A Tight High-Order Entropic Quantum Uncertainty Relation with Applications

Serge Fehr, Christian Schaffner *(CWI Amsterdam, NL)*

Renato Renner *(University of Cambridge, UK)*

Ivan Damgård, Louis Salvail *(University of Århus, DK)*

Crypto-Workshop Dagstuhl

Thursday, September 20th 2007

1970:

Conjugate Coding *

Stephen Wiesner

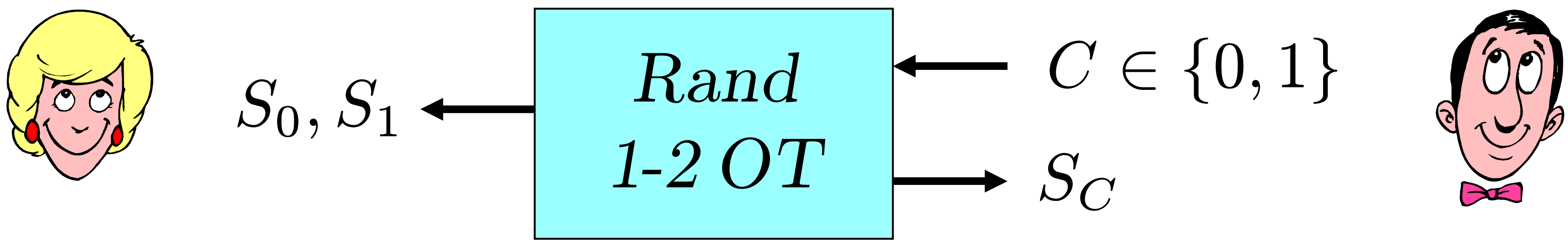
Columbia University, New York, N.Y.

Department of Physics

Example One: A means for transmitting two messages either but not both of which may be received.

The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This

(Randomized) 1-2 Oblivious Transfer



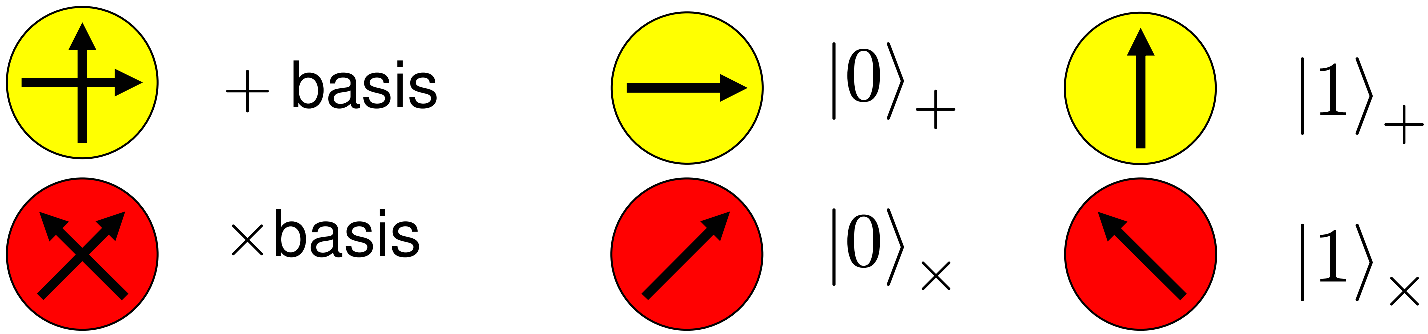
> Example One: A means for transmitting two messages either but not both of which may be received.

- complete for 2-party computation
- impossible in the plain (quantum) model
- possible in the Bounded-Quantum-Storage Model

