Limited-Quantum-Storage Cryptography

From Theory to Practice

Christian Schaffner

CWI Centrum Wiskunde & Informatica, Amsterdam, Netherlands

Workshop in Dagstuhl, July 2009

Contributors and Outline

(in order of appearance)

Ivan Damgaard

Louis Salvail

Serge Fehr

Renato Renner

Stephanie Wehner

Barbara Terhal

Jürg Wullschleger

Carolin Lunemann

Robert König

Hoi-Kwong Lo

Marcos Curty

2004

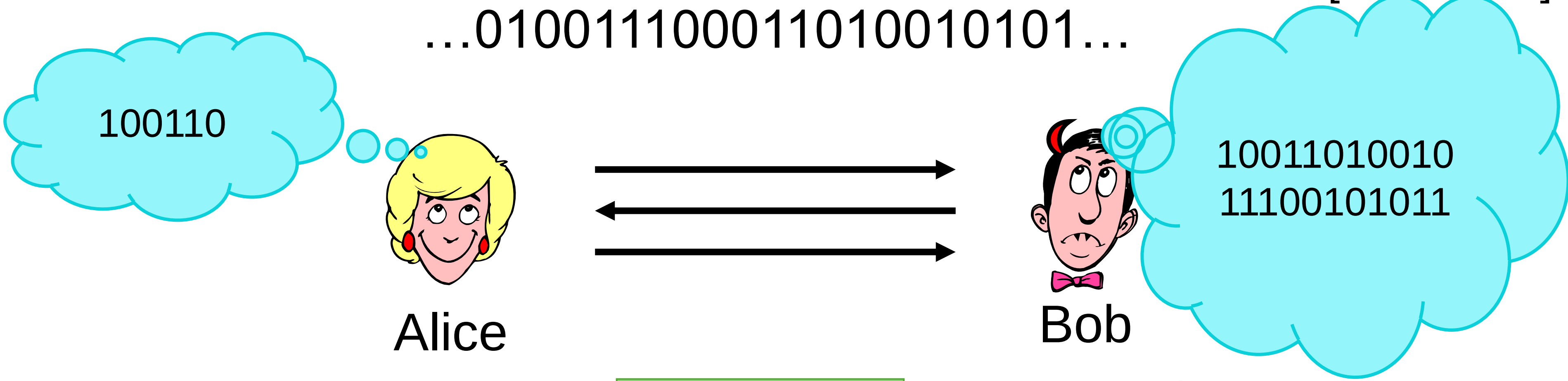
- Bounded Quantum Storage
- The Protocol
- Noisy Quantum Storage
- Secure Identification
- Composability
- Practical Problems

2009

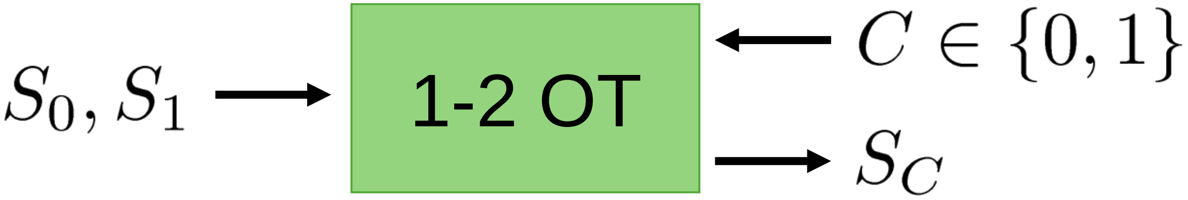
201?

Inspiration: Classical Bounded-Storage

[Maurer 90]



- goal:



