CHSH game with weak randomness source and its use in relativistic bit-commitment

Matej Pivoluska, Marcin Pawłowski, Martin Plesch

Masaryk University, Brno & Institute of Physics, Slovak Academy of Sciences, Bratislava

1st September 2016

arXiv:1601.08095 or Phys. Rev. A 94, 022338

Outline

- CHSH game and its generalizations
- New tight bound on a variant of CHSH with weak randomness
- Relativistic bit-commitment

Non-local games

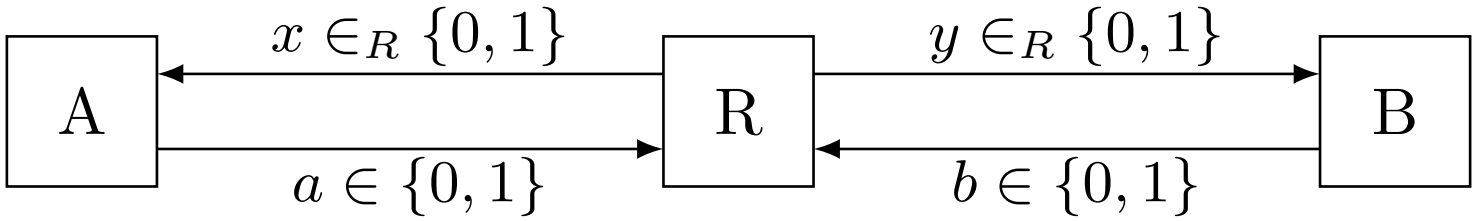
- Two non-communicating players cooperate to win the game
- A referee chooses questions (x, y) according to a known distribution π
- Players receive questions x and y and produce answers a and b respectively
- Players win if $V(x, y, a, b)$ is satisfied (V is a relation)

Non-local games

- Two non-communicating players cooperate to win the game
- A referee chooses questions (x, y) according to a known distribution π
- Players receive questions x and y and produce answers a and b respectively
- Players win if $V(x, y, a, b)$ is satisfied (V is a relation)
- Probability to win a game G with best *classical strategy* is denoted $\omega(G)$
- Probability to win a game G with best *quantum strategy* is denoted $\omega^*(G)$

CHSH game

Arguably the most studied game is the CHSH [1] game



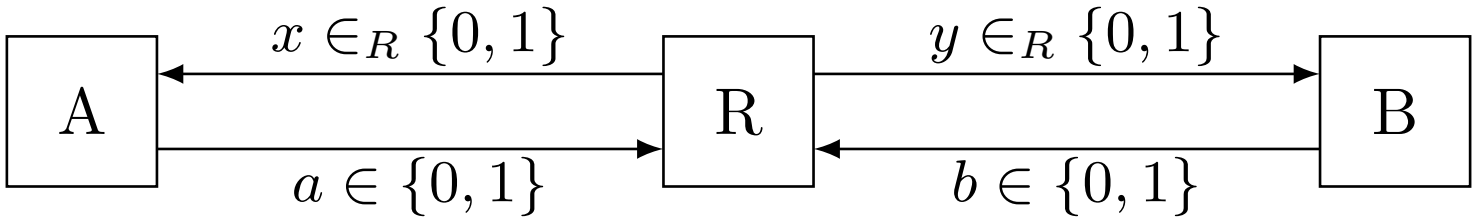
$$a + b = xy \mod 2$$

- $x, y, a, b \in \{0, 1\}$
- (x, y) distributed uniformly

[1] Clauser, Horne, Shimony, Holt, PRL 23, 1969

CHSH game

Arguably the most studied game is the CHSH [1] game



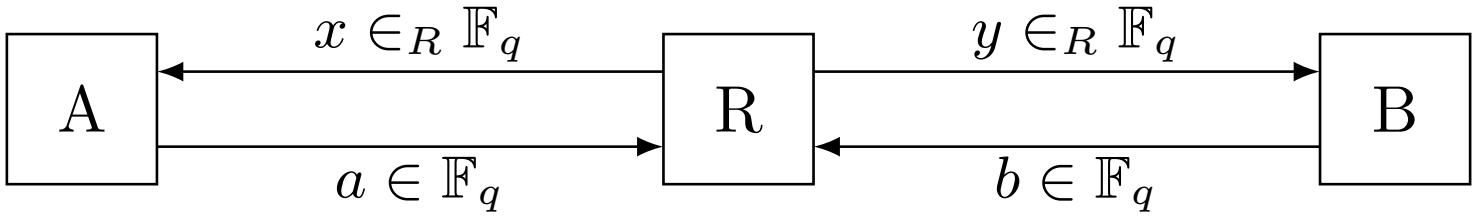
$$a + b = xy \mod 2$$

- $x, y, a, b \in \{0, 1\}$
- (x, y) distributed uniformly
- $\omega(\mathrm{CHSH}) = \frac{3}{4}$ and $\omega^*(\mathrm{CHSH}) = \frac{2+\sqrt{2}}{4} \approx 0.85$

[1] Clauser, Horne, Shimony, Holt, PRL 23, 1969

CHSH_q games

Parametrization q increases the alphabet size [2]



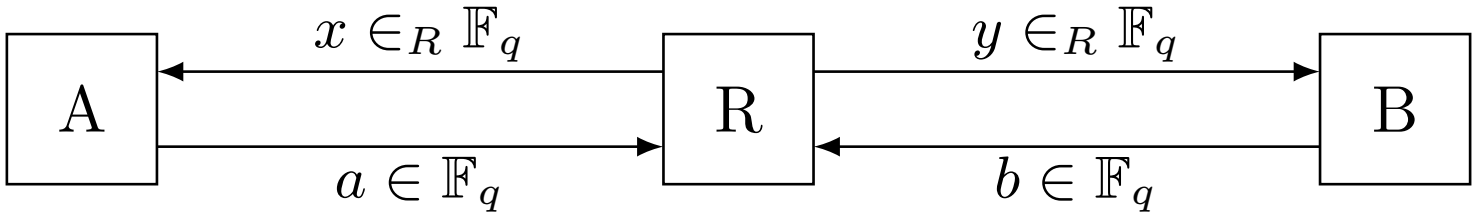
$$a + b = xy$$

- $x, y, a, b \in \mathbb{F}_q$
- (x, y) distributed uniformly
- Addition and multiplication are operations in $\mathbb{F}_q$

[2] see e.g. MPx2, NJP, vol. 18, 2016 or Bavarian and Shor, arXiv: 1311.5186

CHSH_q games

Parametrization q increases the alphabet size [2]