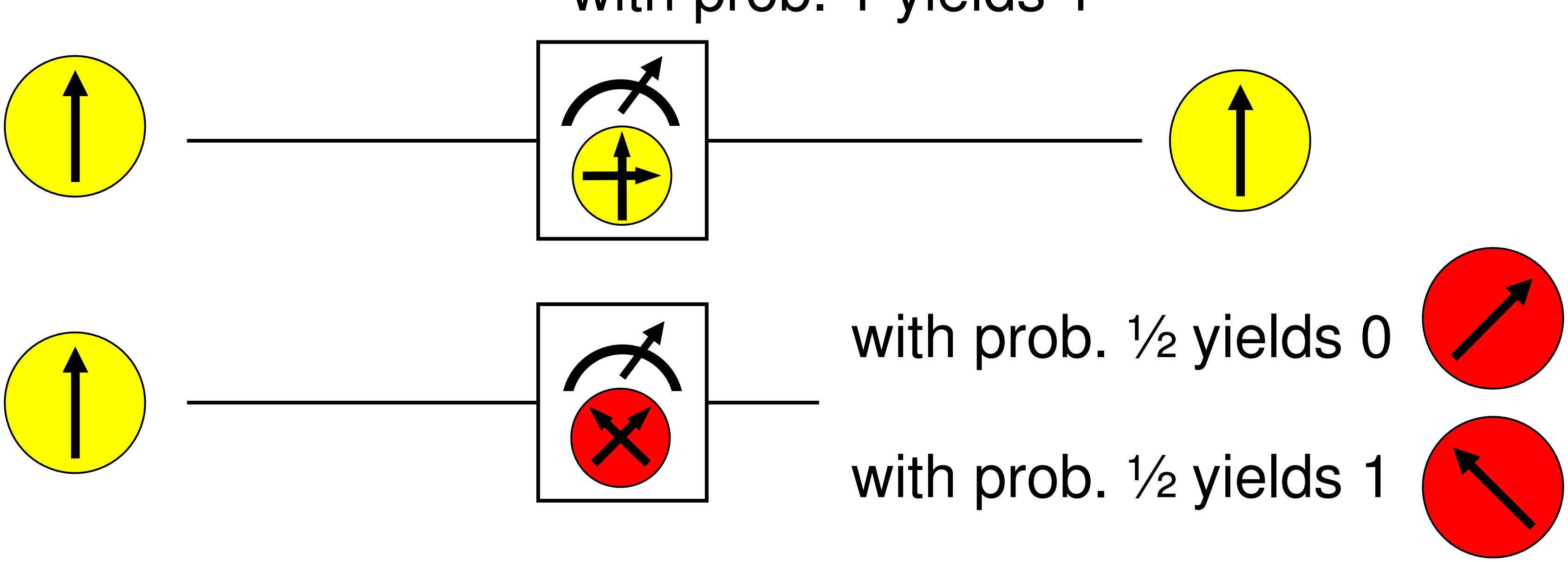
Outline

- Motivation and Notation
- Quantum Uncertainty Relation
- Contributions

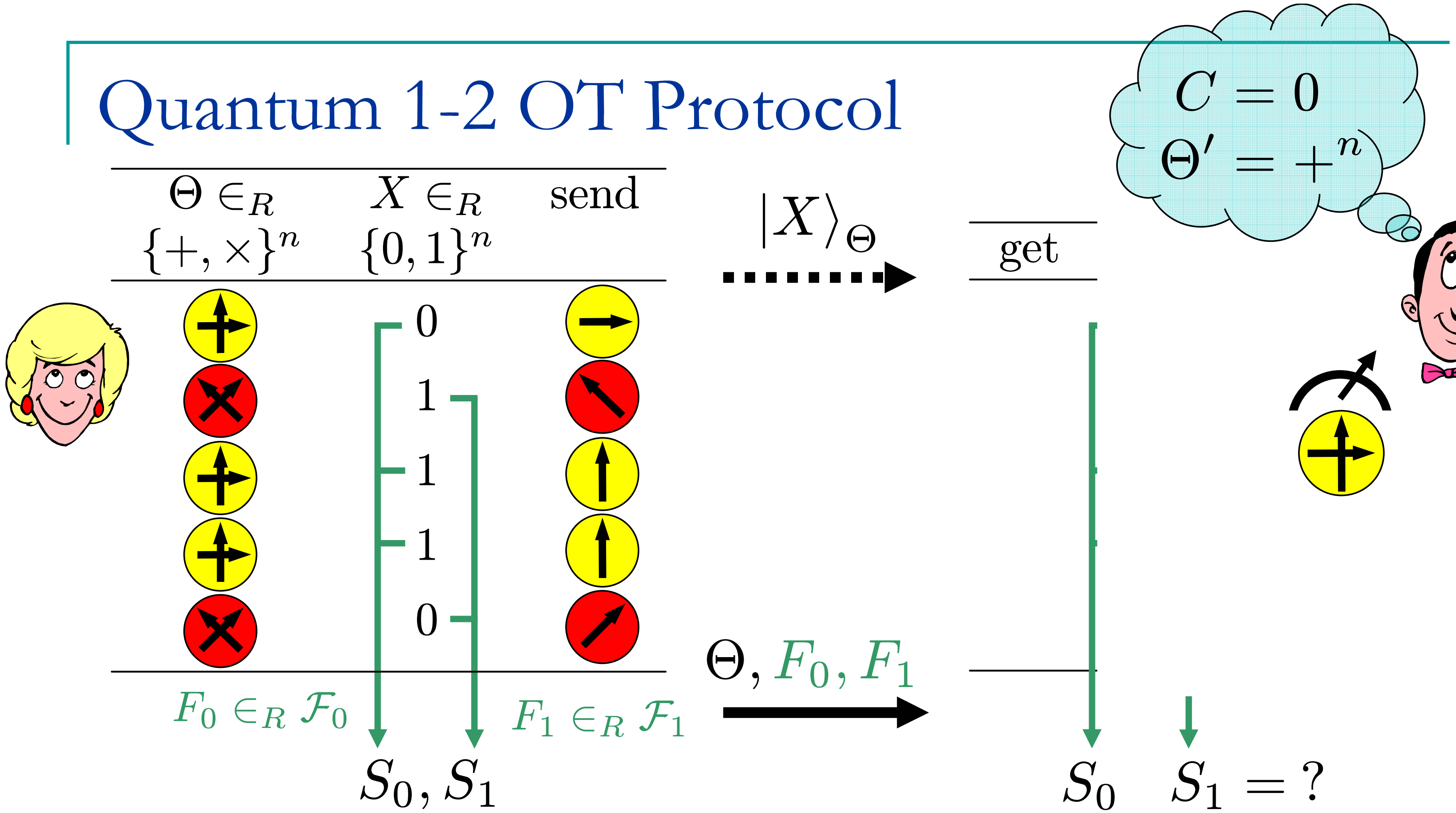
Quantum Mechanics



Measurements:

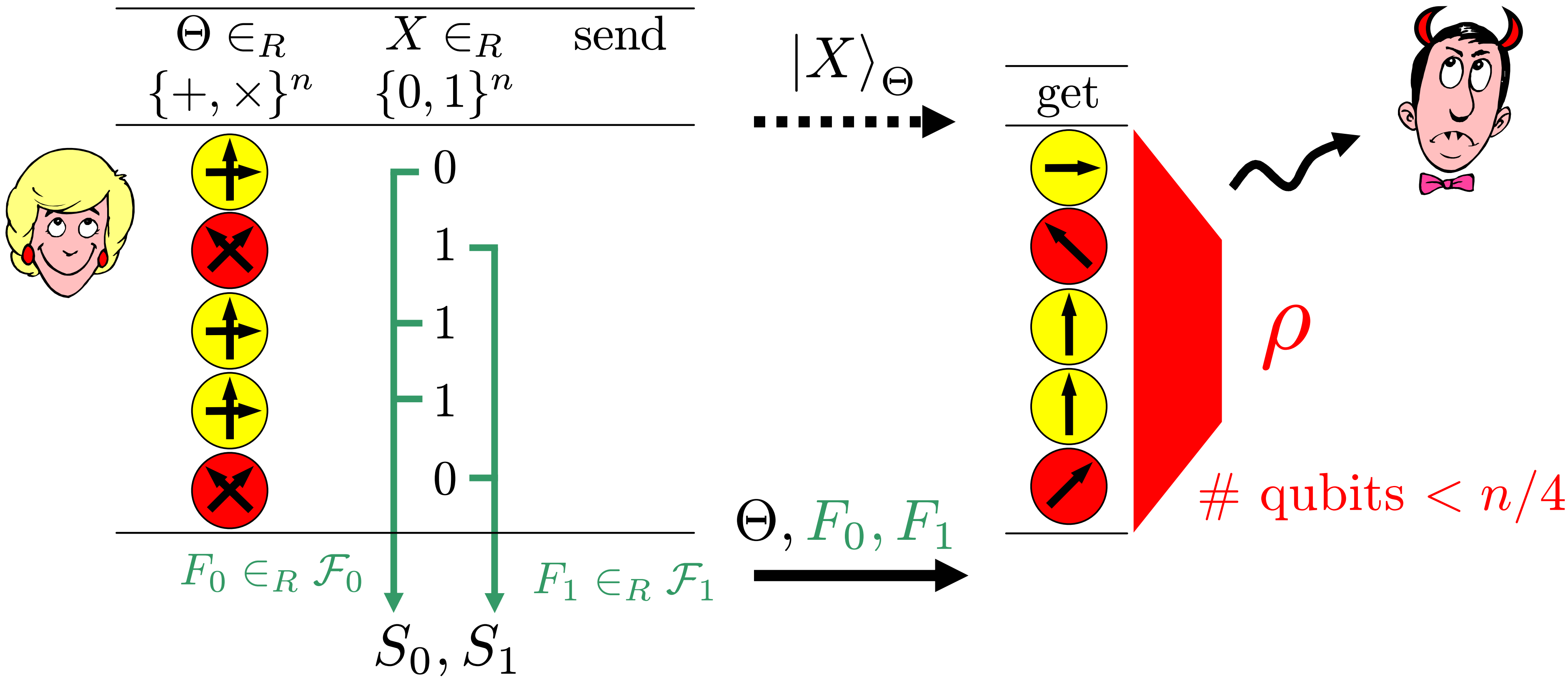


Quantum 1-2 OT Protocol



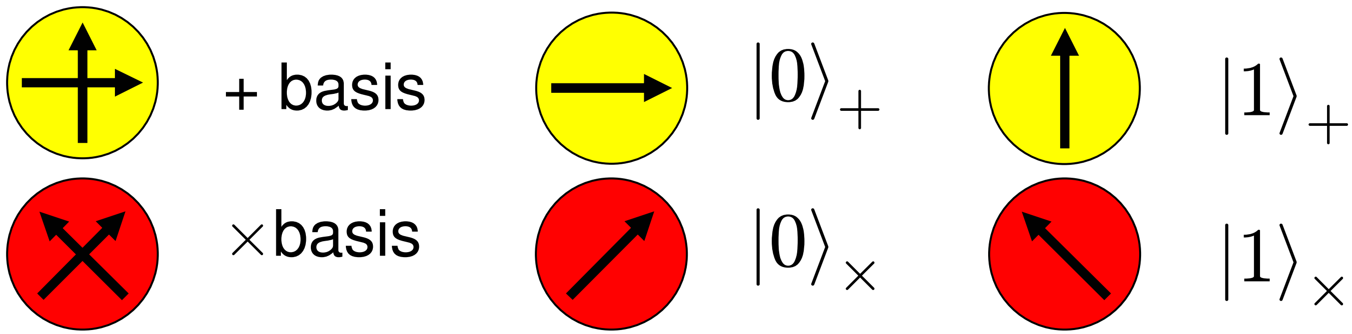
- Correctness ✓
- Receiver-Security against Dishonest Alice ✓

Sender-Security?

