Public Quantum Communication

Fernando GSL Brandão
Jonathan Oppenheim

arXiv:1004.3328
arXiv:1005.1975

University of Cambridge

Public quantum comunication

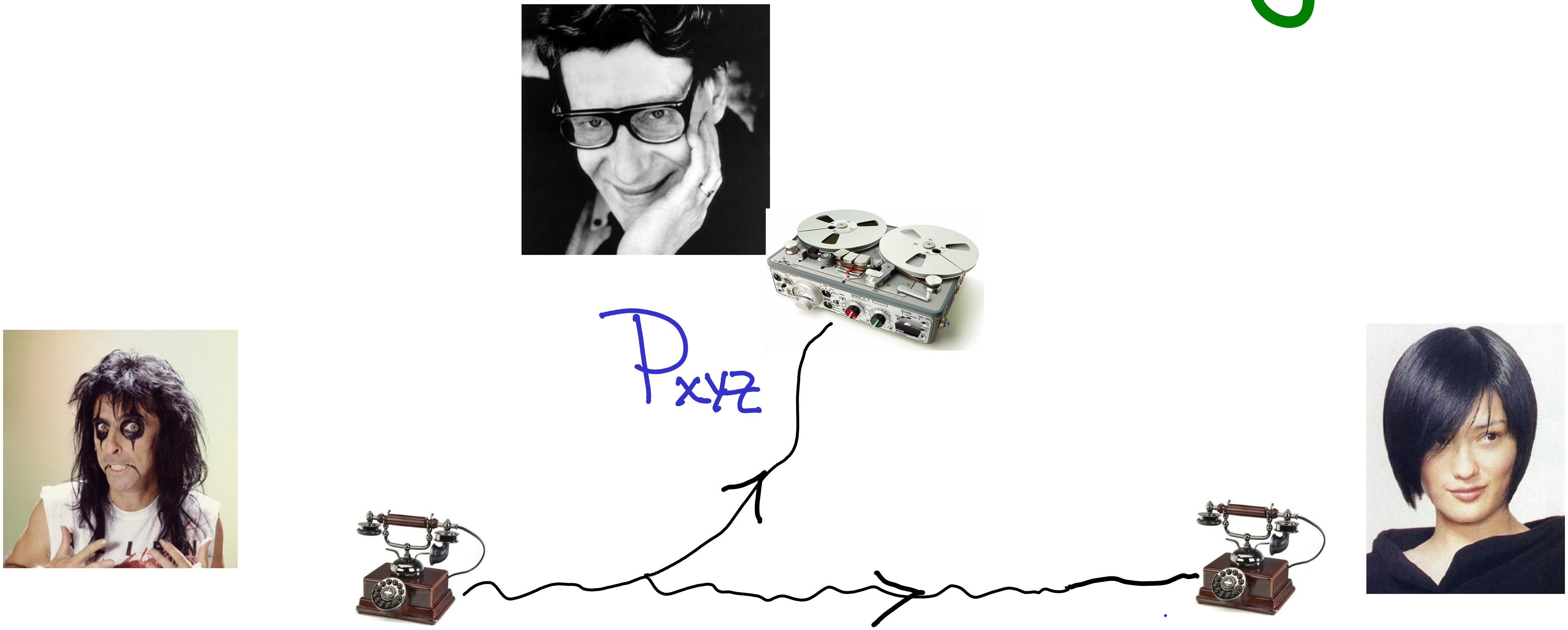
and the quantum one time pad

and superactivation

and mutual independence

and symmetric side-channels

Classical Privacy



Csiszar-Korner(78): The rate $C(P_{xyz})$ of sending encrypted messages w/ one way public communication

