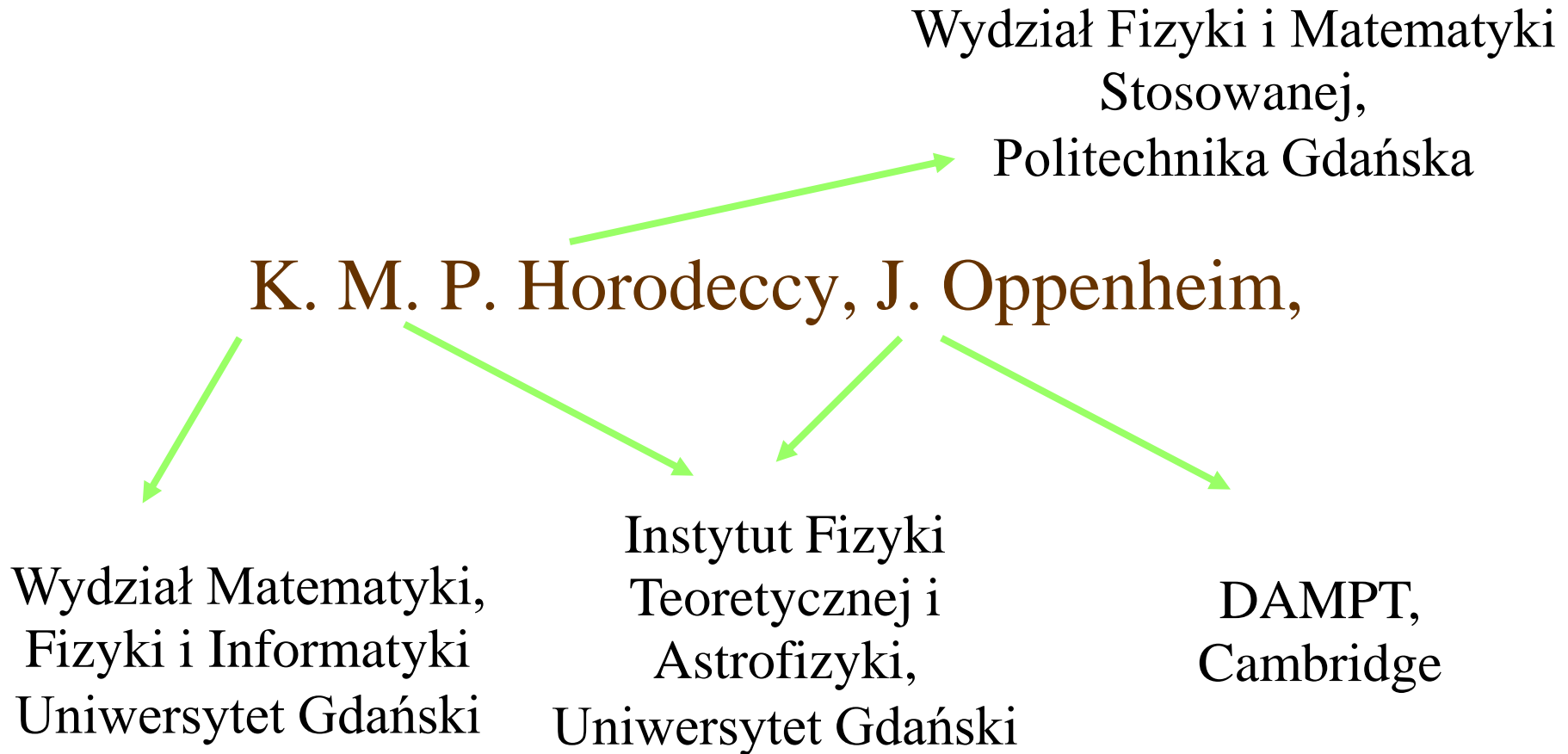


Private key from bound entanglement



Supported by Polish Committee for Scientific Research
and EU grants RESQ, QUPRODIS, PROSECCO

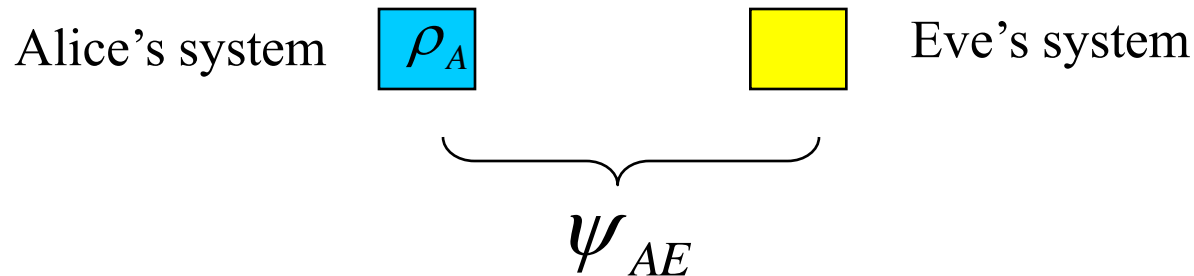
Quant-ph/0309110

Some history

- 1) First entanglement distillation protocols were taken from crypto (BDSW96, BBPSSW96)
- 2) Does there exist analogue of bound entanglement in classical crypto? Is drawing key equivalent to drawing singlets? Pushed forward in (Gisin, Wolf 2000 and subsequent works by Gisin, Acin et al.
- 3) For one-way protocols: YES drawing key is drawing singlets
Devetak, Winter (impact on communication)
- 4) in general, drawing key is not drawing singlets (present work, H³O)

(from Jens and Maciek talks) A connected questions: under Gaussian operations we cannot draw singlets, but can we draw key?

Secure random bit from quantum system and measurement



Suppose Alice can make measurements on her system.

QUESTION: what state ρ_A allows for obtaining private random bit?

