Non-signaling theories and Key-distribution:

(Mohammad Bavarian 04/17/13)

1. CHSH Recap: (2 player 1 round game)

$$\begin{matrix} x \longrightarrow \boxed{A} \longrightarrow a \\ y \longrightarrow \boxed{B} \longrightarrow b \end{matrix}$$ wins if $V(x,y,a,b)$ satisfied

in CHSH: $V(x,y,a,b)$: $a \oplus b = xy$ $\left\{ \begin{array}{l} \omega_c = 75\% \\ \omega_q = 85\% \end{array} \right.$

2. Non-signaling (NS) distributions $p(ab|xy)$: Examples & "Non-examples"

Comment: non-local N.S. distributions are "classically" not achievable

i) Non-example: Game $\begin{matrix} x \longrightarrow \boxed{A} \longrightarrow a = y \\ y \longrightarrow \boxed{B} \longrightarrow b = x \end{matrix}$ wins

Claim: no N.S. advantage

a signaling distribution wins! $p(ab|xy) = \mathbb{1}(a=y)\,\mathbb{1}(b=x)$

Diagram:

		=0 - x - =1			
		=0 a =1			
=0	=0 b	1	0	0	0
	=1	0	0	1	0
y		0	1	0	0
=1		0	0	0	1

$\cancel{b}$- Marginal $\longrightarrow$

1	0	1	0
0	1	0	1

depends on y! ⇒ signaling

Definition: Non-signaling distribution $p(ab|xy)$:⟺

$$\forall a, x, y \,\&\, y' : \quad p(a|xy) \equiv \sum_b p(ab|xy) \overset{!}{=} \sum_b p(ab|xy') \equiv p(a|xy')$$

and $\forall b, y, x \,\&\, x'$: $p(b|xy) = p(b|x'y)$

[this def extends to the multipartite case]

ii) Further game:

$$\begin{matrix} x \longrightarrow \boxed{A} \longrightarrow a \\ y \longrightarrow \boxed{B} \longrightarrow b \end{matrix}$$ wins if $a=b$ (winable classically by agreeing on the same output.)

"Claim": Non-signaling distributions which are <u>not-local</u> imply monogamy

iii) <u>Example:</u> Popescu-Rohrlich box (wins CHSH game)

$$P_{PR}(ab|xy) = \begin{cases} \frac{1}{2} : & a \oplus b = xy \\ 0 : & \text{else} \end{cases}$$

	a		x	
b	1/2	0	1/2	0
	0	1/2	0	1/2
y	1/2	0	0	1/2
	0	1/2	1/2	0

with Marginal $p(a|x) = p(b|y) = \frac{1}{2}$

$\Rightarrow$ N.S.

<u>Theorem:</u> (Monagamy) suppose we have 3 parties A, B, E with N.S. dist. $p(abe|xyz)$

s.th: the marginal $p(ab|xy) = P_{PR}(ab|xy)$

$\Rightarrow$ "secrecy". i.e. one has $\Pr\{b = e\} = \frac{1}{2}$ with uniform inputs x, y, z

(Modest goal)

<u>Proof:</u>

<u>Stronger Thm</u>(Excersise) $\forall$ ab, xy s.th $a \oplus b = xy$

$\forall$ e_0 $\Pr(e_0) > 0$

$\Rightarrow$ $\Pr(ab|xye_0) = \frac{1}{2}$

(conditoned on e_0 the dist. still looks like PR-box)

3. QM allows crypto & Intro to N.S. crypto:

i) one time pad A & B share random keys

Send message m with length(m) = length(s)

$\underset{m,s}{\boxed{A}} \xrightarrow[m\oplus s]{} \underset{s}{\boxed{B}}$ decipher $m = m \oplus s \oplus s$

$m \oplus s$ is random when s is!

ii) N.S. Key distribution:

0) A & B meet to generate N.S. distributon (e.g. exchange Bell pairs....)

