantical

Quantical distributions / states

P_{ABE} is *quantical* if any single party's state can be unambiguously determined by the rest of the parties:*

$$\forall b, e : |\{a : p(a,b,e) \neq 0\}| \leq 1$$
$$\forall a, b : |\{e : p(a,b,e) \neq 0\}| \leq 1$$
$$\forall a, e : |\{b : p(a,b,e) \neq 0\}| \leq 1$$

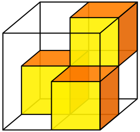


*Similar distributions have appeared in [OSW05, CEH+07]

Quantical distributions / states

P_{ABE} is *quantical* if any single party's state can be unambiguously determined by the rest of the parties:*

$$\forall b, e : |\{a : p(a,b,e) \neq 0\}| \leq 1$$
$$\forall a, b : |\{e : p(a,b,e) \neq 0\}| \leq 1$$
$$\forall a, e : |\{b : p(a,b,e) \neq 0\}| \leq 1$$



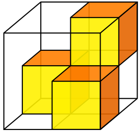
If P_{ABE} is quantical, we call $|\psi\rangle_{ABE} := \sqrt{P_{ABE}}$ *quantical* too

*Similar distributions have appeared in [OSW05, CEH+07]

Quantical distributions / states

P_{ABE} is *quantical* if any single party's state can be unambiguously determined by the rest of the parties:*

$$\forall b, e : |\{a : p(a,b,e) \neq 0\}| \leq 1$$
$$\forall a, b : |\{e : p(a,b,e) \neq 0\}| \leq 1$$
$$\forall a, e : |\{b : p(a,b,e) \neq 0\}| \leq 1$$



If P_{ABE} is quantical, we call $|\psi\rangle_{ABE} := \sqrt{P_{ABE}}$ *quantical* too

Dual nature

- Quantical P_{ABE} and $|\psi\rangle_{ABE}$ describe the same entity
- Entropic quantities for P_{ABE} and $|\psi\rangle_{ABE}$ agree
- Quantical P_{ABE} has a "classical Schmidt decomposition" w.r.t. any bipartition

*Similar distributions have appeared in [OSW05, CEH$^+$07]

Theorem 1

If $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$ is quantical then

- $D(\psi_{ABE}) \geq D(P_{ABE})$ and
- $K(\psi_{ABE}) \geq K(P_{ABE})$

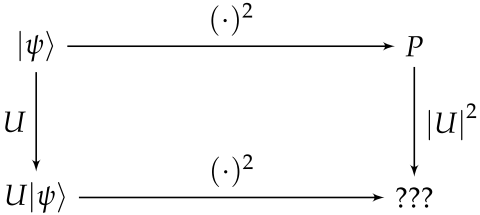
Theorem 1

If $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$ is quantical then

- $D(\psi_{ABE}) \geq D(P_{ABE})$ and
- $K(\psi_{ABE}) \geq K(P_{ABE})$

Proof idea

1. Classical protocol can be promoted to a quantum one



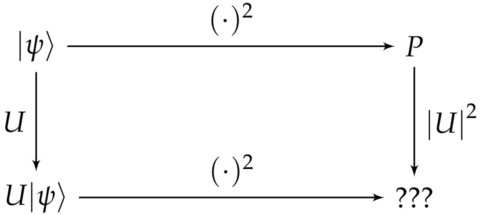
Theorem 1

If $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$ is quantical then

- $D(\psi_{ABE}) \geq D(P_{ABE})$ and
- $K(\psi_{ABE}) \geq K(P_{ABE})$

Proof idea

1. Classical protocol can be promoted to a quantum one
2. P_{ABE} remains quantical throughout the protocol



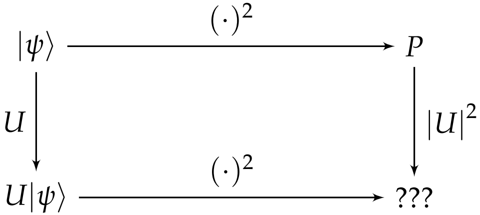
Theorem 1

If $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$ is quantical then

- $D(\psi_{ABE}) \geq D(P_{ABE})$ and
- $K(\psi_{ABE}) \geq K(P_{ABE})$

Proof idea

1. Classical protocol can be promoted to a quantum one
2. P_{ABE} remains quantical throughout the protocol
3. Entropic quantities for P_{ABE} and $|\psi\rangle_{ABE}$ agree



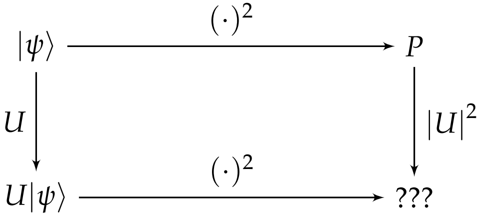
Theorem 1

If $|\psi\rangle_{ABE} = \sqrt{P_{ABE}}$ is quantical then

- $D(\psi_{ABE}) \geq D(P_{ABE})$ and
- $K(\psi_{ABE}) \geq K(P_{ABE})$

Proof idea

1. Classical protocol can be promoted to a quantum one
2. P_{ABE} remains quantical throughout the protocol
3. Entropic quantities for P_{ABE} and $|\psi\rangle_{ABE}$ agree
4. Promoted protocol achieves the same rate



Theorem 2

There exist quantical distributions P_{ABE} with $D(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$

Theorem 2

There exist quantical distributions P_{ABE} with $D(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$

Proof idea

- Choose P_{ABE} so that $\rho_{AB} := \mathrm{Tr}_E\big(|\psi\rangle\langle\psi|_{ABE}\big)$ is PT-invariant

Theorem 2

There exist quantical distributions P_{ABE} with $D(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$

Proof idea

- Choose P_{ABE} so that $\rho_{AB} := \mathrm{Tr}_E\big(|\psi\rangle\langle\psi|_{ABE}\big)$ is PT-invariant
- $\rho_{AB}^{\Gamma} = \rho_{AB} \succeq 0$, hence ρ_{AB} is PPT

Theorem 2

There exist quantical distributions P_{ABE} with $D(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$

Proof idea

- Choose P_{ABE} so that $\rho_{AB} := \mathrm{Tr}_E\big(|\psi\rangle\langle\psi|_{ABE}\big)$ is PT-invariant
- $\rho_{AB}^{\Gamma} = \rho_{AB} \succeq 0$, hence ρ_{AB} is PPT
- $D(P_{ABE}) = 0$, since $D(P_{ABE}) \leq D(\psi_{ABE}) = 0$

Theorem 2

There exist quantical distributions P_{ABE} with $D(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$

Proof idea

- Choose P_{ABE} so that $\rho_{AB} := \mathrm{Tr}_E\big(|\psi\rangle\langle\psi|_{ABE}\big)$ is PT-invariant
- $\rho_{AB}^{\Gamma} = \rho_{AB} \succeq 0$, hence ρ_{AB} is PPT
- $D(P_{ABE}) = 0$, since $D(P_{ABE}) \leq D(\psi_{ABE}) = 0$
- One-way distillable key:

$$K(P_{ABE}) \geq \max_{A \to X} \big[I(X;B) - I(X;E)\big]$$

Theorem 2

There exist quantical distributions P_{ABE} with $D(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$

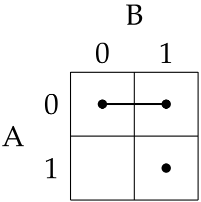
Proof idea

- Choose P_{ABE} so that $\rho_{AB} := \mathrm{Tr}_E\big(|\psi\rangle\langle\psi|_{ABE}\big)$ is PT-invariant
- $\rho_{AB}^{\Gamma} = \rho_{AB} \succeq 0$, hence ρ_{AB} is PPT
- $D(P_{ABE}) = 0$, since $D(P_{ABE}) \leq D(\psi_{ABE}) = 0$
- One-way distillable key:

$$K(P_{ABE}) \geq \max_{A \to X} \big[I(X;B) - I(X;E)\big]$$

- Choose $|X| = 2$ and do numerics

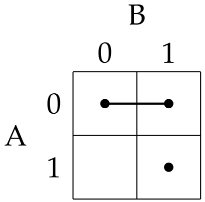
Recipe for quanticality and PT-invariance



$$\left(a|00\rangle_{AB} + b|01\rangle_{AB}\right)|x\rangle_E$$

$$+\, c|11\rangle_{AB} \;\; |y\rangle_E$$

Recipe for quanticality and PT-invariance

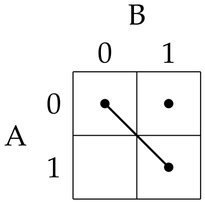


$$\big(a|00\rangle_{AB} + b|01\rangle_{AB}\big)\,|x\rangle_E$$
$$+\, c|11\rangle_{AB}\ \ |y\rangle_E$$