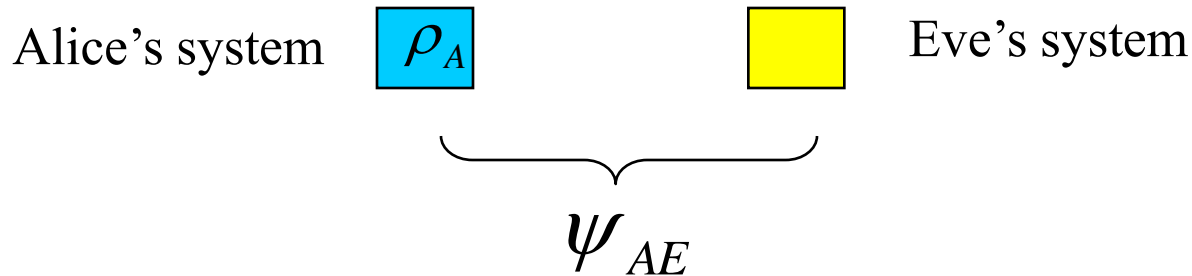
ANSWER 1: if ρ_A is **PURE STATE**, then Alice can get private random bit.

Indeed, since it is pure state, Eve is uncorrelated with outcomes of any Alice's measurements. To get random bit, Alice measures in complementary basis.

If for example $\rho_A = |0\rangle\langle 0|$ then Alice measures in basis

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Secure random bit from Alice's measurement on a system in MIXED STATE



If $\rho_A = \frac{I}{2} = \frac{1}{2} (|0\rangle\langle 0| + |1\rangle\langle 1|)$

then $\psi_{AE} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|e_1\rangle|e_1\rangle^* + |e_2\rangle|e_2\rangle^*)$

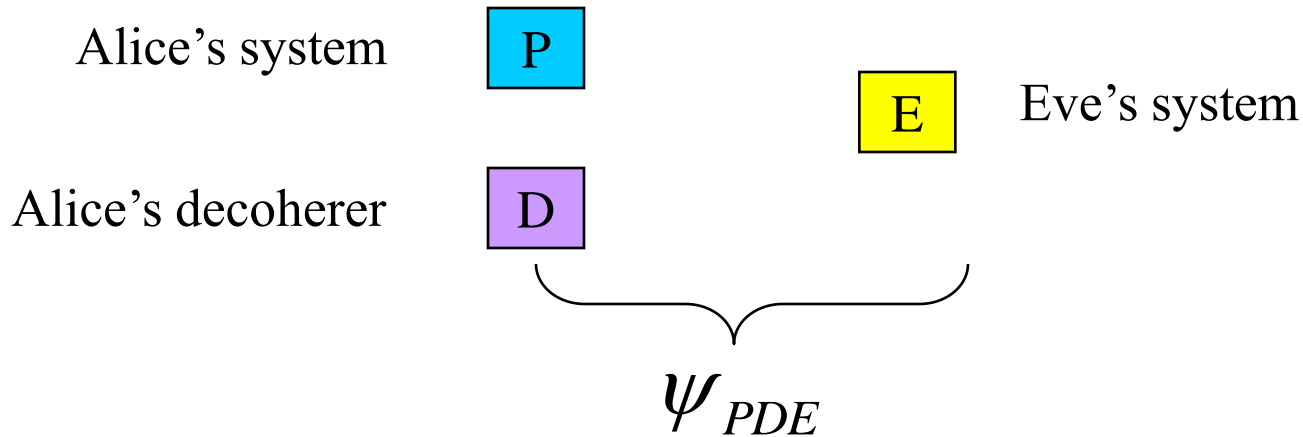
So that when Alice measures in any chosen basis

$$\{|e_1\rangle, |e_2\rangle\}$$

Eve will know the outcome.

PROBLEM: Eve is COHERENTLY correlated with Alice's system, hence she has knowledge about ANY basis

Secure random bit from Alice's measurement on a system in MIXED STATE



EXAMPLE:

$$\Psi_{PDE} = \frac{1}{\sqrt{2}} (|0\rangle_P |0\rangle_D |0\rangle_E + |1\rangle_P |1\rangle_D |1\rangle_E)$$

Reduced density matrix of Eve and Alice's P system:

$$\rho_{PE} = \frac{1}{\sqrt{2}} (|0\rangle_P \langle 0| \otimes |0\rangle_E \langle 0| + |1\rangle_P \langle 1| \otimes |1\rangle_E \langle 1|)$$

is CLASSICALLY correlated, due to decoherence caused by decoherer D.

Thus, Eve will have no knowledge about outcomes of Alice measurement in basis $\{|+\rangle, |-\rangle\}$

Some triviality

Alice state of composite system $\boxed{\text{P}}$ + $\boxed{\text{D}}$

is now of the form:

$$\rho_{PD} = \frac{1}{\sqrt{2}} (|0\rangle_P \langle 0| \otimes |0\rangle_D \langle 0| + |1\rangle_P \langle 1| \otimes |1\rangle_D \langle 1|)$$

Then Alice can apply CNOT to undo the correlations, obtaining state:

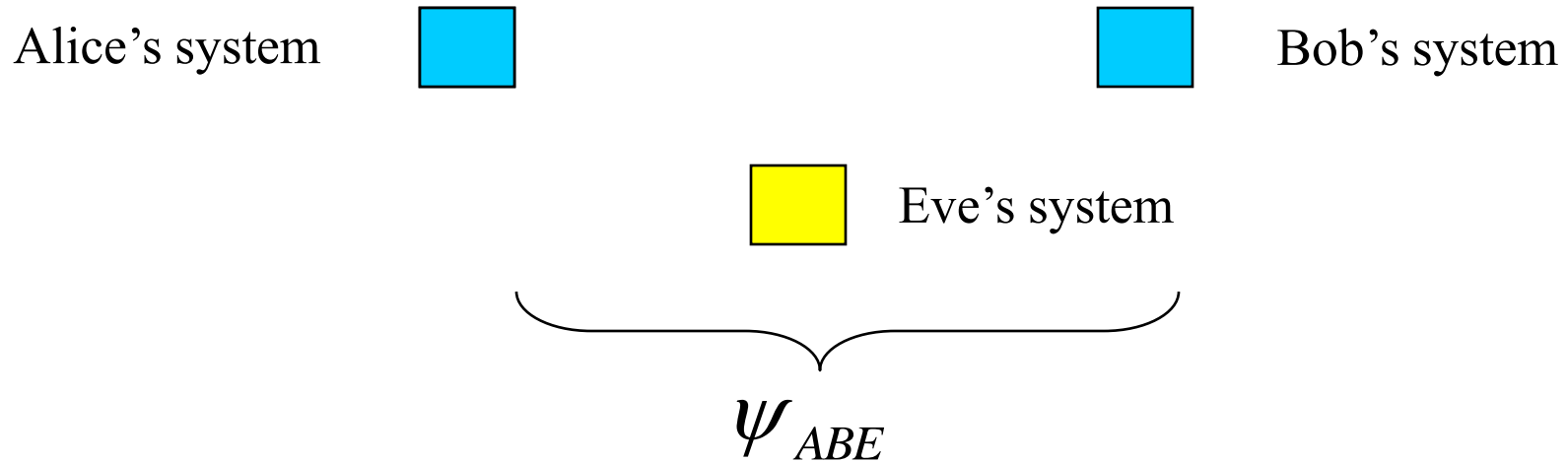
$$\rho_{PD} = \frac{1}{2} (|0\rangle_P \langle 0| + |1\rangle_P \langle 1|) \otimes |0\rangle_D \langle 0|$$

She then removes system P, and her Decoherer is now in pure state

$$\rho_D = |0\rangle_D \langle 0|$$

THUS: PRIVACY OF RANDOM BITS IS EQUIVALENT TO PURITY.

Private KEY out of local measurement on COMPOSITE system



PURE STATE CASE

$$\rho_{AB} = |\psi\rangle_{AB}\langle\psi|$$

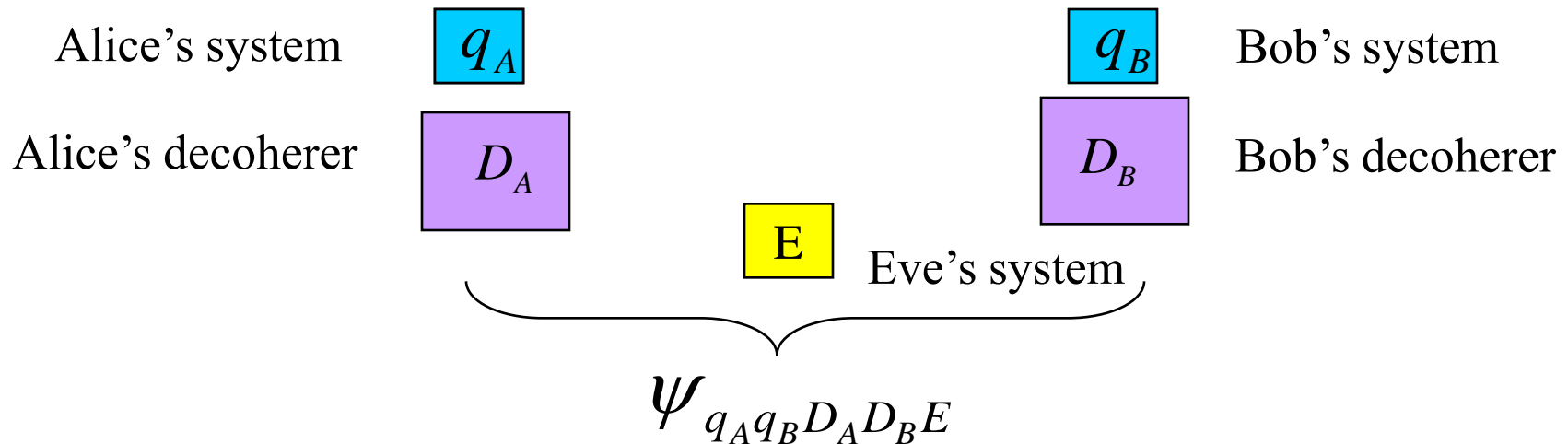
with

$$\psi_{AB} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

KEY = PRIVACY + CORRELATIONS

- 1) PURITY of ρ_{AB} implies PRIVACY of key, because it implies that Eve is completely uncorrelated with AB
- 2) SINGLET FORM implies maximal CORRELATIONS of key

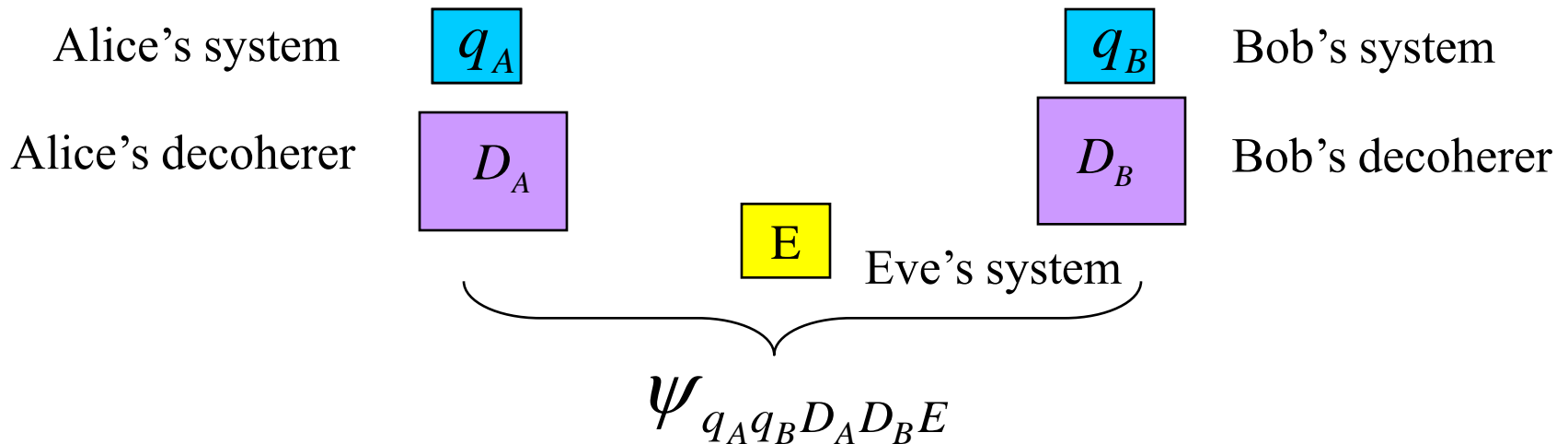
Private KEY from composite system: MIXED STATE