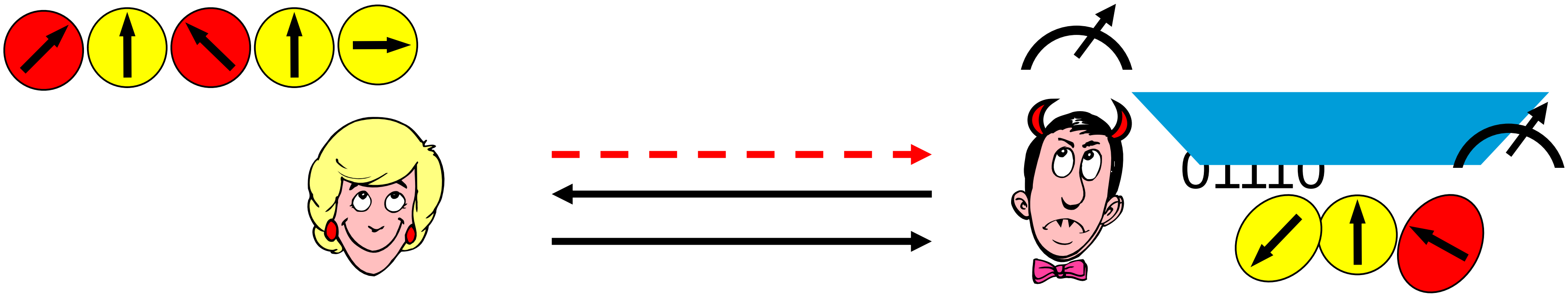
$S_0, S_1 \rightarrow$ 1-2 OT $\leftarrow C \in \{0,1\}$

1-2 OT $\rightarrow S_C$

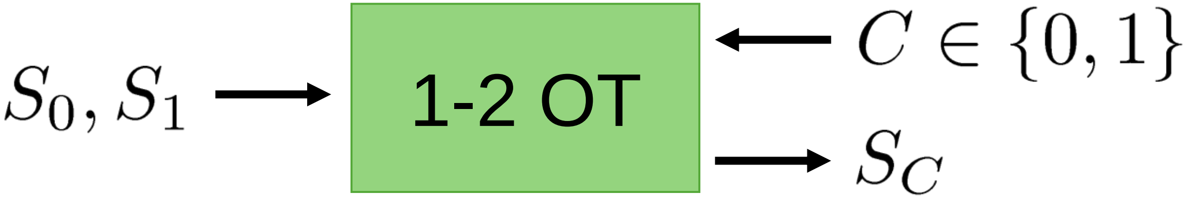
- honest player‘s memory: n
- dishonest player‘s memory: $\leq$ O(**n**^{2})
- information-theoretic security, no time-restrictions
- tight bound [Dziembowski Maurer 04],
relies on the difficulty of storing classical information

Bounded-Quantum-Storage Model

[Damgaard Fehr Salvail Schaffner 05, dito with Renner 07]



- goal:


S_0, S_1

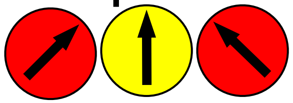
1-2 OT

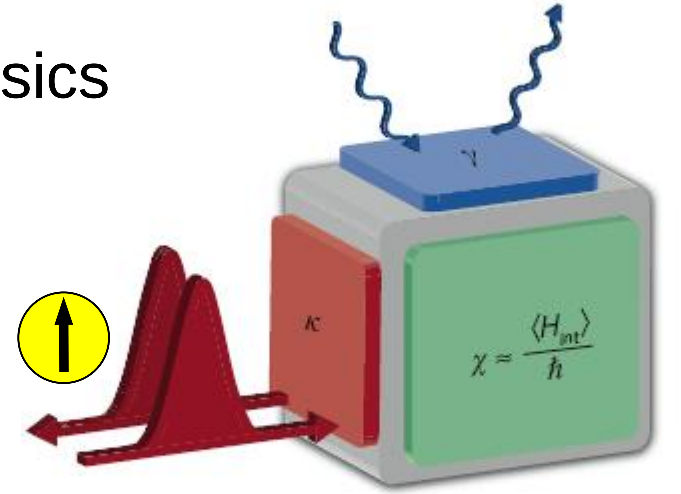
$C \in \{0,1\}$

S_C

- information-theoretic security, no running time-restrictions
- honest player‘s quantum memory: 0
- security as long as
  dishonest player‘s quantum memory: $\leq$ n/4
- relies on technical difficulty of storing quantum information

Storing Photonic Quantum Information

- major research field in quantum physics
- light - ‘flying media’ 
- matter - ‘stationary media’
- goal: light–matter interaction