Quantical

- Union of disjoint cliques
- Each clique is “diagonal” (no repeated rows or columns)

Recipe for quanticality and PT-invariance



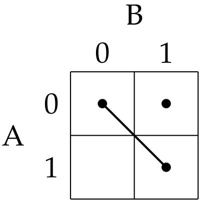
$$\big(a|00\rangle_{AB} + b|11\rangle_{AB}\big)\,|x\rangle_E$$

$$+\,c|01\rangle_{AB}\ \ |y\rangle_E$$

Quantical

- Union of disjoint cliques
- Each clique is "diagonal" (no repeated rows or columns)

Recipe for quanticality and PT-invariance



$$\left(a|00\rangle_{AB} + b|11\rangle_{AB}\right)|x\rangle_E$$
$$+\, c|01\rangle_{AB} \quad |y\rangle_E$$

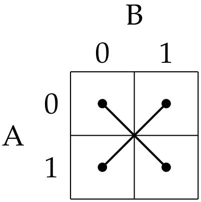
Quantical

- Union of disjoint cliques
- Each clique is “diagonal” (no repeated rows or columns)

PT-invariant

- Union of crosses
- Each cross has zero determinant

Recipe for quanticality and PT-invariance



$$\big(a|00\rangle_{AB} + b|11\rangle_{AB}\big)\,|x\rangle_E$$
$$+\,\big(c|01\rangle_{AB} + d|10\rangle_{AB}\big)\,|y\rangle_E$$

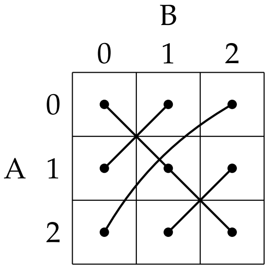
Quantical

- Union of disjoint cliques
- Each clique is “diagonal” (no repeated rows or columns)

PT-invariant

- Union of crosses
- Each cross has zero determinant

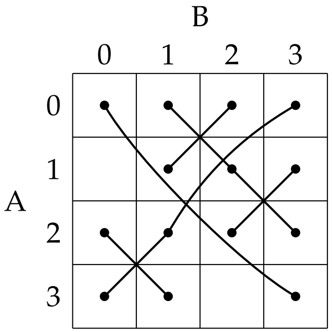
Example in 3×3



$$P_{AB} = \begin{pmatrix} 0.167184 & 0.171529 & 0.001243 \\ 0.089041 & 0.091355 & 0.017492 \\ 0.441714 & 0.017157 & 0.003285 \end{pmatrix}$$

$$D(P_{ABE}) = 0 \quad \text{but} \quad K(P_{ABE}) \geq 0.0057852$$

Example in 4×4

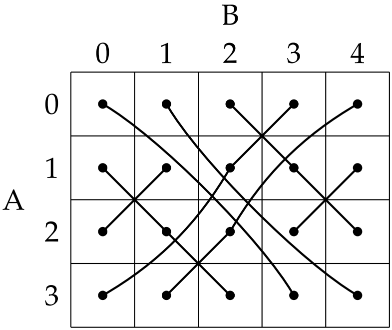


$$K(P_{ABE}) \geq 0.0293914$$

Better than [HPHH08]

$$K(P_{ABE}) \geq 0.0213399$$

Example in 4×5



$$K(P_{ABE}) \geq 0.0480494$$

Conclusions

Results

- New construction of private bound entanglement
- Adding noise can help in one-way classical key distillation

Conclusions

Results

- New construction of private bound entanglement
- Adding noise can help in one-way classical key distillation

Open questions

- How does our construction relate to [HHHO05]?
- Is the optimal protocol for distilling entanglement or key from a quantical state also quantical?

