STATE RANDOMIZATION: 1 BIT IS ENOUGH (\*qubit\*)

... AND WHY THIS IS INTERESTING ...

A. WINTER (U. BRISTOL)

with C.H. BENNETT (IBH)

P. HAYDEN \( \frac{1}{2} \) (CALTECH)

D. LEUNG

P. SHOR (AT&T)

FOR EVERY STATE \( \rho \in \mathcal{S}(\mathbb{C}^4) \):

\[
\frac{1}{4} \left( e^{i \theta} \rho + e^{-i \theta} \rho^* + e^{i \phi} \rho^T + e^{-i \phi} \rho^{T*} \right)
\]

\[= \frac{1}{2} \mathbb{1} \]  

(Application to: Private Quantum Channel)

\( \text{[Classical bit: 1 bit to randomise]} \)

\( \text{Classical Vernam- (1926's)} \)

2 random bits ... can we do with less?
... WELL, **YES** AND **NO**

RELAX A LITTLE BIT...

- **AMBAINIS** et al.
- **BOYKIN** et al.

-1 \( \neq \) FOR \{ \( p; \) \( U_i \) \} for all \( \psi \in \mathcal{S}(C^d) \)

\[
\sum_{p; \psi} \frac{U_i U^*_i}{\| \psi \|^2} = \frac{1}{d} I \otimes \Phi
\]

Then \( H(\{ p; \psi \}) \geq 2 \log d \)

- Equality attained for uniform distr. over Weyl operators \( \{ w_{jk}: j, k = 0, \ldots, d-1 \} \)

**IDEA OF PROOF:**

- BY LINEARITY
  - GIVES FOR \( \psi \in \mathcal{S}(C^d \otimes C^d) \):
  
  \[
  \sum_{p; \psi} \sigma(U_{ij}) \sigma(U^*_{ij}) = \frac{1}{d} I \otimes \sigma
  \]

- CHOOSE \( \psi = \Phi_d \) (MAX. ENTANGLED):
  
  \[
  H(\{ p; \psi \}) \geq S(\sum_i \sigma(U_{ij}) \sigma(U^*_{ij}))
  \]

  \[
  = S(\frac{1}{d^2} I) = 2 \log d \]
RELAXATION OF "RANDOMIZATION":
INTRODUCE $\varepsilon > 0$

$$\forall \varepsilon > 0, \exists N \text{ s.t. } \left| \sum_{i=1}^{N} u_i \sigma_k u_i^* - \frac{1}{d} \mathbb{1} \right| < \varepsilon$$

(THEN THE PROOF DOESN'T WORK!)

THM. LET $P$ BE ANY DISTRIBUTION ON UNITARIES S.T.

$$\forall \varepsilon > 0, \int \| U \sigma_k U^* - \frac{1}{d} \mathbb{1} \| < \varepsilon$$

THEN RANDOM I.I.D. SELECTION OF $U_1, U_2, \ldots, U_n$ ACCORDING TO $P$,

FOR $n = \frac{1}{\varepsilon^2} d \log d$, WILL GIVE

WITH PROBABILITY $\to 1$ AS $d \to \infty$, IF $P$ IS THE HAAR MEASURE,

THIS CAN BE STRENGTHENED TO

$$\forall \varepsilon > 0, \left| \frac{1}{d} \sum_{i=1}^{N} u_i \sigma_k u_i^* - \frac{1}{d} \mathbb{1} \right| < \varepsilon$$

(randomness: $\log d + \log \log d + 2 \log \frac{1}{\varepsilon}$ BITS)
APPLICATIONS:

(1) IF ALICE & BOB PREPARE ON $U_i, \ldots, U_n$ & SHARE RANDOM $i = 1, \ldots, n$:

ASYMPT. 1 BIT OF KEY/CUBIT

& PRIVATE QUANTUM CHANNEL

ALICE: $\rho \rightarrow U_i^* \rho U_i \rightarrow U_i^* \rho U_i = \rho$

BOB: $U_i^* \rho U_i = \rho$

...(FOR HER, ENCRYPTED MAP $M(r) = \frac{1}{n} \sum U_i^* \rho U_i^{*}$ IS ALMOST INDISTINGUISHABLE)

FROM CONSTANT MAP $C(r) = \frac{1}{n} \rho$

EVE: STATE IS

$\frac{1}{n} \sum U_i^* \rho U_i^{*} \approx \frac{1}{n} \rho$

(2) BEWARE! IF EVE IS ENTANGLED WITH ALICE, SHE INTERCEPTS

$\frac{1}{n} \sum_{i=1}^{n} (U_i \otimes 0_1) \rho_{AE} (U_i^* \otimes 0_1) = (R \otimes 1d) (\rho_{AE})$

$\sum_{i=1}^{n} (R \otimes 1d) (\rho_{AE}) = 1$

$\frac{1}{d} \sum_{i=1}^{n} (R \otimes 1d) (\rho_{AE}) \\ \frac{1}{d} (R \otimes 1d) = \frac{1}{d} (C \otimes 1d) (\rho_{AE})$

$\text{RANK} < \text{RANK}^2$
→ If to distinguish R from C:
   - Hard if only pure states on C^n allowed...
   - Almost deterministic if entangled test-state permitted.

(3) \( \text{But:} \; \omega = (R \otimes \text{id}) \rho \) is LOCC-indist.
   \[
   \text{from} \; \frac{1}{\sqrt{d^2}} \text{II} : \text{II} \quad \text{(up to prob.)}
   \]
   \[
   \text{fact, for any separable POVM } (A_i \otimes \Omega_B;).
   \]
   \[
   \sum_i \left| T^* (\omega - \frac{1}{d^2} \text{II}) \right| A_i \otimes \Omega_B ; \right| \leq \epsilon
   \]
   \]
   ... since this is true for all max. entg. states: suitable coding gives data hiding
   (DiVincenzo/Leung/Terhal) of
   1 bit / 1+1 qubit (asympt.)
   (even 1 qubit !)
Remote State Preparation:

(LO'99,

- Alice knows state \( \psi \)
- Constructs
  \[ M_i := \frac{d}{n(n+1)} U_i \psi U_i^* \]
  (povm by **)

- Measures on her share of \( \Phi_d \)
- Bob is told \( i \) (fails w/p. \( \leq \epsilon \))
- He has now \( U_i \psi U_i^* \) \( \Rightarrow \) appl. of \( U_i \) gives him \( \psi \)

Alice:

Bob:

\[ U_i \Psi \]

Rsp. with (AIMP):

- 1 cbit + 1 ebit
- (teleportation)
- 2 cbits!

...vanishing failure prob.

Optimal! 

- \( < 1 \) cbit would violate causality.
- \( < 1 \) ebit implies \( \infty \) cbits (\( \log_2 \delta \) ebits \( \Rightarrow R(\delta) \) cbits...)
THIS IS THE LAST SLIDE.

... THERE IS MORE TO TELL
(2 FORTHCOMING PAPERS):

* FULL EBIT/CBIT TRADEOFF
  FOR R.S.P. OF ENSEMBLES.
* MORE BITS ON DATA HIDING.
* INTERESTING LARGE DEVIATION
  THEORY; HILBERT SPACE GEO-
  METRY.

MORAL: SOMETIMES A
SMALL 
DIFFERENCE MAKES A BIG

DIFFERENCE :)