$$C(P_{xyz}) = \sup_{x \to v \to u} I(V:Y|U) - I(V:Z|U)$$

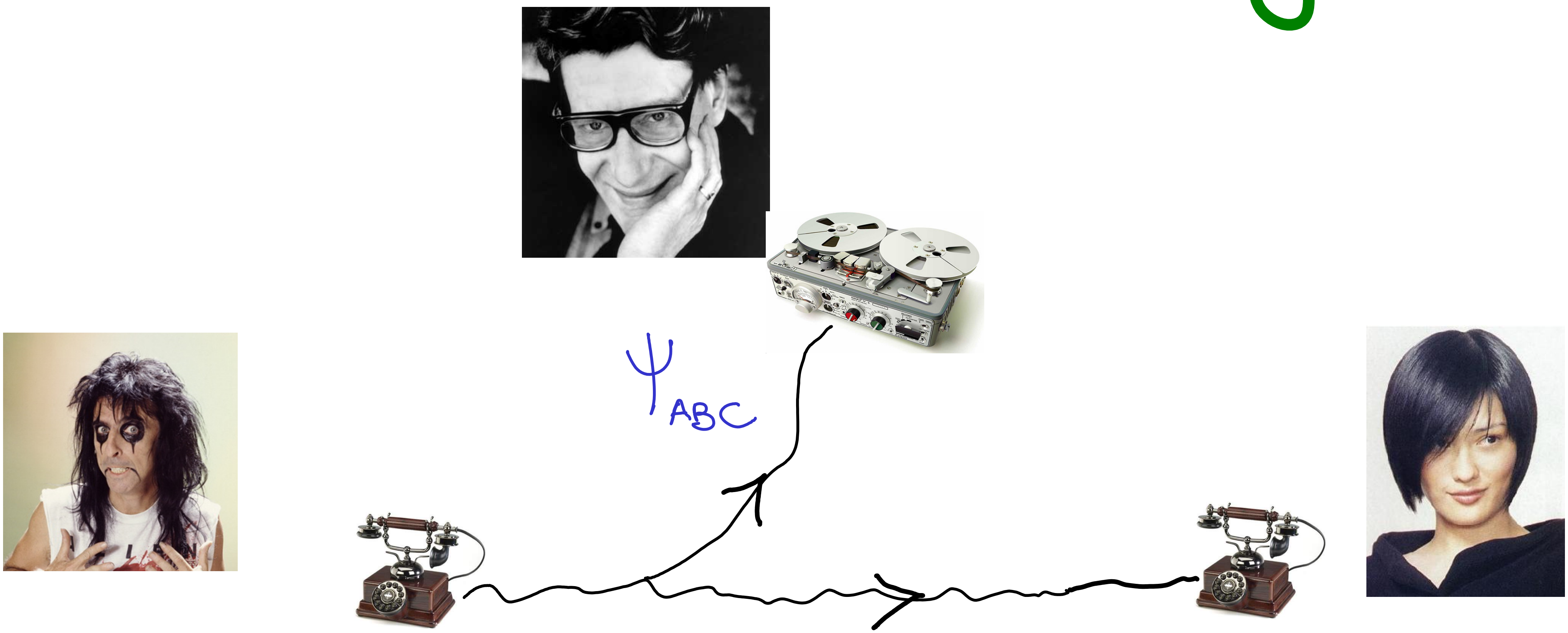
What is the quantum version?

entanglement theory?

quantum crypto?

Both are ugly!

Quantum Privacy



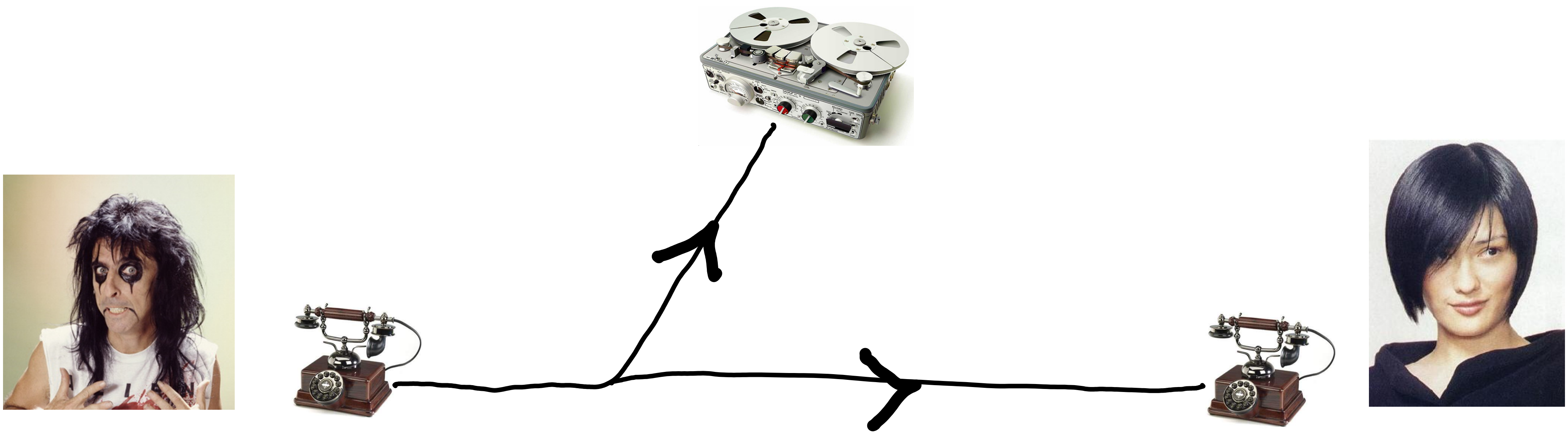
The rate $Q(\psi_{ABC})$ of sending encrypted states w/ one way public quantum communication:

$$Q(\psi_{ABC}) = \sup_{A \to a\alpha} \frac{1}{2}\left[I(a:B|\alpha) - I(a:E|\alpha) \right]$$

