QC Lecture, April 14

- Sec def: $\forall E \quad \exists \rho^{ideal}_{ABE} \in S_{ideal}$

  $TD(\rho^{real}_{ABE}, \rho^{ideal}_{ABE}) \cdot Pr[success] \le \varepsilon$

- Overview: Step 1: $A \longrightarrow B$ EPR-halves

  $|\beta_{00}\rangle := \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

  ρ^{init}_{ABE}

  today:
  - Step 2: "Bell test"

    ρ^{test}
  - Step 3: Measure raw key

  ⋮

$|\tilde{xy}\rangle := |\beta_{x_1y_1}\rangle \otimes |\beta_{x_2y_2}\rangle \otimes \cdots |\beta_{x_ny_n}\rangle$

We want: $|\tilde{00}\rangle$

<u>Idea:</u> Measure each qubit pair using $|\beta_{00}\rangle\langle\beta_{00}|$

<u>Pro:</u> If we pass this test, $\rho^{test} = |\tilde{00}\rangle\langle\tilde{00}|$

<u>Con:</u>
- To measure a qubit pair, need to put them together
- Eve could ~~do~~ do add. cheating while we transfer qubits
- If we move them to some "testing location", we lose them

<u>Idea 2:</u> Measure a randomly chosen subset of qubit pairs with $|\beta_{00}\rangle\langle\beta_{00}|$.

<u>Pro:</u>
- Even if test destroys tested pair, we have untested pairs left.
- If ~~most~~ all tested pairs were good $\Rightarrow$ most untested ones good

<u>Con:</u>
- Need to bring tested qubits into "testing location".

  $\Rightarrow$ Eve can change them.

<u>Idea 3:</u> Use a qubit test <u>s.t.</u> it can be done remotely (local quantum opers + class. comm) "LOCC"

but that tests something weaker than β_{00}.

Bell test

$m :=$ # qubit pairs

$q :=$ # to be tested

$n := m - q$ = # remaining qubit pairs

$t :=$ some parameter (rel to # of errors)

- A&B pick q distinct random indices from $\{1, \ldots, m\}$ (over auth channel)
- For each selected qubit pair:
  - With prob $\frac{1}{2}$, measure with proj:

    $|\beta_{00}\rangle\langle\beta_{00}| + |\beta_{01}\rangle\langle\beta_{01}|$

    (i.e.: test that qubit pair $\in span\{|\beta_{00}\rangle, |\beta_{01}\rangle\}$)

    (if we write state as $|\tilde{xy}\rangle$, meas x_i)
  - With prob $\frac{1}{2}$, —— " ————

    $|\beta_{00}\rangle\langle\beta_{00}| + |\beta_{10}\rangle\langle\beta_{10}|$

    (ie: test $\in span\{|\beta_{00}\rangle, |\beta_{10}\rangle\}$)

    (— " ——, meas y_i)
- Throw away tested qubit

What does this test achieve?

<u>Claim:</u> $\forall \rho_{init} \quad \exists \rho^{test}_{ideal} \in S^{test}_{ideal,t}$:

$TD(\rho^{test}_{ideal}, \rho^{test}) \le$ something small

Ideal pure states: $T_{ideal,t} := span\{|\tilde{xy}\rangle \otimes |\psi_E\rangle : |xy| \le t\}$

($|xy|$:= # of x_iy_i pairs $\neq 00$)

$S^{test}_{ideal,t} := \{\sum p_i |\psi_i\rangle\langle\psi_i| : |\psi_i\rangle \in T_{ideal}\}$

> ρ^{test} close to some probab. distr. of superpos. of Bell pairs with t errors

Simple case: Assume $\rho_{init} = |\tilde{xy}\rangle\langle\tilde{xy}|$ with $|xy| > t$

There are $\ge t+1$ i <u>s.t.</u> $x_iy_i \neq 00$

$\Rightarrow$ Each tested qubit pair is $x_iy_i \neq 00$ ("bad") with prob. $\ge \frac{t+1}{m}$

If it is bad, Bell test fails on that qubit with prob. $\ge 1/2$

$\Rightarrow$ Each test succeeds with prob. $\le 1 - \frac{t+1}{2m}$

$\Longrightarrow Pr[\text{all tests succeed}] \le \left(1 - \frac{t+1}{2m}\right)^q =: \delta_q$

(cheated: this is only obvious if tests are indep.)