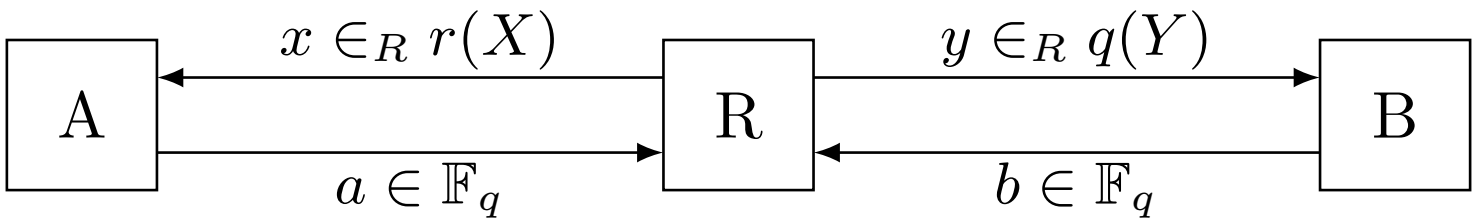
$$a + b = xy$$

- $x, y, a, b \in \mathbb{F}_q$
- (x, y) distributed uniformly
- Addition and multiplication are operations in $\mathbb{F}_q$
- Only upper bounds are known for $\omega(\mathrm{CHSH}_q)$ and $\omega^*(\mathrm{CHSH}_q)$

[2] see e.g. MPx2, NJP, vol. 18, 2016 or Bavarian and Shor, arXiv: 1311.5186

CHSH_q games with non-uniform questions

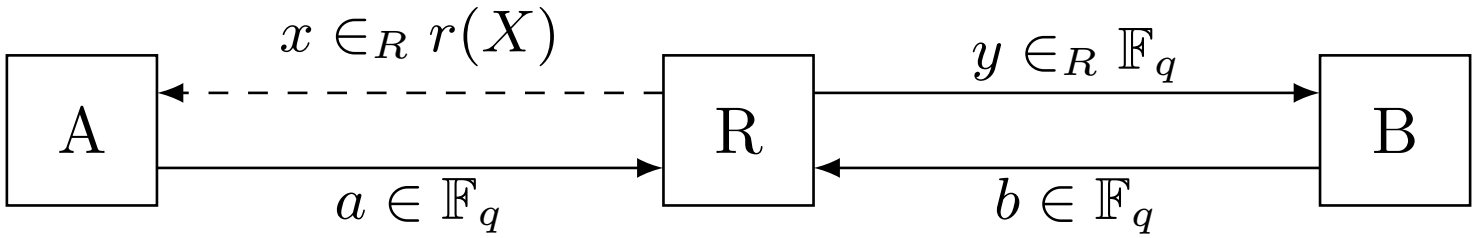
Further generalizations changes the probability distribution of the questions



$$a + b = xy$$

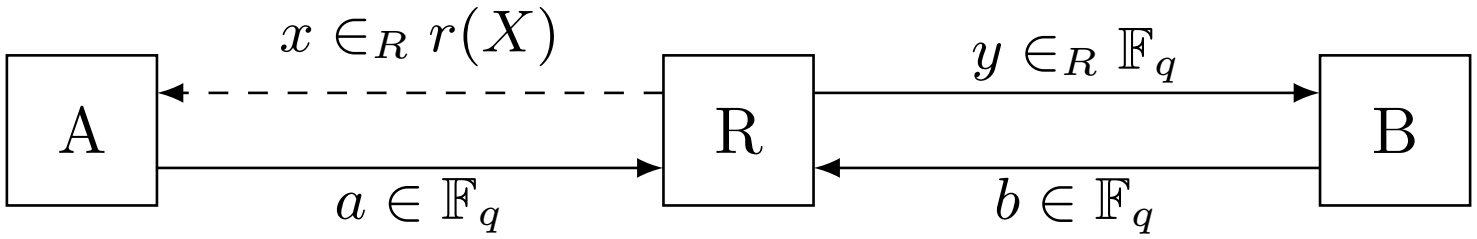
- $x, y, a, b \in \mathbb{F}_q$
- $r(X)$ and $q(Y)$ are independnent (possibly non-uniform) probability distributions
- Addition and multiplication are operations in $\mathbb{F}_q$

A family of CHSH_q games with a weak source



$$a + b = xy$$

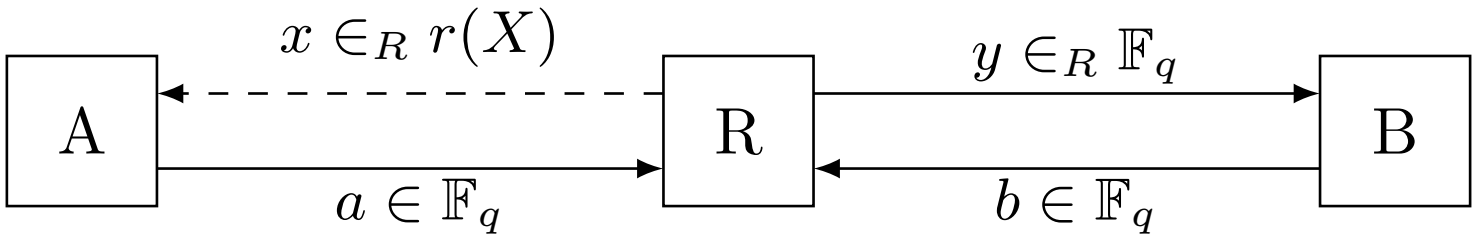
A family of CHSH_q games with a weak source



$$a + b = xy$$

- $q(Y)$ is uniform
- Device producing x is not fully under control of the referee
- It might be a result of some (not fully characterized) random process – *e.g.* past run of the protocol
- Guarantee: Alice (and more importantly Bob) cannot guess x with probability better than p, *i.e.* $max_{x \in \mathbb{F}_q} r(x) \leq p$, *i.e.* $H_{\min}(X) \geq -\log_2(p)$

