STATE RANDOMISATION: 1 BIT IS ENOUGH (✓ QUBIT)

... AND WHY THIS IS INTERESTING ...

A. WINTER (U. BRISTOL)
WITH C. H. BENNETT (IBM)
P. HAYDEN } (CALTECH)
D. LEUNG }
P. SHOR (AT&T)

FOR EVERY STATE $\rho \in \mathcal{S}(\mathbb{C}^2)$:

$$\frac{1}{4}\left[\rho + \sigma_x \rho \sigma_x + \sigma_y \rho \sigma_y + \sigma_z \rho \sigma_z\right] = \frac{1}{2}\mathbb{1}.$$

(APPLICATION TO: PRIVATE QUANTUM CHANNEL)

2 RANDOM BITS ... CAN WE DO WITH LESS?

[CLASSICAL BIT: 1 BIT TO RANDOMISE]

CLASSICAL VERNAM-CIPHER (1920's)

... WELL, **YES** AND NO

RELAX A LITTLE BIT...

- AMBAINIS et al.
- BOYKIN et al.

- IF FOR $\{p_i; U_i\}$

$$\boxed{\forall \rho \in \mathcal{S}(\mathbb{C}^d)\ \sum p_i U_i \rho U_i^* = \frac{1}{d}\mathbb{1}}$$

THEN $H(\{p_i\}) \geq 2 \log d$

- EQUALITY ATTAINED FOR UNIFORM DISTR. OVER WEYL OPERATORS ($W_{jk} : j,k = 0 \dots d-1$)

IDEA OF PROOF:

$\circledast$ — BY LINEARITY

— GIVES FOR $\rho \in \mathcal{S}(\mathbb{C}^d \otimes \mathbb{C}^d)$:

$$\sum_i p_i (U_i \otimes \mathbb{1}) \rho (U_i^* \otimes \mathbb{1}) = \frac{1}{d}\mathbb{1} \otimes \rho_B$$

CHOOSE $\rho = \Phi_d$ (MAX. ENTANGLED):

$$H(\{p_i\}) \geq S\left(\sum_i p_i (U_i \otimes \mathbb{1}) \Phi_d (U_i^* \otimes \mathbb{1})\right)$$

$$= S\left(\frac{1}{d^2}\mathbb{1}\right) = 2 \log d. \blacksquare$$

RELAXATION OF "RANDOMIZATION":

INTRODUCE $\epsilon > 0$

$$\forall \rho \in \mathcal{S}(\mathbb{C}^d) \quad \left\| \sum_i p_i U_i \rho U_i^* - \frac{1}{d}\mathbb{1} \right\|_1 \le \epsilon \qquad (*)$$

(THEN THE PROOF DOESN'T WORK!)

<u>THM.</u> LET p BE ANY DISTRIBUTION ON UNITARIES S.T.

$$\forall \rho \quad \int dp(U)\, U \rho U^* = \frac{1}{d}\mathbb{1}.$$

THEN RANDOM I.I.D. SELECTION OF $U_1, U_2, \ldots, U_n$ ACCORDING TO p, FOR $n = \frac{1}{\epsilon^2} d \log d$, WILL GIVE $(*)$ WITH PROBABILITY $\to 1$ AS $d \to \infty$.

RANDOMNESS: $\boxed{\log d + \log\log d + 2\log\frac{1}{\epsilon}}$ BITS

$$\forall \rho \quad \left\| \frac{1}{n}\sum_{i=1}^{n} U_i \rho U_i^* - \frac{1}{d}\mathbb{1} \right\|_1 \le \epsilon \qquad (*)$$

IF p IS THE HAAR MEASURE, THIS CAN BE STRENGTHENED TO

$$\forall \rho \quad \frac{(1-\epsilon)}{d}\mathbb{1} \le \frac{1}{n}\sum_{i=1}^{n} U_i \rho U_i^* \le \frac{(1+\epsilon)}{d}\mathbb{1} \qquad \boxed{**}$$

APPLICATIONS:

(1) IF ALICE & BOB PREAGREE ON $\mathcal{U}_1, \dots, \mathcal{U}_n$ & $\underbrace{\text{SHARE RANDOM } i = 1, \dots, n}_{\text{ASYMPT. 1 BIT OF KEY / QUBIT}}$:

$\Leftarrow$ PRIVATE QUANTUM CHANNEL

ALICE: BOB:

$$\rho \mapsto \mathcal{U}_i \rho \mathcal{U}_i^* \dashrightarrow \mathcal{U}_i^* \cdot \mathcal{U}_i = \rho$$

