Parallel Device-Independent Quantum Key Distribution

Rahul Jain

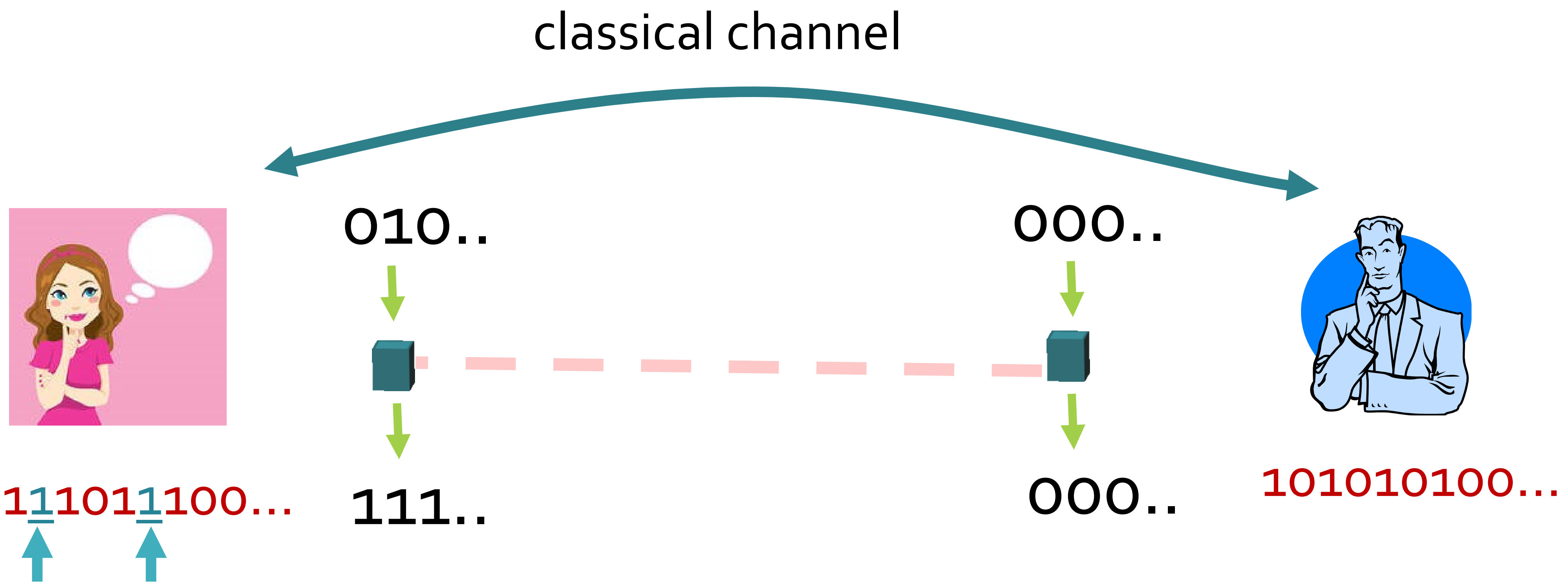
National University of Singapore

Centre for Quantum Technologies (CQT)

Based on R. Jain, C. Miller, Y. Shi, "Parallel Device-Independent Quantum Key Distribution," (arXiv:1703.05426)

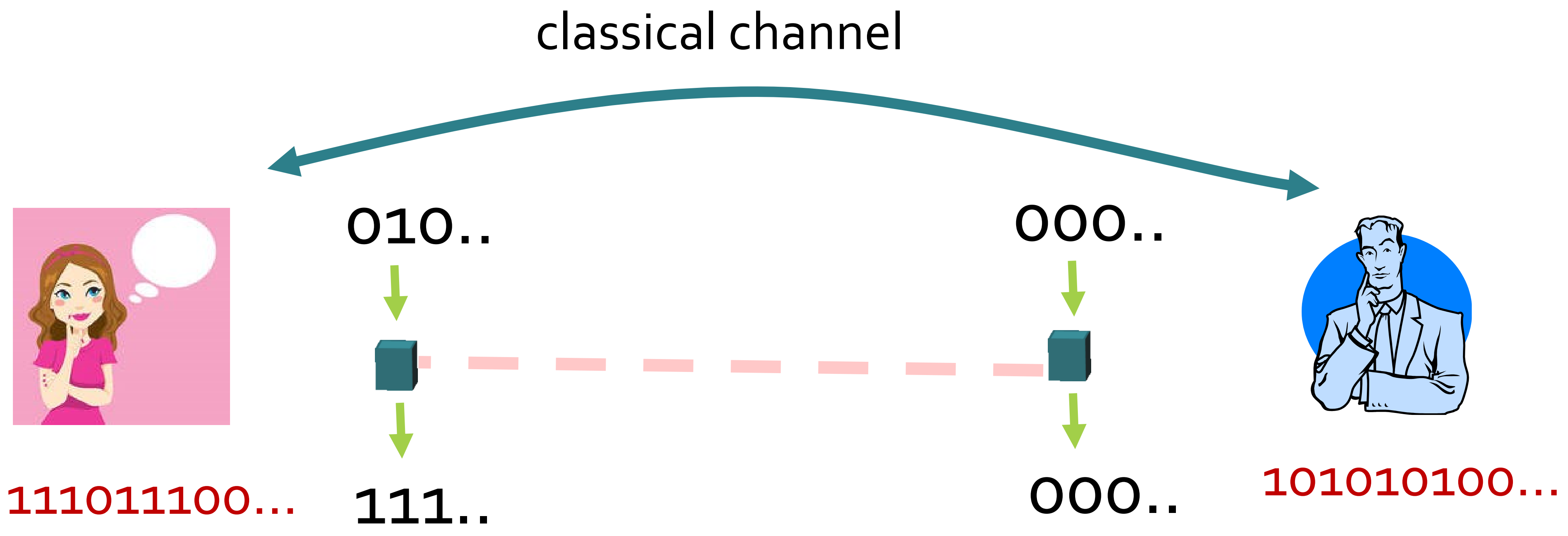
Device-Independent Protocols

Quantum Key Distribution [VV12, MS14, AVR16]



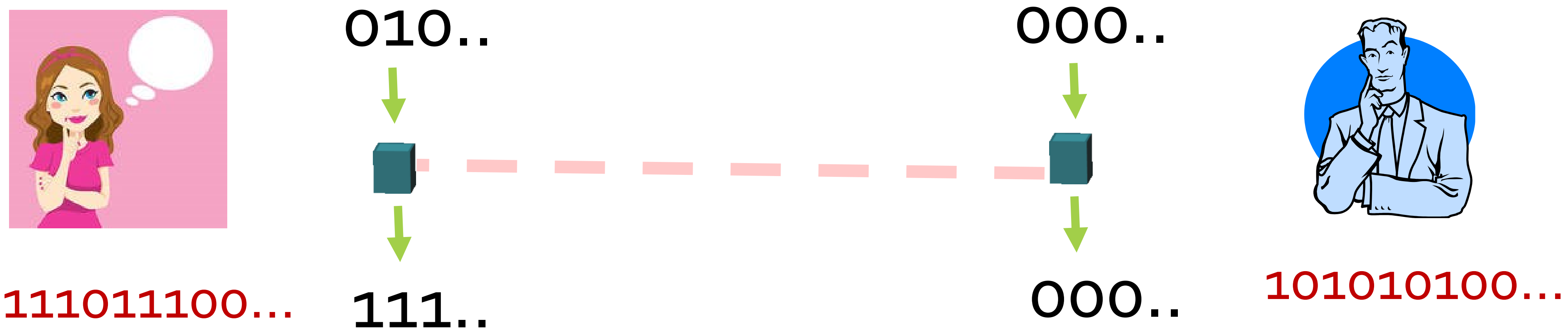
Device-Independent Protocols

Quantum Key Distribution [VV12, MS14, AVR16]



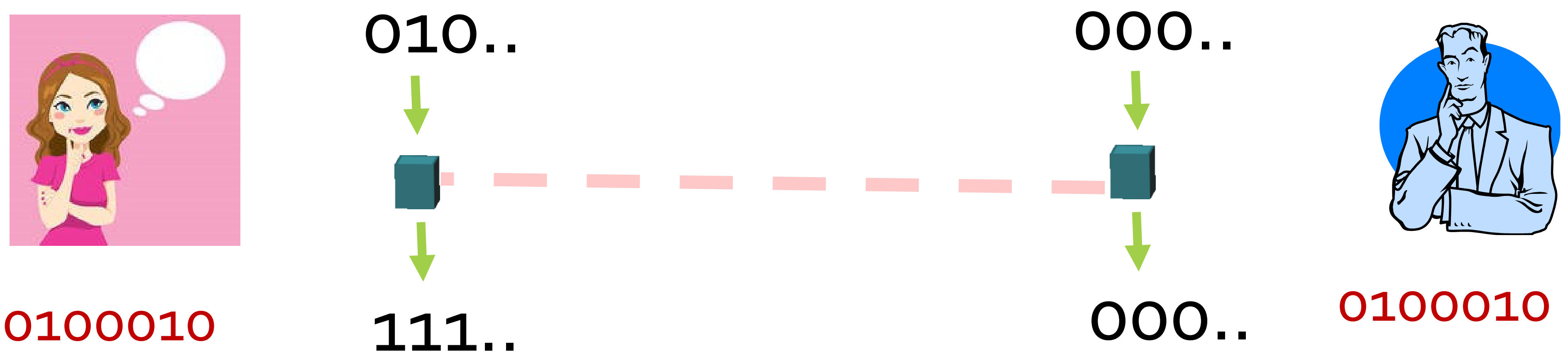
Device-Independent Protocols

Quantum Key Distribution [VV12, MS14, AVR16]



Device-Independent Protocols

Quantum Key Distribution [VV12, MS14, AVR16]

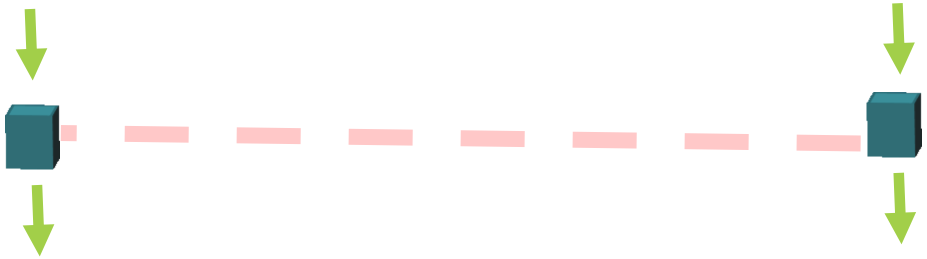


Device-Independent Protocols

Question: What are minimal assumptions for DI-QKD?

Current assumptions [VV12, MS14, AVR16]:

1. No information leakage from labs.
2. Random inputs are generated and revealed sequentially.



Device-Independent Protocols

Question: What are minimal assumptions for DI-QKD?

Current assumptions [VV12, MS14, AVR16]:

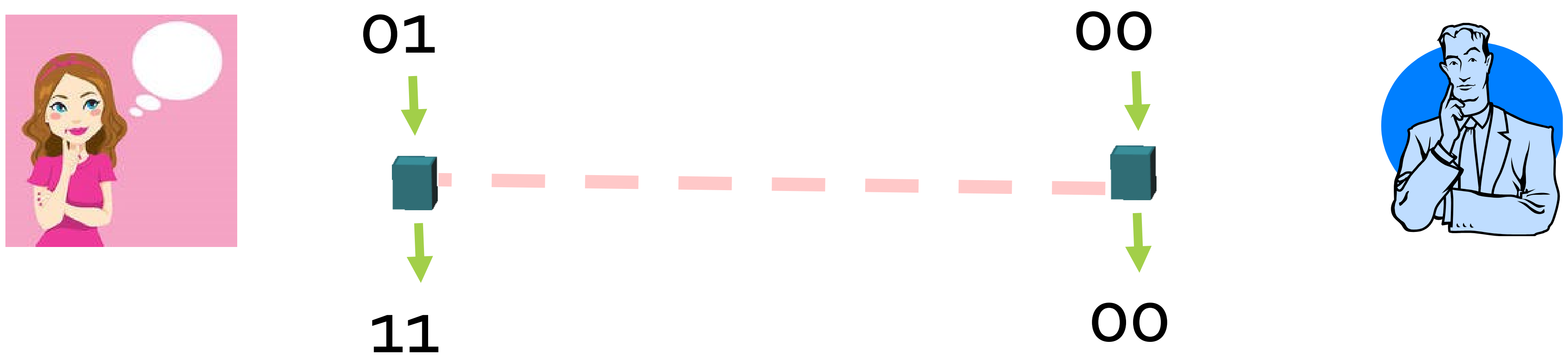
1. No information leakage from labs.
2. Random inputs are generated and revealed sequentially.

Device-Independent Protocols

Question: What are minimal assumptions for DI-QKD?

Current assumptions [VV12, MS14, AVR16]:

1. No information leakage from labs.
2. Random inputs are generated and revealed sequentially.

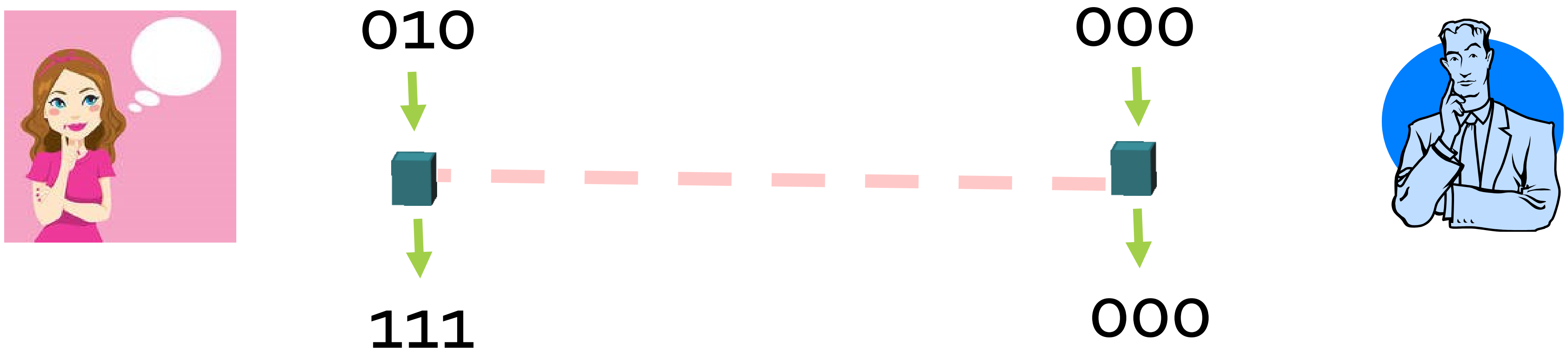


Device-Independent Protocols

Question: What are minimal assumptions for DI-QKD?

Current assumptions [VV12, MS14, AVR16]:

1. No information leakage from labs.
2. Random inputs are generated and revealed sequentially.

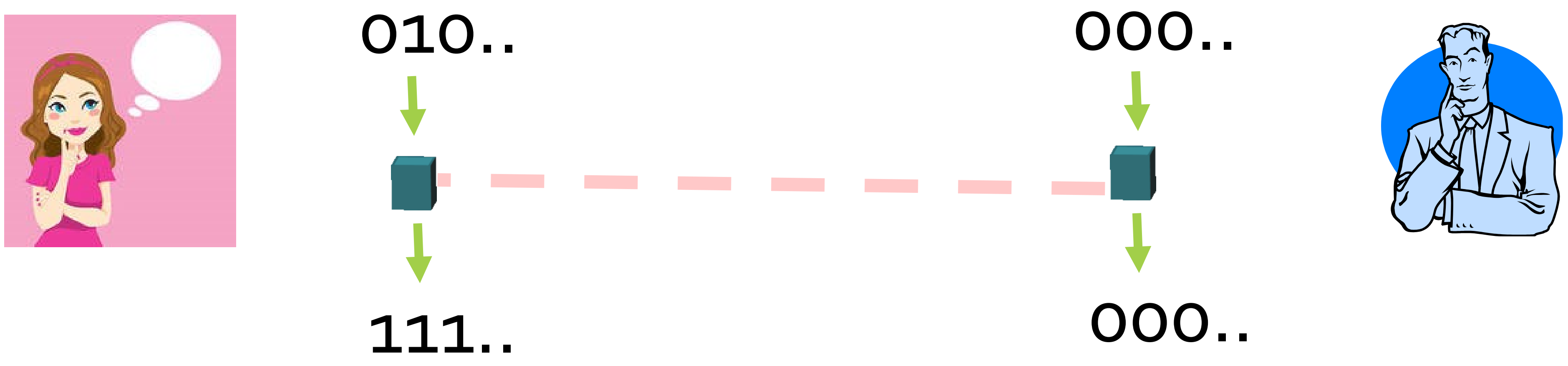


Device-Independent Protocols

Question: What are minimal assumptions for DI-QKD?

Current assumptions [VV12, MS14, AVR16]:

1. No information leakage from labs.
2. Random inputs are generated and revealed sequentially.



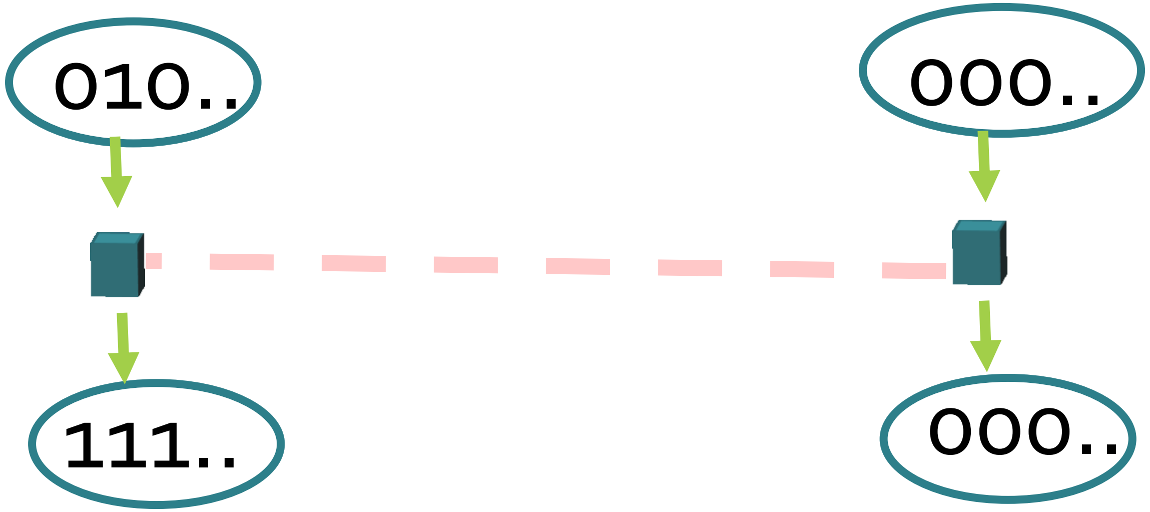
Device-Independent Protocols

Our work: Proof of QKD with <u>parallel</u> inputs.

- No need for instantaneous input generation or security within labs.

- Simplifies experiment.

Robust, with a positive key rate.



First Attemps

The Magic Square Game

The game is won if:

Random row number

0	1	1

Random column number

	1	
	1	
	1	

The Magic Square Game

The game is won if:

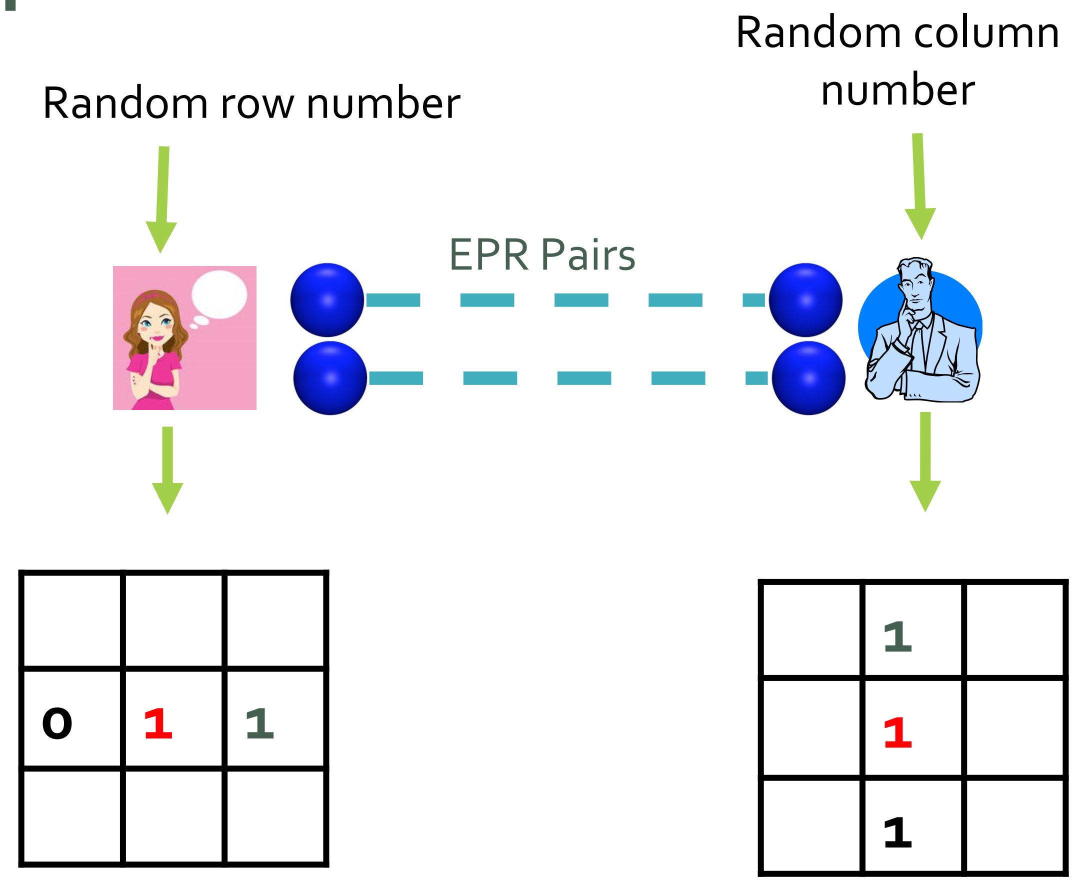
(1) The overlap square matches.

(2) Alice's parity is even.

(3) Bob's parity is odd.

w_c (MAGIC) = 8/9 (classical)

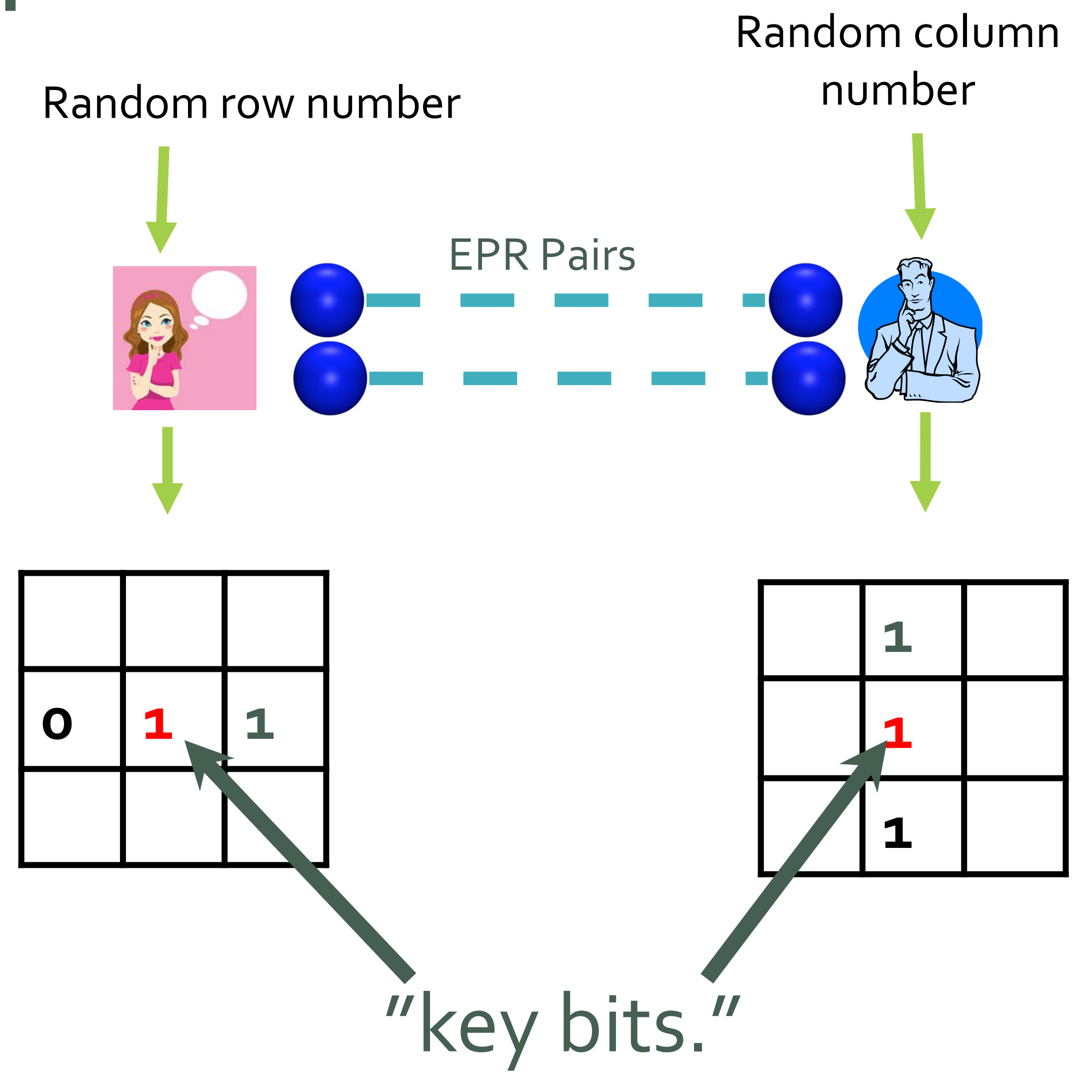
w (MAGIC) = 1 (quantum)



The Magic Square Game

The Magic Square game is rigid [Wu16].

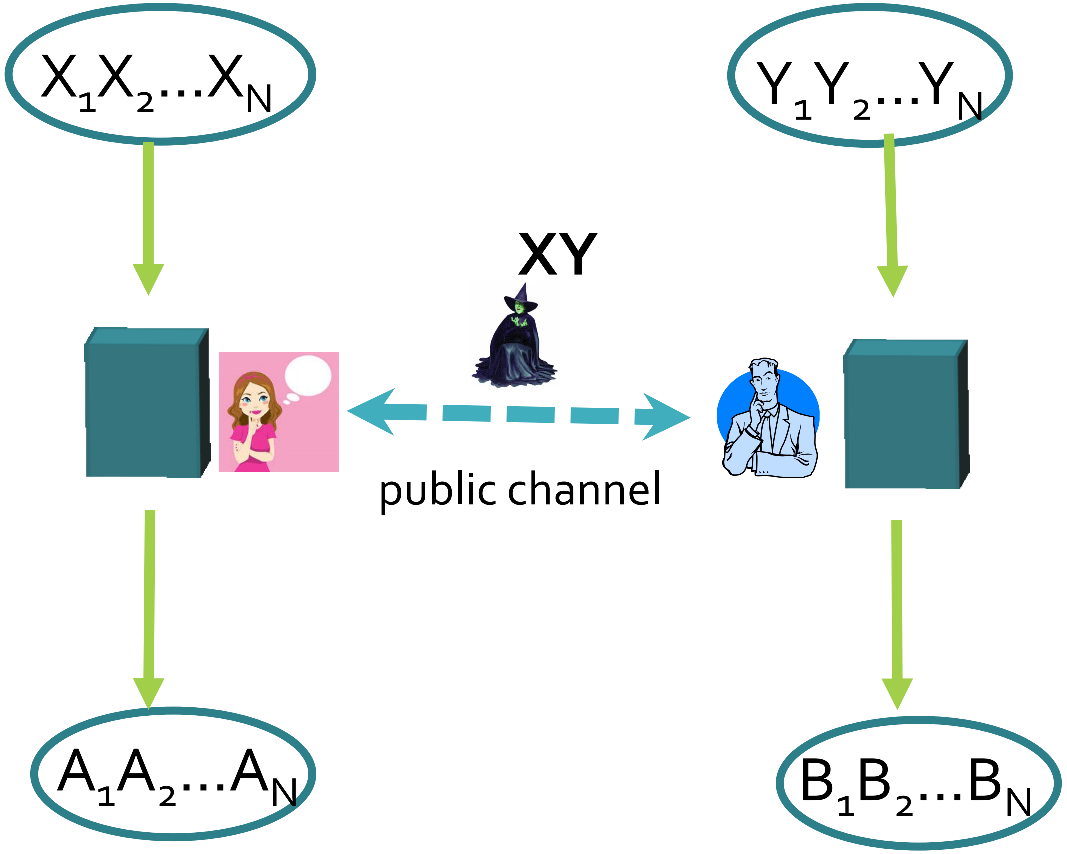
Near-optimal expected score
=> near-perfect key bit pair!



Parallel QKD?

1. Alice and Bob play Magic Square N times in **parallel**.
2. They share their inputs.
3. They share a few chosen key bits; if win avg. too low, abort.
4. Information reconciliation & privacy amplification on key bits.

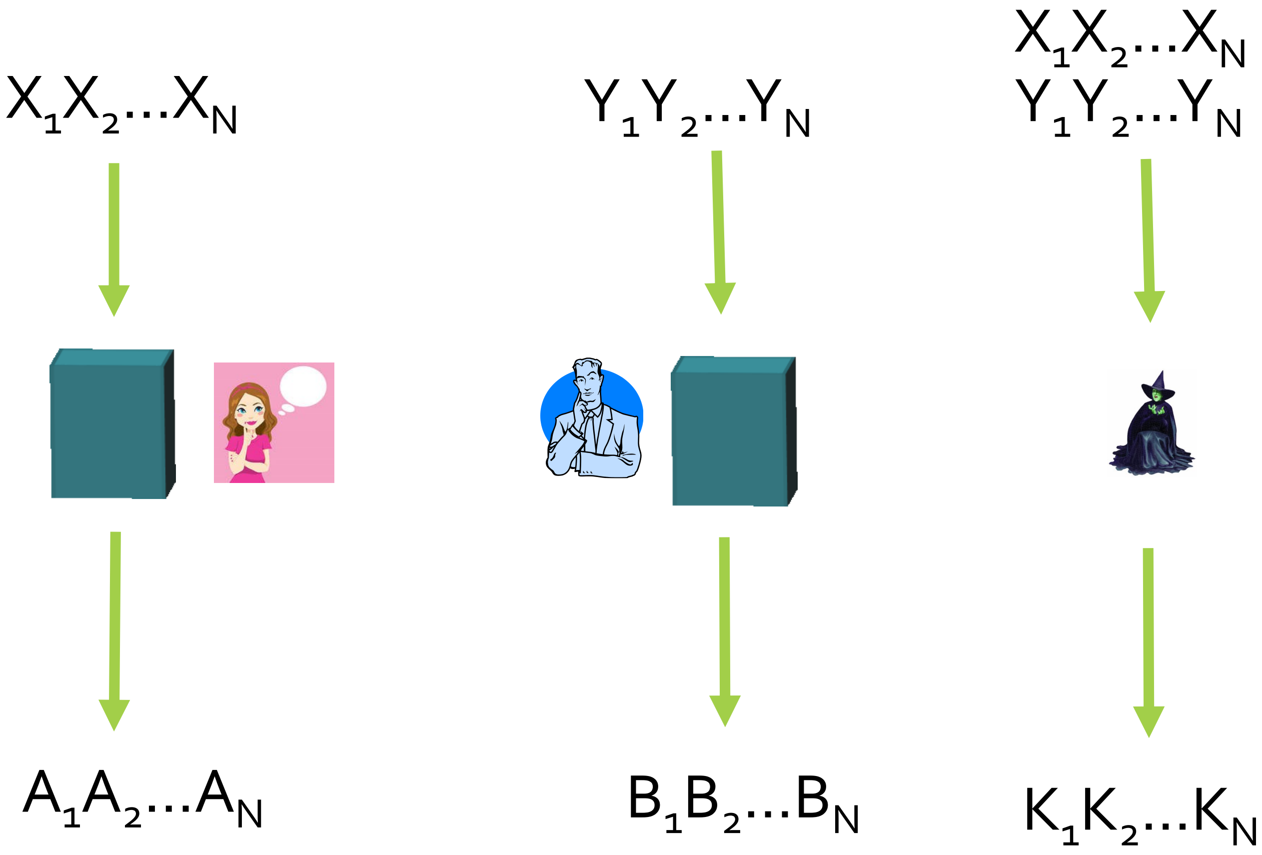
For security, it would suffice to show that Alice's raw key bits are exponentially unpredictable to Eve.



A 3-Player Game

The game is won if:
(1) MS conditions hold, and
(2) K_i = Alice's ith key bit for all i.

Does the probability of winning this game vanish exponentially?

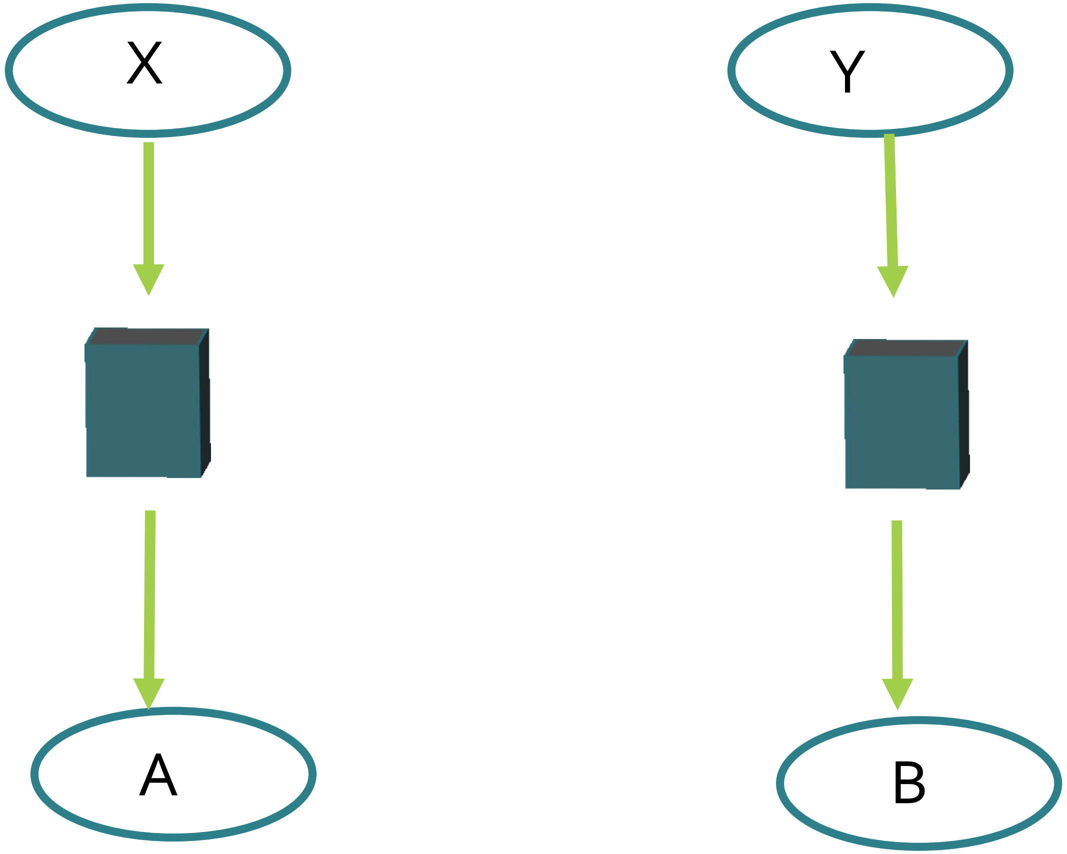


Interlude: Parallel Repetition of Nonlocal Games

The Problem With Parallel

The CHSH game(*) satisfies

w_c (CHSH) = 3/4.



(*): Binary game, won if $A \oplus B = X \wedge Y$

The Problem With Parallel

The CHSH game(*) satisfies

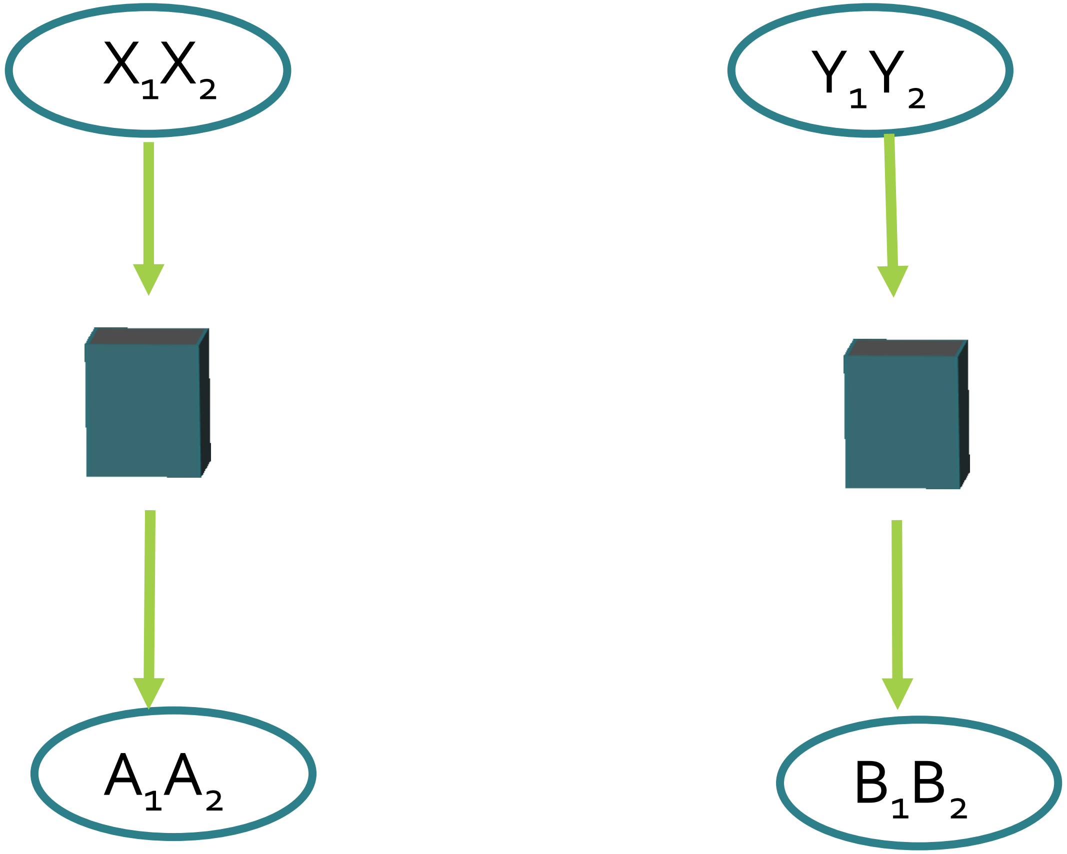
w_c (CHSH) = 3/4.

But w_c (CHSH^2) >= 5/8 > $(3/4)^2$!!

There's a strategy with

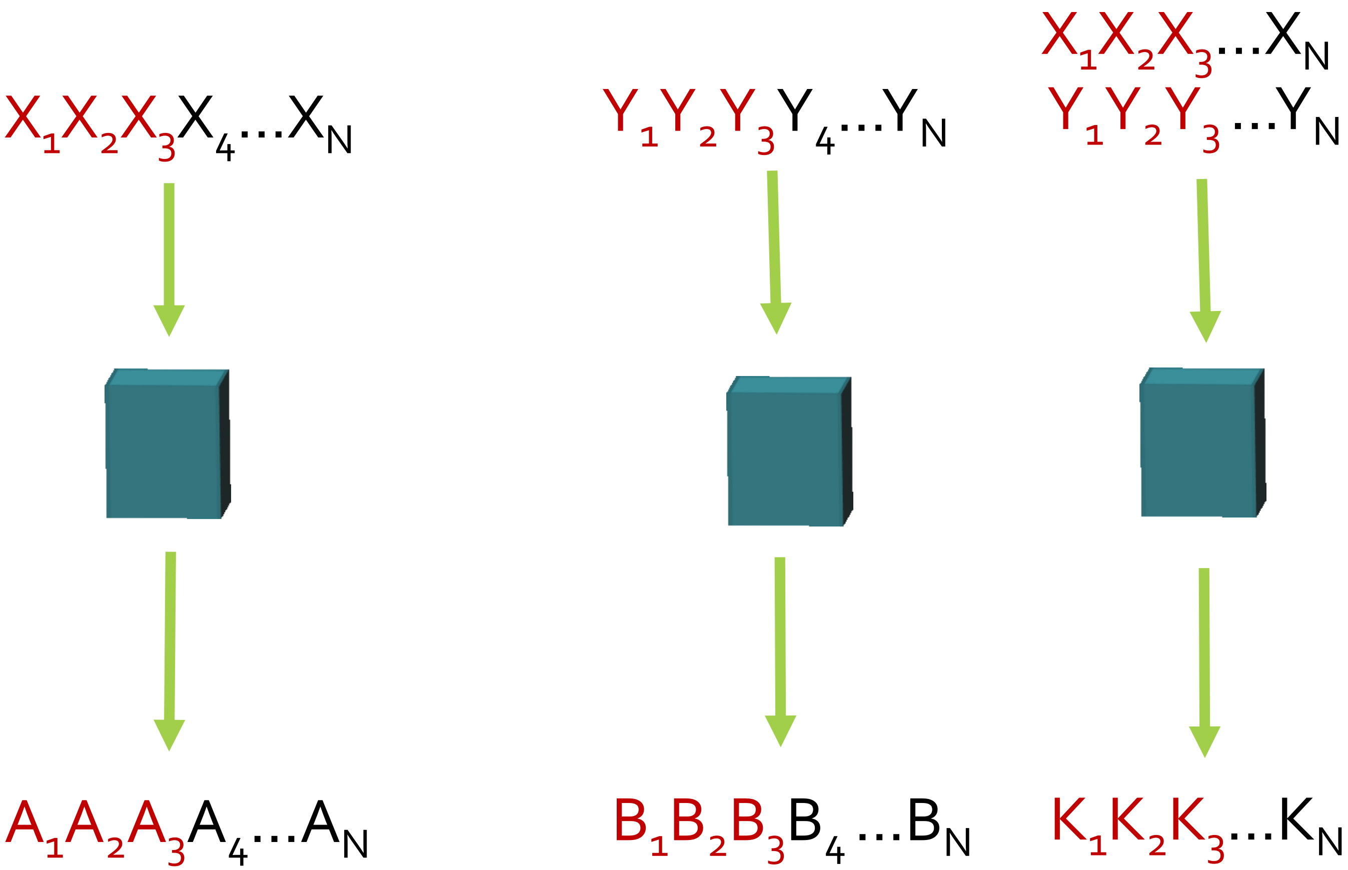
P(WIN1) = 3/4

P(WIN2 | WIN1) = 5/6!!



(*): Binary game, won if $A \oplus B = X \wedge Y$

Is it possible that correctly guessing the outcomes of the first few rounds will allow winning all the rest?



The Entropy Defense

[Raz 84, Chailloux+ 14, Jain+ 14, Chung+ 15, Bavarian+ 15]

Let G be a **free** game (product distribution on inputs).

$X_1 X_2 X_3 X_4 X_5 \ldots$

$A_1 A_2 A_3 A_4 A_5 \ldots$

$Y_1 Y_2 Y_3 Y_4 Y_5 \ldots$

$B_1 B_2 B_3 B_4 B_5 \ldots$

The Entropy Defense

[Raz 84, Chailloux+ 14, Jain+ 14, Chung+ 15, Bavarian+ 15]

Let G be a **free** game (product distribution on inputs).

For randomly chosen rounds j, k,

$$\boxed{\mathbf{P}(\mathrm{WIN}_j \mid \mathrm{WIN}_k) \leq w(G) + O(1/\sqrt{N})}$$

Why: Conditioning k only reveals O (1/N) bits of information about inputs on round j.

$X_1\ X_2\ X_3\ X_4\ X_5\ \ldots$

$A_1\ A_2\ A_3\ A_4\ A_5\ \ldots$

$Y_1\ Y_2\ Y_3\ Y_4\ Y_5\ \ldots$

$B_1\ B_2\ B_3\ B_4\ B_5\ \ldots$

The Entropy Defense

[Raz 84, Chailloux+ 14, Jain+ 14, Chung+ 15, Bavarian+ 15]

One can show:

$$\boxed{\mathbf{P}(\mathrm{WIN}_1 \cdots \mathrm{WIN}_N) \leq C^N}$$

for some fixed C < 1.

More tightly, if S is a small randomly chosen subset,

$$\boxed{\mathbf{P}(\mathrm{WIN}_S) \leq (w(G) + \delta)^{|S|}}$$

$X_1\ X_2\ X_3\ X_4\ X_5\ \ldots$

$A_1\ A_2\ A_3\ A_4\ A_5\ \ldots$

$Y_1\ Y_2\ Y_3\ Y_4\ Y_5\ \ldots$

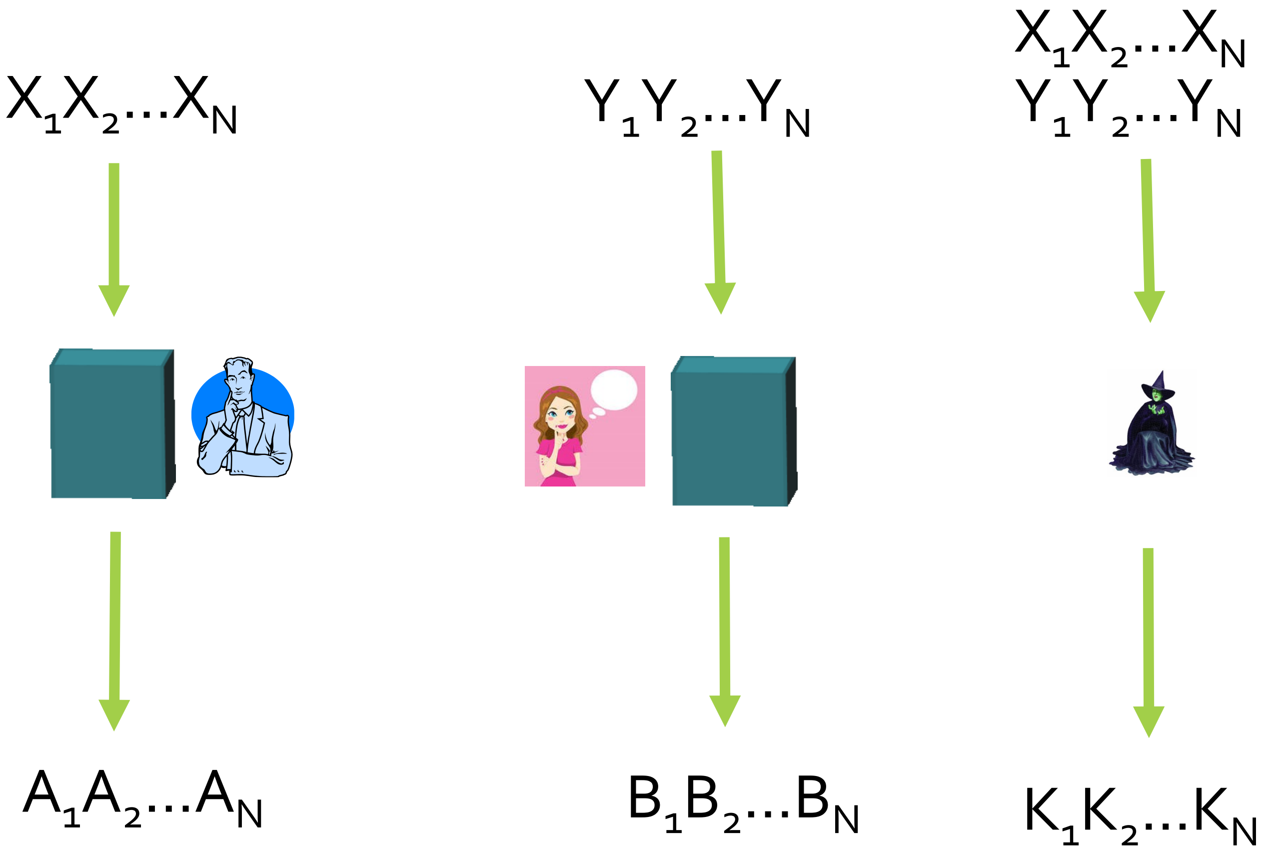
$B_1\ B_2\ B_3\ B_4\ B_5\ \ldots$

First Attempts (cont.)

A 3-Player Game

FIRST ATTEMPT:
Apply the entropy defense to this game.

Not a free game.



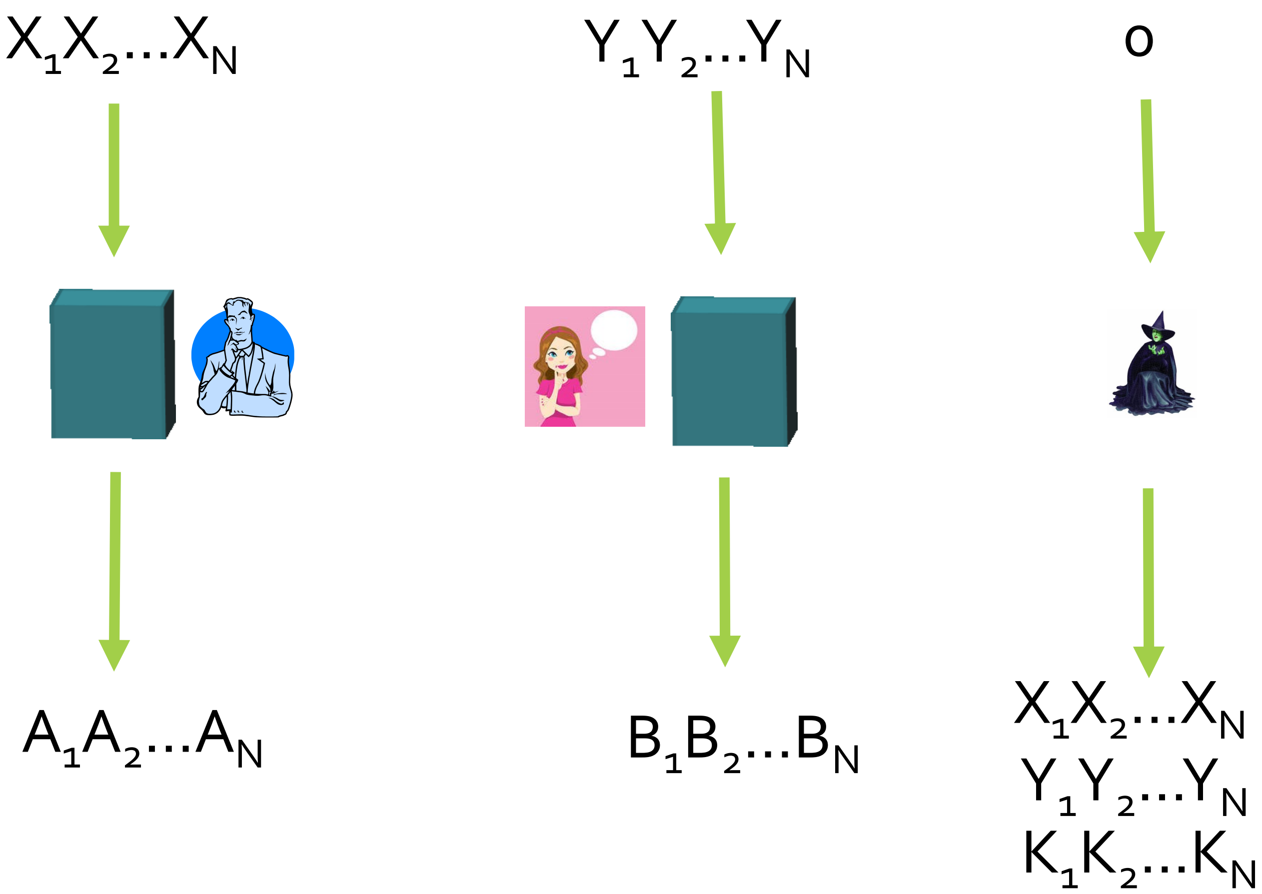
A 3-Player Game

SECOND ATTEMPT:

Have Eve guess **XY** <u>and</u> the key bits. Show

$$w(G^N) << (1/9)^N$$

Can't get an exponential coefficient that small.

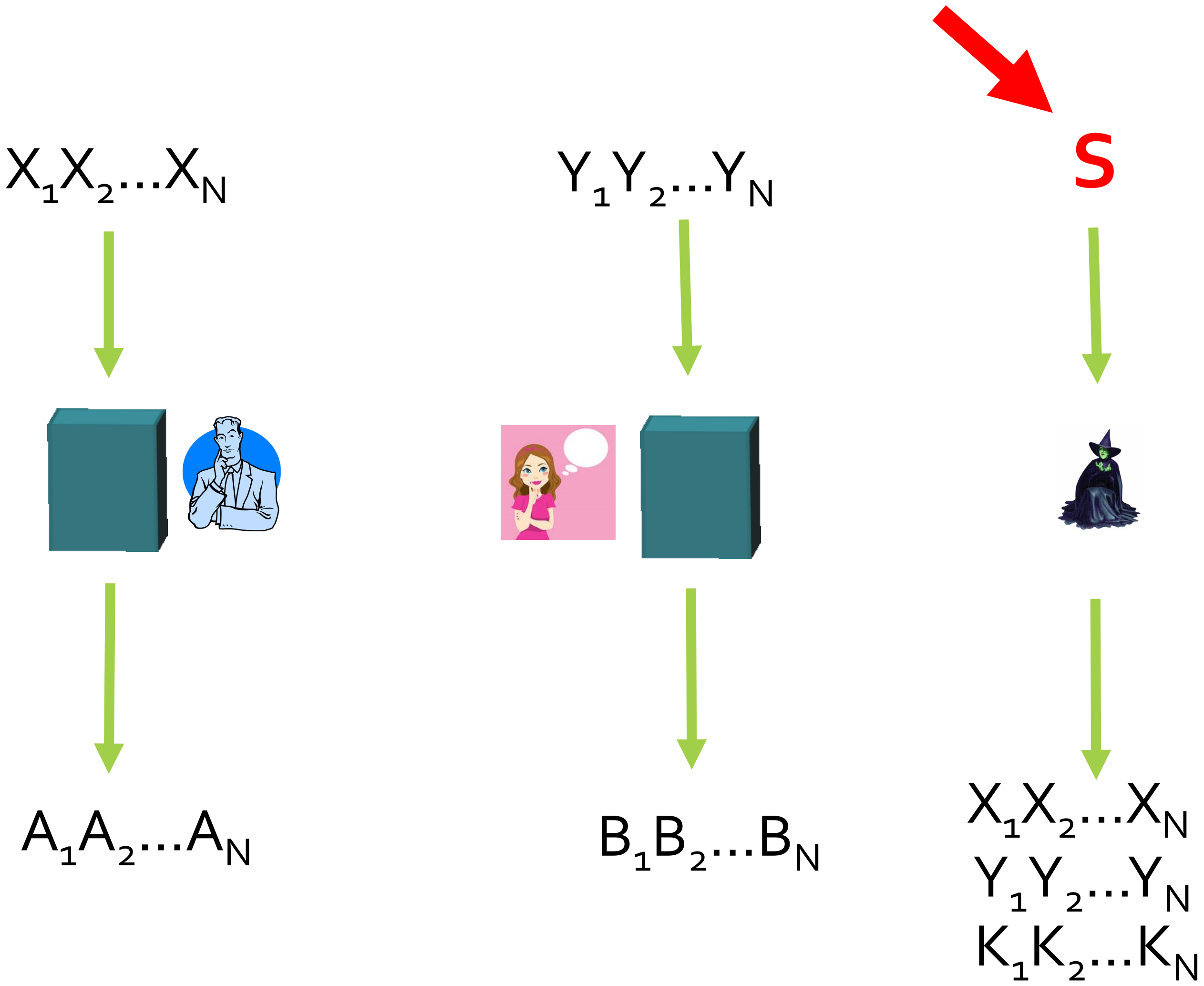


A 3-Player Game

THIRD ATTEMPT:

We know **P**(WIN_S) << $(1/9)^{|S|}$ for small random subset S.

Conclude that Eve's probability in QKD of guessing the S-inputs & S-key bits is << $(1/9)^{|S|}$.



The Mirror Adversary

Collision Entropy

Γ_{XE} = classical-quantum register

$$H_2(X \mid E)_\Gamma = -\log\left[\sum_x \Gamma_x (\Gamma^E)^{-1/2} \Gamma_x (\Gamma^E)^{-1/2}\right]$$

X

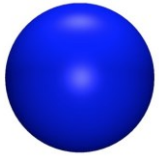
E

Idea: H_2 measures unpredictability against the "pretty good measurement," $\{(\Gamma^E)^{-1/2}\Gamma_x(\Gamma^E)^{-1/2}\}_x$.

($H_{min}(X \mid E)_\Gamma$ = unpredictability against an optimal measurement.)

An Alternative Interpretation

Suppose X was obtained from a measurement on Q.

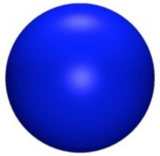


Q

An Alternative Interpretation

Suppose X was obtained from a measurement on Q.

Then, $2^{H_2(X|E)}$ is the guessing probability for a **mirror adversary.**

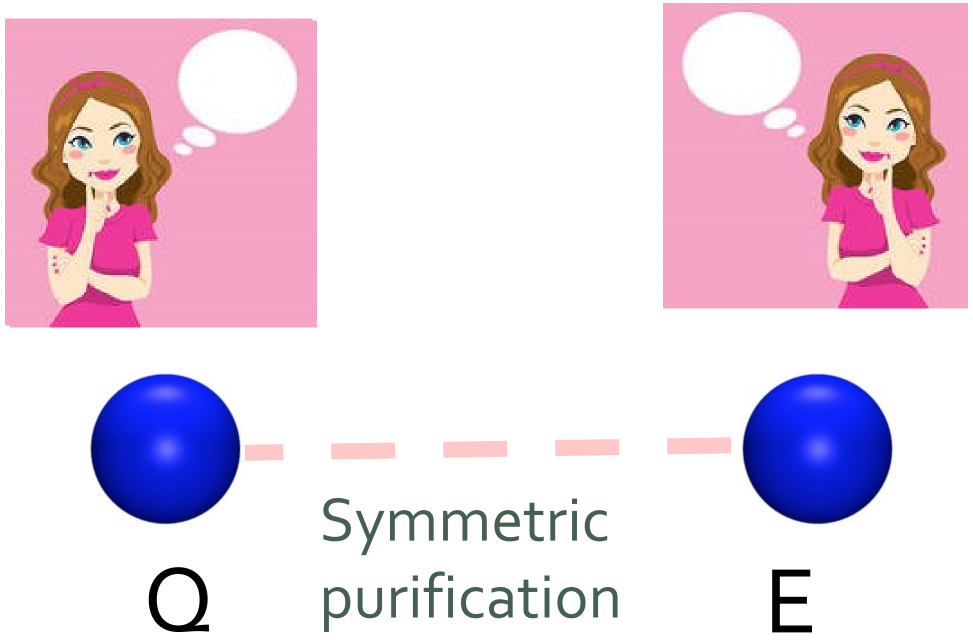


Q

An Alternative Interpretation

Suppose X was obtained from a measurement on Q.

Then, $2^{H_2(X|E)}$ is the guessing probability for a **mirror adversary.**



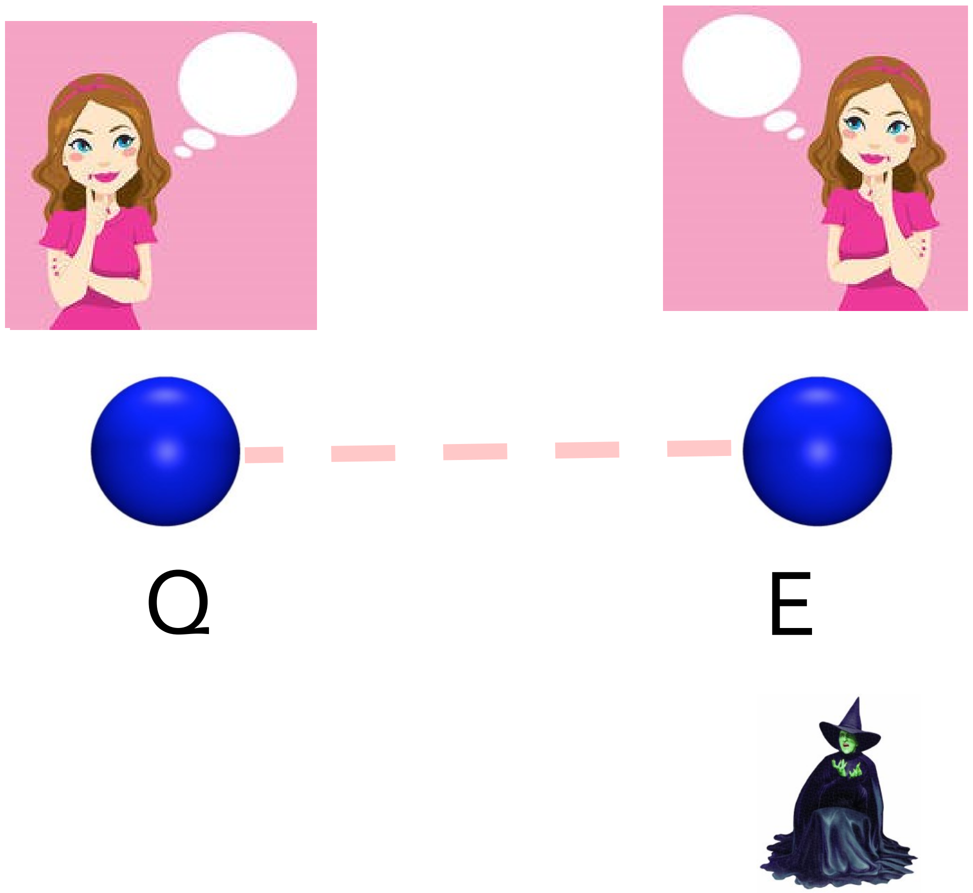
An Alternative Interpretation

This is good for us, because:

$$\left| H_{min}^{\delta}(X \mid E) - H_2(X \mid E) \right| \leq O(\log \delta)$$

[Tomamichel+ 08]

Interpretation: You are your own worst enemy. (Approximately.)

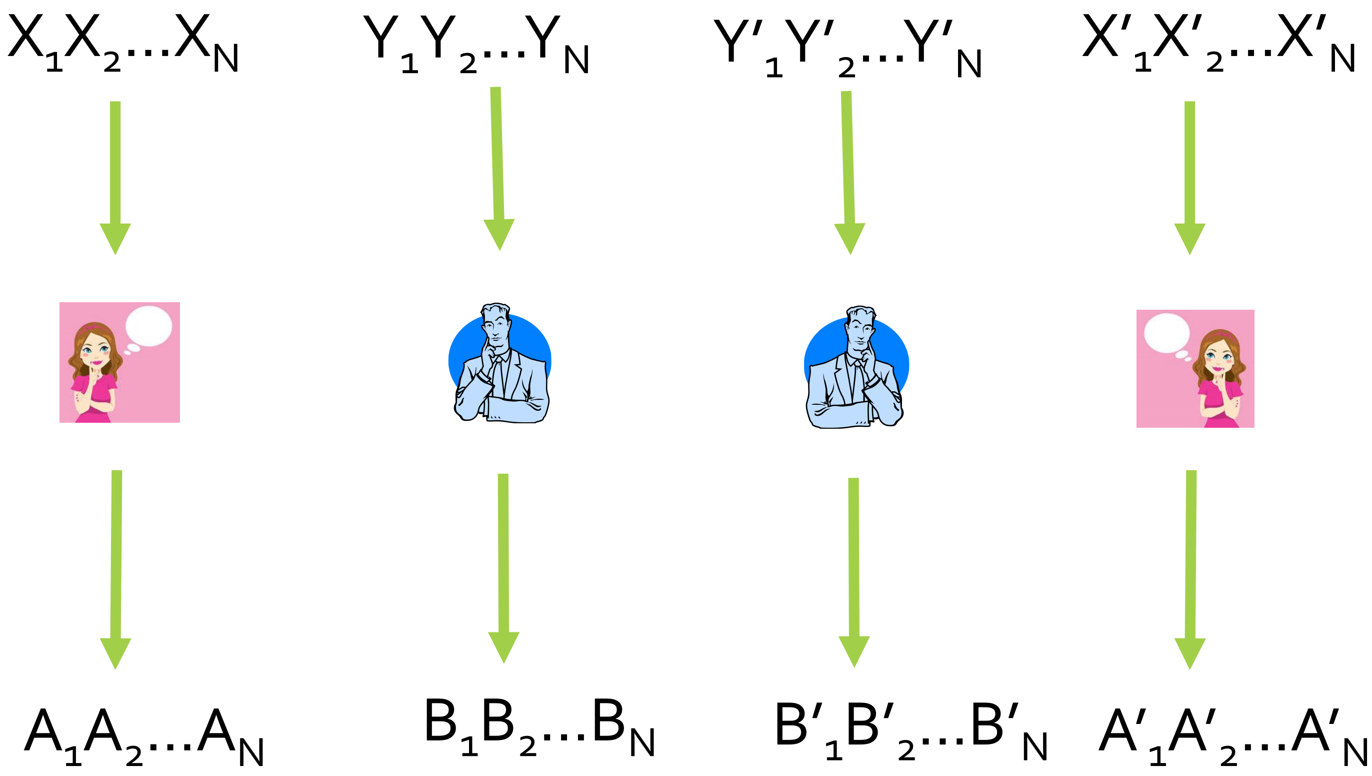


Our proof

A Non-Robust Result

The ith game is won if:

1. Inputs match mirror.
2. Alice's key bit matches mirror.
3. Alice and Bob win Magic Square.



For small random S.

$$\mathbf{P}(WIN_S) << (1/9)^{|S|}$$

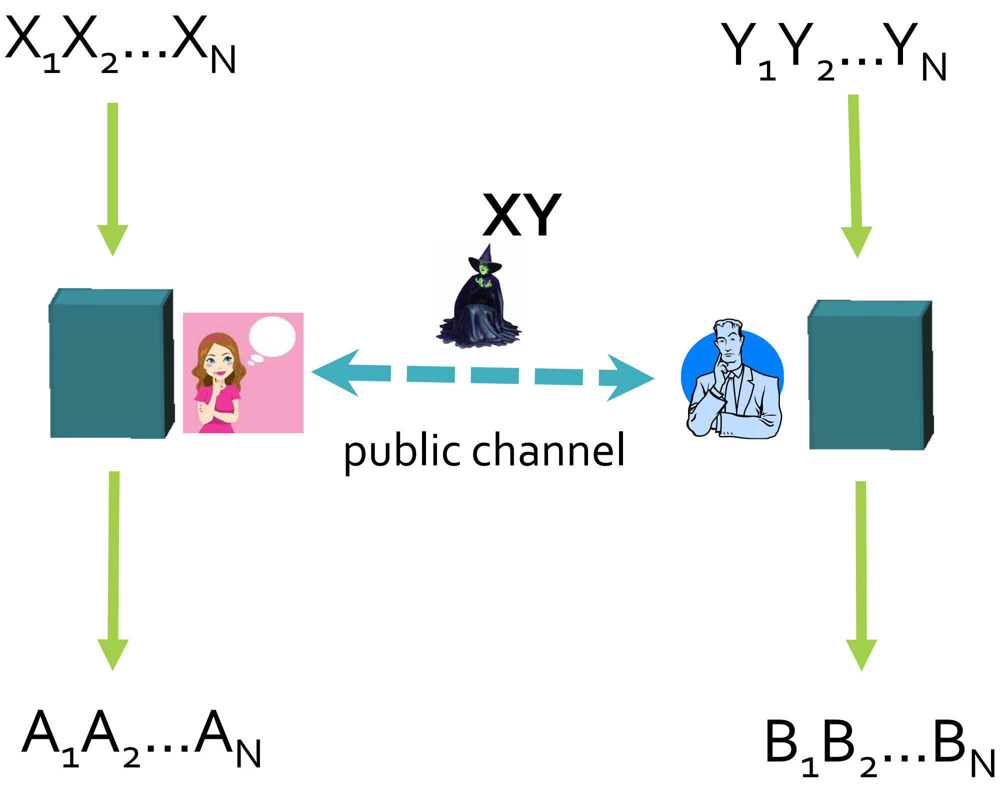
A Non-Robust Result

Conclusion:

If Alice and Bob win Magic Square on all rounds in S, their key bits have a positive amount of min-entropy!

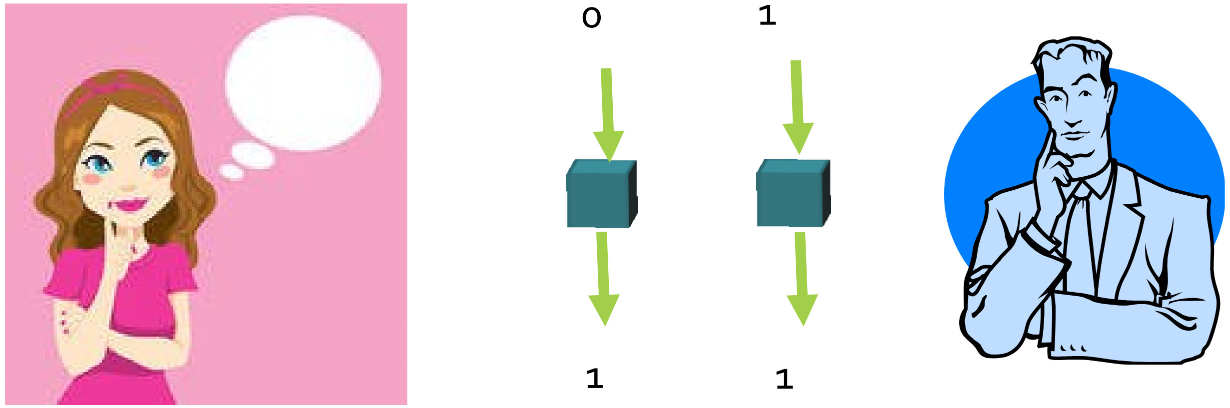
SUCCESS!!

(Almost)



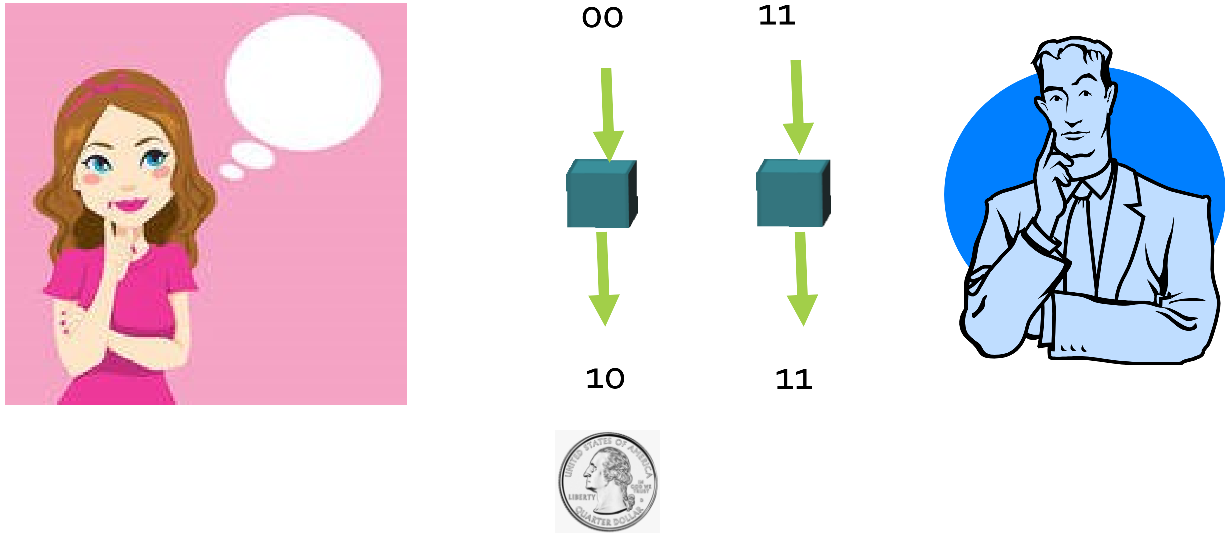
Robustness: Sequential Case

[Miller+ 14, Dupuis+ 16]: Each time the devices lose, add a coin flip to their output.



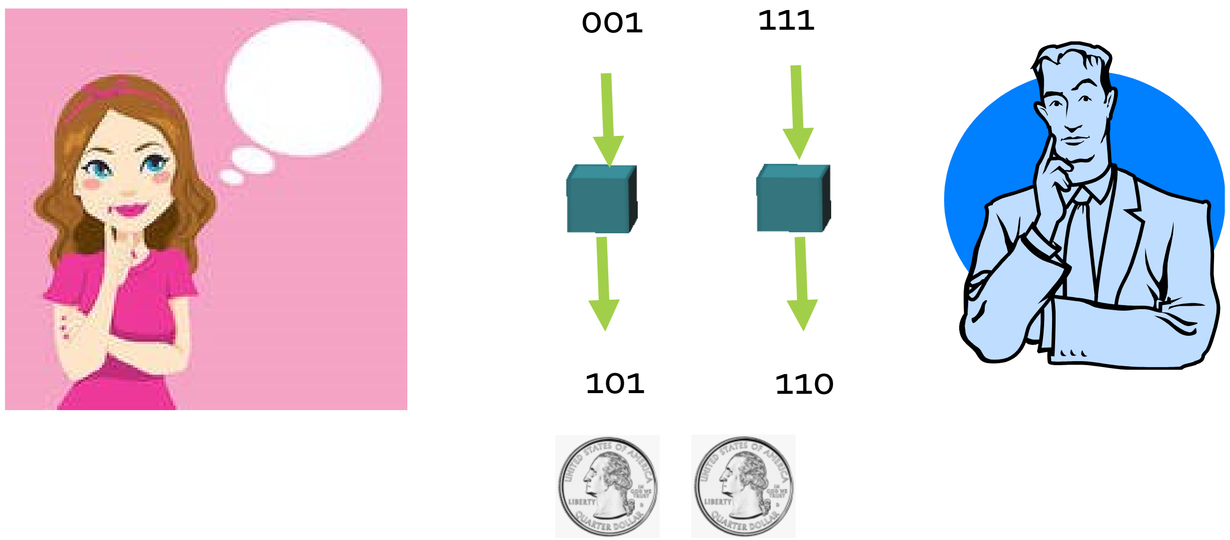
Robustness: Sequential Case

[Miller+ 14, Dupuis+ 16]: Each time the devices lose, add a coin flip to their output.



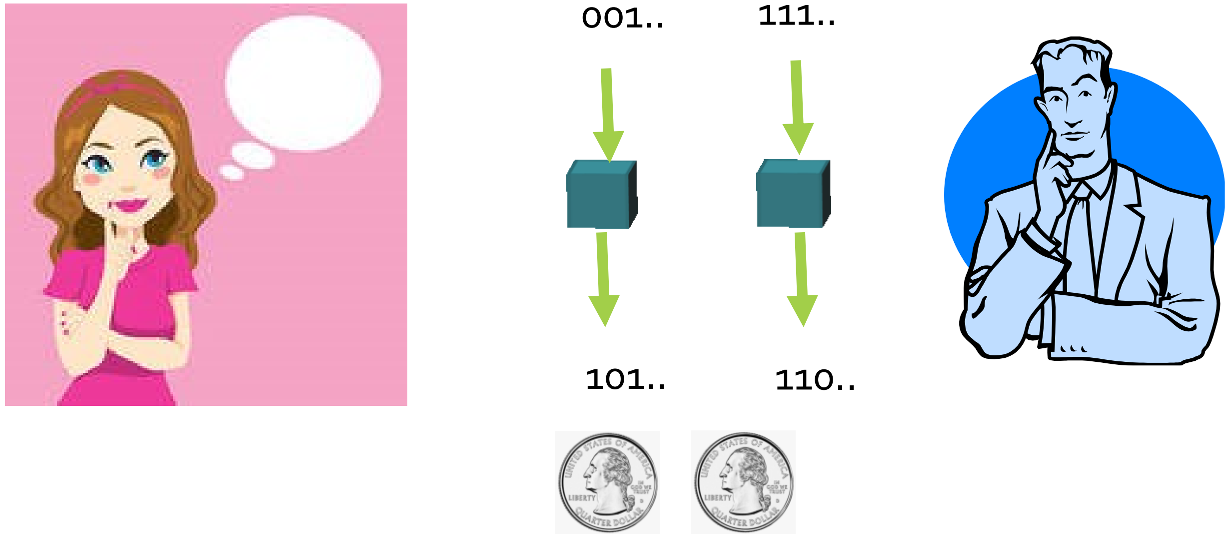
Robustness: Sequential Case

[Miller+ 14, Dupuis+ 16]: Each time the devices lose, add a coin flip to their output.



Robustness: Sequential Case

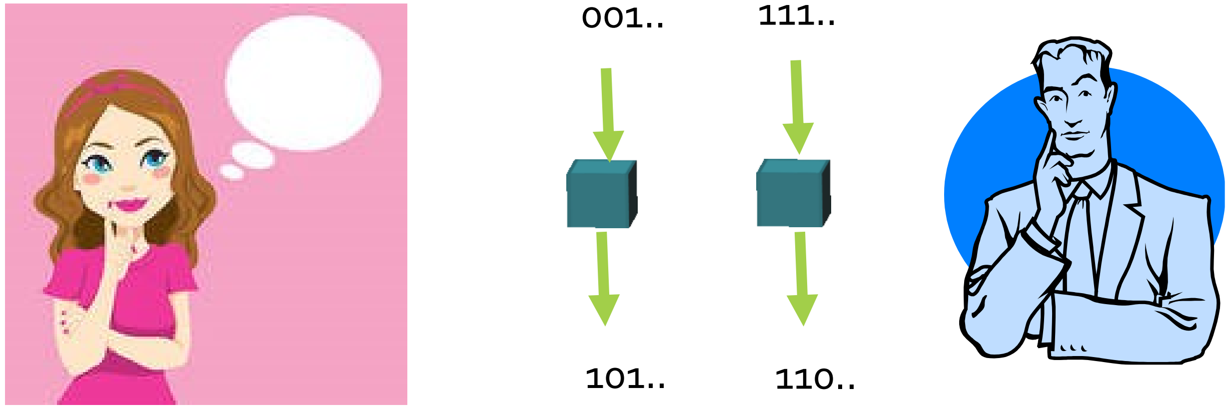
[Miller+ 14, Dupuis+ 16]: Each time the devices lose, add a coin flip to their output.



Robustness: Sequential Case

[Miller+ 14, Dupuis+ 16]: Each time the devices lose, add a coin flip to their output.

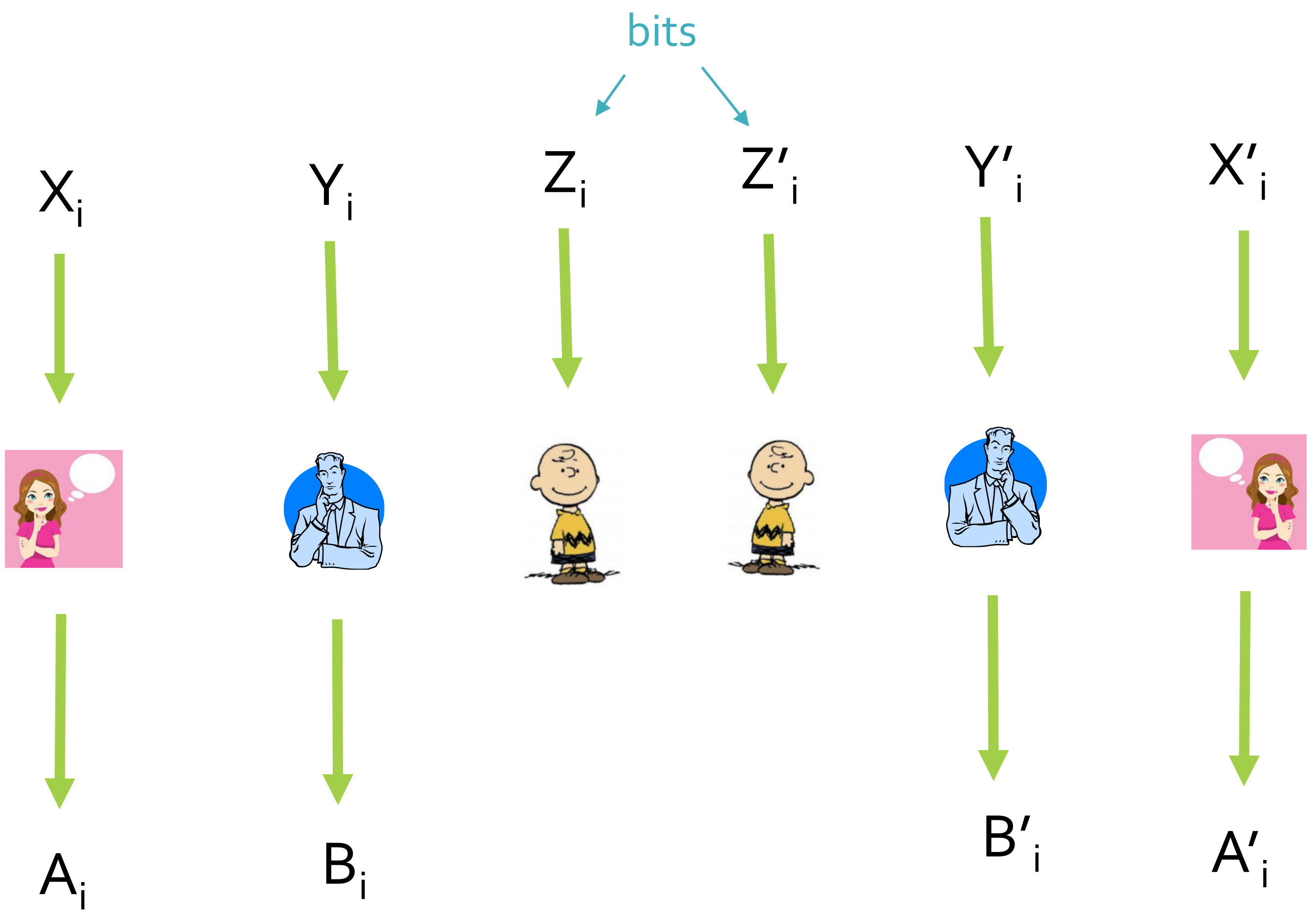
Then, after the protocol succeeds, take the coins back.



A 6-Player Game

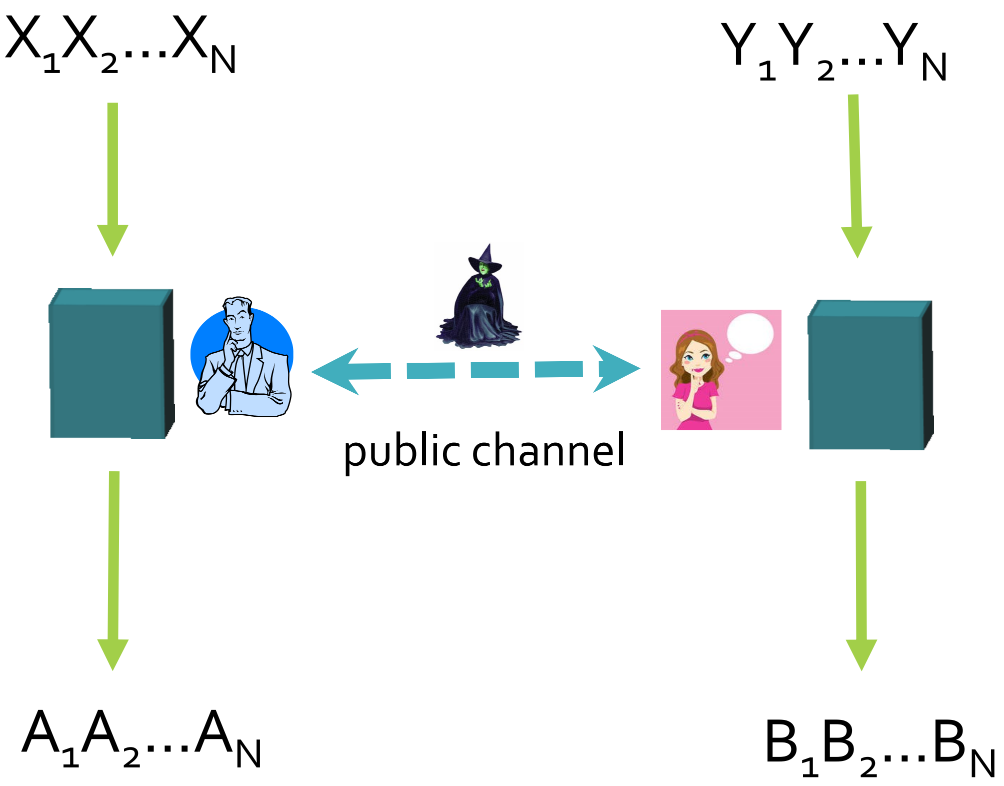
New rule: If Alice and Bob don't succeed at Magic Square, they still win **if** $Z_i = Z'_i$.

SUCCESS!!



MagicQKD

1. Alice and Bob play Magic Square N times in parallel.
2. They share inputs on εN randomly chosen rounds.
3. They share outputs on $\varepsilon^2 N$ randomly chosen rounds; if avg. score $< 1 - \varepsilon$, abort.
4. Record key bits, discard the rest.



MagicQKD

1. Ali
   Squ
2. The
   ran
3. The
   ran
   avg
4. Rec
   rest.

Security Statement:

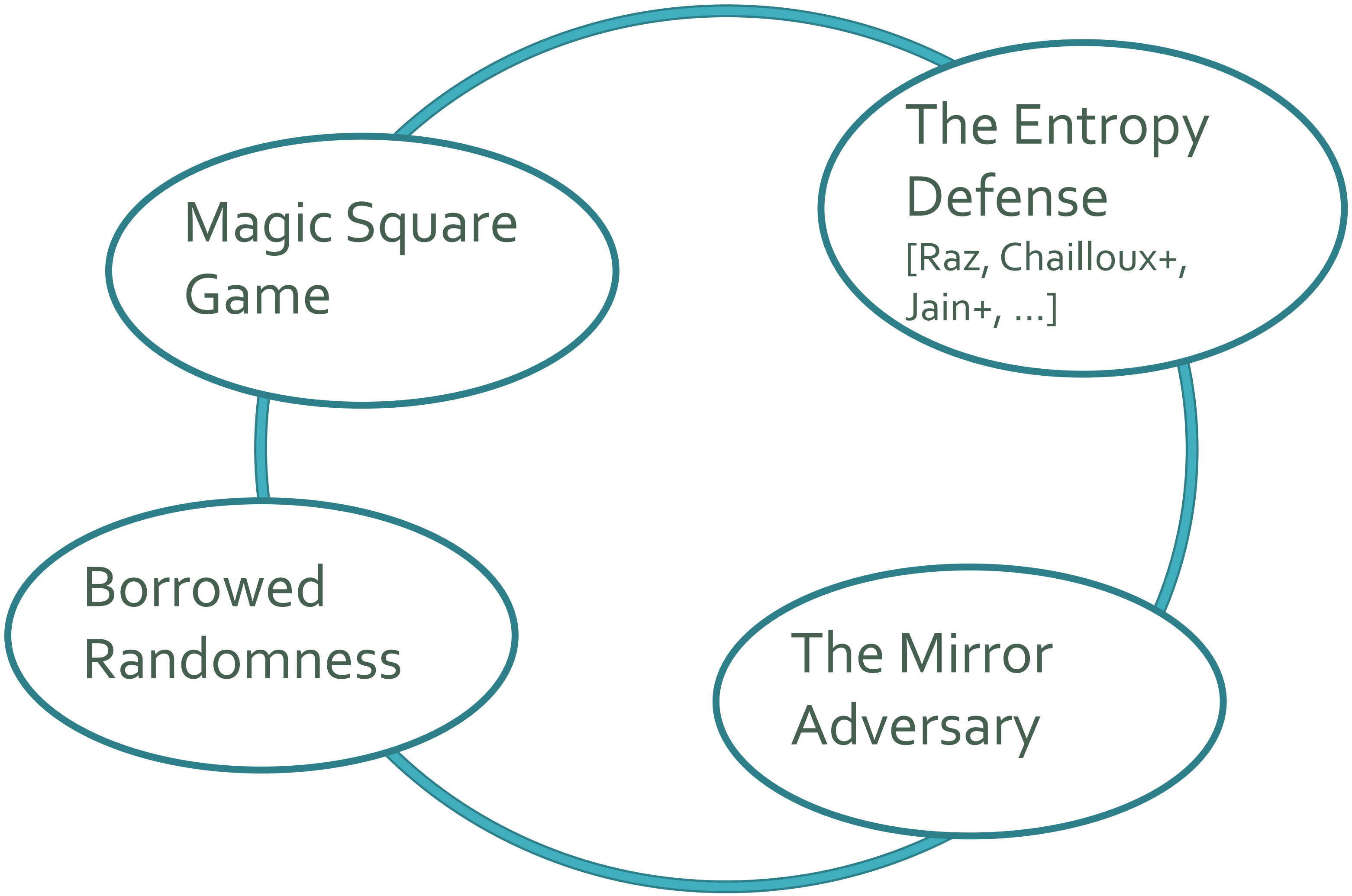
For fixed δ sufficiently small,

$$H^{\delta}_{min}(AliceKey \mid Eve) - H^{\delta}_{0}(AliceKey \mid BobKey) \quad \geq \quad \Omega(N).$$

$_2 \ldots Y_N$

$A_1A_2 \ldots A_N$

$B_1B_2 \ldots B_N$

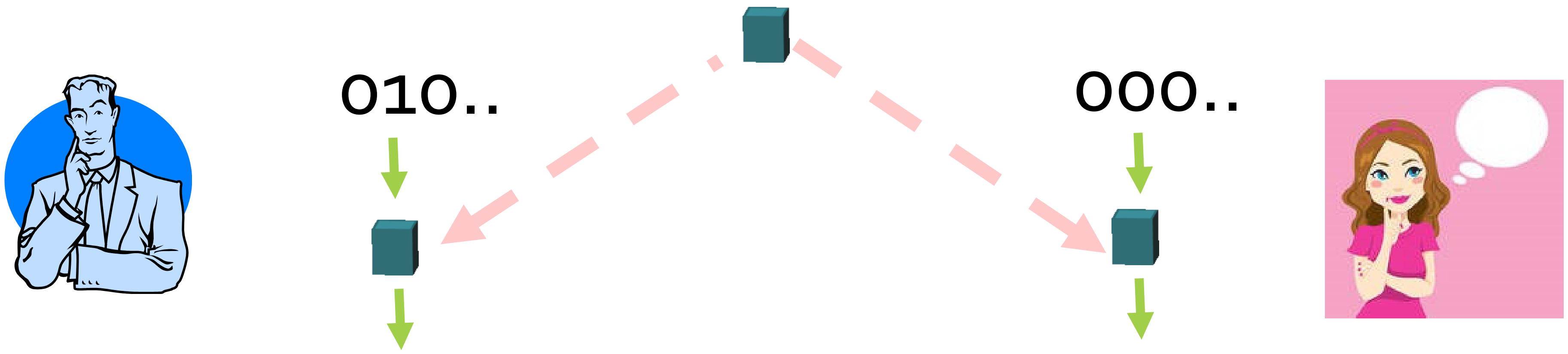


Magic Square Game
The Entropy Defense
[Raz, Chailloux+, Jain+, …]
Borrowed Randomness
The Mirror Adversary

Conclusions

Minimizing assumptions for QKD*

- Bell equipment (untrusted)
- Public classical channel (trusted)
- Private randomness for each player (trusted)

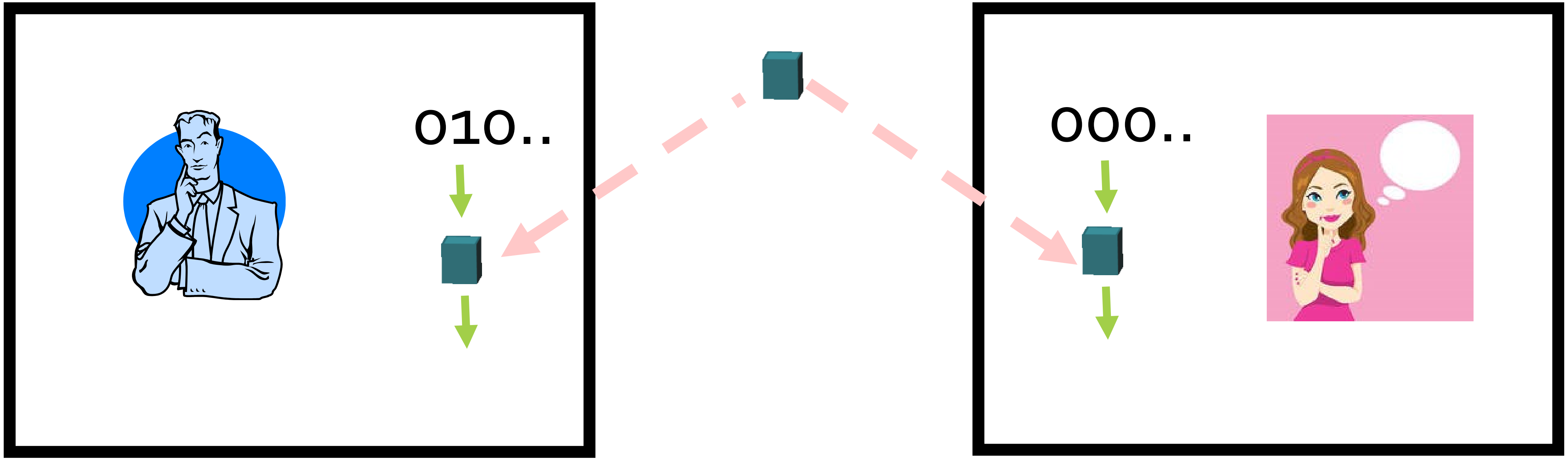


* Similar result as ours subsequently obtained by [Vidick 17] using “Anchored-Games”.

Minimizing assumptions for QKD

Only experimental assumption:

- Information can be contained in Alice's and Bob's labs.



Minimizing assumptions for QKD

Only experimental assumption:

- Information can be contained in Alice's and Bob's labs.

0101011101
1000010110
1010100010
0101110111
1111000101
010100101…

??????????
??????????
??????????
??????????
??????????
????????..

0101011101
1000010110
1010100010
0101110111
1111000101
010100101…

New Frontier: Parallel Device-Independence

Known Tools:

- Quantum parallel repetition theorems for various games (XOR, unique, free, anchored, …)
- Self-testing for parallel repeated games.

Tasks to study:

- Randomness expansion
- Universal quantum computation

Thank You !