To produce a mixed state, but retain the possibility of getting key, decoherer should:

- 1) decohere in a basis **COMPLEMENTARY** to the basis in which Alice and Bob will measure (this destroys **PURITY**, but retains **PRIVACY**)
- 2) the decohered basis should be chosen in such a way, that after decoherence, there are **CORRELATIONS** in basis in which Alice and Bob measure, i.e. correlations 00 vs 11.

Private KEY from composite system: MIXED STATE



Such a good basis, to decohere in is Bell basis, if applied e.g. to state $|11\rangle$

EXAMPLE:

$$\rho_{q_A q_B D_A D_B} = \frac{1}{2} P_{\psi_+}^{q_A q_B} \otimes P_{\xi}^{D_A D_B} + \frac{1}{2} P_{\psi_-}^{q_A q_B} \otimes P_{\tilde{\xi}}^{D_A D_B}$$

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

and $\xi, \tilde{\xi}$ are “pointer” states (or FLAG states).

Perfect decoherence: if flag states are orthogonal $\xi \perp \tilde{\xi}$

Perfect decoherence (=orthogonality of flags) assures perfect security

Alice and Bob state:

$$\rho_{q_A q_B D_A D_B} = \frac{1}{2} P_{\psi_+}^{q_A q_B} \otimes P_{\xi}^{D_A D_B} + \frac{1}{2} P_{\psi_-}^{q_A q_B} \otimes P_{\tilde{\xi}}^{D_A D_B}$$

Total Alice, Bob

and Eve state:

$$\psi_{q_A q_B D_A D_B E} = \frac{1}{\sqrt{2}} (|\psi_+\rangle_{q_A q_B} |\xi\rangle_{D_A D_B} |0\rangle_E + |\psi_-\rangle_{q_A q_B} |\tilde{\xi}\rangle_{D_A D_B} |1\rangle_E)$$

If flags are orthogonal, i.e. $\xi \perp \tilde{\xi}$ then the state of systems ABE reads:

$$\rho_{q_A q_B E} = \frac{1}{2} P_{\psi_+}^{q_A q_B} \otimes |0\rangle_E \langle 0| + \frac{1}{2} P_{\psi_-}^{q_A q_B} \otimes |1\rangle_E \langle 1|$$

So that Eve knows perfectly, whether Alice and Bob share ψ_+ or ψ_-

but whether Alice and Bob get 00 or 11 is for her completely unknown

Eve is CLASSICALLY CORRELATED with ψ_+ and ψ_-

Flags are the same: no privacy

Total Alice, Bob
and Eve state

$$\psi_{q_A q_B D_A D_B E} = \frac{1}{\sqrt{2}} (|\psi_+\rangle_{q_A q_B} |\xi\rangle_{D_A D_B} |0\rangle_E + |\psi_-\rangle_{q_A q_B} |\tilde{\xi}\rangle_{D_A D_B} |1\rangle_E)$$

When flags are the same, i.e. $|\xi\rangle = |\tilde{\xi}\rangle$ then

$$\psi_{q_A q_B D_A D_B E} = \frac{1}{\sqrt{2}} (|\psi_+\rangle_{q_A q_B} |0\rangle_E + |\psi_-\rangle_{q_A q_B} |1\rangle_E) |\xi\rangle_{D_A D_B}$$

The state of systems ABE (key-Eve) is PURE and can be written as :

$$\psi_{q_A q_B E} = \frac{1}{\sqrt{2}} (|00\rangle_{q_A q_B} |+\rangle_E + |11\rangle_{q_A q_B} |-\rangle_E)$$

The less orthogonal are flags, the more Eve is QUANTUMLY CORRELATED with system $q_A q_B$.