..... FOR HER, ENCRYPTION MAP $R(\rho) = \frac{1}{n} \sum_i \mathcal{U}_i \rho \mathcal{U}_i^*$ IS ALMOST INDISTINGUISH. FROM CONSTANT MAP $C(\rho) = \frac{1}{d} \mathbb{1}$

EVE: STATE IS

$$\frac{1}{n} \sum_{i=1}^{n} \mathcal{U}_i \rho \mathcal{U}_i^* \approx \frac{1}{d} \mathbb{1}$$

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

$$\frac{1}{n} \sum_{i=1}^{n} (\mathcal{U}_i \otimes \mathbb{1}) \rho_{AE} (\mathcal{U}_i^* \otimes \mathbb{1}) = (R \otimes id)(\rho_{AE})$$

$$\triangle!\ F\Big((R \otimes id)\Phi_d, \underbrace{(C \otimes id)\Phi_d}_{= \frac{1}{d^2} \mathbb{1}}\Big) \sim \frac{1}{d}$$

! RANK $n \ll d^2$!

⇒ IF TO DISTINGUISH R FROM C:

- HARD IF ONLY PURE STATES ON $\mathbb{C}^d$ ALLOWED...
- ALMOST DETERMINISTIC IF ENTANGLED TEST-STATE PERMITTED.

(3) **BUT** $\omega = (R \otimes id)\Phi_d$ IS LOCC-INDIST. (UP TO PROB. $\leq \epsilon$) FROM $\frac{1}{d^2}\mathbb{1}$: IN FACT, FOR ANY SEPARABLE POVM $(A_i \otimes B_i)_i$:

$$\sum_i \left| \mathrm{Tr}\left(\omega - \frac{1}{d^2}\mathbb{1}\right)(A_i \otimes B_i)\right| \leq \epsilon$$

... SINCE THIS IS TRUE FOR ALL MAX. ENTG. STATES: SUITABLE CODING GIVES DATA HIDING (DIVINCENZO/LEUNG/TERHAL) OF

$\underbrace{1 \text{ BIT}}_{\text{(EVEN 1 QUBIT!)}}$ / 1+1 QUBIT (ASYMPT.)

(4) REMOTE STATE PREPARATION:

(LO'99, ...)

- ALICE KNOWS STATE "ψ"

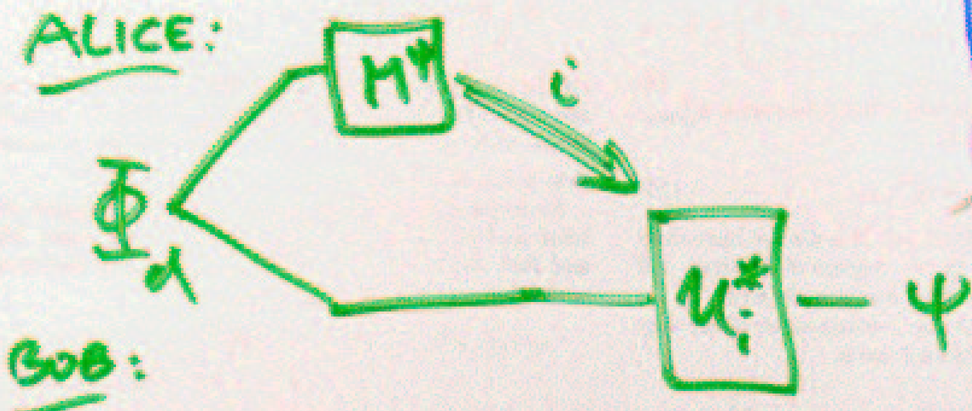
  CONSTRUCTS $\underbrace{M_i := \frac{d}{n(1+\epsilon)} \mathcal{U}_i \psi \mathcal{U}_i^*}_{\text{POVM BY } \boxed{\text{[illegible]}}}$

  MEASURES ON HER SHARE OF Φ_d

- BOB IS TOLD i (FAILS W/P. $\leq \epsilon$)

  HE HAS NOW $\mathcal{U}_i \psi \mathcal{U}_i^*$ ...> APPL. OF

  $\mathcal{U}_i^*$ GIVES HIM ψ



RSP. WITH (ASYMP.) 1 CBIT + 1 EBIT / QUBIT

(TELEPORTATION: 2 CBITS!)

...VANISHING FAILURE PROB.

OPTIMAL!

- < 1 CBIT WOULD VIOLATE CAUSALITY.
- < 1 EBIT IMPLIES ∞ CBITS ($\log d - \epsilon$ EBITS $\Rightarrow$ $\Omega(d)$ 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 GEOMETRY.

<u>MORAL</u>: SOMETIMES A SMALL ϵ MAKES A **BIG** DIFFERENCE :-)