REMOTE PREPARATION OF QUANTUM STATES

ANDREAS WINTER, BRISTOL

JOINT WORK WITH

CHARLES BENNETT, PATRICK HAYDEN, DEBBIE LEUNG, PETER SHOR

[PREVIOUS WORK BY LO 2000, PATI 2001, BENNETT et al. 2001, DEVETAK & BERGER 2001]

OVERVIEW

I. TELEPORTATION (1ebit + 2cbit $\Rightarrow$ 1qubit)

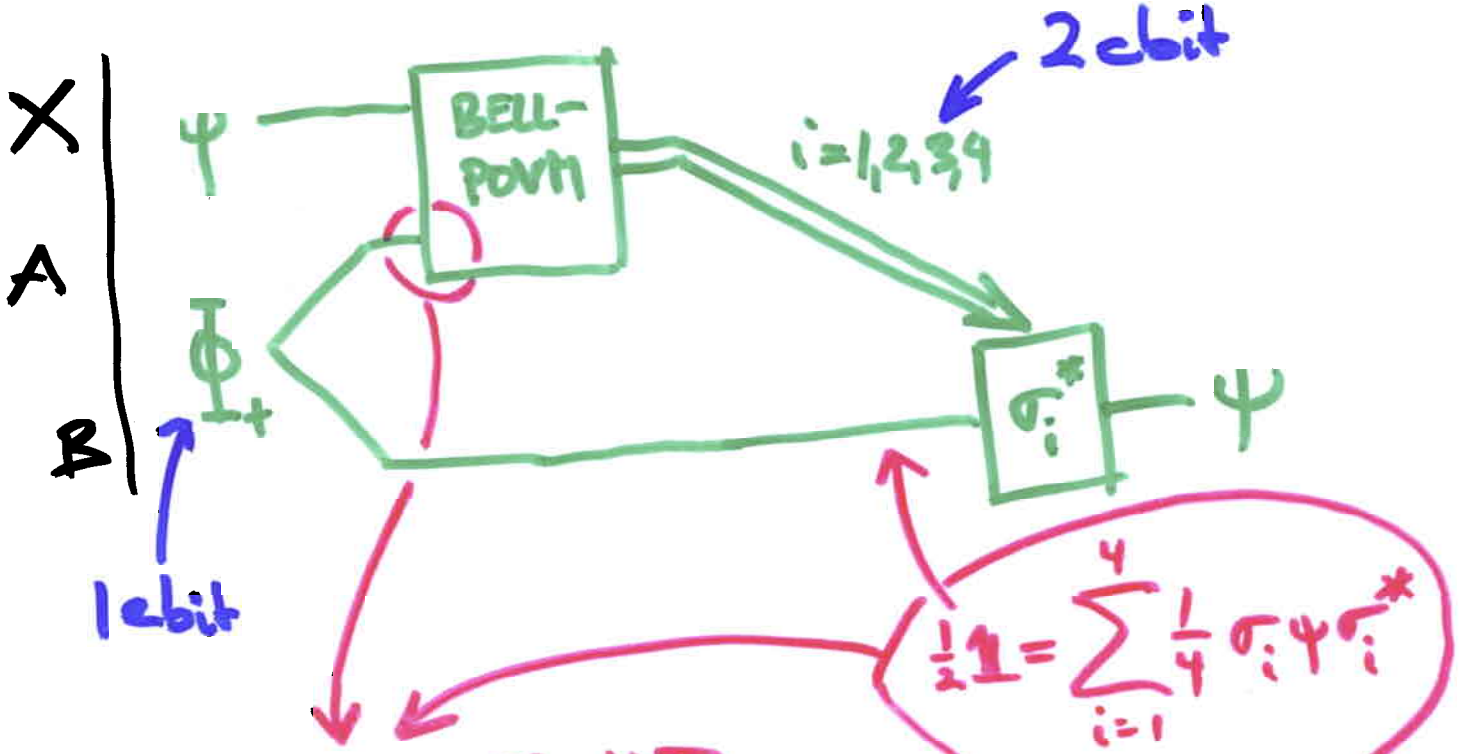
II. REMOTE STATE PREP.:
1ebit + 1cbit + 1$\to$bit $\Rightarrow$ 1qubit