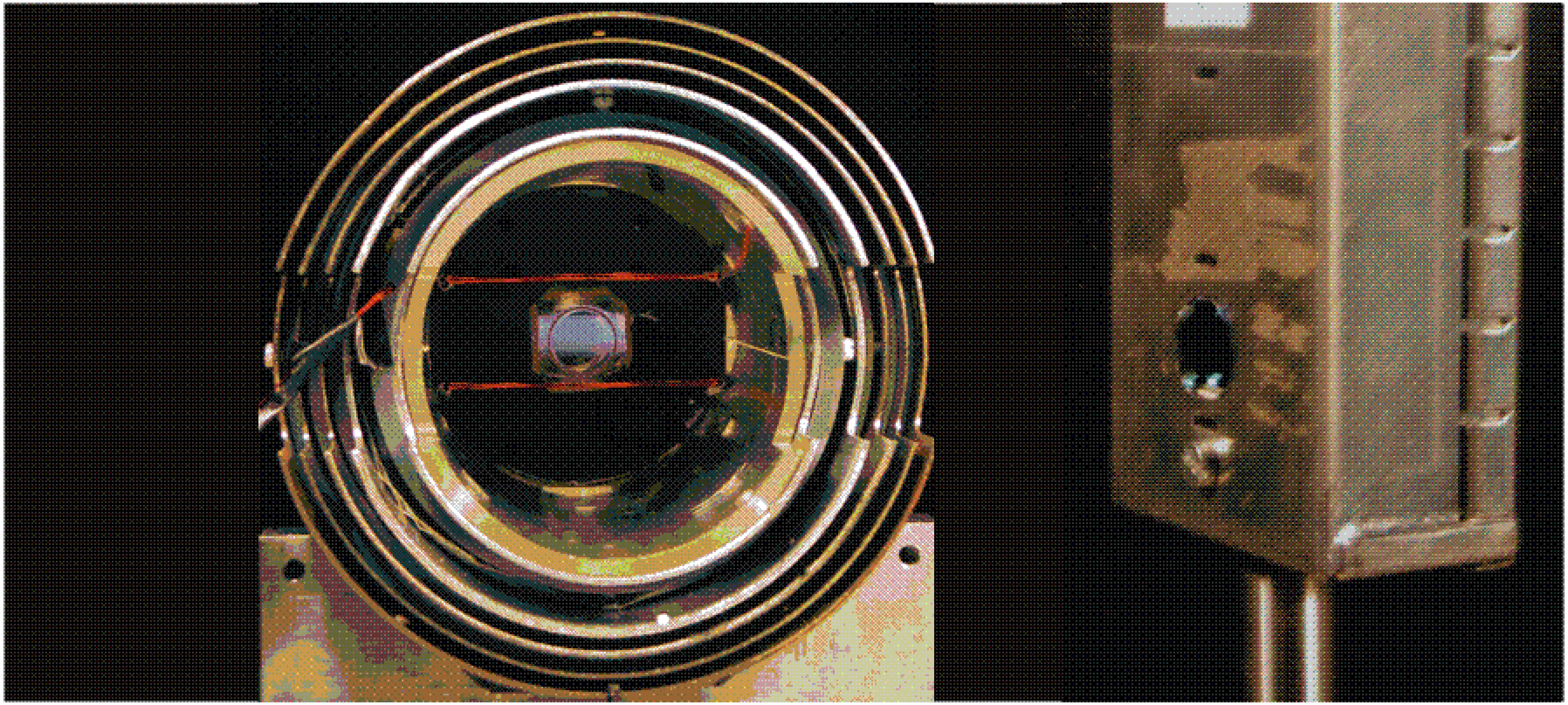
“The Quantum Internet” [Kimble 08]

- early stage: only special purpose experiments
- despite the efforts:
  - storage times of only microseconds
  - low success probabilities
- **storing quantum information is difficult**, i.e. limited quantum-storage is realistic assumption

Storing Photonic Quantum Information

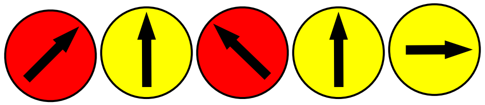
[physics group of Eugene Polzik, Copenhagen (DK)]

- 70% fidelity, few milliseconds, …



The Protocol

[Wiesner ~70, Bennett Brassard Crepeau Skubiszewska 92]