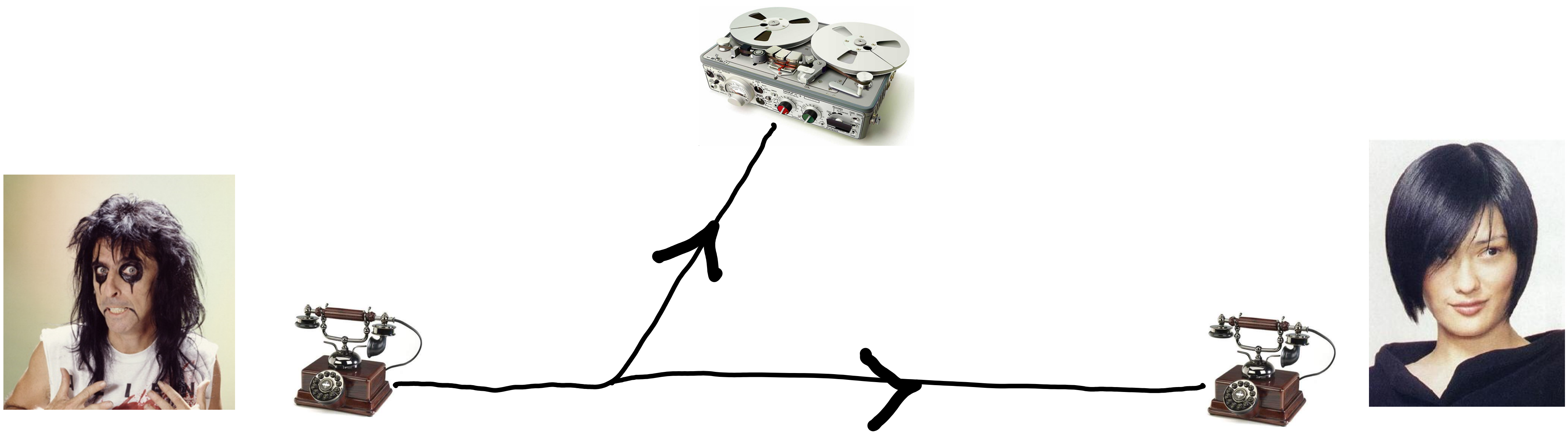
$Q(\psi_{ABE})$ is additive and single-letter

$$\cancel{Q = \lim_{n\to\infty} \frac{Q^{(1)}(\psi^{\otimes n})}{n}}$$

Classical	Quantum
probability distribution P_{XYZ}	quantum state ψ_{ABE}
	key K_{XY} (DW)
distill key K_{XY}	EPR pairs $\vert\psi^-_{AB}\rangle$ (LSD)
	send messages
send messages	send states (AMTW, BR, L)
public communication	classical communication



Public Quantum communication?



Public Quantum Communication?