III. OPTIMALITY OF ebit AND cbit RESOURCES

IV. PRIVATE QUANTUM CHANNELS & OTHER ISSUES

V. TRADE-OFF FOR ENSEMBLES OF PURE AND ENTANGLED STATES

I. TELEPORTATION (BENNETT et al. 1993)



TRANSLATES INTO POVM ON A:

$$\mathbb{1} = \sum_{i=1}^{4} \frac{1}{2} \sigma_i \psi \sigma_i^*$$

(COMPLEX CONJUGATE)

↕

THIS IS AN OPTION IF ALICE KNOWS ψ (R.S.P.)

GENERAL: $2 \to D$ $(4 \to D^2)$

$$|\Phi\rangle_B = \frac{1}{\sqrt{D}} \sum |i\rangle_A |i\rangle_B$$

$\log D$ ebit

$\Rightarrow$ SEND $2 \log D$ cbit

II. REMOTE STATE PREPARATION

D : LARGE , $\sum_i p_i U_i \varphi U_i^* = \frac{1}{D} \mathbb{1} \quad \forall \varphi$

CAN WE SELECT FEW ($\approx D$) U_i's TO MIX GIVEN ψ : $\frac{1}{K} \sum_{k=1}^{K} U_k \psi U_k^* \approx \frac{1}{D} \mathbb{1}$

YES, WE CAN! PICK THEM AT RANDOM — THEN USE "OPERATOR-CHERNOFF" BOUND TO ESTIMATE SUCCESS PROBABILITY.

LEMMA (AHLSWEDE, R., IEEE-IT 48 (2002), 569)

LET $X_1, \dots, X_K$ BE I.I.D. RVs IN $\mathcal{B}(\mathcal{H})_{\dim \mathcal{H} = D}$, $0 \le X_k \le \mathbb{1}$, WITH EXPECTATION $M = \mathbb{E} X_k \ge s \mathbb{1}$; $0 \le \eta \le \frac{1}{2}$

THEN

$$\Pr\left\{ \frac{1}{K} \sum_{k=1}^{K} X_k \notin [(1-\eta) M, (1+\eta) M] \right\} \le 2D \exp\left(-M \cdot \frac{\eta^2 s}{2 \ln 2} \right)$$

OUR CASE ($\pi = \frac{1}{D}\mathbb{1}$, $X_k = U_i \psi U_i^*$ WITH PROB. p_i).

GET $\frac{1}{K}\sum_{k=1}^{K} U_{i_k} \psi U_{i_k}^* = \frac{1 \pm \epsilon}{D}\mathbb{1}$ W.H.P.

IF $K \gtrsim D \log D$

↓

CAN FORM POVM WITH OPERATORS

$$A_k := \frac{D}{K(1+\epsilon)} U_{i_k} \psi U_{i_k}^* \quad , \quad A_0 = \mathbb{1} - \sum_{k=1}^{K} A_k$$

$$0 \le A_0 \le 2\epsilon\,\mathbb{1}$$

PROTOCOL (ψ GIVEN VISIBLY TO ALICE):

(1) A & B SELECT RANDOMLY $U_{i_1}, \dots, U_{i_K}$

[USING SHARED RANDOMNESS]

(2) WITH PROB. $1-\epsilon$ ALICE CAN FORM THE POVM $(A_0, \dots, A_K)$ → OTHERWISE A "FAILURE"

→ MEASURES ON HER HALF OF Φ_D & TELLS BOB k

(3) IF $k \neq 0$, BOB INVERTS U_{i_k}

→ GETS ψ

PERFORMANCE:

- OUTPUTS k EXACTLY WITH PROB $1-3\epsilon$
- USES $\log D$ ebit AND $\log D + O(\log\log D)$ cbit

[PLUS LOTS OF SHARED RANDOMNESS BUT WITH STANDARD DERANDOMISATION TECHNIQUES ONE CAN PUSH THIS DOWN TO $\log D + O(\log\log D)$ rbit]