In general, ρ_{init} not of this simple form.

Define: $P_{ok} :=$ proj. on $T_{ideal,t} = \{|\tilde{xy}\rangle \otimes |\psi_E\rangle : |xy| \le t\}$

By tedious calculation:

$Pr[P_{ok} \text{ says yes given } \rho_{test}] \ge 1 - \frac{\delta_q}{Pr[success]}$

<u>Thm:</u> If $Pr[P \text{ says yes given } \rho] \ge 1-\varepsilon$ then $\exists \tilde{\rho}$ s.t.:
- $TD(\rho, \tilde{\rho}) \le \sqrt{\varepsilon}$
- $\hat{\rho} = \sum p_i |\psi_i\rangle\langle\psi_i|$ for $|\psi_i\rangle \in im\, P$

<u>Here:</u> $\exists \rho^{test}_{ideal}$: $\quad TD(\rho_{test}, \rho^{test}_{ideal}) \le \sqrt{\frac{\delta_q}{Pr[success]}}$

and $\rho^{test}_{ideal} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ for $|\psi_i\rangle \in im\, P_{ok} = T_{ideal,t} = \{|\tilde{xy}\rangle \otimes |\psi_E\rangle : |xy| \le t\}$

($\in S^{test}_{ideal,t}$)

<u>Summary:</u> $\forall \rho_{init}: \exists \rho^{ideal}_{test} \in S^{test}_{ideal,t}$:

$TD(\rho_{test}, \rho^{test}_{ideal}) \cdot Pr[success] \le \sqrt{\frac{\delta_q}{Pr[success]}} \cdot Pr[success]$

$\le \sqrt{\delta_q}$

<u>Step 3:</u> Measure A's/B's state

We get: A, B have class key, E still has q state

$\rho_{rawkey} = \sum_{k_A,k_B} p_{k_Ak_B} |k_A\rangle\langle k_A| \otimes |k_B\rangle\langle k_B| \otimes \rho_E$

We can ask two questions:
- Is $K_A = K_B$? Or at least $|K_A \oplus K_B| \le t$?
- With what prob. can E guess K_A? (Or K_B?)

→ If $\rho_{test} \in S^{test}_{ideal}$: $|K_A \oplus K_B| \le t$ holds for ρ_{rawkey}

→ If $\rho_{test} \in S^{test}_{ideal}\left(= S^{t\text{-}error}_{ideal}\right)$: $Pr[E \text{ guesses } K_A \text{ for } \rho_{rawkey}]$

$\le (3n+1)^t \cdot 2^{-n}$

<u>Def:</u> min-entropy: K, E are parts of q system, K class.

$H_\infty(K|E) := -\log \max_F Pr[K = x : x \leftarrow F \text{ on } E]$

(pr. of guessing K given E)

<u>Example:</u>

K is indep of E, uniform n-bit: $Pr[K = x] \le 2^{-n}$

$\Rightarrow H_\infty(K|E) = n$

<u>Example</u> K uniform n bits, E = last 5 bits of K

$\Rightarrow Pr[K = x] \le 2^{-(n-5)} \Rightarrow H_\infty(K|E) = n - 5$

$\Rightarrow$ If $\rho_{test} \in S^{test}_{ideal} \Longrightarrow H_\infty(K_A|E) \ge -\log (3n+1)^t \cdot 2^{-n}$

$= n - t\log(3n+1)$

<u>Conclusion:</u> If $\rho_{test} \in S^{test}_{ideal}$: $\rho^{rawkey} \in S^{raw}_{ideal}$

$S^{ideal}_{raw} := \{\rho : H_\infty(K_A|E) \ge n - t\log(3n+1), |K_A \oplus K_B| \le t\}$

$\forall \rho_{init}: TD(\rho_{test}, \rho^{ideal}_{test}) \cdot Pr[succ] \le \sqrt{\delta_q}$

$\Rightarrow TD(step3(\rho_{test}), step3(\rho^{ideal}_{test})) \cdot Pr[success] \le \sqrt{\delta_q}$

($step3(\rho_{test}) = \rho_{rawkey}$, $step3(\rho^{ideal}_{test}) \in S^{raw}_{ideal}$)

> $\Rightarrow TD(\rho_{rawkey}, \rho_{ideal}) \cdot Pr[success] \le \sqrt{\delta_q}$
>
> for some $\rho_{ideal} \in S^{raw}_{ideal}$