No Cloning

Public Classical Communication

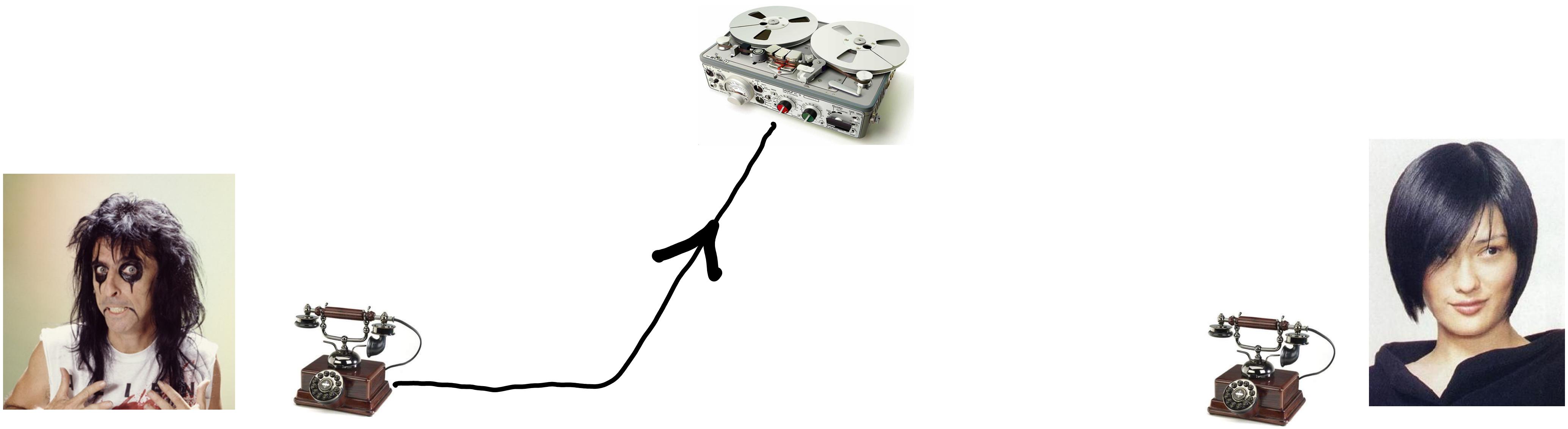
- Eve gets a copy of everything that's sent to Bob

Alternative Formulation

- Eve could intercept the messages sent to Bob

- Alice's messages are mapped symmetrically to Bob & Eve

Insecure quantum channel



If Eve intercepts Alice's quantum communication we demand security

Insecure quantum channel

If Bob recieves Alice's quantum communicatio
he can decode the message/state

Quantum one time pad

- arbitrary mixed state $\psi_{ABE}^{\otimes n}$
- forward insecure quantum communication (Alice to Bob, but Eve might intercept
- The probability that Eve learns the message can be made arbitrarily small if she intercepts.
- C : rate of sending private classical messages when no interception $= 2Q$
- Q: rate of sending private quantum states

Quantum one time pad

- In the case when ψ_{AB} is initially in a product state with Eve,

$$C(\psi_{AB}) = I(A:B)$$ Schumacher, Westmorland (06)

$$\boxed{Q(\psi_{ABE}) = \frac{1}{2} C(\psi_{ABE}) = \sup_{A \to a\alpha} \frac{1}{2}\left[I(a:B|\alpha) - I(a:E|\alpha) \right]}$$

- single letter!
- same form as classical result
- has made a previous appearance as the quantum capacity assisted by symmetric side channels (Smith, Smolin, Winter)

public quantum communication makes equal, different kinds of privacy

- entanglement
- mutual independence
- weak mutual independence

- $Q(\Psi_{ABE}) = Q_{ss} = I_{ind,ss}(\Psi_{ABE}) = W_{ind,ss}$

What does this have to do with mutual independence?

Key:

$K = \frac{1}{K}\sum |xx\rangle\langle xx|$

private
correlated (perfectly)
uniform
classical

mutual indepedence:

private
correlated

Kinds of private states

key	$\frac{1}{\lvert K \rvert} \sum \lvert xx \rangle\langle xx \rvert_{AB} \otimes \rho_E$
mutual independence I_{ind}	$\rho_{AB} \otimes \rho_E$ $\frac{1}{2} I(A:B)$ Horodecki, Oppenheim, Winter 09
weak mutual independence W_{ind}	$\rho_A \otimes \rho_E$ $\frac{1}{2} I(A:B)$

Assistance by channel Λ

I_Λ, W_Λ assisted by Λ

e.g. Λ_{ss}, the symmetric side channel

$$\rho_{AB} = \mathrm{tr}_E U_{BE} \Psi_{AB} |0\rangle_E\langle 0| U^\dagger_{BE}$$

$$\rho_{AE} = \mathrm{tr}_B U_{BE} \Psi_{AB} |0\rangle_E\langle 0| U^\dagger_{BE}$$

$$\rho_{AB} = \rho_{AE}$$

Eg erasure channel: $p = 1/2$ $\mathbb{1}_B$, Eve gets erasure flag

$p = 1/2$ Bob gets erasure flag, $\mathbb{1}_E$

Consider I_{ss}, the mutual independence assisted by symmetric side channels.