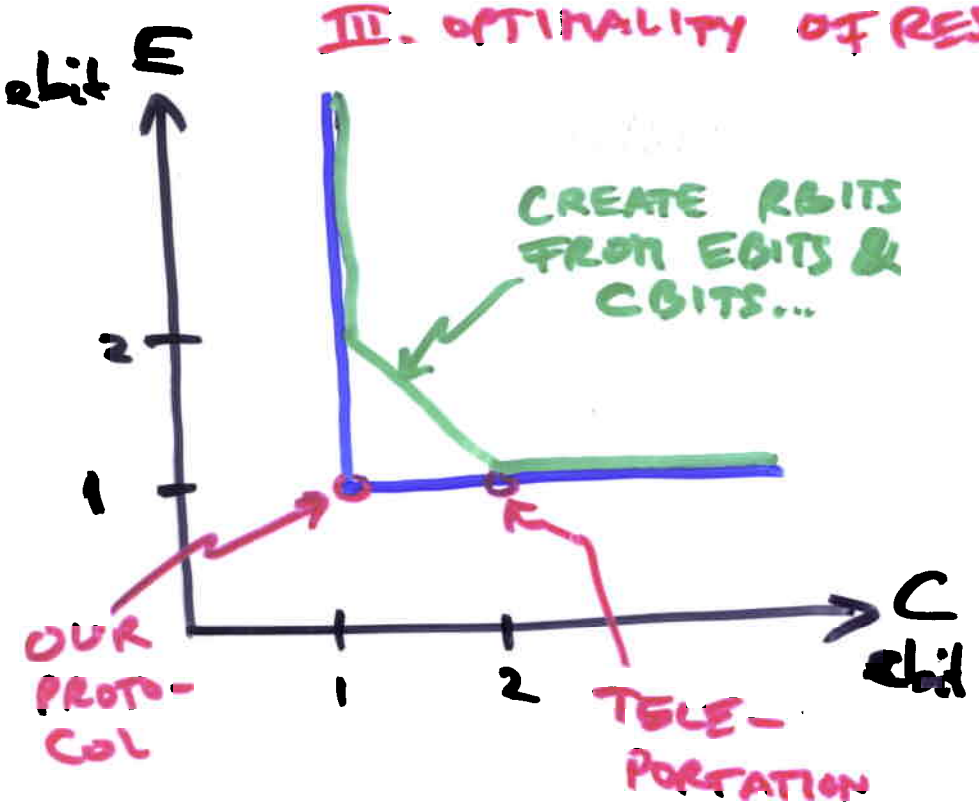
INCIDENTALLY THIS ALSO USES CHERNOFF BOUND...

I.E., NORMALISED TO QUBIT UNITS:

$$1\,\text{ebit} + 1\,\text{cbit} + 1\,\text{rbit} \Rightarrow 1\,\text{qubit} + 1\,\text{rbit}$$

BECAUSE COMMUNICATED MEASUREMENT RESULT k IS RANDOM!

III. OPTIMALITY OF RESOURCES



OBSERVE: • $C \geq 1$ ("CAUSALITY": CAN USE R.S.P. TO SEND ORTHOGONAL STATES!)

• $E \geq 1$ (OTHERWISE THERE WOULD BE A WAY OF ENCODING STATES $\psi \in \mathbb{C}^D$ USING A MUCH SMALLER QU. SYSTEM & CLASSICAL INFO

UNLESS $C = \infty$

→ VOLUME ARGUMENT SHO THAT THIS REQUIRES $\Omega(D)$ cbit : EXPONENTIAL IN $\log D$

IV. RECONSIDERATION & SPIN-OFFS

(1) WE CAN TWIST OUR PROTOCOL S.T. "FAILURE" IS ANNOUNCED WITH PROBABILITY EXACTLY ϵ AND ALL OTHER MESSAGES HAVE EQUAL PROB $\frac{1-\epsilon}{K}$ IN CASE OF SUCCESS BOB ONLY GETS ψ (AGAIN, EXACTLY)

AND ONLY IN THE FAILURE CASE THERE IS A BIT OF INFORMATION LEAKING FROM THIS HALF OF ϕ_B

→ "ALMOST" OBLIVIOUS (TO BOB)

[COMPARE TO RESULT OF LEUNG, SHOR FOR $\epsilon = 0$:

PROTOCOL IS TELEPORTATION

→ REQUIRES 2 cbit / qubit !