$|X_1\rangle_{\Theta_1} \ldots |X_n\rangle_{\Theta_n}$ $\dashrightarrow$

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

$X \in_R \{0,1\}^n$

$\Theta' \in_R \{+,\times\}^n$

$\rightsquigarrow X' \in \{0,1\}^n$

$\xrightarrow{\Theta}$

$\xleftarrow{\mathcal{I}_0, \mathcal{I}_1}$

$\mathcal{I}_C := \{i : \Theta_i = \Theta'_i\}$

$\mathcal{I}_{1-C} := \{i : \Theta_i \neq \Theta'_i\}$

$X_0 := X|_{\mathcal{I}_0}, X_1 := X|_{\mathcal{I}_1}$

$F_0, F_1 \in_R \mathcal{F}$

$\xrightarrow{F_0, F_1}$

$M_0 := S_0 \oplus F_0(X_0)$

$M_1 := S_1 \oplus F_1(X_1)$

$S_C := M_C \oplus F_C(X'_C)$

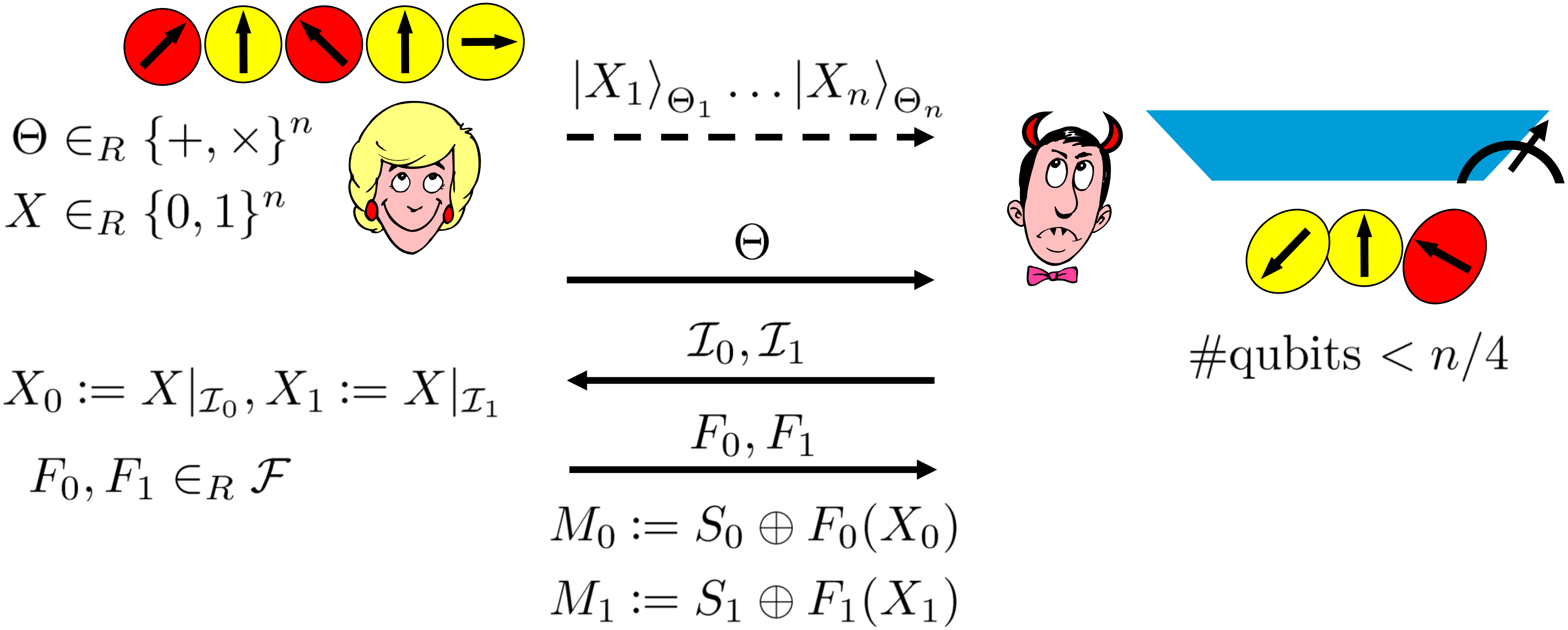
- goal: $S_0, S_1 \longrightarrow \boxed{\text{1-2 OT}} \longleftarrow C \in \{0,1\}$, $\boxed{\text{1-2 OT}} \longrightarrow S_C$

✓ correct

✓ secure against cheating Alice

Dishonest Bob with Bounded Q Storage

[Damgaard Fehr Renner Salvail Schaffner 07]