Some triviality

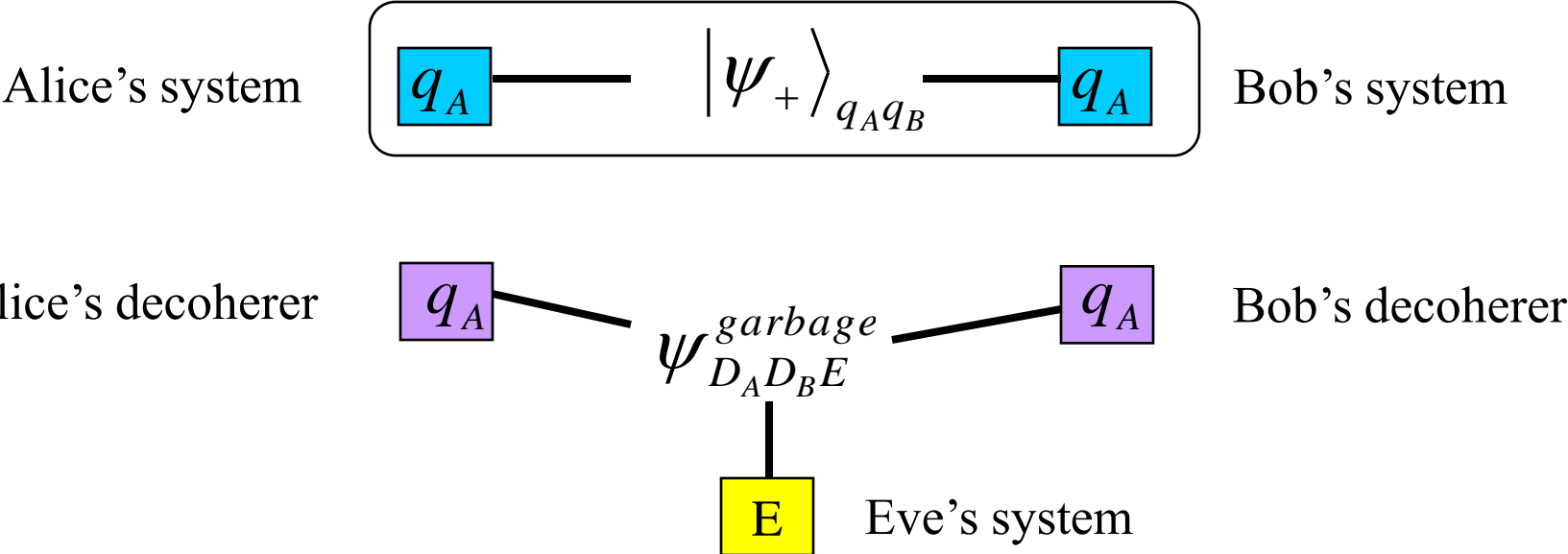
Consider state with orthogonal flags (full privacy):

$$\rho_{q_A q_B D_A D_B} = \frac{1}{2} P_{\psi_+}^{q_A q_B} \otimes P_{\xi}^{D_A D_B} + \frac{1}{2} P_{\psi_-}^{q_A q_B} \otimes P_{\tilde{\xi}}^{D_A D_B}$$

Any two pure orthogonal states can be distinguished by LOCC Hardy, Walgate, Vedral, ?

Alice and Bob distinguish between flags, and conditionally rotate singlet, obtaining state:

$$\rho_{q_A q_B D_A D_B} = |\psi_+\rangle_{q_A q_B} \langle \psi_+| \otimes \rho_{D_A D_B}^{garbage}$$



Mixed flags

$$\rho_{q_A q_B D_A D_B} = \frac{1}{2} P_{\psi_+}^{q_A q_B} \otimes \rho_+^{D_A D_B} + \frac{1}{2} P_{\psi_-}^{q_A q_B} \otimes \rho_-^{D_A D_B}$$

Privacy condition: the key obtained from measuring qubits AB in standard basis is perfectly secure, iff flags are orthogonal:

$$\rho_+^{D_A D_B} \perp \rho_-^{D_A D_B} \text{ or equivalently } \text{Tr} \rho_+^{D_A D_B} \rho_-^{D_A D_B} = 0$$

$$\rho_{q_A q_B D_A D_B} = \frac{1}{4} \begin{bmatrix} \rho_+ + \rho_- & 0 & 0 & \rho_+ - \rho_- \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \rho_+ - \rho_- & 0 & 0 & \rho_+ + \rho_- \end{bmatrix}$$

Take trace norm of blocks, you obtain singlet!

$$\frac{1}{4} \begin{bmatrix} \text{Tr}(\rho_+ + \rho_-) & 0 & 0 & \text{Tr}|\rho_+ - \rho_-| \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \text{Tr}|\rho_+ - \rho_-| & 0 & 0 & \text{Tr}(\rho_+ + \rho_-) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = |\psi_+\rangle\langle\psi_+|$$

Nontrivial case: flags that are badly distinguishable by LOCC

There exist states which are globally orthogonal, but exhibit arbitrary low probability of success of distinguishing by LOCC

(DiVincenzo, Terhal, Leung, and Eggeling and Werner)

$$\rho_{q_A q_B D_A D_B} = p P_{\psi_+}^{q_A q_B} \otimes \rho_+^{D_A D_B} + (1-p) P_{\psi_-}^{q_A q_B} \otimes \rho_-^{D_A D_B}$$

We take: $p = \frac{d-1}{2d}$, $\rho_+ = \rho_{SYM}$, $\rho_- = \rho_{ANTY}$

The state has at least one bit of key: $K_D \geq 1$

QUESTION: what about distillable entanglement E_D ?

We can use bound for distillable entanglement (Werner1998, HHH2000)

$$E_D(\rho) \leq E_N(\rho) = \log \left\| \rho^\Gamma \right\|_{\text{Tr}} \quad \text{where } \Gamma \text{ is partial transpose}$$

Nontrivial case: flags that are badly disintguishable by LOCC

$$\rho_{q_A q_B D_A D_B} = \frac{1}{2} \begin{bmatrix} p\rho_{SYM} + q\rho_{ANTY} & 0 & 0 & p\rho_{SYM} - q\rho_{ANTY} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ p\rho_{SYM} - q\rho_{ANTY} & 0 & 0 & p\rho_{SYM} + q\rho_{ANTY} \end{bmatrix}$$

Partially transposed state:

$$\rho_{q_A q_B D_A D_B}^\Gamma = \frac{1}{2} \begin{bmatrix} p\rho_{SYM} + q\rho_{ANTY} & 0 & 0 & 0 \\ 0 & 0 & p\rho_{SYM}^\Gamma - q\rho_{ANTY}^\Gamma & 0 \\ 0 & p\rho_{SYM}^\Gamma - q\rho_{ANTY}^\Gamma & 0 & 0 \\ 0 & 0 & 0 & p\rho_{SYM} + q\rho_{ANTY} \end{bmatrix}$$

$$E_N = \log(1 + 2\|p\rho^\Gamma - q\rho^\Gamma\|_{Tr}) = \log(1 + \frac{1}{d}) \Rightarrow$$

