

Remarks on complementarity, privacy, entanglement and maybe even channel superactivation and quantum data hiding.

---

First, the general overview. What are we trying to accomplish in the "Physical Underpinnings of Privacy" paper?

- The main point is that we can really (formally) think of quantum information as classical "bit" and "phase" information, as suggested by QECC (particularly stabilizer codes).  
As in: if Alice and Bob share full correlations in conjugate bases, they share entanglement.
- We can prove the hashing inequality and rate of secret key distillation in this approach. From the former we also get the channel capacity. Almost forgot to mention state merging works, too.
- This is in contrast to the standard approach of decoupling. So to prove the hashing inequality, we don't try to find a (big) subspace in  $\rho^{AB}$  which is decoupled from Eve, we instead focus on "concentrating" the two types of correlations.

How does it work? Consider entanglement distillation.

1. A perfect maximally-entangled state is essentially any state  $\rho^{AB}$  for which  $S(Z^A|B) = S(X^A|B) = 0$ .

Here  $S(O^A|B) = S(\bar{\rho}^{AB}) - S(\rho^B)$  for  $\bar{\rho}^{AB}$  the state after measuring observable  $O^A$ .  $Z^A$  and  $X^A$  are the generalized Pauli operators  $Z = \sum_{k=1}^d \omega^k |k\rangle\langle k|$   $X = \sum_{k=1}^d |k\rangle\langle k+1|$

$$\rho^{AB} \rightarrow |\psi\rangle^{ABE} = \sum_{k=1}^d \sqrt{p_k} |k\rangle^A |\varphi_k\rangle^{BE} \rightarrow \sum_{k=1}^d \sqrt{p_k} |k\rangle^A |k\rangle^C |\varphi_k\rangle^{BE} \quad \otimes$$

$$\text{but } |\psi\rangle^{ABE} = \sum_{x=1}^d \sqrt{q_x} |\tilde{x}\rangle^A |\theta_x\rangle^{BE} \quad \text{for } |\tilde{x}\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^d \omega^{kx} |k\rangle$$

this means  $\langle k | \psi \rangle = \sqrt{p_k} |\varphi_k\rangle = \frac{1}{\sqrt{d}} \sum_{x=1}^d \sqrt{q_x} \omega^{kx} |\theta_x\rangle$ , so the state

$$\otimes \text{ is } \sum_{x,k=1}^d \left( \frac{q_x}{d} |kk\rangle^{AC} \omega^{kx} |\theta_x\rangle^{BE} \right) = \sum_{x=1}^d Z_C^x |\Phi\rangle_{AC} \sqrt{q_x} |\theta_x\rangle_{BE}$$

but the states  $\theta_x^B$  are disjoint by the second criterion, so Bob can undo the  $Z_C^x$  and produce  $|\Phi\rangle_{AC}$ .

2. This also works approximately, in the sense that if on  $\rho_{AB}$  there exist mmts  $\Lambda_B^k$  and  $\tilde{\Lambda}_B^x$  such that the error probs

$$P_e = \sum_k p_k \text{Tr}[(\mathbb{1}_B - \Lambda_B^k) \varphi_B^k] \leq \varepsilon \quad \bar{P}_e = \sum_x q_x \text{Tr}[(\mathbb{1}_B - \tilde{\Lambda}_B^x) \theta_B^x] \leq \varepsilon$$

then Bob, acting alone, can create a state  $\Phi'_{AB}$  such that

$$\|\Phi_{AC} - \Phi'_{AC}\| \leq O(\varepsilon).$$

Entirely similar to above proof, making use of the fact that if a mmt succeeds on a state w/ high prob, it doesn't disturb it much.

3. Now, distillation.  $\rho_{AB}^{\otimes n}$  with  $S(Z_A|B), S(X_A|B) \geq 0$ . Choose  $Z_A$  diagonal in the eigenbasis of  $\rho_A$ .

Idea: Bob is missing information about  $Z_A$  and  $X_A$ , so just send it to him! More precisely: send some info so that the  $\{\varphi_k\}$  and  $\{\theta_x\}$  consistent with this info are each distinguishable

Hurdles:  $Z_A$  and  $X_A$  cannot be simultaneously measured.

Will we get the best possible rate? (Hashing bound)

For each observable separately, Alice and Bob are in the "static" analog of sending classical information over a quantum channel.