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

$X \in_R \{0,1\}^n$

$|X_1\rangle_{\Theta_1} \dots |X_n\rangle_{\Theta_n}$

Θ

$\mathcal{I}_0, \mathcal{I}_1$

$X_0 := X|_{\mathcal{I}_0}, X_1 := X|_{\mathcal{I}_1}$

F_0, F_1

$F_0, F_1 \in_R \mathcal{F}$

$M_0 := S_0 \oplus F_0(X_0)$

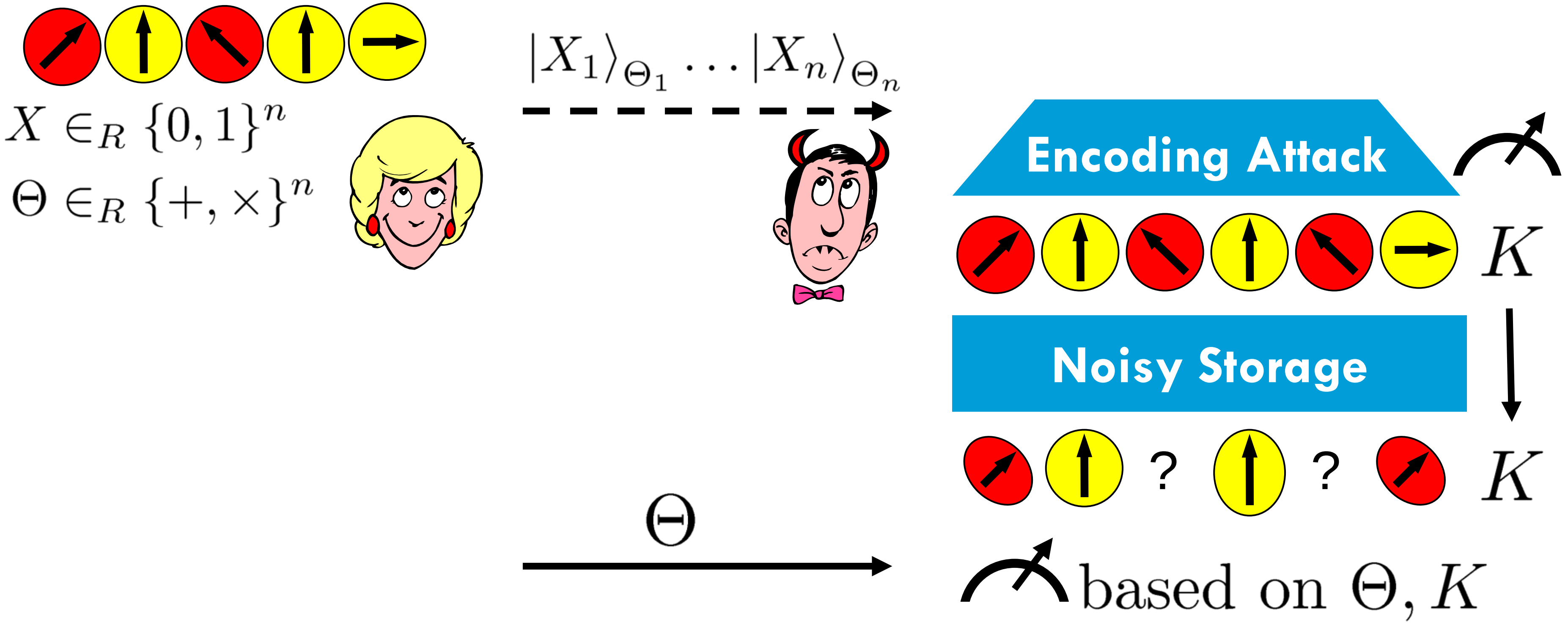
$M_1 := S_1 \oplus F_1(X_1)$

$\#\text{qubits} < n/4$

- purification argument (as in QKD)
- entropic uncertainty relation: $H_{\min}^{\varepsilon}(X|\Theta) \geq n/2$
- privacy amplification against quantum adversaries [Renner Koenig 07]

Noisy-Quantum-Storage Model

[Wehner Schaffner Terhal 08, König Wehner Wullschleger 09]



$X \in_R \{0,1\}^n$

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

$|X_1\rangle_{\Theta_1} \dots |X_n\rangle_{\Theta_n}$

Encoding Attack

K

Noisy Storage

? ?