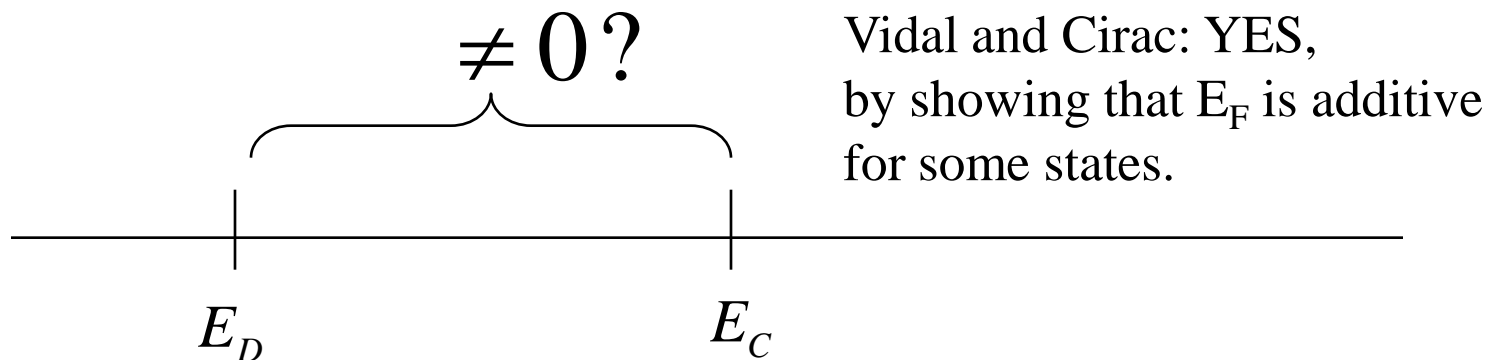
$$E_D \leq \log(1 + \frac{1}{d})$$

$$E_K \geq 1$$

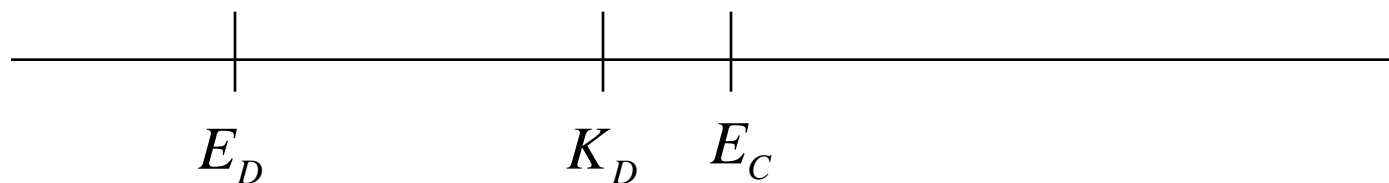
How this connects with LOCC
distinguishability”?

$$p_{success}(\rho_1, \rho_2) \leq \frac{1}{2} + \frac{1}{4} \|p\rho_1^\Gamma - q\rho_2^\Gamma\| = \frac{1}{2} + \frac{1}{2d}$$

By-product: new technique of providing states with entanglement cost strictly greater than distillable entanglement



Our technique: provide gap between E_D and K_D



States with perfect key: p-bits

Theorem: qqDD state is a p-bit i.e. it has perfect key on qq iff it is of the form

$$\gamma = U \psi_+^{q_A q_B} \otimes \rho_{D_A D_B} U^*$$

where

$$U = \sum_{ij} |ij\rangle\langle ij| \otimes U_{ij}$$

$$\gamma_{q_A q_B D_A D_B E} = \frac{1}{2} \begin{bmatrix} U_{00} \rho_{D_A D_B} U_{00}^* & 0 & 0 & U_{00} \rho_{D_A D_B} U_{11}^* \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ U_{11} \rho_{D_A D_B} U_{00}^* & 0 & 0 & U_{11} \rho_{D_A D_B} U_{11}^* \end{bmatrix}$$

Proof: directly, by looking at the Alice, Bob, Eve total pure state

$$\psi_{q_A q_B D_A D_B E} = \frac{1}{\sqrt{2}} (|00\rangle_{q_A q_B} |\varphi_0\rangle_{D_A D_B E} + |11\rangle_{q_A q_B} |\varphi_1\rangle_{D_A D_B E})$$

Imposing conditions that Eve's density matrices correlated with 00 and 11 are identical.

Bad news: p-bits are always NPT!

$$\mathcal{Y}_{q_A q_B D_A D_B}^\Gamma = \frac{1}{2} \left[\begin{array}{ccc|ccc} U_{00} \rho_{D_A D_B} U_{00}^* & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & (U_{00} \rho_{D_A D_B} U_{11}^*)^\Gamma & 0 & 0 & 0 \\ 0 & (U_{11} \rho_{D_A D_B} U_{00}^*)^\Gamma & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & U_{11} \rho_{D_A D_B} U_{11}^* \end{array} \right]$$

The block in the middle will always produce a negative eigenvalue.

Even worse: p-bits are always distillable!

Easy to see for singlets with flags: the flags are not equal, hence there is small chance to distinguish, this produces a small bias between singlets, and hashing protocol BDSW96 can be applied

How to produce bound entangled state with distillable key

What is the problem with p-bit:

$$1) \quad p\text{-bit} = \begin{bmatrix} \times & 0 & 0 & \times \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \times & 0 & 0 & \times \end{bmatrix} \quad (p\text{-bit})^\Gamma = \begin{bmatrix} \times & 0 & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & 0 & \times \end{bmatrix}$$

The zeros which cause trouble, are responsible for the fact that the key is error-less (i.e. only 00 and 11 terms are present)

2) For singlets with flags, the flags should be at least non-distillable; otherwise, Alice and Bob can measure singlets, distinguish them and distill entanglement from flags.