Conclusions

Results

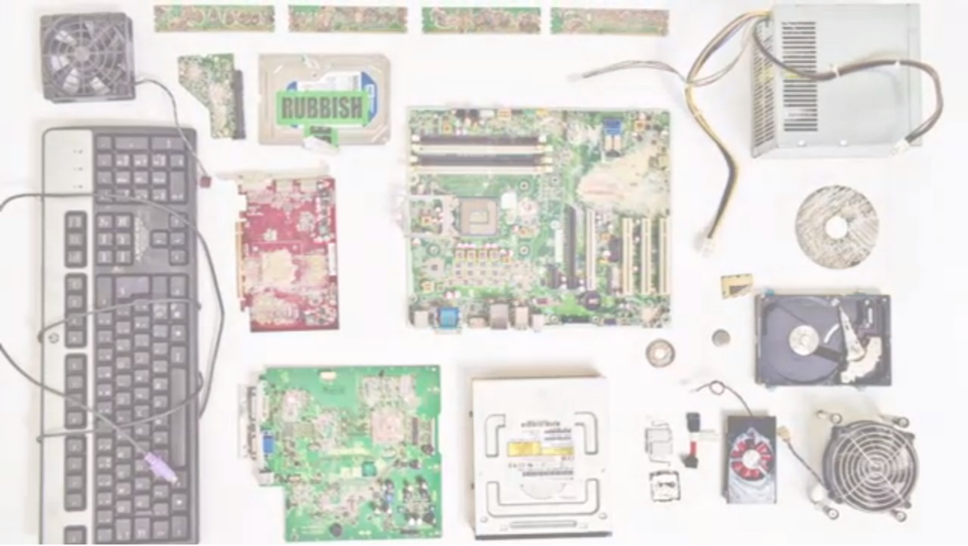
- New construction of private bound entanglement
- Adding noise can help in one-way classical key distillation

Open questions

- How does our construction relate to [HHHO05]?
- Is the optimal protocol for distilling entanglement or key from a quantical state also quantical?

Work in progress…

- Quantical mechanics and a classical analogue of superactivation (of the quantical capacity)



That’s it!

Image: destroyed Guardian computer with Snowden files

Bibliography I

[CEH+07] Matthias Christandl, Artur Ekert, Michał Horodecki, Paweł Horodecki, Jonathan Oppenheim, and Renato Renner.
Unifying classical and quantum key distillation.
In Salil P. Vadhan, editor, *Theory of Cryptography*, volume 4392 of *Lecture Notes in Computer Science*, pages 456–478. Springer, 2007.
arXiv:quant-ph/0608199,
doi:10.1007/978-3-540-70936-7_25.

[CP02] Daniel Collins and Sandu Popescu.
Classical analog of entanglement.
Phys. Rev. A, 65(3):032321, Feb 2002.
arXiv:quant-ph/0107082,doi:10.1103/PhysRevA.65.032321.

[HHHO05] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim.
Secure key from bound entanglement.
Phys. Rev. Lett., 94(16):160502, Apr 2005.
arXiv:quant-ph/0309110,
doi:10.1103/PhysRevLett.94.160502.

Bibliography II

[HPHH08] Karol Horodecki, Łukasz Pankowski, Michał Horodecki, and Paweł Horodecki.
Low-dimensional bound entanglement with one-way distillable cryptographic key.
Information Theory, IEEE Transactions on, 54(6):2621–2625, 2008.
arXiv:quant-ph/0506203, doi:10.1109/TIT.2008.921709.

[OSW05] Jonathan Oppenheim, Robert W. Spekkens, and Andreas Winter.
A classical analogue of negative information.
2005.
arXiv:quant-ph/0511247.

[PBR12] Matthew F. Pusey, Jonathan Barrett, and Terry Rudolph.
On the reality of the quantum state.
Nature Physics, 8(6):475–478, 2012.
arXiv:1111.3328, doi:10.1038/nphys2309.

[Spe07] Robert W. Spekkens.
Evidence for the epistemic view of quantum staappendices oftes: A toy theory.
Phys. Rev. A, 75(3):032110, Mar 2007.
arXiv:quant-ph/0401052, doi:10.1103/PhysRevA.75.032110.