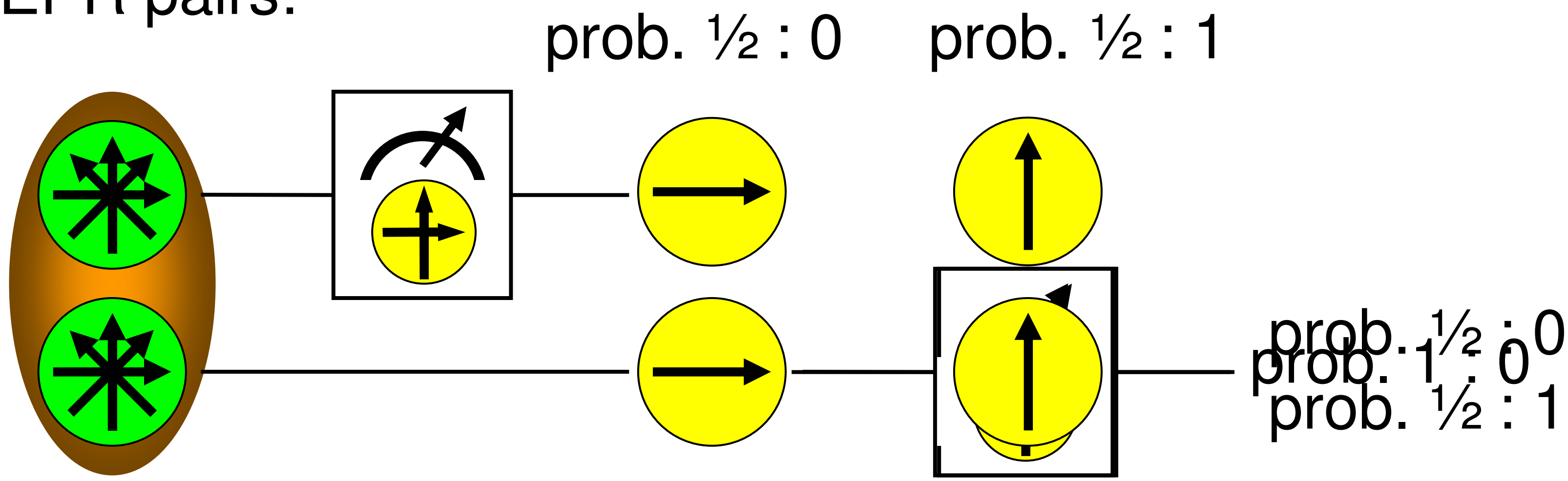


- Sender-Security: one of the strings looks completely random to dishonest Bob

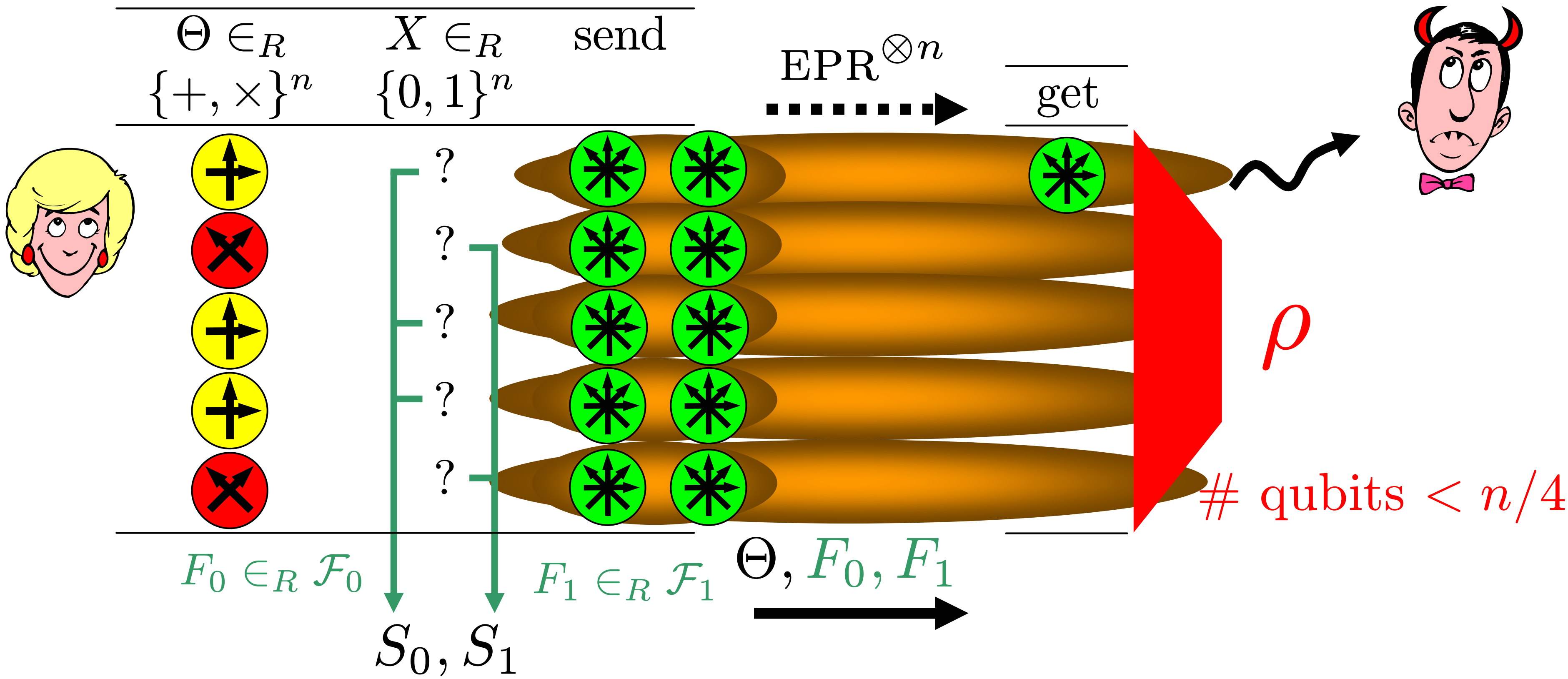
Quantum Mechanics II



EPR pairs:

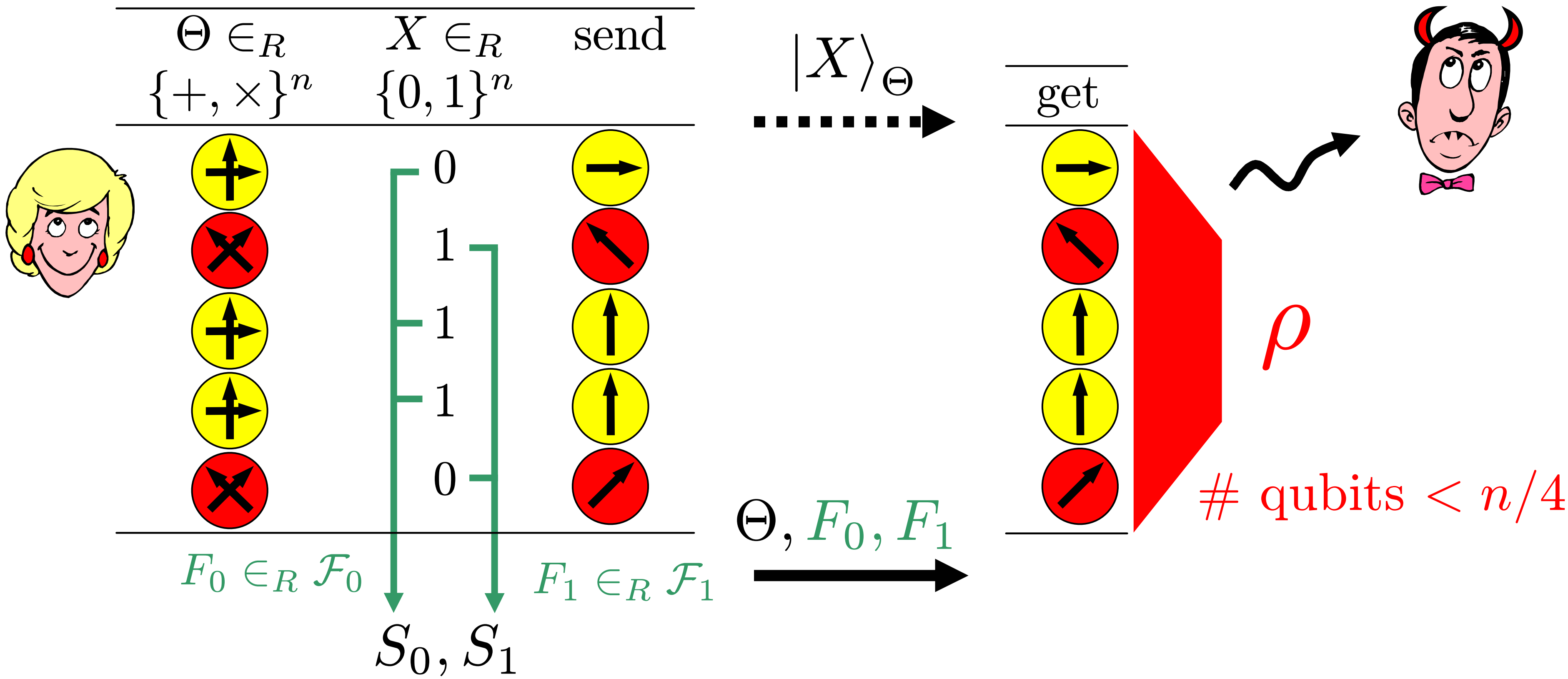


Entanglement-Based Protocol



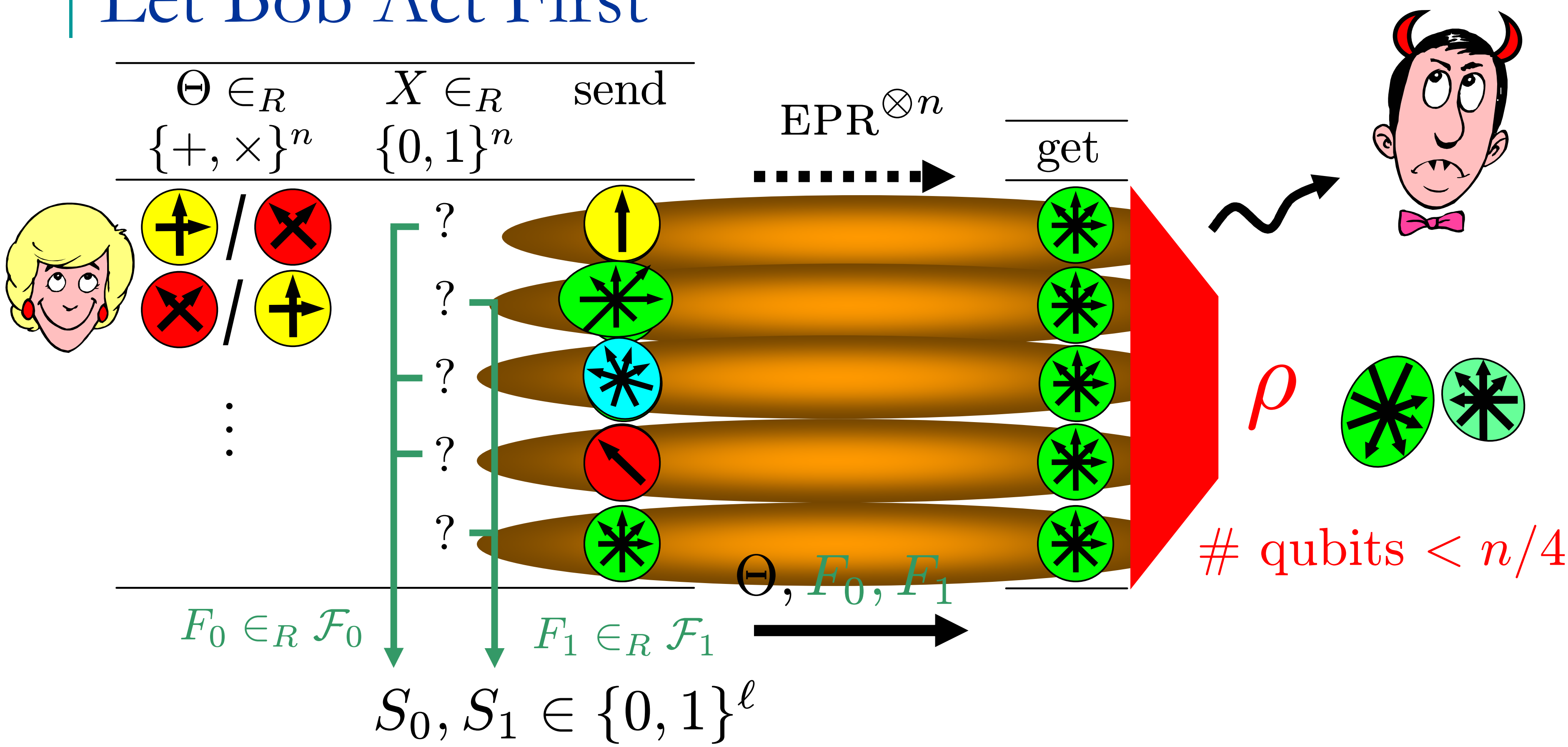
- Sender-Security: One of the strings looks completely random to dishonest Bob