Ad 2) Werner and Eggeling provided SEPARABLE states, which are arbitrary orthogonal (needed for privacy) and arbitrarily badly distinguishable by LOCC (needed for PPT).

Ad 2) ADD ERRORS! (the zero blocks causing the trouble make non-zero)

EXAMPLE

$$\tau_1 = \rho_{SYM}^{\otimes K}$$

and

$$\tau_2 = \left[\frac{1}{2} (\rho_{SYM} + \rho_{ANTY}) \right]^{\otimes K}$$

when $K \longrightarrow \infty$ or $d \longrightarrow \infty$ they become :

- 1) globally orthogonal
- 2) indistinguishable by LOCC

$$\rho(n, K, d) = \begin{bmatrix} \frac{p}{2}(\tau_1 + \tau_2) & 0 & 0 & \frac{p}{2}(\tau_1 - \tau_2) \\ 0 & (\frac{1}{2} - p)\tau_2 & 0 & 0 \\ 0 & 0 & (\frac{1}{2} - p)\tau_2 & 0 \\ \frac{p}{2}(\tau_1 - \tau_2) & 0 & 0 & \frac{p}{2}(\tau_1 + \tau_2) \end{bmatrix}$$

The state is PPT for:

$$p \leq \frac{1}{3} \quad \text{and} \quad \sqrt[K]{\frac{1-p}{p}} (d-1) \geq d$$

How to get the key

1) To apply BDSW recurrence without twirling
(same as apply Maurer advantage distillation coherently)

$$\rho_{new}(n, K, d) = \frac{1}{C(K, l, d)} \begin{bmatrix} \left[\frac{p}{2}(\tau_1 + \tau_2)\right]^{\otimes n} & 0 & 0 & \left[\frac{p}{2}(\tau_1 - \tau_2)\right]^{\otimes n} \\ 0 & \left[\left(\frac{1}{2} - p\right)\tau_2\right]^{\otimes n} & 0 & 0 \\ 0 & 0 & \left[\left(\frac{1}{2} - p\right)\tau_2\right]^{\otimes n} & 0 \\ \left[\frac{p}{2}(\tau_1 - \tau_2)\right]^{\otimes n} & 0 & 0 & \left[\frac{p}{2}(\tau_1 + \tau_2)\right]^{\otimes n} \end{bmatrix}$$

Here $C(K, l, d)$ is normalization constant.

The state converges to p-bit, when trace norm of upper right corner approaches 1/2.

$$\left\| \left[\frac{p}{2}(\tau_1 + \tau_2) \right]^{\otimes n} / C \right\| = \frac{1}{2} \left(1 - \frac{1}{2^K}\right)^n \frac{1}{1 + \left(\frac{1-2p}{2p}\right)^n}$$

The protocol does not give a finite rate of key. However, if a state is close to p-bit, one can apply Devetak-Winter'03 results for cq, to get the finite rate

Privacy under controlled unitaries

Since p-bit is of the form

$$\gamma = U \psi_+^{q_A q_B} \otimes \rho_{D_A D_B} U^*$$

The unitary can be “undone” producing

$$\psi_+^{q_A q_B} \otimes \rho_{D_A D_B}$$

The operation is global, hence it can produce entanglement. However it preserves privacy in the following sense

When Alice and Bob measure in standard basis the qu-d-its q_A and q_B , they obtain ccq state shared with Eve

$$\rho_{q_A q_B E}^{ccq} = \sum_{i,j} p_{ij} |ij\rangle_{q_A q_B} \langle ij| \otimes \rho_E^{(ij)}$$

Theorem:

- 1) The operation of “undoing” does not change the form of ccq state
- 2) When unitaries are controlled only by one qu-dit, then the form of ccq state is unchanged.

RULE: what serves for control, should be c, other things can be q

For states of the form:

$$\rho_{q_A q_B D_A D_B} = \begin{bmatrix} \times & 0 & 0 & \times \\ 0 & \times & \times & 0 \\ 0 & \times & \times & 0 \\ \times & 0 & 0 & \times \end{bmatrix}$$

The partial trace over decoherer is

$$\rho_{q_A q_B} = \begin{bmatrix} Tr \times & 0 & 0 & Tr \times \\ 0 & Tr \times & Tr \times & 0 \\ 0 & Tr \times & Tr \times & 0 \\ Tr \times & 0 & 0 & Tr \times \end{bmatrix}$$

Such state is often separable, and its form does not contain info about privacy

Apply controlled unitary to the whole state and then perform partial trace:

$$\begin{bmatrix} Tr \times & 0 & 0 & Tr U_{00}(\times) U_{11}^* \\ 0 & Tr \times & Tr U_{01}(\times) U_{10}^* & 0 \\ 0 & Tr U_{10}(\times) U_{01}^* & Tr \times & 0 \\ Tr U_{11}(\times) U_{00}^* & 0 & 0 & Tr \times \end{bmatrix} \rightarrow \begin{bmatrix} Tr \times & 0 & 0 & \|\times\|_{Tr} \\ 0 & Tr \times & \|\times\|_{Tr} & 0 \\ 0 & \|\times\|_{Tr} & Tr \times & 0 \\ \|\times\|_{Tr} & 0 & 0 & Tr \times \end{bmatrix}$$

Convergence to p-bits and security criteria

Claim: distillable key is rate of obtaining p-bits from given state by LOCC

In the case of obtaining perfect key it is obviously true: if Alice and Bob can obtain a p-bit, they measure it and have ccq key, and vice-versa, if they obtain ccq key, the coherent version of their actions will produce p-bit