K

Θ

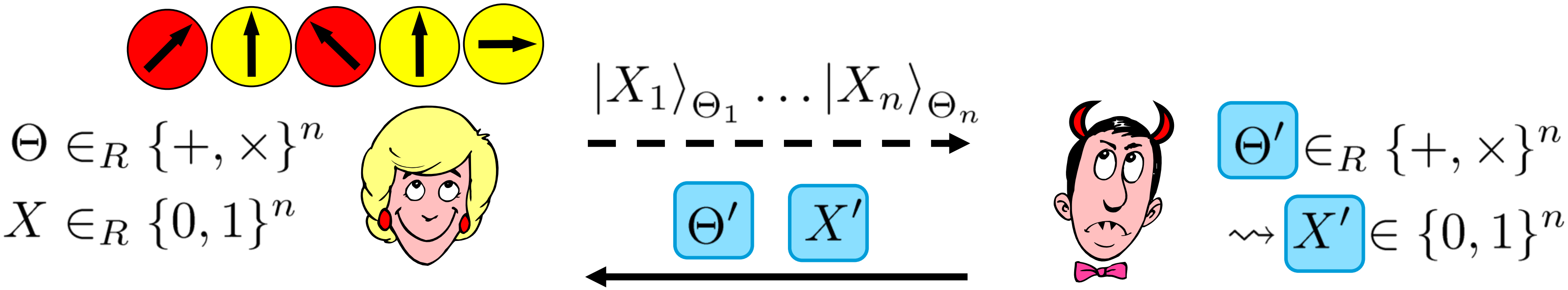
based on Θ, K

- more realistic limitation on quantum storage capabilities
- first step: individual-storage attacks
- recent result: general attacks
- related to classical capacities of quantum channels

Combining Security Assumptions

[Damgaard Fehr Lunemann Salvail Schaffner 09]

- two-party cryptography in the plain quantum model is impossible [Lo 96]
- security can be based on
  - difficulty of storing quantum information
  - computational assumptions
- can be combined!
- idea from [BBCS92]: commit to bases and outcomes



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

$X \in_R \{0,1\}^n$

$|X_1\rangle_{\Theta_1} \cdots |X_n\rangle_{\Theta_n}$

$\boxed{\Theta'}$ $\boxed{X'}$

$\boxed{\Theta'} \in_R \{+,\times\}^n$

$\rightsquigarrow \boxed{X'} \in \{0,1\}^n$

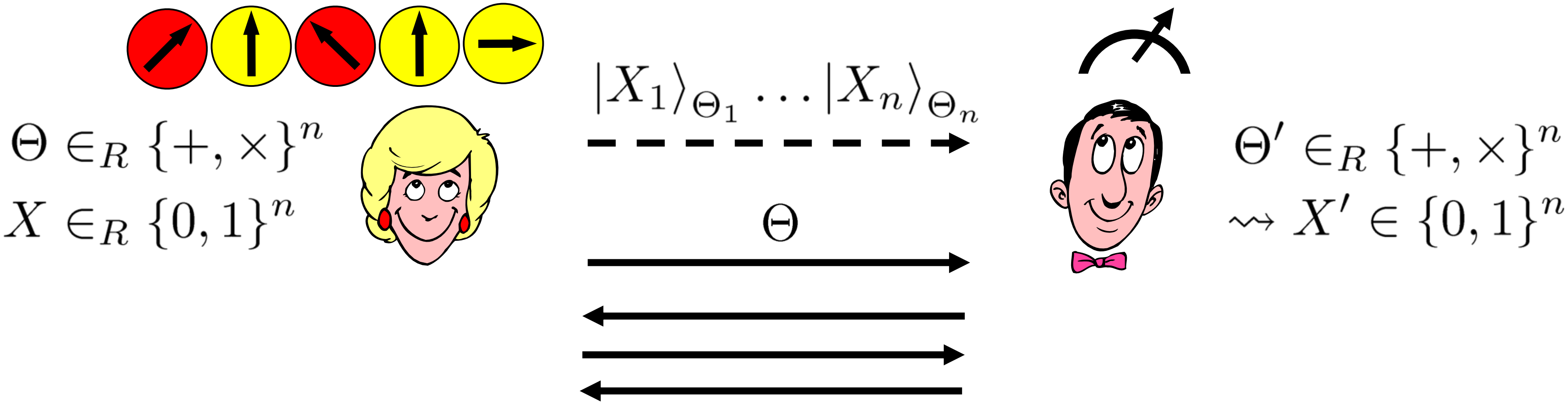
- forces adversary to have almost no quantum memory

Outline

- ✓ Bounded Quantum Storage
- ✓ The Protocol
- ✓ Noisy Quantum Storage
- Secure Identification
- Composability
- Practical Problems
- Future

Secure Identification

[Damgaard Fehr Salvail Schaffner 07]