(2) "1 ebit / 1 cbit" BASED ON HAVING RANDOM BATCHES OF $\simeq D \log D$ UNITARIES U_{ps} (IN FACT $\simeq D \log D$ ARE SUFFICIENT), S.T. $\forall \psi$

$$P_{m_p}\left\{ \frac{1}{|S|} \sum_{s \in S} U_{ps} \psi U_{ps}^{*} \simeq \frac{1}{D} \mathbb{1} \right\} \geq 1 - \epsilon$$

$\longrightarrow$ "ENCRYPTION MAP"

$$T : \psi \longmapsto \frac{1}{|P|} \sum_{p \in P} |p\rangle\langle p| \otimes \frac{1}{|S|} \sum_{s \in S} U_{ps} \psi U_{ps}^{*}$$

$$|P| = |S| \simeq D \log D$$

$$\forall \psi \quad T(\psi) \simeq \frac{1}{|P|} \mathbb{1} \otimes \frac{1}{D} \mathbb{1}$$

& KNOWING $s \in S$ ONE CAN RECOVER ψ

THIS IS A PRIVATE QUANTUM CHANNEL WITH 1 SECRET + 1 PUBLIC KEY BIT PER QUBIT !

- PREVIOUSLY, NEEDED 2 SECRET KEY BITS/QUBIT

[PROVABLE, IF EITHER [MOSCA, TAPP, DEWOLF 2000]

- $\epsilon = 0$ OR
- REQUIRE EVEN $T \otimes id$ TO ENCRYPT (RANDOMISE) ENTANGLED STATES

- UNCLEAR IF PUBLIC + SECRET KEY STILL HAS TO BE 2 BIT/QUBIT

IN FACT, FOR OUR MAP T:

$(T \otimes id)\Phi_{max}$ VERY FAR

FROM $\frac{1}{|\Gamma|}\mathbb{1} \otimes \frac{1}{D}\mathbb{1} \otimes \frac{1}{D}\mathbb{1}$!

I. TRADE-OFF FOR ENSEMBLES OF PURE & ENTANGLED STATES

CAN TRADE ENT. FOR CC IF SPECIAL STATE SETS ARE CONSIDERED → ENSEMBLE ASYMPTOTICS (ALSO ALLOWS COMPLETE DERANDOMISATION).

(1) PURE STATE ENSEMBLE $\{p_i, \psi_i\}$

(AND BLOCKS $\psi_I = \psi_{i_1} \otimes \cdots \otimes \psi_{i_n}$

$p_I = p_{i_1} \cdots p_{i_n}$)

- Q-C-COMPRESSION [HAYDEN, JOZSA, W.; JMP 43 (2002), 4404] WITH nR cbit, $nQ^*(R)$ qubit → USE R.S.P. TO OBTAIN:

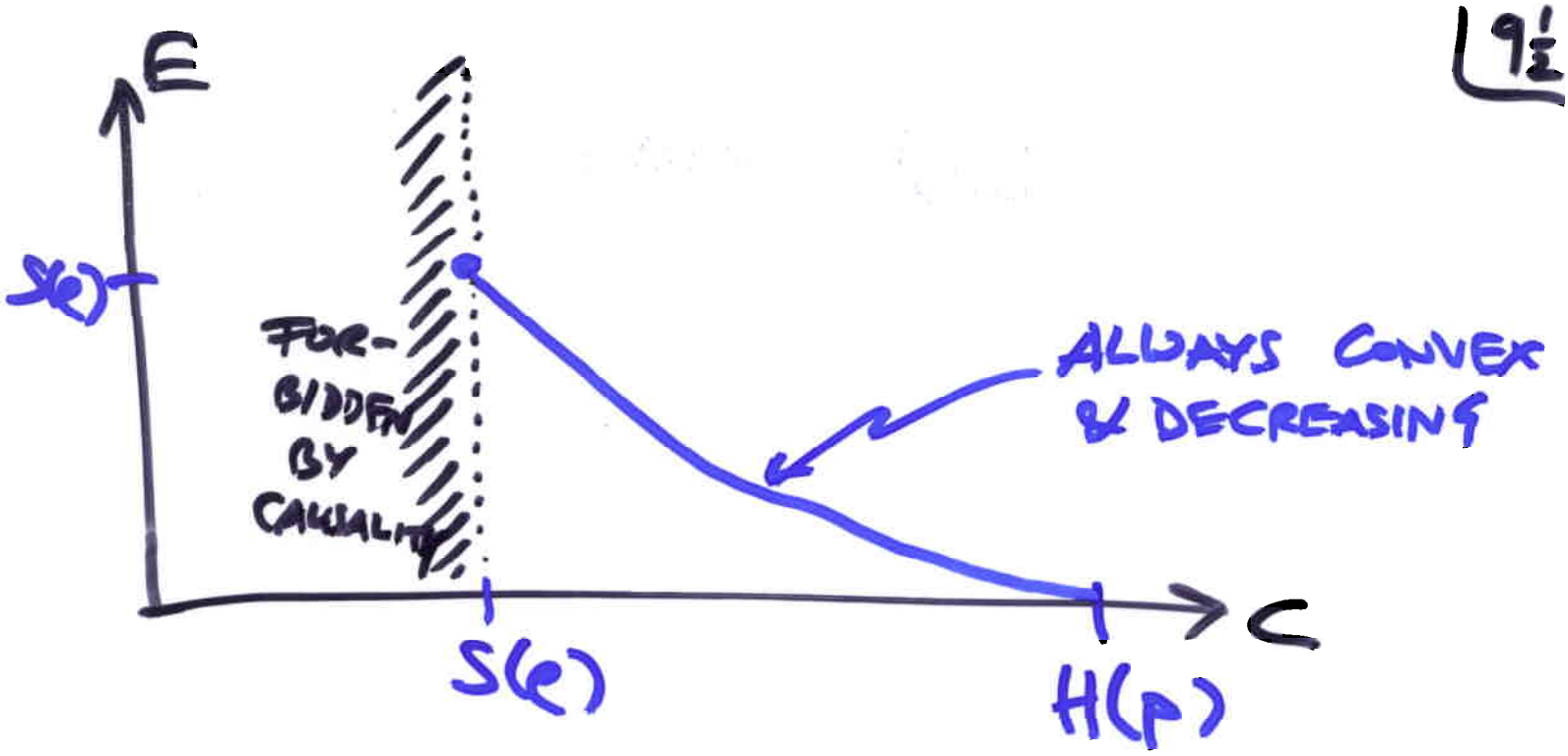
  $n(R + Q^*(R))$ cbit & $nQ^*(R)$ ebit

- TURNS OUT TO BE THE EXACT CURVE:

  $E^*(C_Q) = \min\{S(A:B|C) \mid S(AC) \leq Q$

  WITH TRIPARTITE STATES

  $\omega = \sum_i p_i |i\rangle\langle i|_A \otimes \psi_{i\,B} \otimes \sum_j p(j|i) |j\rangle\langle j|_C$



- "WORST CASE" ALWAYS UNIFORM ENSEMBLE (DIM d)
  [ONLY KNOWN FOR $d=2$: DEVETAK, BERGER 2001]

→ IS "THE" TRADE-OFF CURVE FOR ARBITRARY BLOCKS OF n QU-d-ITS!