Entanglement-Based Protocol



- Sender-Security: One of the strings looks completely random to dishonest Bob

Let Bob Act First

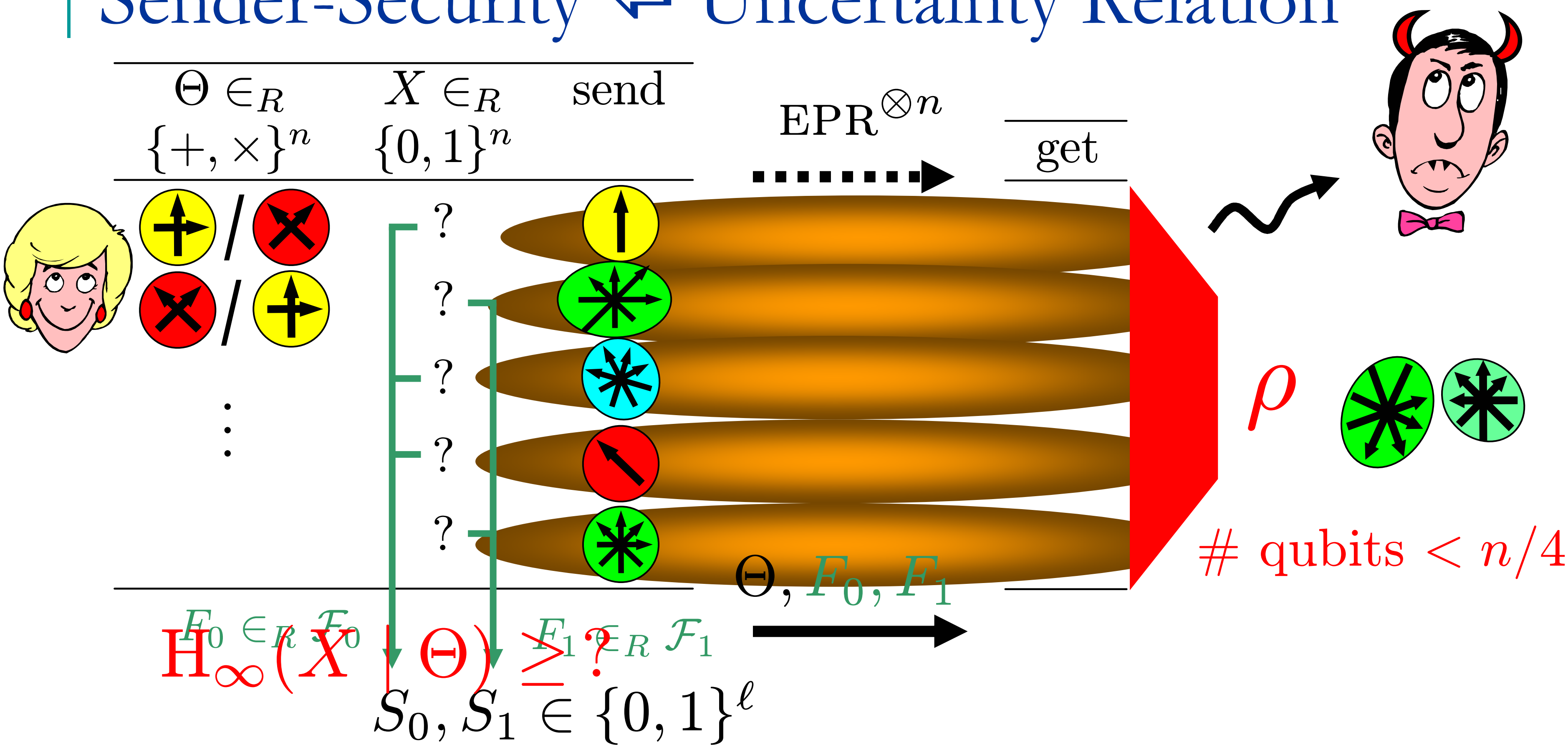


- Sender-Security: One of the strings looks completely random to dishonest Bob

$$\mathbf{PA} : 2\ell \approx \mathrm{H}_\infty(X \mid \Theta, \rho)$$

[Renner König 05, Renner 06]

Sender-Security ⇦ Uncertainty Relation



- Sender-Security: One of the strings looks completely random to dishonest Bob

$$\mathbf{PA}: 2\ell \approx \mathrm{H}_\infty(X \mid \Theta, \rho) \geq \underbrace{\mathrm{H}_\infty(X \mid \Theta)}_{\geq ?} - \underbrace{\#\text{ qubits}}_{<n/4}$$

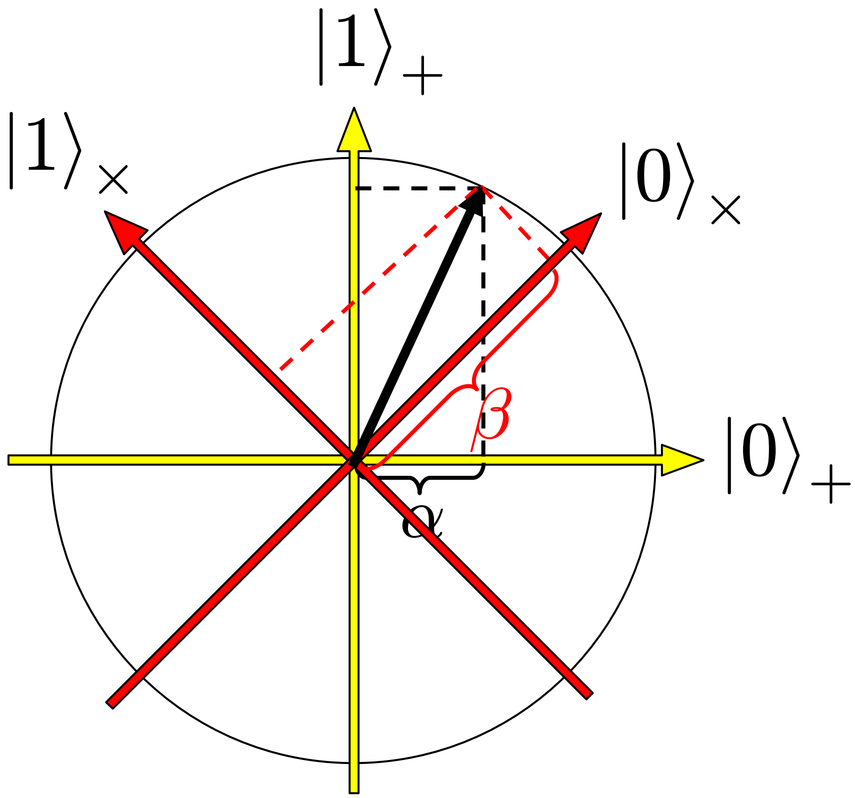
[Renner König 05, Renner 06]