A family of games $\mathrm{CHSH}_q(p)$

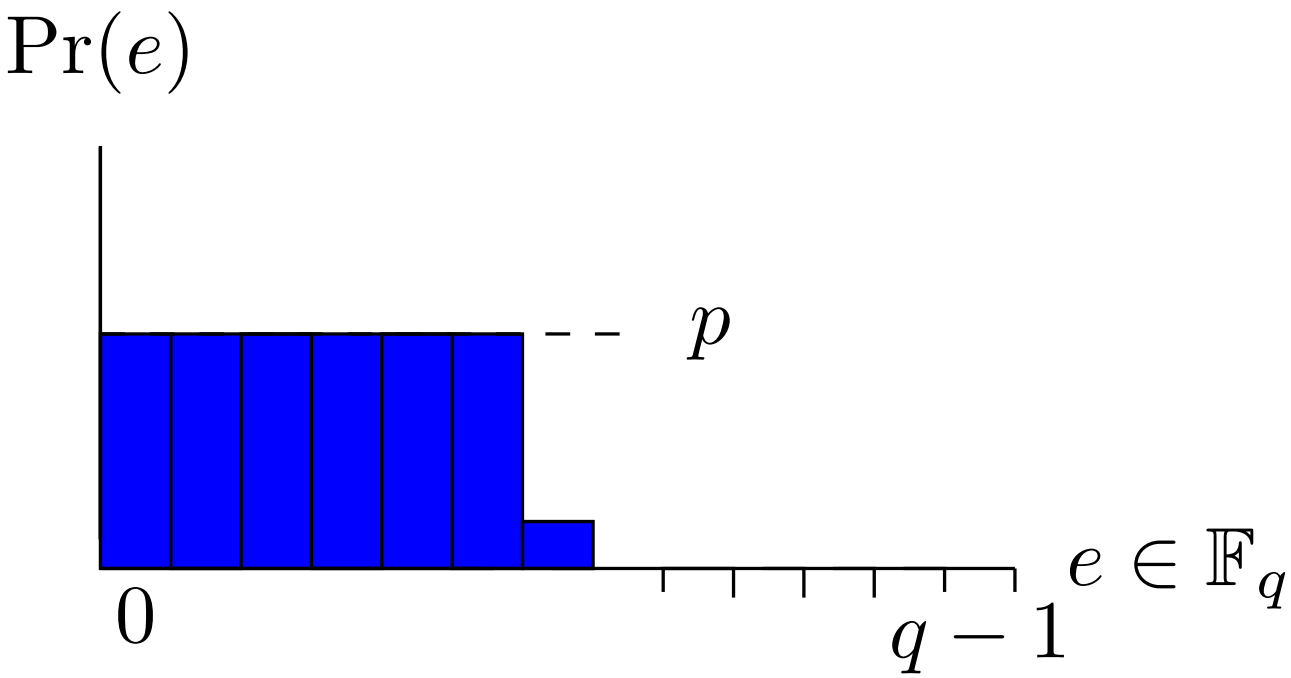


$$a + b = xy$$

- How to characterize winning probability of this scenario?
- Referee doesn't know exactly which non-local game is played
- Many games are possible – they differ in Alice's input distribution
- $\mathrm{CHSH}_q(p)$ – family of games with $max_{x \in \mathbb{F}_q} r(x) \leq p$
- $\omega(\mathrm{CHSH}_q(p)) = \max_{G_i \in \mathrm{CHSH}_q(p)}(\omega(G_i))$

The easiest game in $\mathrm{CHSH}_q(p)$

- We need to characterize the easiest game in $\mathrm{CHSH}_q(p)$
- For *every* fixed strategy (*i.e.* deterministic response functions of Alice and Bob), the optimal Alices input distribution is (almost) flat
- What is the best classical strategy for (almost) flat distributions?



Towards upper bound – point-line incidence problem

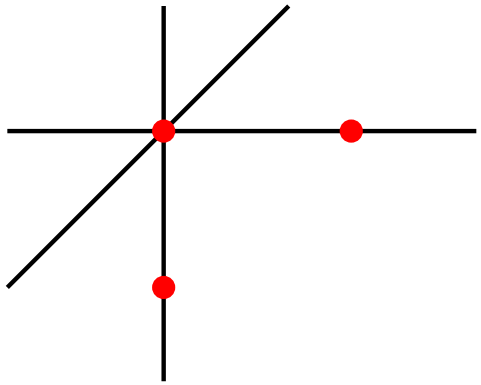
- Both points and lines in $\mathbb{F}_q^2$ can be defined by a pair of numbers
- A line $\ell_{a,b}$ characterized by $(a, b) \in \mathbb{F}_q^2$ contains all points (x, y) such that $y = ax + b$.

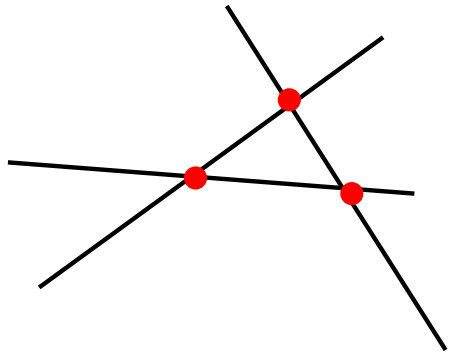
Towards upper bound – point-line incidence problem

- Both points and lines in $\mathbb{F}_q^2$ can be defined by a pair of numbers
- A line $\ell_{a,b}$ characterized by $(a, b) \in \mathbb{F}_q^2$ contains all points (x, y) such that $y = ax + b$.
- A line $\ell_{a,b}$ and point (x, y) are incident if $(x, y) \in \ell_{a,b}$
- Point line incidence problem: How many incidences can a set of points P of size $|P| = n$ and set of lines L of size $|L| = k$ have?

Towards upper bound – point-line incidence problem

- Both points and lines in $\mathbb{F}_q^2$ can be defined by a pair of numbers
- A line $\ell_{a,b}$ characterized by $(a, b) \in \mathbb{F}_q^2$ contains all points (x, y) such that $y = ax + b$.
- A line $\ell_{a,b}$ and point (x, y) are incident if $(x, y) \in \ell_{a,b}$
- Point line incidence problem: How many incidences can a set of points P of size $|P| = n$ and set of lines L of size $|L| = k$ have?





CHSH_q strategy as an incidence problem

- Recall the winning condition is $a + b = xy$

CHSH_q strategy as an incidence problem

- Recall the winning condition is $a + b = xy$
- Bob has a set of lines $L = \{\ell_{y,-b}\}_{y \in \mathbb{F}_q}$
- Alice has set of points $P = \{(x, a)\}_{x \in \mathbb{F}_q}$
- P does not contain points above each other
- L does not contain lines with the same slope
- They win the CHSH_q game iff (x, a) lies on $\ell_{y,-b}$

CHSH_q strategy as an incidence problem

- Recall the winning condition is $a + b = xy$
- Bob has a set of lines $L = \{\ell_{y,-b}\}_{y \in \mathbb{F}_q}$
- Alice has set of points $P = \{(x, a)\}_{x \in \mathbb{F}_q}$
- P does not contain points above each other
- L does not contain lines with the same slope
- They win the CHSH_q game iff (x, a) lies on $\ell_{y,-b}$
- Let $I(n, k)$ be the maximum number of incidences between n points and k lines
- In CHSH_q with uniform inputs we have $n = k = q$
- $\omega(\mathrm{CHSH}_q) \leq \frac{I(q,q)}{q^2}$

Hardness of the incidence problem

- How hard is the incidence problem?

[3] [Geometric and Functional Analysis, 14(1), 2004]

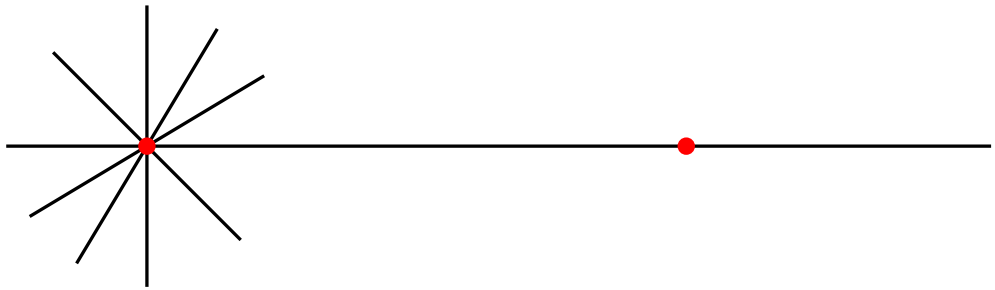
Hardness of the incidence problem

- How hard is the incidence problem?
- Generally very hard
- Breakthrough result by Bourgain, Katz and Tao[3] shows that $I(n,n) \leq n^{\frac{3}{2}-\epsilon}$

[3] [Geometric and Functional Analysis, 14(1), 2004]

Hardness of the incidence problem

- How hard is the incidence problem?
- Generally very hard
- Breakthrough result by Bourgain, Katz and Tao[3] shows that $I(n,n) \leq n^{\frac{3}{2}-\epsilon}$
- However, easy for instances, where $|L| \gg |P|$
- $I(2,k) = k+1$



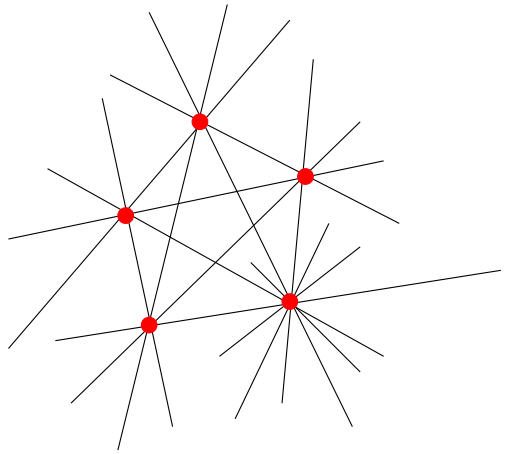
[3] [Geometric and Functional Analysis, 14(1), 2004]

The size of $|P|$ and $|L|$ in $\mathrm{CHSH}_q(p)$

- Suppose a fixed strategy $(x, a), (y, b)$
- Bob receives uniformly one of q questions
- Alices distribution is flat
- This results in instance $|P| = \left\lceil \frac{1}{p} \right\rceil$ and $|L| = q$

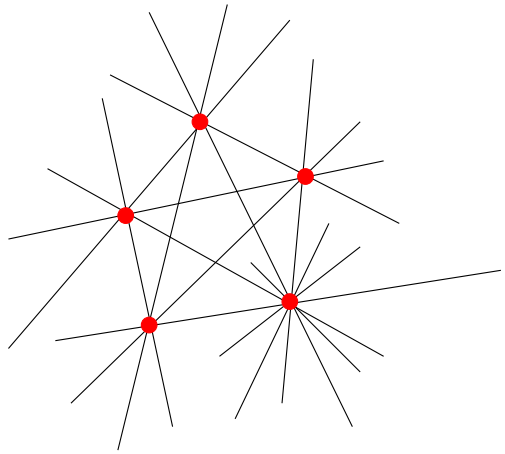
The easy instances

- If we have enough lines, the complete graph is optimal



The easy instances

- If we have enough lines, the complete graph is optimal

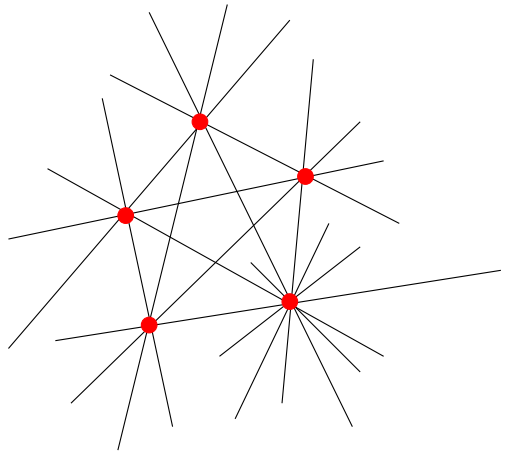


- For $n = \left\lceil \frac{1}{p} \right\rceil$ and $q \geq \frac{n(n-1)}{2}$,

$$\omega(\mathrm{CHSH}_q(p)) \leq p + \frac{n-1}{q}\left(1 - \frac{np}{2}\right).$$

The easy instances

- If we have enough lines, the complete graph is optimal



- For $n = \left\lceil \frac{1}{p} \right\rceil$ and $q \geq \frac{n(n-1)}{2}$,

$$\omega(\mathrm{CHSH}_q(p)) \leq p + \frac{n-1}{q}\left(1 - \frac{np}{2}\right).$$

- If restrictions for a proper CHSH_q strategy can be fulfilled, this is tight
- We have a construction with restrictions for $q > (n-1)\left[\frac{(n-2)^2}{2} + 1\right]$

Comparison to the best known upper bound

- For $p > \frac{1}{\sqrt{2q}}$,

$$\omega(\mathrm{CHSH}_q(p)) \leq p + \frac{1}{2pq}.$$

Comparison to the best known upper bound

- For $p > \frac{1}{\sqrt{2q}}$,

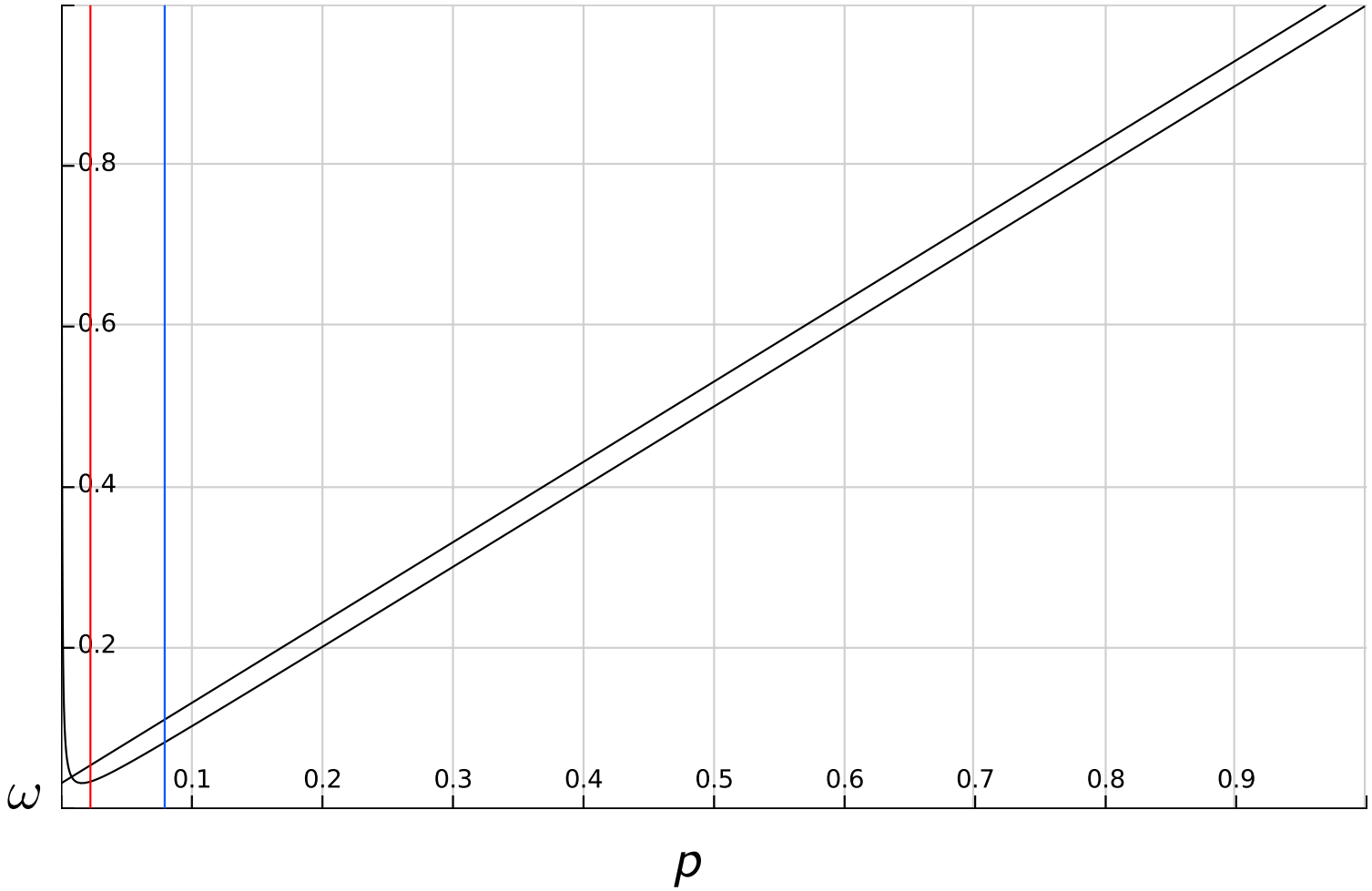
$$\omega(\mathrm{CHSH}_q(p)) \leq p + \frac{1}{2pq}.$$

- Best previous bound [Chakraborty et. al., PRL 115, 250501, 2015]:

$$\omega(\mathrm{CHSH}_q(p)) \leq p + \sqrt{\frac{2}{q}}.$$

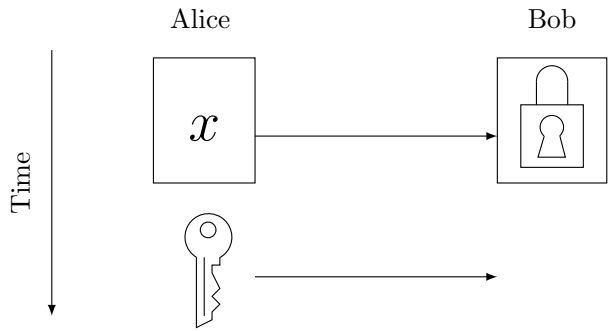
Comparison to the best known upper bound

Plot for $q = 2017$:



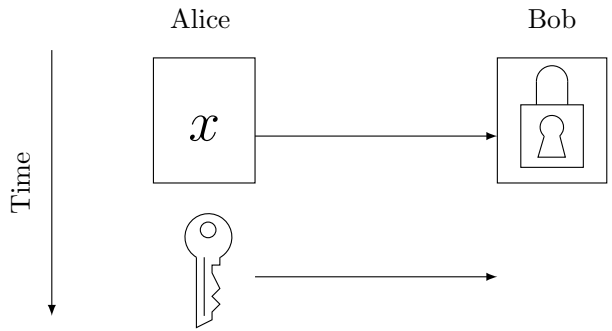
Bit commitment

- Goal:
  - Alice commits to a bit x
  - Later she reveals her commitment



Bit commitment

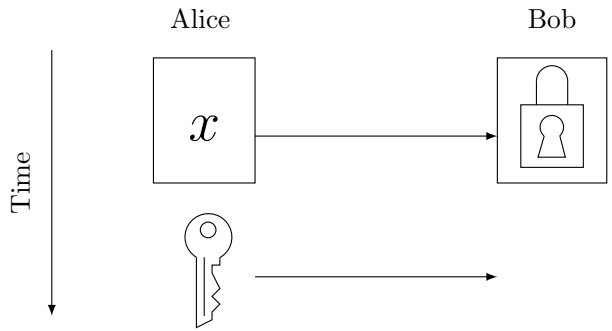
- Goal:
  - Alice commits to a bit x
  - Later she reveals her commitment



- Requirements:
  - Alice cannot reveal $\neg x$ if she commited to x (binding)
  - Bob cannot guess value of x before reveal phase (hiding)

Bit commitment

- Goal:
  - Alice commits to a bit x
  - Later she reveals her commitment



- Requirements:
  - Alice cannot reveal $\neg x$ if she commited to x (binding)
  - Bob cannot guess value of x before reveal phase (hiding)
- Both requirements simultaneously are impossible without additional assumptions

Commitment with two non-communicating Alices

A_1 and A_2 share $b \in \mathbb{F}_q$, and they want to commit to a bit x

1. B sends a random challenge $y \in \mathbb{F}_q$ to A_1
2. A_1 replies with a commitment $a = b + (x \cdot y)$
3. A_2 reveals x and b
4. B checks if $a = b + x \cdot y$

Commitment with two non-communicating Alices

A_1 and A_2 share $b \in \mathbb{F}_q$, and they want to commit to a bit x

1. B sends a random challenge $y \in \mathbb{F}_q$ to A_1
2. A_1 replies with a commitment $a = b + (x \cdot y)$
3. A_2 reveals x and b
4. B checks if $a = b + x \cdot y$

- Hiding and binding properties?

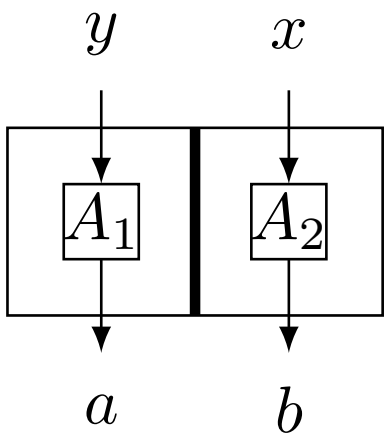
Commitment with two non-communicating Alices

A_1 and A_2 share $b \in \mathbb{F}_q$, and they want to commit to a bit x

1. B sends a random challenge $y \in \mathbb{F}_q$ to A_1
2. A_1 replies with a commitment $a = b + (x \cdot y)$
3. A_2 reveals x and b
4. B checks if $a = b + x \cdot y$

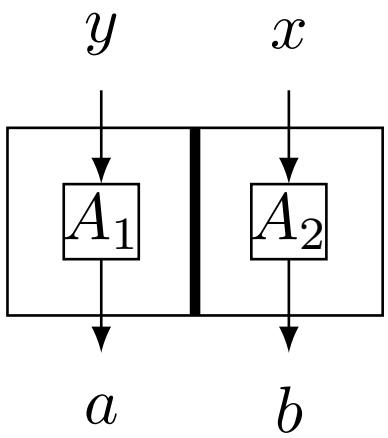
- Hiding and binding properties?
- Protocol is binding, secret b serves as a one time pad
- Denote p_x the probability to reveal x
- Protocol is ε-binding iff $p_0 + p_1 \leq 1 + \varepsilon$

Analysis of the protocol



$$a + (-b) = xy$$

Analysis of the protocol



$$a + (-b) = xy$$

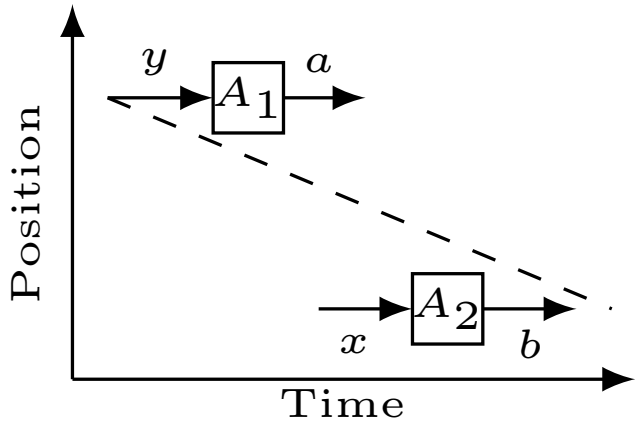
- Suppose A_2 wants to reveal 0 with probability $\frac{1}{2}$
- We have

$$\frac{1}{2}p_0 + \frac{1}{2}p_1 \leq \omega\left(\mathrm{CHSH}_q\left(\frac{1}{2}\right)\right)$$

- Therefore against classical Alices we have

$$p_0 + p_1 \leq 2\omega\left(\mathrm{CHSH}_q\left(\frac{1}{2}\right)\right) \leq 2\left(\frac{1}{2} + \frac{1}{q}\right) = 1 + \frac{2}{q}$$

Relativistic bit-commitment



- Impose non-communication of A_1 and A_2 via special theory of relativity
- Split Bob into B_1 and B_2, so communication between Bobs and Alices is much faster than communication between Alices
- Disatvantage: If A_1 is on south pole and A_2 is on north pole, commitment holds for $\approx \frac{1}{15}$ of a second

Relativistic bit-commitment with sustain phase

Solution – Additional sustain phase: [4]

1. *Preparation.* A_1 and A_2 share k random numbers $b_1, \ldots, b_k \in \mathbb{F}_q$ and B_1 and B_2 have k random numbers $y_1, \ldots, y_k \in \mathbb{F}_q$

[4] [Lunghi, Kaniewski et. al., PRL 115, 030502, 2015]

Relativistic bit-commitment with sustain phase

Solution – Additional sustain phase: [4]

1. *Preparation.* A_1 and A_2 share k random numbers $b_1, \ldots, b_k \in \mathbb{F}_q$ and B_1 and B_2 have k random numbers $y_1, \ldots, y_k \in \mathbb{F}_q$
2. *Commit phase.* B_1 sends y_1 to A_1 who replies with $a_1 = b_1 + (y_1 \cdot x)$

[4] [Lunghi, Kaniewski et. al., PRL 115, 030502, 2015]

Relativistic bit-commitment with sustain phase

Solution – Additional sustain phase: [4]

1. *Preparation.* A_1 and A_2 share k random numbers $b_1, \ldots, b_k \in \mathbb{F}_q$ and B_1 and B_2 have k random numbers $y_1, \ldots, y_k \in \mathbb{F}_q$
2. *Commit phase.* B_1 sends y_1 to A_1 who replies with $a_1 = b_1 + (y_1 \cdot x)$
3. *Sustain phase.* B_2 sends y_2 to A_2 who replies with $a_2 = b_2 + (y_2 \cdot b_1)$. Sustain phase continues in this fashion with alternate communication between A_1 and B_1 or A_2 and B_2

[4] [Lunghi, Kaniewski et. al., PRL 115, 030502, 2015]

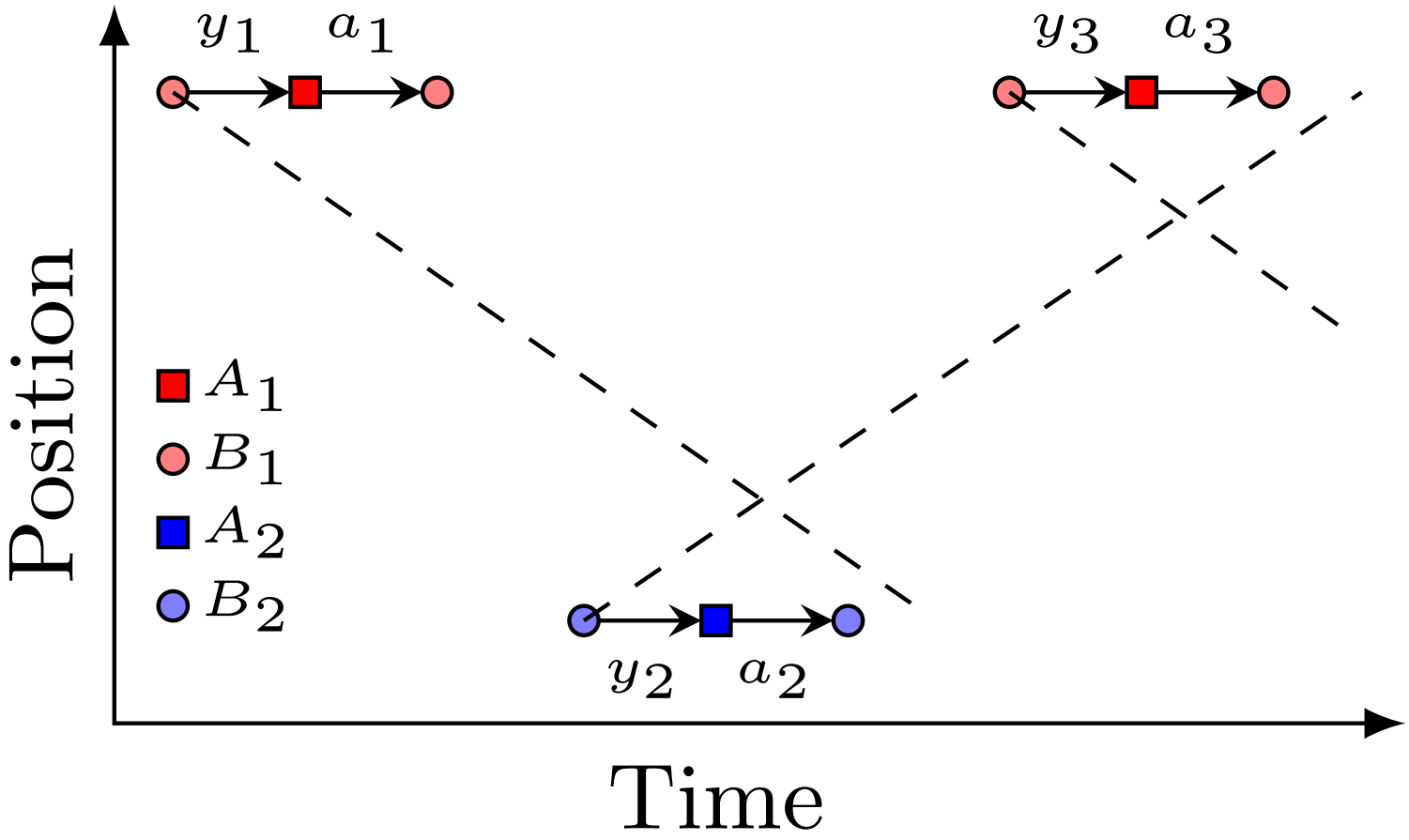
Relativistic bit-commitment with sustain phase

Solution – Additional sustain phase: [4]

1. *Preparation.* A_1 and A_2 share k random numbers $b_1, \ldots, b_k \in \mathbb{F}_q$ and B_1 and B_2 have k random numbers $y_1, \ldots, y_k \in \mathbb{F}_q$
2. *Commit phase.* B_1 sends y_1 to A_1 who replies with $a_1 = b_1 + (y_1 \cdot x)$
3. *Sustain phase.* B_2 sends y_2 to A_2 who replies with $a_2 = b_2 + (y_2 \cdot b_1)$. Sustain phase continues in this fashion with alternate communication between A_1 and B_1 or A_2 and B_2
4. *Reveal phase.* A_i which did not communicate in the last sustain round sends b_k and x to B_i. Bobs calculate $b_1 = a_1 - (x \cdot y_i)$ and then iteratively calculate $b_i = a_i - (b_{i-1} \cdot y_i)$ and verify whether $a_i = b_i + (b_{i-1} \cdot y_i)$ for all $k \geq i \geq 2$.

[4] [Lunghi, Kaniewski et. al., PRL 115, 030502, 2015]

Relativistic bit-commitment with sustain phase



Analysis of k round protocol

- We need to find ε_k, such that $p_0^k + p_1^k \leq 1 + \varepsilon_k$

Analysis of k round protocol

- We need to find ε_k, such that $p_0^k + p_1^k \leq 1 + \varepsilon_k$
- If A_1 and A_2 are dishonest, *the correct* $b_i = a_i - (b_{i-1} \cdot y_i)$, *i.e.* each b_i can be seen as a function of challenges $y_i, y_{i-1}, \ldots, y_1$ and the to be revealed bit x
- In i^{th} round, communicating Alice has only an estimate of value b_{i-1}

$$\bar{b}_{i-1}(y_{i-2}, \ldots, y_1, x)$$

Analysis of k round protocol

- We need to find ε_k, such that $p_0^k + p_1^k \leq 1 + \varepsilon_k$
- If A_1 and A_2 are dishonest, *the correct* $b_i = a_i - (b_{i-1} \cdot y_i)$, *i.e.* each b_i can be seen as a function of challenges $y_i, y_{i-1}, \ldots, y_1$ and the to be revealed bit x
- In i^{th} round, communicating Alice has only an estimate of value b_{i-1}

$$\bar{b}_{i-1}(y_{i-2}, \ldots, y_1, x)$$

- p_x^k is the probability that

$$\bar{b}_k(y_{k-1}, y_{k-2}, \ldots, y_1, x) = b_k(y_k, y_{k-1}, \ldots, y_1, x),$$

where the probability is calculated over all the challenges $(y_k, y_{k-1}, \ldots, y_1)$

Analysis of k round protocol – fixing history

- Let us denote $h_{k-2} = (y_{k-2}, y_{k-3}, \ldots, y_1)$

Analysis of k round protocol – fixing history

- Let us denote $h_{k-2} = (y_{k-2}, y_{k-3}, \ldots, y_1)$
- We will investigate $p_x^k(h_{k-2})$ – the probability to reveal x after k rounds with fixed history h_{k-2}, *i.e.*

$$p_x^k(h_{k-2}) = \Pr[\bar{b}_k(y_{k-1}, h_{k-2}, x) = b_k(y_k, y_{k-1}, h_{k-2}, x)],$$

where the probability is calculated over the last two challenges y_k, y_{k-1} only

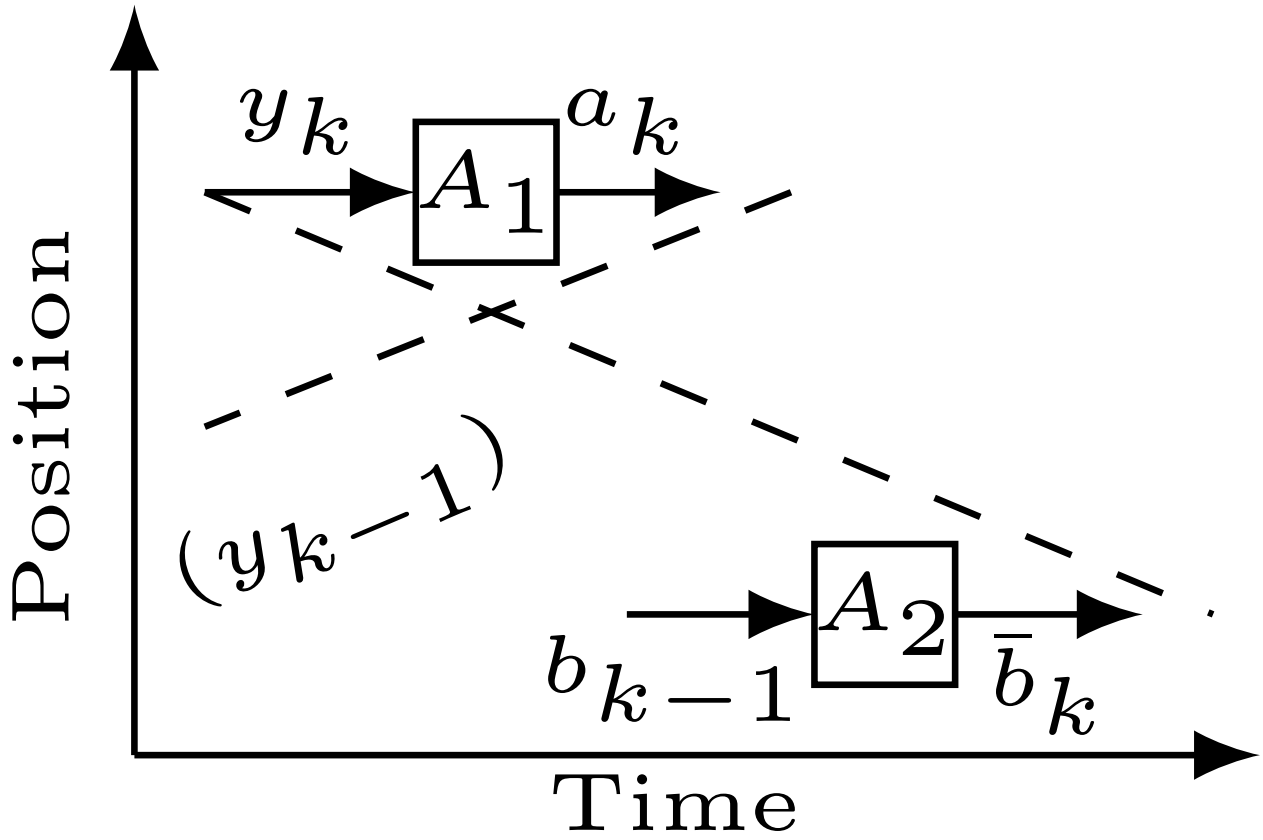
Analysis of k round protocol – fixing history

- Let us denote $h_{k-2} = (y_{k-2}, y_{k-3}, \ldots, y_1)$
- We will investigate $p_x^k(h_{k-2})$ – the probability to reveal x after k rounds with fixed history h_{k-2}, *i.e.*

$$p_x^k(h_{k-2}) = \Pr[\bar{b}_k(y_{k-1}, h_{k-2}, x) = b_k(y_k, y_{k-1}, h_{k-2}, x)],$$

  where the probability is calculated over the last two challenges y_k, y_{k-1} only
- This probability can be seen as a winning probability of a non-local game, where A_1 receives y_k and outputs a_k, while A_2 receives b_{k-1} and outputs $\bar{b}_k$
- They win (correctly reveal x), iff $a_k - \bar{b}_k = b_{k-1} \cdot y_k$

Analysis of k round protocol – picture



Analysis of k round protocol – the non-local game

- Input y_k of A_1 is distributed uniformly
- How about input b_{k-1} of A_2?

Analysis of k round protocol – the non-local game

- Input y_k of A_1 is distributed uniformly
- How about input b_{k-1} of A_2?
- In fact we need to investigate what A_1 knows about b_{k-1}
- A_1 does not know y_{k-1} before she needs to produce a_k, therefore we are interested in

$$\Pr[\bar{b}_{k-1}(h_{k-2}, x) = b_{k-1}(y_{k-1}, h_{k-2}, x)] \leq p_x^{k-1}(h_{k-2})$$

Analysis of k round protocol – the non-local game

- Input y_k of A_1 is distributed uniformly
- How about input b_{k-1} of A_2?
- In fact we need to investigate what A_1 knows about b_{k-1}
- A_1 does not know y_{k-1} before she needs to produce a_k, therefore we are interested in

$$\Pr[\bar{b}_{k-1}(h_{k-2}, x) = b_{k-1}(y_{k-1}, h_{k-2}, x)] \leq p_x^{k-1}(h_{k-2})$$

- Therefore

$$p_x^k(h_{k-2}) \leq \omega(\mathrm{CHSH}_q(p_x^{k-1}(h_{k-2})))$$

Analysis of k round protocol – final touch

- It remains to take the expectation over the history string h_{k-2}

Analysis of k round protocol – final touch

- It remains to take the expectation over the history string h_{k-2}
- Using original bound of Chakraborty *et. al.*

$$\omega(\mathrm{CHSH}_q(p)) \leq p + \sqrt{\frac{2}{q}}$$

leads to

$$p_x^k \leq p_x^{k-1} + \sqrt{\frac{2}{q}}$$

Analysis of k round protocol – final touch

- It remains to take the expectation over the history string h_{k-2}
- Using original bound of Chakraborty *et. al.*

$$\omega(\mathrm{CHSH}_q(p)) \leq p + \sqrt{\frac{2}{q}}$$

leads to

$$p_x^k \leq p_x^{k-1} + \sqrt{\frac{2}{q}}$$

- Together with $p_0^1 + p_1^1 \leq 1 + \sqrt{\frac{2}{q}}$ this gives us linear decrease in security after k challenges:

$$p_0^k + p_1^k \leq 1 + 2k\sqrt{\frac{2}{q}}$$

Analysis of k round protocol – using our bound

- Using our bound we get

$$E_{h_{k-2}}\left(p_x^k(h_{k-2})\right) \leq E_{h_{k-2}}\left(p_x^{k-1}(h_{k-2}) + \frac{1}{2qp_x^{k-1}(h_{k-2})}\right)$$

- Our bound is not concave, so the original proof doesn't go through :(
- Originally we thought we can improve the analysis and show security decreases only with $\sqrt{k}$

[5] arXiv:1608.03820 (2016)

Analysis of k round protocol – using our bound

- Using our bound we get

$$E_{h_{k-2}}\left(p_x^k(h_{k-2})\right) \leq E_{h_{k-2}}\left(p_x^{k-1}(h_{k-2}) + \frac{1}{2qp_x^{k-1}(h_{k-2})}\right)$$

- Our bound is not concave, so the original proof doesn't go through :(
- Originally we thought we can improve the analysis and show security decreases only with $\sqrt{k}$
- Recently our improved analysis suggests we can achieve improvement only by the factor of 2

[5] arXiv:1608.03820 (2016)

Analysis of k round protocol – using our bound

- Using our bound we get

$$E_{h_{k-2}}\left(p_x^k(h_{k-2})\right) \leq E_{h_{k-2}}\left(p_x^{k-1}(h_{k-2}) + \frac{1}{2qp_x^{k-1}(h_{k-2})}\right)$$

- Our bound is not concave, so the original proof doesn't go through :(
- Originally we thought we can improve the analysis and show security decreases only with $\sqrt{k}$
- Recently our improved analysis suggests we can achieve improvement only by the factor of 2
- Bricout and Chailloux[5] recently published an attack which achieves linear decrease in security, suggesting the original analysis is essentially optimal

[5] arXiv:1608.03820 (2016)

THANK YOU! QUESTIONS?