
DISTILLATION
MACROSE.
FLUX CRUST

DISTILLATION OF SECRET KEY AND ENTANGLEMENT FROM QUANTUM STATES

IGOR DEVETAK — IBM
ANDREAS WINTER — U. BRISTOL
(quant-ph/ very soon)

ENTANGLEMENT:

$$|\Phi^+\rangle = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$$

...IS JUST WONDERFUL! TO

- VIOLATE BELL'S INEQUALITIES
- DO QUANTUM CRYPTOGRAPHY
- TELEPORT QUBITS

⋮

UNLESS...

...IT'S DIRTY:

E.G. $\rho = p\,\Phi^+ + (1-p)\frac{1}{4}$

WAYS TO AVOID THIS:

* WHEN DISTRIBUTING / STORING STATES, USE QUANTUM ERROR CORRECTION.

→ ALL FINE, BUT WHAT IF IT HAS ALREADY HAPPENED?

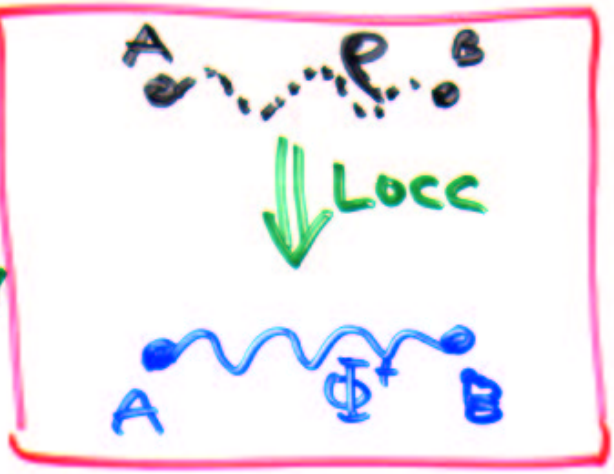
* RESCUE WHAT'S STILL IN ρ:

(BBPSW'96)
(BDSW'96)

LOCC { LOCAL OPERATIONS + CLASSICAL COMM.

"ENTANGLEMENT DISTILLATION"

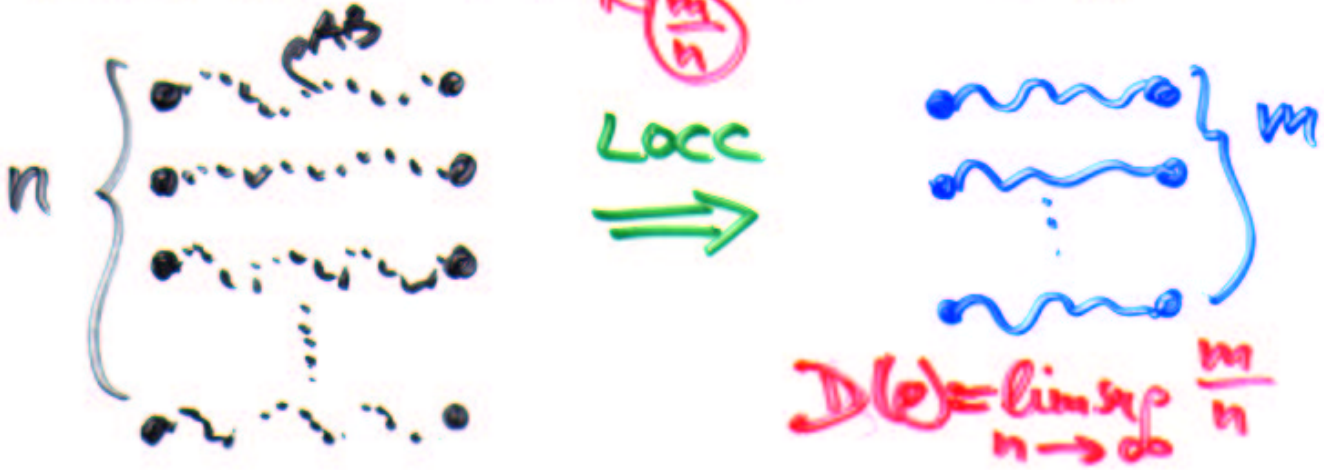
- WHY LOCC ?
  - RESTRICTION MAKES SENSE: A, B USUALLY SEPARATED.
  - CANNOT CREATE ENTANGLEMENT.
  - INTERESTED IN ULTIMATE LIMITS.