(2) MIXED STATE ENSEMBLE

$\{p_i, \rho_i\}$ (AND BLOCKS) $\rho = \sum_i p_i \rho_i$

WANT TO PREPARE <u>PURIFICATIONS</u>

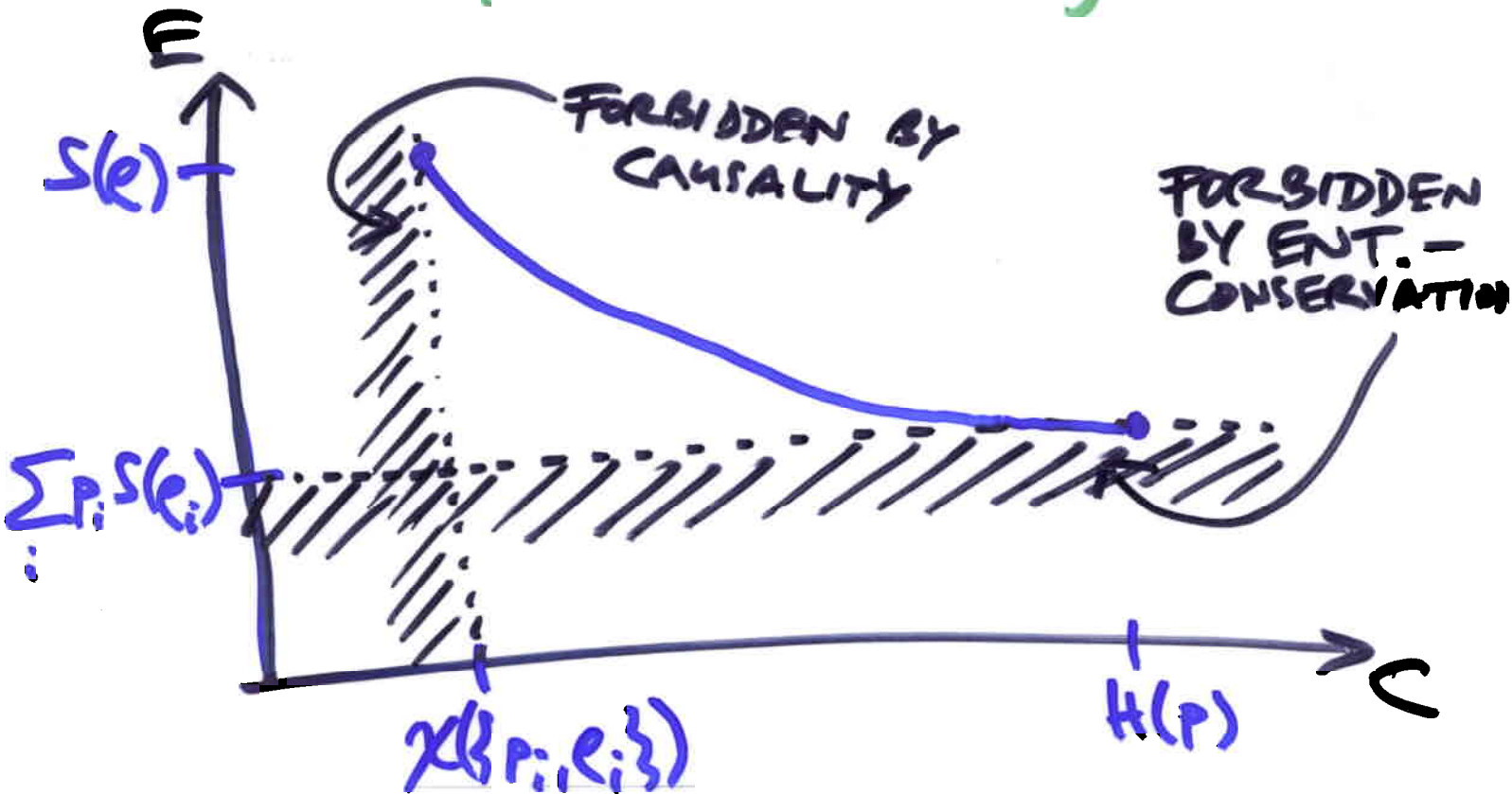
ϕ_i OF ρ_i BETWEEN A &B

CURVE GIVEN BY

$$E^*(C) = \min \{ S(B|C) \mid S(XBC) \leq C \}$$

WITH 4-PARTITE STATES

$$\omega = \sum_i p_i |i\rangle\langle i|_X \otimes \phi_{i:AB} \otimes \sum_j p(j|i) |j\rangle\langle j|_Y$$



* LEFT UPPER POINT IS SIMULATION OF THE cq-CHANNEL, WITH STATES $\{\rho_i\}$, ON P-TYPICAL INPUTS, BY A NOISELESS CHANNEL OF CAPACITY $\chi(\{p_i, \rho_i\})$

— IN THE PRESENCE OF ∞ ENTANGLEMENT: Q.R.S.T.

(↔ CHARLES BENNETT'S TALK ON TUESDAY)

* ONLY QUESTION LEFT:

HOW MUCH SHARED RANDOMNESS IS NEEDED IN THE UNIVERSAL PROTOCOL?