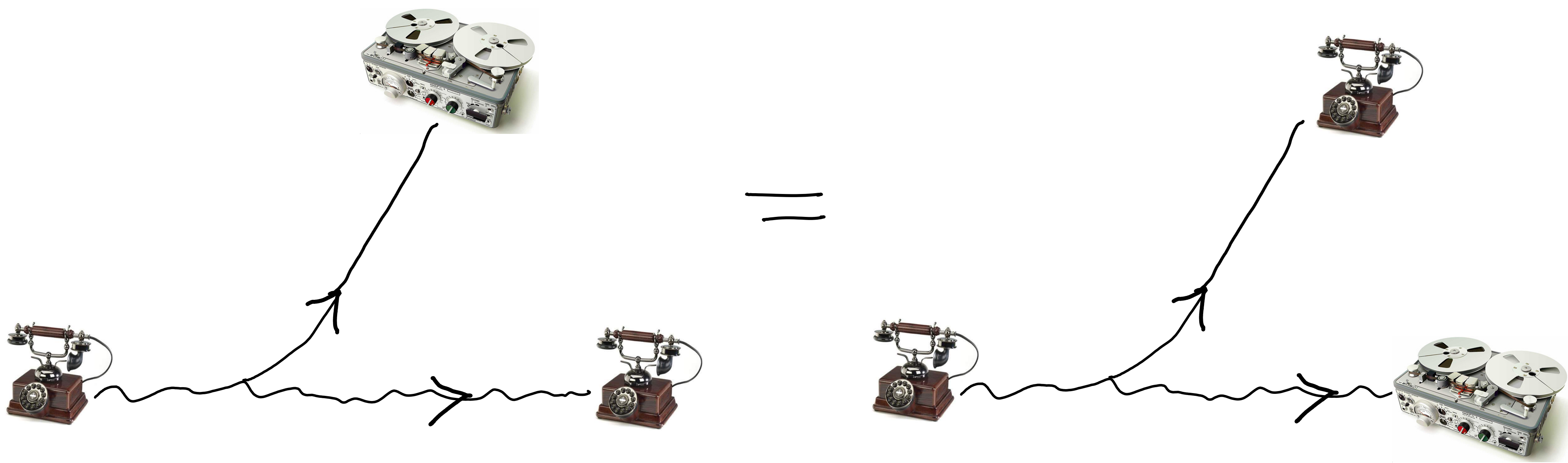
$$I_{ss}(\psi_{AB}) = \sup_{A \to a\alpha} \frac{1}{2}\left[I(a:B|\alpha) - I(a:E|\alpha)\right]$$

First, assume it and show $\frac{1}{2}C = I_{ss}$

$\frac{1}{2}C \geq I_{ss}$

Imagine Alice and Bob had a symmetric side-channel. Then they could use it to make themselves product with Eve, and retain I_{ss} bits of mutual information. They could then use the Schumacher-Westmorland protocol, to convert this mutual information to key.

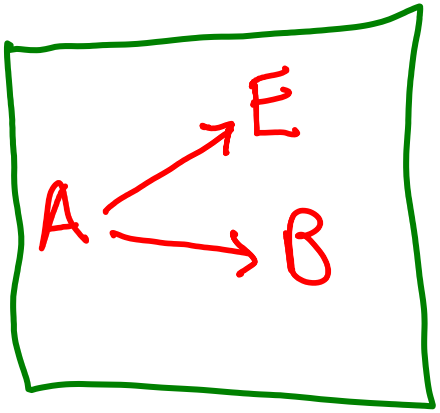
But they don't have a symmetric side channel!



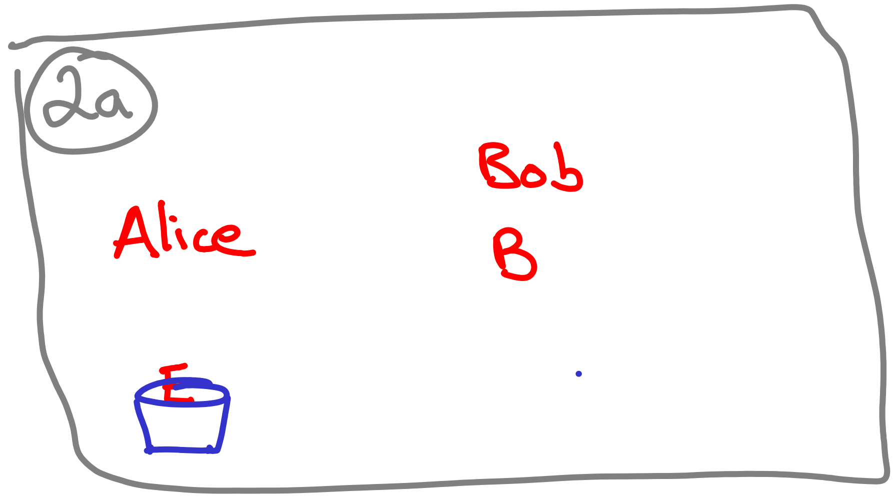
also smells like public quantum communication