- VARIANTS OF THE TASK:
  - IS IT POSSIBLE AT ALL ?
    (I.E. IS THERE NONZERO PROB. TO GET ONE EPR-PAIR FROM (MANY COPIES OF) ρ^{AB} ?

"DISTILLABILITY" → OPEN

  - OPTIMAL RATE & PROTOCOLS?



FROM BDSW'96:

- BOUNDS / FORMULAS FOR $D(\rho)$?
- "ENTANGLEMENT MEASURES" ?
  [ENTANGLEMENT OF FORMATION; AXIOMATIC WORK BY VIDAL, HORODECCI, ...]

MILESTONE: "HASHING PROTOCOL"

FOR $\rho = \underbrace{p_{00}\Phi^+ + p_{01}\Phi^- + p_{10}\Psi^+ + p_{11}\Psi^-}_{\text{MIXTURE OF BELL-STATES}}$

GET $\underbrace{D_{\rightarrow}(\rho)}_{\text{DISTILLABLE ENTG. UNDER LO+ FORWARD CC}} \geq 1 - H(\{p\})$

CONJECTURE (WHO ? WHEN ?)
THE "HASHING INEQUALITY"

$$D_{\rightarrow}(\rho^{AB}) \geq S(\rho^B) - S(\rho^{AB}) =: I_c(A\rangle B)$$

IS TRUE FOR ALL STATES ρ^{AB}.

...OK, IF IT'S TRUE - SO WHAT?

THM. (SCHUMACHER ET AL. '96 + '98 HORODECKI 2000): THE CONJ. IMPLIES:

- $D_{\to}(\rho) = \lim_{n\to\infty} \frac{1}{n} \sup_{\substack{\text{1-LOCC} \\ \rho^{\otimes n} \mapsto \sigma}} I_c(A\rangle B)_\sigma$

- $D_{\leftrightarrow}(\rho) = \lim_{n\to\infty} \frac{1}{n} \sup_{\substack{\text{LOCC} \\ \rho^{\otimes n} \mapsto \sigma}} I_c(A\rangle B)_\sigma$

- SIMILAR FORMULAS FOR QUANTUM CAPACITY OF QUANTUM CHANNELS T:

$$Q(T) = Q_{\to}(T) = \lim_{n\to\infty} \frac{1}{n} \sup_{\sigma = (T\otimes \mathrm{id})\psi} I_c(A\rangle B)_\sigma$$

BARNUM ET AL. '98 — SHOR '02

AND EVEN FOR $Q_{\leftrightarrow}(T)$...

[NOT PERFECT (BECAUSE OF $\lim_{n\to\infty}$: "NONCOMPUTABLE"), BUT AT LEAST IT LOOKS LIKE INFORMATION THEORY...]

... FINALLY PROVED THE BLOODY THING.