Shared ensemble  $\{P_k, P_k \otimes \varphi_k\}_{k=1}^{\otimes n}$ ; would like to extract <sup>full</sup> correlations.

↳ projector onto  $|k\rangle \approx$  classical random variable.

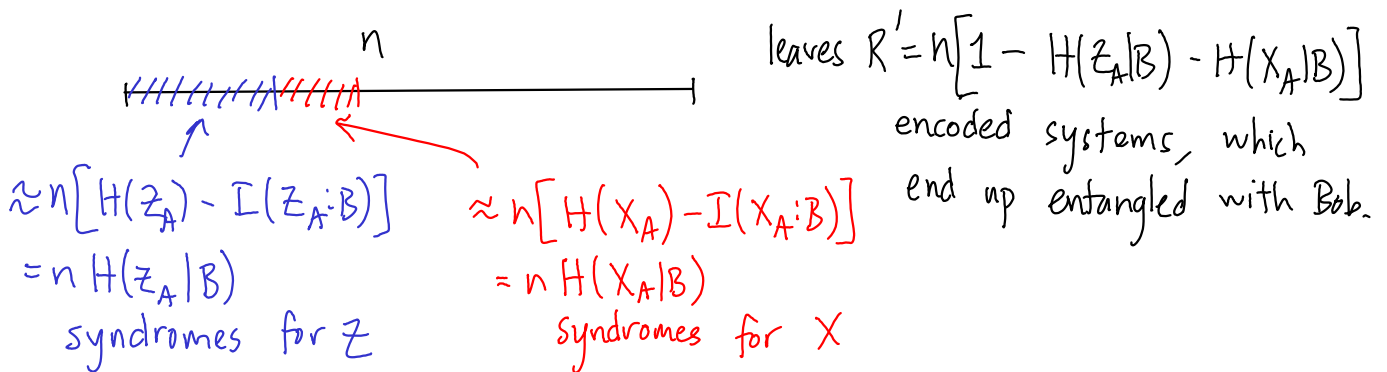
Use the HSW theorem! Over a channel, Alice can select a subset of  $K$  (codewords) such that the corresponding  $\varphi_k$  are more or less disjoint. The rate is given by  $\chi(P_k, \varphi_k) = I(Z_A; B)$

This also applies here - Alice can choose the codewords after the fact, as it were. Only a slight modification to the original proof.

Can use any 2-universal hash function to select the subset of  $k$ .

4. Great! So we know what Alice needs to send to Bob. But can she do both  $X$  and  $Z$ ? Yes! By using a CSS code. (random linear functions are 2-universal.) Measure syndromes and send to Bob.

And what about the rate. We want to get  $-S(A|B) = S(B) - S(AB)$ , the hashing bound. What do we have so far? Consider Alice's systems



Sadly  $\frac{R'}{n} \neq -H(A|B)$ . So we were stuck for a while.

It happens to be equal in cases of interest to QKD, but still unsatisfactory.

Wait a minute! After Bob receives the  $Z$  syndromes, he can determine  $k$ . Maybe this helps him with  $X$  somehow?

It does! Instead of basing her choice of  $X$  stabilizers on the state  $|\psi\rangle = \sum_x \sqrt{p_x} |\tilde{x}\rangle_A |\theta_x\rangle_{BE}$ , the relevant state for Alice is  $|\psi'\rangle = \sum_k \sqrt{p_k} |kk\rangle_{AC} |\varphi_k\rangle_{BE}$ , where  $C$  is a register holding the copy of  $k$ . Then we'll get  $R = n[1 - H(Z_A|B) - H(X_A|BC)]$

It turns out that  $r = \frac{R}{n} = 1 - H(A|B)$ , so it worked!

We created a protocol achieving the hashing bound by considering only  $X$  and  $Z$  information.

- Secret key distillation at the rate  $I(Z_A:B) - I(Z_A:E)$  follows immediately, once we establish that the purification of any secret key (called a private state) is such that

$$H(Z_A|B) = H(X_A|BS) = 0$$

where  $S$ , the shield, is whatever Alice and Bob share besides the key itself.

- State merging also works. We first need to compress Alice's system and then show how to adapt the HSW mmt for the conjugate basis. Not hard, but requires a little more work.