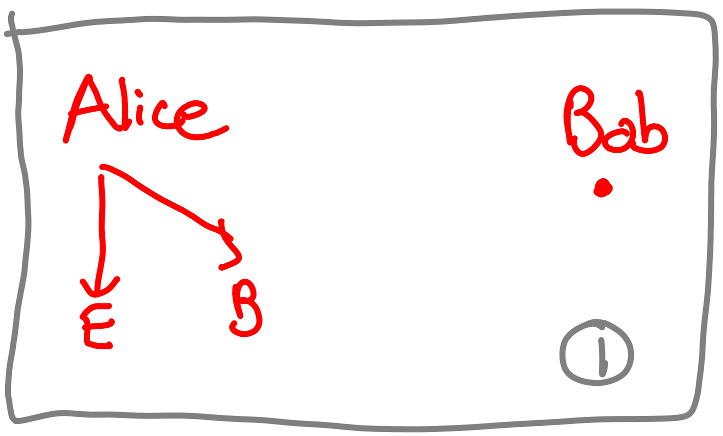
Indeed the insecure quantum channel is only ever used to simulate a symmetric side channel.

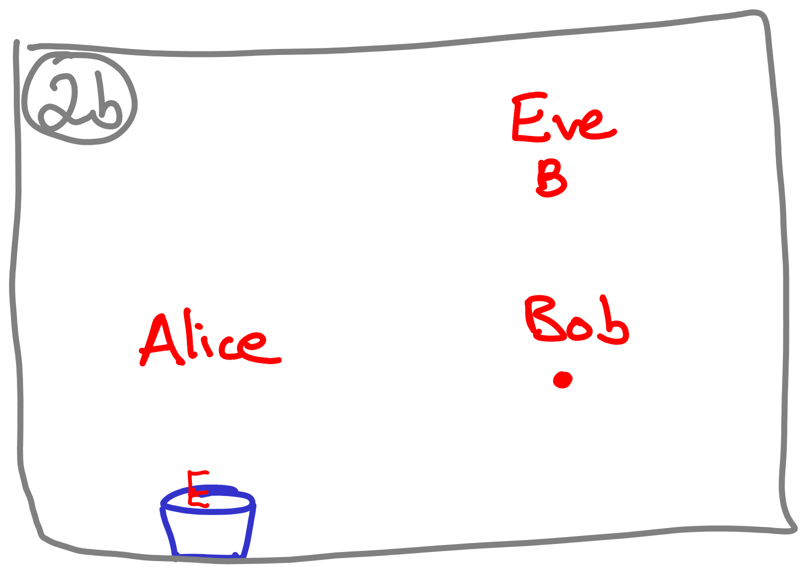
$$\frac{1}{2} C(\psi_{ABC}) \geq I_{ss}(\psi_{ABC})$$