In general (imperfect p-bits, imperfect ccq keys):

Theorem: Convergence to p-bit in trace norm is equivalent to obtain ccq key with small Eve's Holevo information.

$$\rho_{q_A q_B E}^{ccq} = \sum_{i,j} p_{ij} |ij\rangle_{q_A q_B} \langle ij| \otimes \rho_E^{(ij)}$$

$$F(\{p_{ij}\}, \{\frac{1}{d}\}) < \varepsilon \quad S(\sum_{ij} p_{ij} \rho_E^{(ij)}) - \sum_{ij} p_{ij} S(\rho_E^{(ij)}) < \delta$$

So the convergence in norm to p-bits give rate of key obtained in COMPOSABLE

Way ([M. Ben-Or and D. Mayers], [M. Ben-Or, D. Mayers, M. Horodecki, D. Leung and J. Oppenheim], unpublished)

Relative entropy of entanglement is upper bound for distillable key

$$\rho^{\otimes n} \rightarrow \sigma^{\otimes m} \qquad R(\rho \rightarrow \sigma) = \lim \frac{m}{n}$$

Central formula for “information theories”: (Vidal JMO98, HHH 00, M.H. QIC00)

$$R(\rho \rightarrow \sigma) \leq \frac{M^\infty(\rho)}{M^\infty(\sigma)}$$

For any M being asymptotically continuous function, monotonic under allowed class of operation (in our case LOCC).

$$K_D = R(\rho \rightarrow \gamma)$$

Problem: obtaining p-bits usually does not mean obtaining tensor products!
Rather, one obtains one, greater and greater p-bits with huge correlated garbage

So, though we will follow the ideas of the proof of the above inequality, modification of the proof are unavoidable.

It is enough to show that if a state is close to p-dit, then its relative entropy of entanglement should be of order $\log d$

In other words: relative entropy of entanglement should feel the singlet hidden there.

The main problem is that the decoherer can have arbitrary dimension. In order to proceed, we have to control dimension.

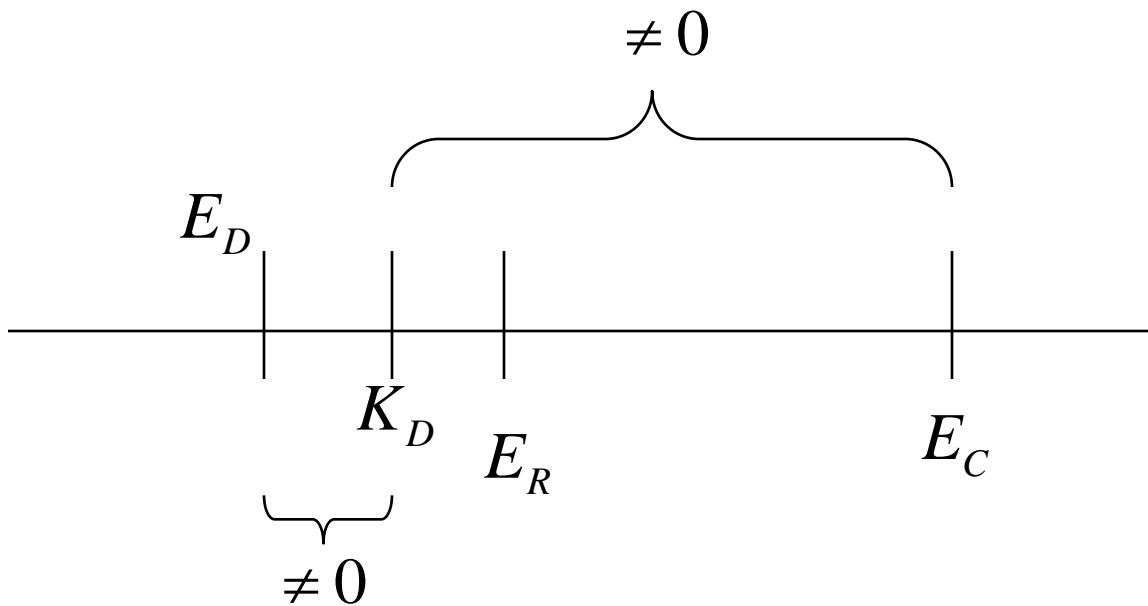
Idea of controlling dimension

$$\begin{aligned} S(\gamma_d | \rho_{sep}) &= S(U\gamma_d U^* | U\rho_{sep} U^*) = S(\psi_+^{q_A q_B} \otimes \rho_{D_A D_B} | U\rho_{sep} U^*) \geq \\ &\geq S(\psi_+^{q_A q_B} | \text{Tr}_{D_A D_B} [U\rho_{sep} U^*]) \equiv S(\psi_+^{q_A q_B} | \sigma_{q_A q_B}) \end{aligned}$$

The state σ is no longer a separable state. HOWEVER with respect to this particular singlet $\psi_+^{q_A q_B}$ it behaves as separable state:

$$F(\psi_+^{q_A q_B}, \sigma_{q_A q_B}) \leq \frac{1}{d} \quad \text{implying} \quad S(\psi_+^{q_A q_B} | \sigma_{q_A q_B}) \geq \log d$$

Distillable key and other entanglement measures



Conclusions

- new notion: p-bit - a state having at least one bit of perfect key
- p-bit contains “twisted singlet”
- unlike singlets, p-bits can be approached asymptotically by PPT states
 - there exist bound entangled states with nonzero distillable key
- privacy is conserved under GLOBAL controlled unitaries
- rate of distilling p-bits by means of LOCC is equal to rate of distilling key with security condition equivalent to composability (roughly speaking Eve is product with the key in trace norm)
- distillable key is bounded by relative entropy of entanglement

- indentifying new operational measure of entanglement
- providing new tools to find gaps between E_D and E_C

Main open problem:

- still for low dimensional bound entangled states distillable key may be zero