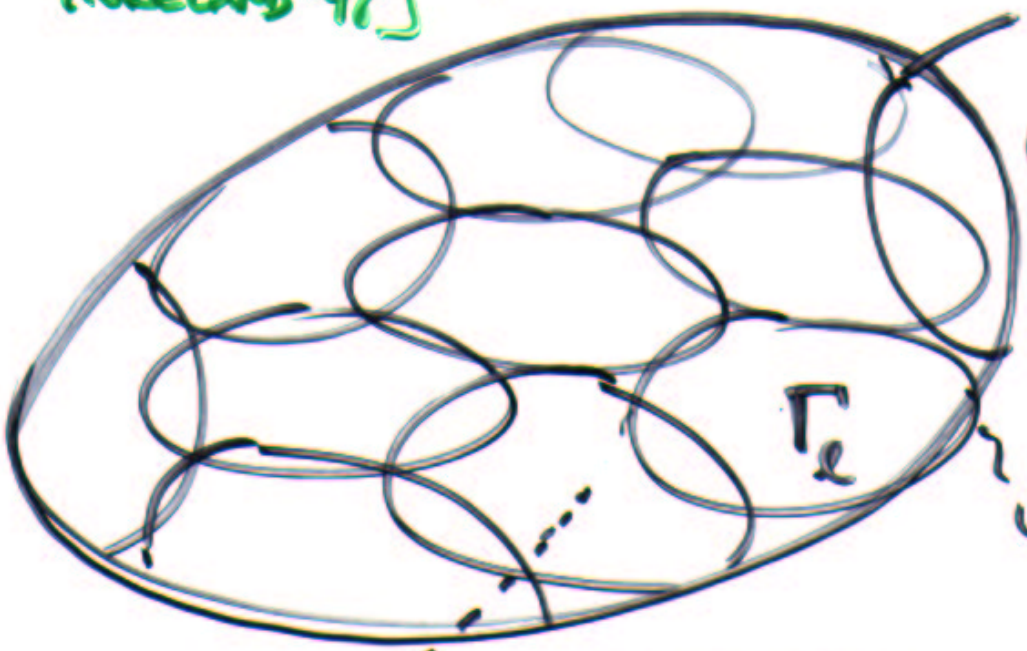
HOW IT WORKS

LITTLE DIGRESSION: SECRET KEY DISTILLATION

FROM $\rho^{ABE} = \sum_x p(x) |x\rangle\langle x| \otimes \rho_x^{BE}$

(n COPIES)

[CLASSICAL MODEL:
MAURER '93
AHLSWEDE/CSISZÁR '93
⋮
THIS: SCHUMACHER/WEST-MORELAND '97]



GOOD CODE FOR $x \mapsto \rho_x^B$ ($\approx 2^{nI(X;B)}$)

PA CODE FOR $x \mapsto \rho_x^E$:
RANDOM CODE-WORDS HAS OUTPUT $\approx \tau_E$ ON $\rho_E = \sum p(x) \rho_x^E$ ($\approx 2^{nI(X;E)}$)

KEY AGREEMENT:

(1) ALICE OBSERVES x^n: FINDS ℓ S.T. $x^n \in T_\ell$

& TELLS BOB (EVE ALSO GETS ℓ!!)

(2) DETERMINES m_1 S.T. $x^n \in C_m$ } $m = m'$ W.H.P. & UNIFORM

(3) BOB 'DECODES' m_1's!

IF $\rho^{ABE} = |\psi\rangle\langle\psi|$,

- $|\psi\rangle = \sum \sqrt{P(x)}\, |x\rangle^A |\varphi_x\rangle^{BE}$;
- ALICE MEASURES $|x\rangle$:

KEY RATE: $S(B) - S(E)$
$= S(B) - S(AB)$

(EVE: $\ell, \rho^E_{x^n}$ ALMOST INDEP. OF m)

KEY RATE:
$I(X;B) - I(X;E)$

DO ALL THIS COHERENTLY, EXCEPT (1):

(2)+(3): LEADS TO A STATE

$$\approx \sum_{m,s} |m\rangle^A |s\rangle^{A'} |m\rangle^B |s\rangle^{B'} |\psi_{m,s}\rangle^{B''E}$$

(4) ALICE MEASURES A' IN QFT-CONJ. BASIS
→ TELLS BOB RESULT $|\hat{s}\rangle$ → HE DOES PHASE CORRECTION ON B':

$$\approx \sum_{m,s} |m\rangle^A |m\rangle^B |s\rangle^{B'} |\psi_{m,s}\rangle^{B''E}$$

... IN $\sum_{m,s} |m\rangle^A |m\rangle^B |s\rangle^{B'} |\psi_{ms}\rangle^{BE}$, EACH

$|s\rangle_M := \sum_s |s\rangle^{B'} |\psi_{ms}\rangle^{B''E}$ $(\forall m!)$ IS $\approx$ PURIFICATION OF $\sigma_E^{\otimes n} \Rightarrow$

$\exists$ UNITARY U_m: $(U_m^{B'B''} \otimes \mathbb{1}^E)|s_m\rangle = |s_0\rangle$

(5) BOB APPLIES $\sum_m |m\rangle\langle m|^B \otimes U_m^{B'B''}$:

FINAL STATE: $\approx \underbrace{\sum_m |m\rangle^A |m\rangle^B}_{\text{CA. } n(S(B)-S(AB)) \text{ EPR-PAIRS.}} |s_0\rangle^{BB'E}$ .B

CONCLUSION

→ PROVED HASHING INEQUALITY VIA SECRET KEY DISTILLATION

→ OPTIMAL KEY RATES FOR FORWARD DISTILLATION; SEVERAL QUANTUM & ENTG.-DISTILLATION CAPACITY FORMULAS

→ OPEN: SINGLE-LETTER FORMULAS FOR THESE... OR AT LEAST GOOD UPPER + LOWER SINGLE-LETTER BOUNDS ?!