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

$X \in_R \{0,1\}^n$

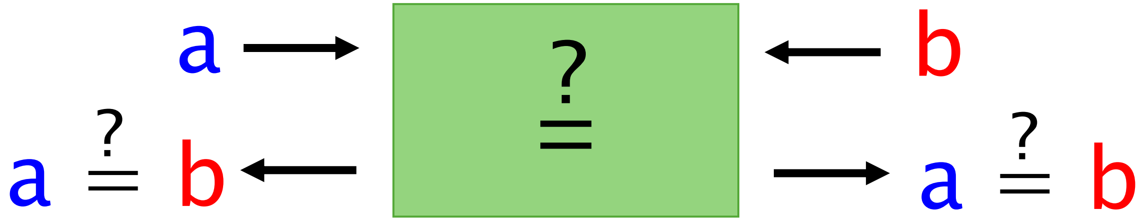
$|X_1\rangle_{\Theta_1} \dots |X_n\rangle_{\Theta_n}$

Θ

$\Theta' \in_R \{+,\times\}^n$

$\rightsquigarrow X' \in \{0,1\}^n$

- goal:



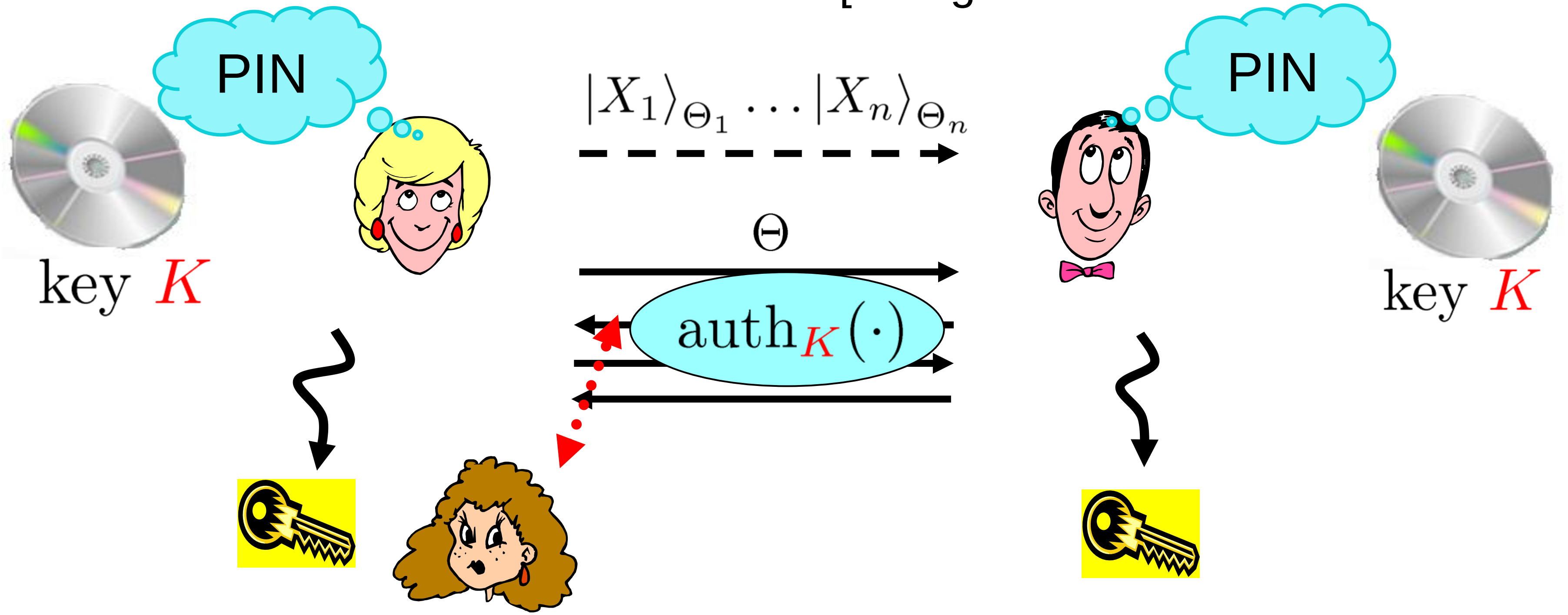
$a \rightarrow \boxed{\overset{?}{=}} \leftarrow b$

$a \overset{?}{=} b \leftarrow \qquad \rightarrow a \overset{?}{=} b$

- 3 classical messages, much more efficient than relying on reduction to 1-2 OT
- secure against adversaries with quant memory < const n
- can be made secure against man-in-the middle attacks