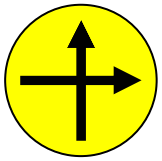
Outline

- ✓ Motivation and Notation
- Quantum Uncertainty Relation
- Contributions

Quantum Uncertainty Relation needed

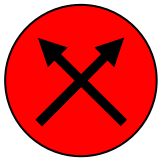
qubit as unit vector in $\mathbb{C}^2$





$\Pr[X = 0] = |\alpha|^2$

$\Pr[X = 1] = 1 - |\alpha|^2$



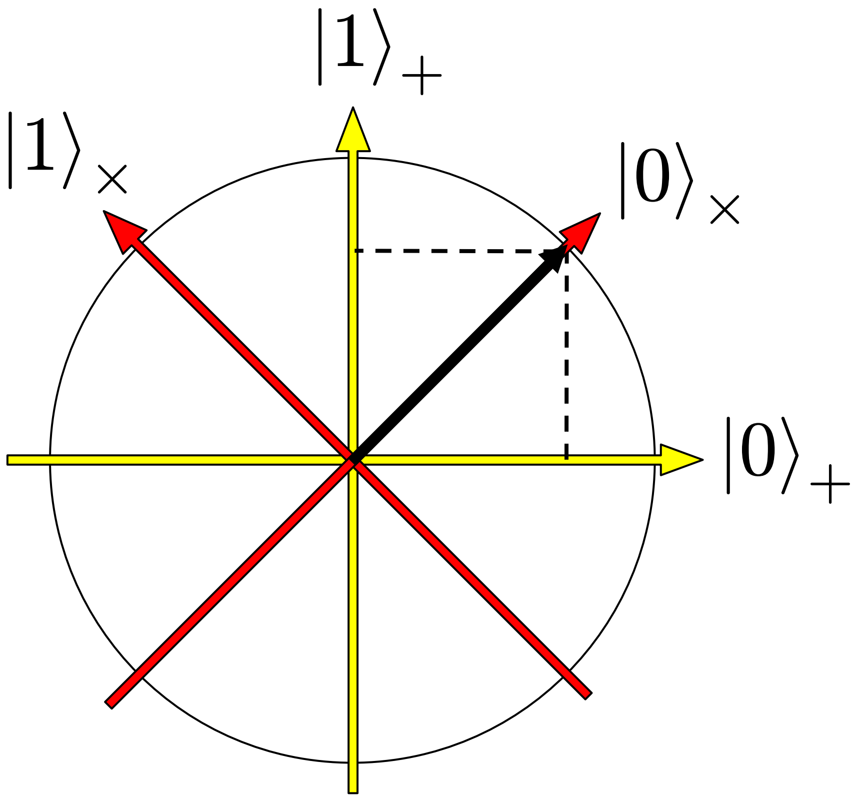
$\Pr[X = 0] = |\beta|^2$

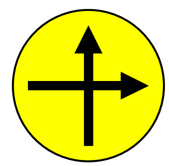
$\Pr[X = 1] = 1 - |\beta|^2$

Uncertainty Relation for One Qubit

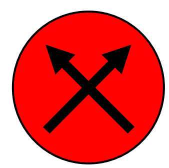
Maassen Uffink 88: Let ρ_i be a 1-qubit state.
$\Theta_i \in_R \{+, \times\}$, X_i the outcome of measuring ρ_i in basis Θ_i. Then,

$$\mathrm{H}(X_i \mid \Theta_i) = \frac{1}{2}\Big(\underbrace{\mathrm{H}(X_i \mid \Theta_i = +) + \mathrm{H}(X_i \mid \Theta_i = \times)}_{\geq 1}\Big) \geq \frac{1}{2}.$$





$\Pr[X = 0] = 1/2$
$\Pr[X = 1] = 1/2$



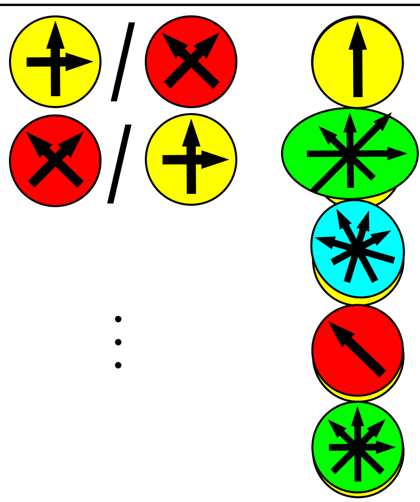
$\Pr[X = 0] = 1$
$\Pr[X = 1] = 0$

Quantum Uncertainty Relation needed

Maassen Uffink 88: Let ρ_i be a 1-qubit state.
$\Theta_i \in_R \{+, \times\}$, X_i the outcome of measuring ρ_i in basis Θ_i. Then,

$$\mathrm{H}(X_i \mid \Theta_i) = \tfrac{1}{2}\big(\underbrace{\mathrm{H}(X_i \mid \Theta_i = +) + \mathrm{H}(X_i \mid \Theta_i = \times)}_{\geq 1}\big) \geq \tfrac{1}{2}.$$

$\Theta \in_R \{+, \times\}^n$	state ρ



$\vdots$

$\mathrm{H}_\infty(X \mid \Theta) \geq ?$

$\mathrm{H}(X_i \mid \Theta_i) \geq \frac{1}{2}$

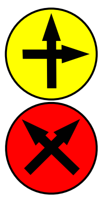
X_i independent

$\Rightarrow \mathrm{H}^{\varepsilon}_\infty(X^n \mid \Theta) \overset{n\to\infty}{\approx} n \cdot \mathrm{H}(X_i \mid \Theta_i) \geq n/2$

except with prob $\leq \varepsilon$

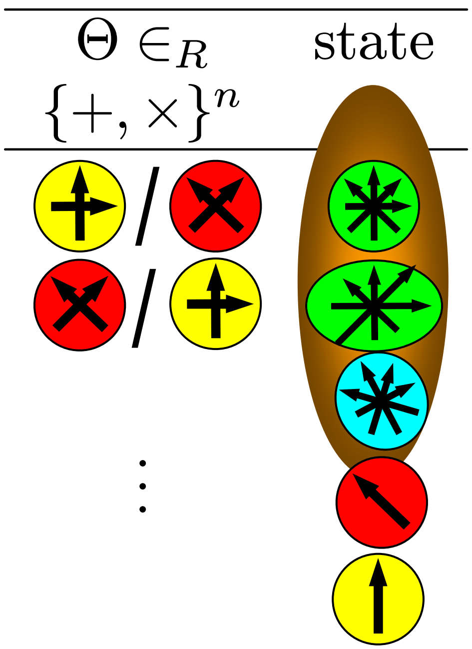
$X^i := X_1, \ldots, X_i$
$X := X^n = X_1, \ldots, X_n$

Main Result



Maassen Uffink 88: Let ρ_i be a 1-qubit state. $\Theta_i \in_R \{+, \times\}$, X_i the outcome of measuring ρ_i in basis Θ_i. Then,

$$H(X_i \mid \Theta_i) = \frac{1}{2}\Big(\underbrace{H(X_i \mid \Theta_i = +) + H(X_i \mid \Theta_i = \times)}_{\geq 1}\Big) \geq \frac{1}{2}.$$



$H_\infty(X \mid \Theta) \geq ?$

$$H(X_i \mid \Theta_i) \geq \frac{1}{2}$$

$$H(X_i \mid \Theta_i, X^{i-1} = x^{i-1}, \Theta^{i-1} = \theta^{i-1}) \geq \frac{1}{2}$$

X_i dependent

Quantum Uncertainty Relation: *Let $X = (X_1, \ldots, X_n)$ be the outcome. Then,*

$$H_\infty^\varepsilon(X \mid \Theta) \gtrsim n/2$$

with ε negligible in n.

Main Technical Lemma

$Z_1, \ldots, Z_n$ (dependent) random variables
with $\mathrm{H}(Z_i \mid Z^{i-1} = z^{i-1}) \geq h$.

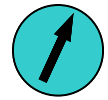
Then, $\mathrm{H}_\infty^\varepsilon(Z) \gtrsim n \cdot h$ with ε negligible in n

Proof:

- information theory
- generalized Chernoff bound (**Azuma inequality**)

Proof of Quantum Uncertainty Relation

Thm: $\mathrm{H}(Z_i \mid Z^{i-1} = z) \geq h \;\Rightarrow\; \mathrm{H}_\infty^\varepsilon(Z^n) \gtrsim hn$

MU: ρ 1-qubit state: $\mathrm{H}(X_0 \mid \Theta_0) \geq \frac{1}{2}$ 

$$Z_i := (X_i, \Theta_i)$$

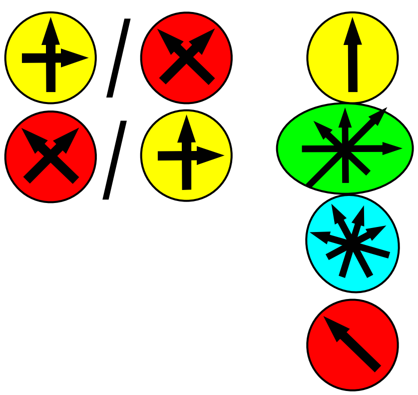
$$\mathrm{H}(Z_i \mid Z^{i-1} = z) = \mathrm{H}(X_i \mid \Theta_i, Z^{i-1} = z) + \mathrm{H}(\Theta_i \mid Z^{i-1} = z)$$

$$\geq \tfrac{1}{2} + 1 =: h.$$

$$\mathrm{H}_\infty^\varepsilon(X \mid \Theta) \approx \mathrm{H}_\infty^\varepsilon(Z^n) - \mathrm{H}_0(\Theta) \gtrsim n/2 + n - n.$$

□

$\Theta \in_R \{+, \times\}^n$	state ρ

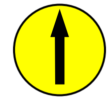


Quantum Uncertainty Relation: *Let $X = (X_1, \ldots, X_n)$ be the outcome. Then,*

$$\mathrm{H}_\infty^\varepsilon(X \mid \Theta) \gtrsim n/2$$

with ε negligible in n.

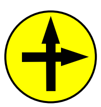
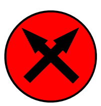
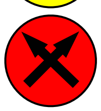
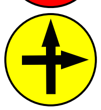
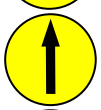
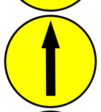
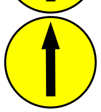
Tight?

MU: ρ 1-qubit state: $\mathrm{H}(X_0 \mid \Theta_0) \geq \frac{1}{2}$ 

$$\mathrm{H}(X \mid \Theta) = \tfrac{1}{2}\Big(\underbrace{\mathrm{H}(X \mid \Theta = +)}_{=0} + \underbrace{\mathrm{H}(X \mid \Theta = \times)}_{=1}\Big) = \tfrac{1}{2}.$$

For the pure state $|0\rangle^{\otimes n}$, the X are independent and we know that $\mathrm{H}_\infty^\varepsilon(X \mid \Theta) \overset{n\to\infty}{\approx} \mathrm{H}(X \mid \Theta) = n/2$.

$\Theta \in_R \{+, \times\}^n$	state ρ
 / 	
 / 	
	
	

Quantum Uncertainty Relation: *Let $X = (X_1, \ldots, X_n)$ be the outcome. Then,*

$$\mathrm{H}_\infty^\varepsilon(X \mid \Theta) \gtrsim n/2$$

with ε negligible in n.

Outline

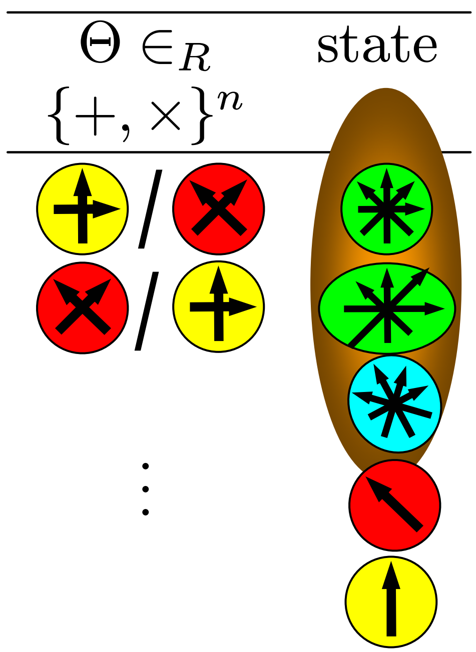
- ✓ Motivation and Notation
- ✓ Quantum Uncertainty Relation
- Contributions

Contributions I: Uncertainty Relations

- classical general lemma:

  $$\mathrm{H}(Z_i \mid Z^{i-1} = z) \geq h \;\Rightarrow\; \mathrm{H}^{\varepsilon}_{\infty}(Z^n) \gtrsim hn$$

- instantiate it for various quantum codings:



- conjugate coding / BB84:

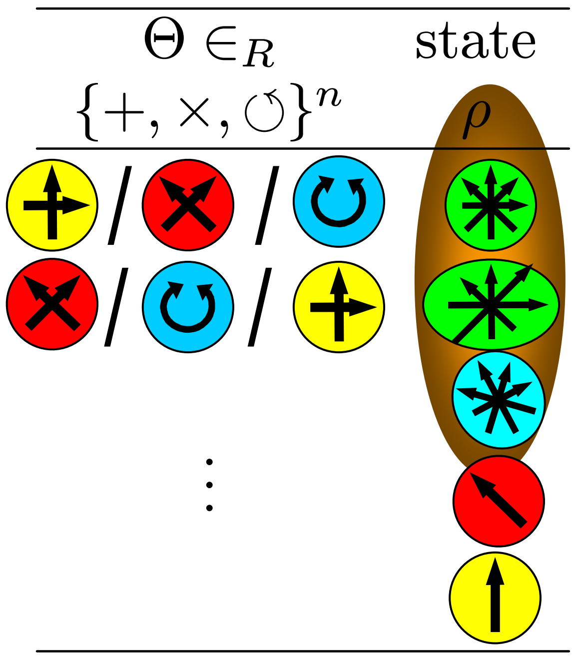
  $$\mathrm{H}^{\varepsilon}_{\infty}(X \mid \Theta) \geq n/2$$

Contributions I: Uncertainty Relations

- classical general lemma:

  $\mathrm{H}(Z_i \mid Z^{i-1} = z) \geq h \;\Rightarrow\; \mathrm{H}^{\varepsilon}_{\infty}(Z^n) \gtrsim hn$

- instantiate it for various quantum codings:



- conjugate coding / BB84:

  $\mathrm{H}^{\varepsilon}_{\infty}(X \mid \Theta) \geq n/2$

- three bases / six-state:

  $\mathrm{H}^{\varepsilon}_{\infty}(X \mid \Theta) \geq \frac{2}{3}n$

- ...

Contributions II: Applications

- **Bounded-Quantum-Storage Model:** Non-interactive, practical protocols for 1-2 OT and BC secure according new composable security definitions.