1) k.n uses of N.S. box, generate x_i, y_i locally & random

$x_1 \longrightarrow \boxed{A} - a_1$ $x_{kn} \longrightarrow \boxed{a} \rightarrow a_{kn}$

$y_1 \rightarrow \boxed{B} \rightarrow b_1$ .... $y_{kn} \longrightarrow \boxed{B} \rightarrow b_{kn}$

2) announce all (x_i, y_i) publicly. choose n points where $x_i = y_i$.
Since we have $x_i = y_i$ N.S. dist implies $a_i = b_i$

3) announce other points for k-1 at random (a_i, b_i) to check whether we have PR-box. If yes ↪ "Monogamy implies secrecy" and key is good.

4. Quantum protocals

Requirements: $\begin{cases} \text{noise free Q-channel} \\ \text{authenticated classical channel} \end{cases}$

i) "Eckert's" protocoll

0) A & B share n EPR-pairs: $\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)^{\otimes n}$

1) A draws $x_i \in \{0,1,2\}$ uni-random and measures in Basis
$\Theta^a_0 = 0$, $\Theta^a_1 = \frac{\pi}{4}$, $\Theta^a_2 = \frac{\pi}{8}$
B draws $Y_i \in \{0,1,2\}$ and measures in $\Theta^b_0 = \frac{\pi}{3}$, $\Theta^b_1 = \frac{\pi}{4}$, $\underbrace{\Theta^b_2 = -\frac{\pi}{8}}_{\text{actually not needed}}$,

2) A & b announce their list $\{x_i\}$ & $\{Y_i\}$ publicly!

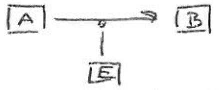
3) generate 2 Groups: grp 1: $\{ i \in [n] \mid \text{with } (x_i, y_i) = (1,1) \}$
grp 2: $\{ i \in [n] \mid \text{else} \}$

use grp2 to check Bell-violation:

4) If Bell inequality not violated, discard.
else use outcomes of grp1 measurement as secret key.

Claim: securiy through monogamy: Proof is hard, uses de-Finetti to reduce [illegible] attacks for Eve.

Simple Attack:



Eve copies qubit in $\frac{\pi}{4} = \theta_2$ basis

$$\Rightarrow \left(\tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)^{\otimes n} |0\rangle_E^{\otimes n} \rightarrow \left(\tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\right)^{\otimes n}$$

reduced state $\rho_{AB} = \left(\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)\right)^{\otimes n} \neq \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)^{\otimes n}$

does not violate Bell

$\hookrightarrow$ securiy through monogamy!

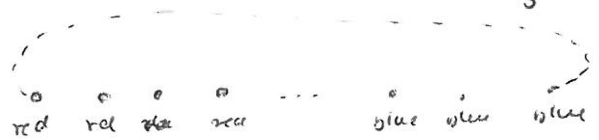
ii) BHK Protocol & The path game

2 Player A & B (size of Game N)

1) Input: integer $x \bmod_N \in [0,1,\dots,N-1]$ s.th $(x-y) \bmod_N \in \{0,1,-1\}$
output: a^* & b^* in $\{0,1\}$

2) Referee's predicate : take (a,b) post process. $b = b^*$
if $(x,y) = (0,N-1) \vee (N-1,0)$ $a = 1-a^*$, otherwise $a = a^*$: Check $a^* = b^*$

3) Classical value of Game: $1 - \frac{2}{3}N$. Quantum $1 - \mathcal{O}(\frac{1}{N^2})$ => asymptotic separation



$\Big\{$ two ends •—• same colour
front & back with differt colors.

BHK Protocol Two parameters: $M \ll N$ $M \approx N^{3/4}$ large integers

1) A & B share MN^2 entangled states $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

2) For MN^2 devices choose uniformly @ random $y_i, x_i \in [0,\dots,N-1]$
and measure qubits in basis $\theta_i = \frac{\pi y_i}{2N}$

3) announce all (x_i, y_i) publicly : Discard any output if $(x_i - y_i) \bmod_N$
is not $\{-1,0,1\}$

4) If # good devices $< 2MN$ abort.

5) Good devices: A choose random s (single outcome)
and announces the rest. Bob checks whether they are the same as
his outputs. If not abort. else keep s as secret shared bit.

Produces single bit s, with $\varepsilon = poly(N^{-}$[illegible]$)$ security.