Man-In-The-Middle Security and QKD

[Damgaard Fehr Salvail Schaffner 07]

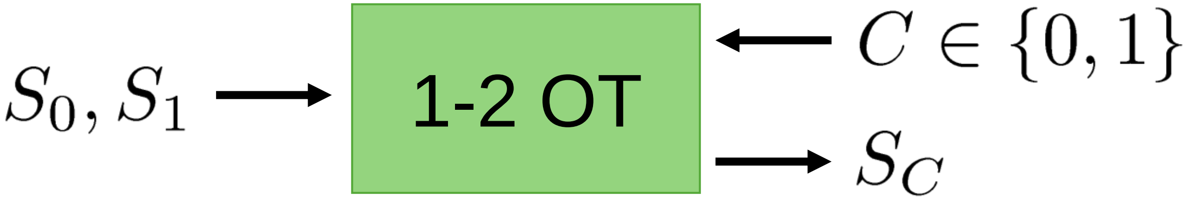


- non-trivial extension is also secure against man-in-the middle attacks (while preserving original security)
- QKD: key K can be reused, even if scheme is disrupted, i.e. q-memory bounded Eve cannot make honest players run out of auth key.

Composable Security Definitions

[Wehner Wullschleger 08, Fehr Schaffner 09, Unruh 09]

- goal:



$S_0, S_1 \rightarrow$ 1-2 OT $\leftarrow C \in \{0,1\}$

$\rightarrow S_C$

- want to use primitive in an classical outer protocol
  - or compose it with other quantum protocols
- subtle in the quantum domain, quantum information cannot be copied and carried through to the end
- need the right security definitions!
- general frameworks: [Ben-Or Mayers 02], [Unruh 04]
- simulation-based definitions allow for sequential composition

Practical Problems

[Wehner Curty Lo Schaffner 09]

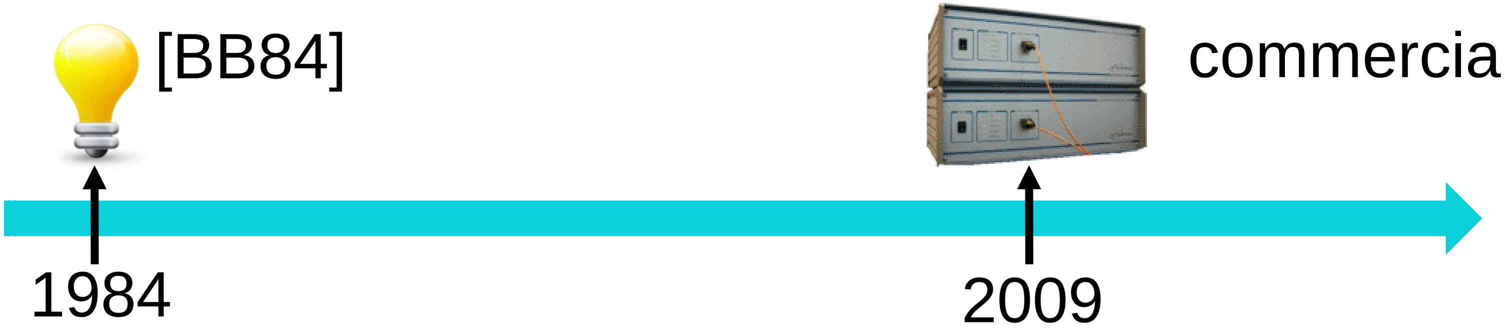
- imperfections similar to QKD:
  - approximation to single-photon sources (weak coherent pulses or parametric-down-conversion)
  - erasures in the channel
  - bit errors in the channel
  - dark counts
  - ...

– no trusted peer

+ shorter distances

- solutions: adapted security analyses, error-correction
- computational efficiency of classical post-processing
- physical size of devices

Similarities to QKD



- QKD know-how is now available
- similar technology can be used for limited-quantum-storage applications!
- but with different parameter ranges (e.g. shorter distances)
- big potential:

Practical Quantum Crypto

Limited-Q-Storage Crypto:

- identification
- comparison

other difficulties in doing quantum comp

QKD

Near and Far Future

Technology:

- harvest QKD knowledge
- conduct experiments
- check assumptions
- miniaturize devices

Theory:

- find more direct protocols
- continuous variables

- more realistic models for the difficulty of storing quantum information
- exploit other difficulties in doing quantum computation

win-win situation:

either large-scale quantum computing is possible or the reason why not can be exploited for cryptography