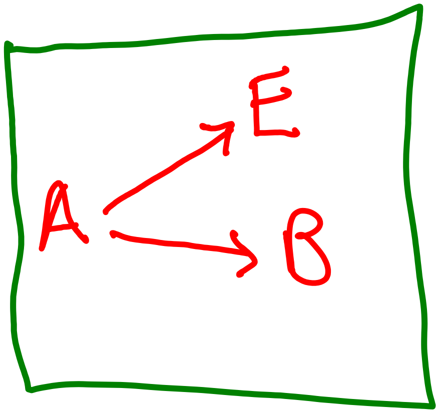
Simulating Λ_{ss}



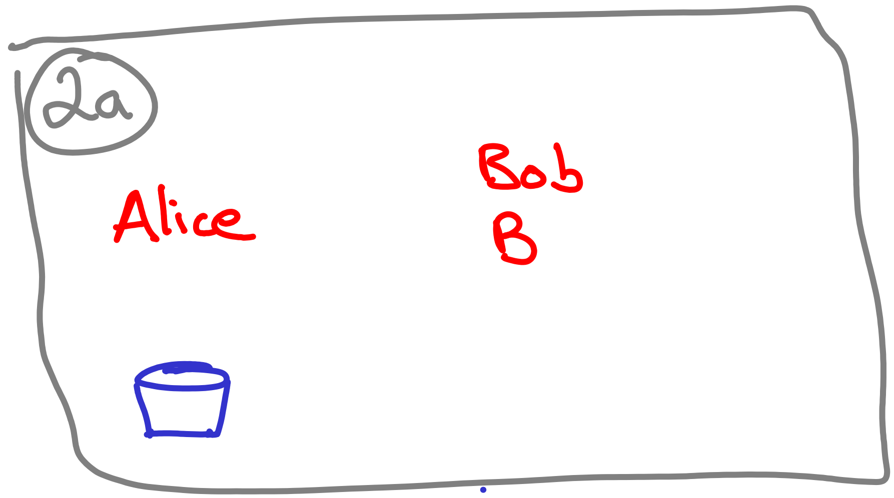


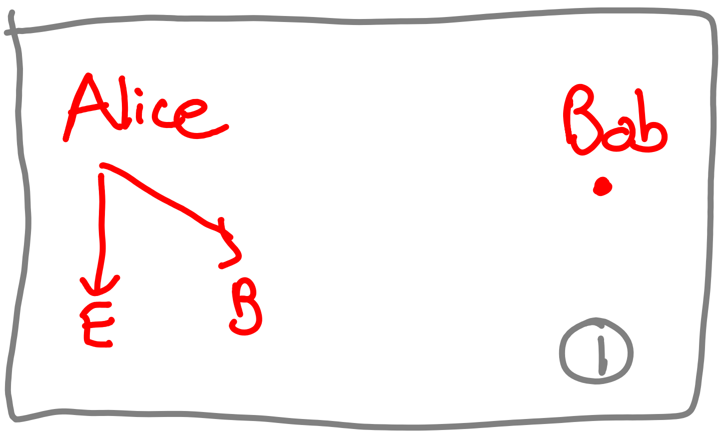


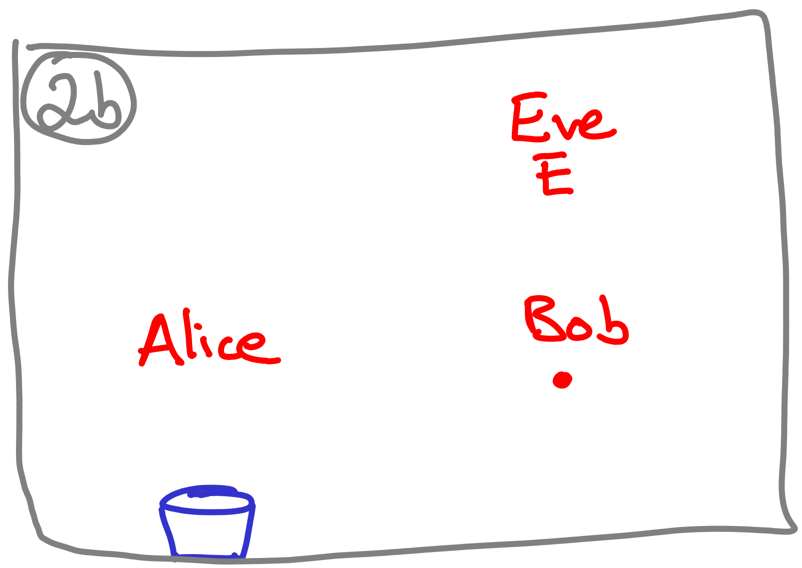
$$\frac{1}{2}C(\psi_{ABC}) \geq I_{ss}(\psi_{ABC})$$



Simulating Λ_{ss}







The symmetric-side channel is equivalent to an insecure quantum channel!

i.e. in the optimal protocol the insecure quantum channel is only used to simulate a symmetric side channel

$$\frac{1}{2} C(\psi_{ABC}) \leq I_{ss}(\psi_{ABC})$$

In the optimal protocol, Alice applies $\mathcal{E}_{k,n} \otimes I_{BE}$ with probability $p_{k,n}$, generating

$$\{ p_{k,n}, \mathcal{E}_{k,n}(\psi_{ABE}) \}$$

$$C(\psi_{AB}) = \lim_{n \to \infty} \frac{1}{n} \chi(p_{k,n}, \mathcal{E}_{k,n} \otimes \mathbb{1}_B(\psi_{AB}))$$

$$\rho^n_{KABE} := \sum_k p_{k,n} |k\rangle_K\langle k| \otimes \mathcal{E}_{k,n} \otimes \mathbb{1}_{BE}(\psi_{ABE})$$

$$I_{ss} \geq \frac{1}{2}[I(k:B\alpha)_\rho - I(k:E\alpha)]$$

$$\simeq \frac{1}{2} C(\psi_{ABE})$$

It remains to prove the formula for I_{ss}. In fact for ψ_{ABE} pure

$I_{ss} = W_{ss} = D_{ss}$ (distillable entanglement w/ Λ_{ss})

pf] Clearly $D_{ss} \le I_{ss} \le W_{ss}$

We now show $D_{ss} \ge W_{ss}$

Imagine the optimal protocol which extracts weak mutual independence. In the final step, after discarding α, the state $\phi^n_{a\alpha:B:E}$ is

$$\lim_{n\to\infty} \| \phi^n_{a:E} - \phi^n_a \otimes \phi^n_E \|_1 = 0$$

$$W_{ss} = \lim_{n\to\infty} \inf \frac{1}{2n} I(a,B)_\phi$$

Instead of discarding α, send it down erasure channel (like sending shield)

$$\frac{1}{\sqrt{2}}\phi_{a:B\alpha:E}\otimes e_{E'}+\frac{1}{\sqrt{2}}\phi_{a:B:E\alpha}\otimes e_{B'}$$

$$\boxed{\text{recall} \\ I(a\rangle B):=S(B)-S(aB)}$$

$$D_{ss}\geq\lim_{n\to\infty}\tfrac{1}{2}I(a\rangle B)+\tfrac{1}{2}I(a\rangle B\alpha)$$

$$=\lim_{n\to\infty}\tfrac{1}{2}I(a\rangle B)-\tfrac{1}{2}I(a\rangle E)$$

$$=\lim_{n\to\infty}\tfrac{1}{2}I(a\rangle B)+\tfrac{1}{2}S(a)$$

$$=\lim_{n\to\infty}\tfrac{1}{2}I(a:B)$$

$$=W_{ss}$$

$$D_{ss}(\psi_{ABE}) = I_{ss}(\psi_{ABE}) = W_{ss}(\psi_{ABE})$$

smells like classical case, where public communication also makes these equal

$$D_E(\psi_{ABE}) = I_E(\psi_{ABE}) = W_E(\psi_{ABE})$$

For all we know $D_{ss} = D_E = W_\phi$

with W_ϕ being the weak mutual independence without communication

Conjecture: $D_{ss} > K_{ss}$

Superactivation

$0 + 0 = 1$

(Smith, Yard, Science 09)

2 zero capacity channels

symmetric side channel

private ppt channel Horodecki$^{\otimes 3}$, Oppenheim (05)

Combine to give positive capacity!

What is the most general state which gives a private key upon measurement?

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$$

shield

$$\gamma_{ABA'B'} = U \, \Phi^+_{AB} \otimes \rho_{A'B'} \, U^\dagger$$

key

$$U = |0\rangle_A\langle 0| \otimes \mathbb{1}_{A'B'} + |1\rangle_A\langle 1| \otimes V_{A'B'}$$

Horodecki$^{\otimes 3}$, Oppenheim (05)

There exist $\gamma_{ABA'B'}$ which are nondistillable

$$\text{Key} \neq E_D$$

Use one zero capacity channel to create $\gamma_{ABA'B'}$

Send shield down erasure channel

J.O. Science, 2008

A connection between privacy and distillable entanglement?

Yes, in a relaxed sense!
The symmetric side channel allows for conversion of noisy privacy (I, W) into E.P.R. pairs (error correction)

When looking for superactivation protocols, it suffices to focus on the more indescriminate task of making Alice's state product with the environment.

Summary

- A single letter formula for the quantum one time pad in the presence of an eavesdropper

- As in the classical case, public quantum communication makes the theory simpler, more elegant
  - insecure quantum channel
  - symmetric channel
    (operational interpretation)

- superactivation:
  conversion of weak mutual independence into E.P.R. pairs
  by a public quantum channel

Open questions

$$\begin{aligned} & > D_E \\ W_{ss} & > W_\phi \quad ? \\ & > K_{ss} \end{aligned}$$

perhaps communication is only needed for correcting errors.

Is the erasure channel the best symmetric channel for distillation

Can we upper bound the size of the register that goes into the symmetric channel

Are there states with $W > 0$, $K = 0$

Other channels Λ ?

$$G_C = \sup_{\rho \in C} \frac{1}{2}\left[I(a:B|\alpha) - I(a:E|\tilde{\alpha}) \right]$$

Eg mutal independence

- I° w/ no classical communication

(important for Shannon theory)

- can even consider classical example

	AB	E
$p = 1-\varepsilon$	00	k
	11	
$p = \epsilon$	01	$\bar{k}$
	11	

$$\longrightarrow \quad \sigma_{AB} \otimes \rho_E$$

$$I(A:B) > \delta$$

Thank you for
your attention