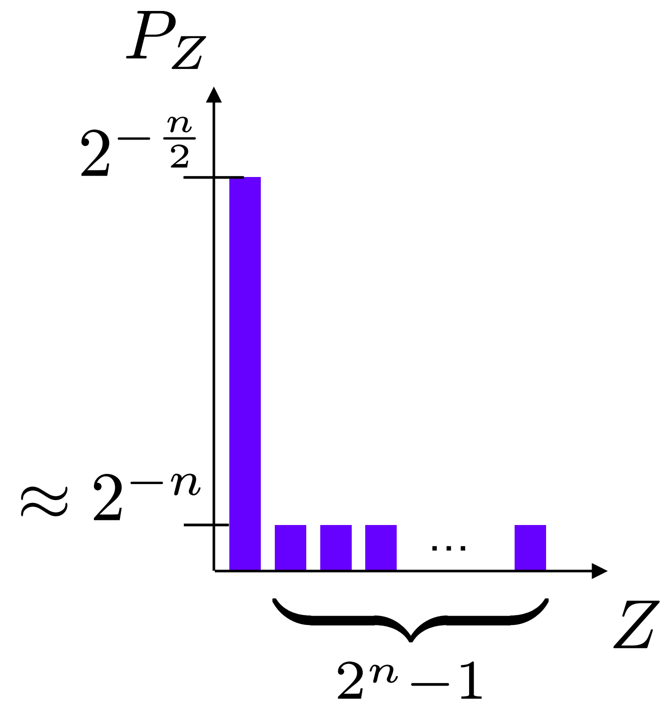
- **Quantum Key Distribution**: Security proofs in realistic setting of a quantum-memory bounded eavesdropper. Tolerate higher error rates than against unbounded adversaries.

- **Composition of certain Quantum Ciphers:** key-uncertainty adds up in terms of min-entropy.

Entropies

Z random variable over $\{0,1\}^n$

name	definition
$H_0(Z)$	$\log \left\| \{z \mid P_Z(z) > 0\} \right\|$
$H(Z)$	$-\sum_z P_Z(z) \log (P_Z(z))$
$H_\infty(Z)$	$-\log (\max_z P_Z(z))$



$H_\infty \leq H \leq H_0$

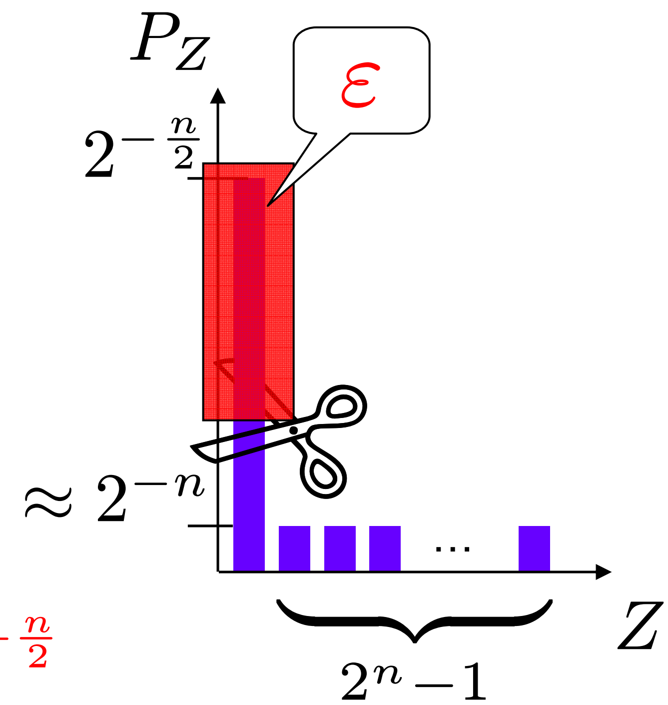
lowerbound on H $\not\Rightarrow$ lowerbound on H_∞

Smooth Min-Entropy

Z random variable over $\{0,1\}^n$

name	definition	
$\mathrm{H}_0(Z)$	$\log \left\lvert \{z \mid P_Z(z) > 0\} \right\rvert$	n
$\mathrm{H}(Z)$	$-\sum_z P_Z(z) \log\left(P_Z(z)\right)$	$\approx n$
$\mathrm{H}_\infty(Z)$	$-\log\left(\max_z P_Z(z)\right)$	$n/2$
$\mathrm{H}_\infty^\varepsilon(Z)$	$\max_{\Pr[\mathcal{E}] \geq 1-\varepsilon} \mathrm{H}_\infty(Z\mathcal{E})$	

for $\varepsilon = 2^{-\frac{n}{2}}$



Open Questions

- two-way post processing
- QKD with more bases
- in higher-dimensional (non-binary) systems
- using less randomness: avoid sifting stage

Smooth Min-Entropy [Renner Wolf 05]

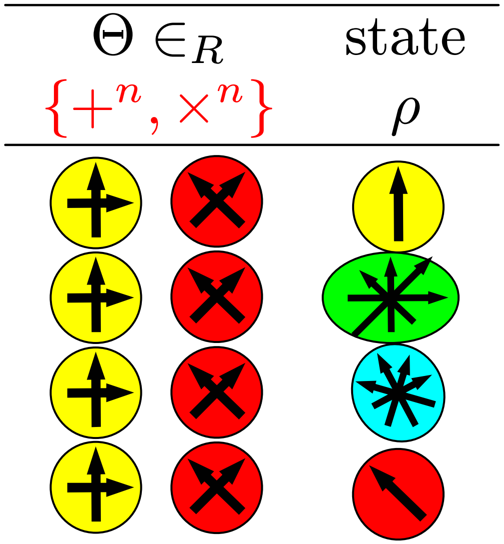
Z random variable over $\{0,1\}^n$

$\mathrm{H}_\infty^\varepsilon(Z) := \max_{\Pr[\mathcal{E}]\geq 1-\varepsilon} \mathrm{H}_\infty(Z\mathcal{E})$

$Z^i := Z_1, \ldots, Z_i$

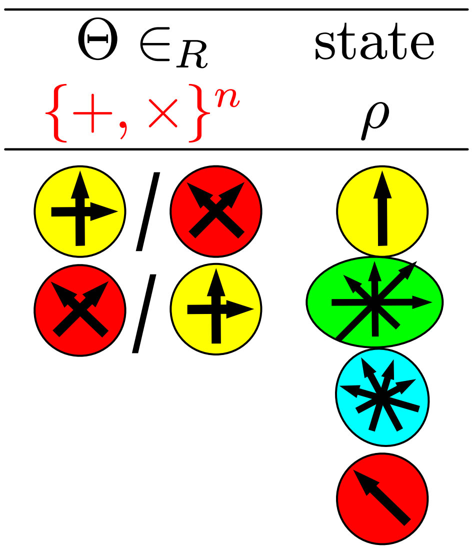
- many Shannon-like properties: chain rule, sub-additivity, monotonicity, e.g. $\mathrm{H}_\infty^\varepsilon(Z \mid V) \approx \mathrm{H}_\infty^\varepsilon(ZV) - \mathrm{H}_0(V)$
- for Z_i *iid*: $\mathrm{H}_\infty^\varepsilon(Z^n) \overset{n\to\infty}{\approx} \mathrm{H}(Z^n) = \mathrm{H}(Z_i) \cdot n$
- Privacy Amplification: $\mathrm{H}_\infty^\varepsilon(Z \mid V)$ is the *optimal* amount of extractable randomness

Comparison to Previous Bound



Previous: *There exists an event* $\mathcal{E}$ *with* $\Pr[\mathcal{E}] \gtrsim \frac{1}{2}$ *such that*

$$\mathrm{H}_\infty(X \mid \mathcal{E}, \Theta) \geq n/2.$$



New: $\mathrm{H}_\infty^\varepsilon(X \mid \Theta) \gtrsim n/2$ *with negligible* ε

$\forall \theta \in \{+, \times\}^n$
$\exists$ event $\mathcal{E}_\theta$ with $2^{-n} \sum_\theta \Pr[\mathcal{E}_\theta] \approx 1$ and

$$\mathrm{H}_\infty(X \mid \mathcal{E}_\theta, \Theta = \theta) \gtrsim n/2.$$