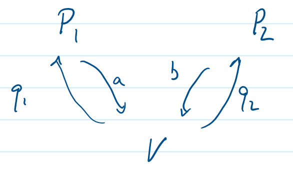
Lecture 2 - Compilation of nonlocal games

Wednesday, 22 January 2025 15:48

Recall: a nonlocal game is



$(q_1, q_2) \sim \pi$
check $a, b \mid q_1, q_2$.

ex: MS game $q_1 = \ell \in \{r_1, r_2, r_3, c_1, c_2, c_3\}$
$q_2 = j \in \{1, \dots, 9\}$
check parity constraints

Today: NL game + crypto assumption QFHE $\Rightarrow$ 1. prover - interactive test of quantumness.

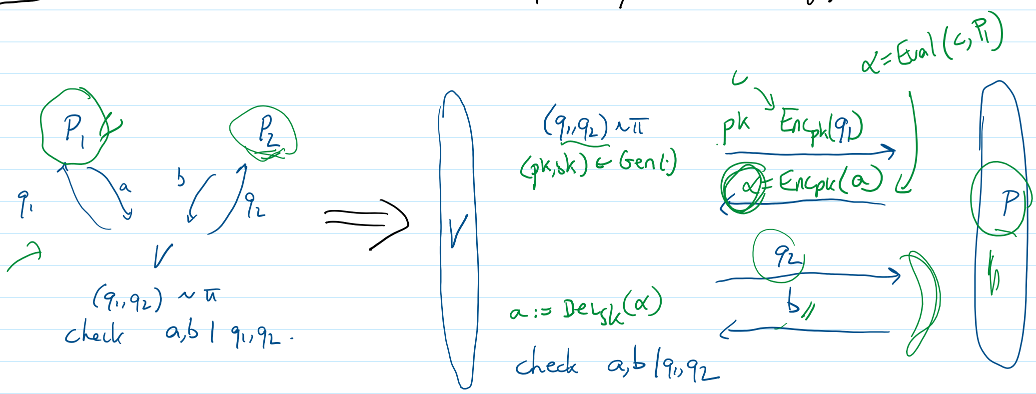
<u>Def</u> A computationally sound test of quantumness is a classical polytime verifier V s.t.

- $\exists$ a BQP prover P s.t. V accepts P w.p. $\geq 2/3$
- $\forall$ BPP prover P, ―――――― $\leq 1/3$

<u>Rk</u> • At a minimum, need to assume BPP $\neq$ BQP
We will assume that post-q. hardness of LWE

- Idea of compilation widely used classically, to construct <u>efficient</u> (communication, verifier and prover runtimes) arguments for e.g. NP.

Idea (due to Kalai et al. '22 for the quantum setting):



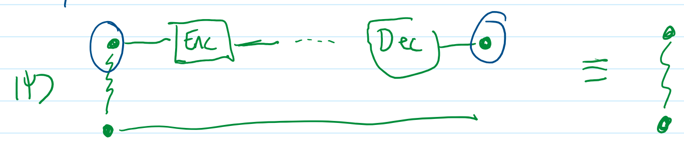
Def A QFHE scheme is (Gen, Enc, Eval, Dec) s.t.:

- $(pk, sk) \leftarrow Gen(1^\lambda)$
- $c \leftarrow Enc_{pk}(m)$
- $c' \leftarrow Eval_{pk}(c, F)$
- $m' \leftarrow Dec_{sk}(c')$

correctness: $m' = F(m)$

* Also works if F is a quantum circuit
$\longrightarrow$ c' is a quantum state

* Preserves quantum correlations



$\rightarrow$ G a nonlocal game

$\omega :=$ max succ prob (classical)

$\omega^* :=$ ———— (quantum)

$\rightarrow V = V(G)$ the verifier in the compiled protocol

$\bar{\omega} =$ max succ prob (classical)

$\bar{\omega}^* =$ ———— (quantum)

Kalai

single-prover

$\bar{\omega}^* =$ ______ (quantum)

Kalai

Lemma 3 : $\forall G, \quad \bar{\omega}^* \geq \omega^*$

Natarajan · Zhang

Lemma 4 : $\forall G, \quad \bar{\omega} \leq \omega + negl(\lambda)$

single-prover test of quantumness

Lemma 5 : For G^{CHS}, $\quad \bar{\omega}^* \leq \omega^* + negl(\lambda)$

Moreover, [some statement about anti-commutation]

Lemma 3 : $\forall G, \quad \bar{\omega}^* \geq \omega^*$

Proof of Lemma 3

Create $|\psi\rangle$ shared by P_1 and P_2 in G

V:

$(q_1, q_2) \sim \pi$

$(pk, sk) \leftarrow Gen$

$c \leftarrow Enc_{pk}(q_1)$

$\xrightarrow{pk \quad c}$

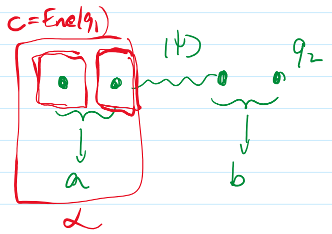
$\xleftarrow{\alpha}$ $\qquad \alpha := Eval(c, P_1)$

$\xrightarrow{q_2}$

$a \leftarrow Dec_{sk}(\alpha)$

$\xleftarrow{b}$

check $a, b \mid q_1, q_2$



Lemma 4 : $\forall G, \quad \bar{\omega} \leq \omega + negl(\lambda)$

Proof of Lemma 4

→ Suppose P succeeds w.p. $\bar{\omega}$ against V

- Define P_1, P_2 :
  - Fix $(q_1', q_2') \sim \pi$. Let $c' := Enc(q_1')$ Game starts.
  - P_2 : Receive q_2
    Respond as P, if first message from V was c'
  - P_1 : Receive q_1
    For every $q_2'' \sim q_1$, compute b'' as P_2
    Return a that maximizes exp. win prob.

for every $q_2 \sim q_1$, compute b as P_2

Return a that maximizes exp. win prob.

- Let w be P_1, P_2 success prob in the nonlocal game.

Obs 1: Conditioned on $q_1 = q_1'$, $w \geq \bar{w}$

- P_2's answer is distributed exactly as P_1's second answer
- P_1's strategy can only lead to an improvement

Obs 2: Suppose that $w \ll \bar{w}$, conditioned on $q_1 \neq q_1'$

$\rightarrow$ break semantic security of encryption scheme

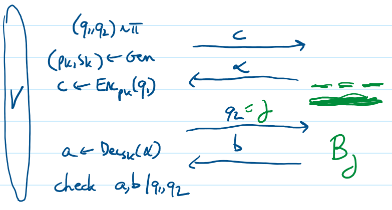
need to make P_1 efficient using sampling.

lemma 5: For $G = MS$, $\bar{w}^* \leq \overset{1}{w^*} + negl(\lambda)$

Moreover; [some statement about anti-commutation]

Proof of lemma 5:

§



$B_2 B_4 = - B_4 B_2$

Prover strategy:

- $|\psi_{c\alpha}\rangle$: state conditioned on receiving c and returning α

$$\{ |\psi_{c\alpha}\rangle \}_{\substack{c \leftarrow Enc(q_1) \\ \alpha}} \underset{ind}{\simeq} \{ |\psi_{c'\alpha'}\rangle \}_{\substack{c' \leftarrow Enc(q_1') \\ \alpha'}}$$

- B_j : observable measured in second round, on receiving question j

win w.p. $\simeq 1$ $\Rightarrow$ relations:

- If $c = Enc(\ell)$ and $j \in \ell$ then

$$B_j |\psi_{c\alpha}\rangle = (-1)^{Dec(\alpha)_j} |\psi_{c\alpha}\rangle$$

- If $c = \mathrm{Enc}(\ell)$ and $\ell = \{j_1, j_2, j_3\}$ then

$$B_{j_1} B_{j_2} |\psi_{c\alpha}\rangle = \pm 1 B_{j_3} |\psi_{c\alpha}\rangle$$

- B_j are BQP observables so any polynomial in them can be efficiently implemented

$$\begin{matrix} \boxed{Y_1} & Y_2 & Y_3 \\ Y_4 & Y_5 & Y_6 \\ Y_7 & Y_8 & \boxed{Y_9} \end{matrix}$$

Following

Lemma 2: If $Y_1, \ldots, Y_9$ are a (non-commutative) Solution to the Magic Square, then $Y_2 Y_4 = -Y_4 Y_2$

$$\mathop{\mathbb{E}}_{c,\alpha} \left\| \left(B_2 B_4 + B_4 B_2 \right) |\psi_{c\alpha}\rangle \right\|^2 \leq \mathrm{negl}(\lambda)$$

Rk: Proof is indirect. In general, round to commuting strategies

Summary of Lectures 1 + 2:

- Magic square game: two-player, one-round game s.t. Classical players win w.p. $\leq 17/18$
  quantum ———————— $= 1$

  Good quantum players need to use incompatible measurements

- "Compiled" Magic Square game is two-round classical verifier game s.t.

  Classical polytime prover wins w.p. $\leq \frac{17}{18} + \mathrm{negl}$

Quantum prover can win w.p. 1

Good polytime quantum prover must use incompatible measurements.

Next Time: