

# Provable post-quantum security

Renato Renner  
Institute for Theoretical Physics  
ETH Zurich, Switzerland

# Pre- and post-quantum physics

- **Pre-quantum physics**

State of physical system described by a point  $(x,p)$  in phase space  $\Gamma$ .

⇒ Parameters directly observable.

- **Quantum physics**

State of physical system described by a vector  $v$  in a Hilbert space  $H$ .

⇒ Parameters cannot be observed directly.

# Pre- and post-quantum info

- **Pre-quantum information**  
Information represented by states that are accurately described by *pre-quantum* physics.
- **Quantum information**  
Information represented by states that are accurately described by *quantum* physics.

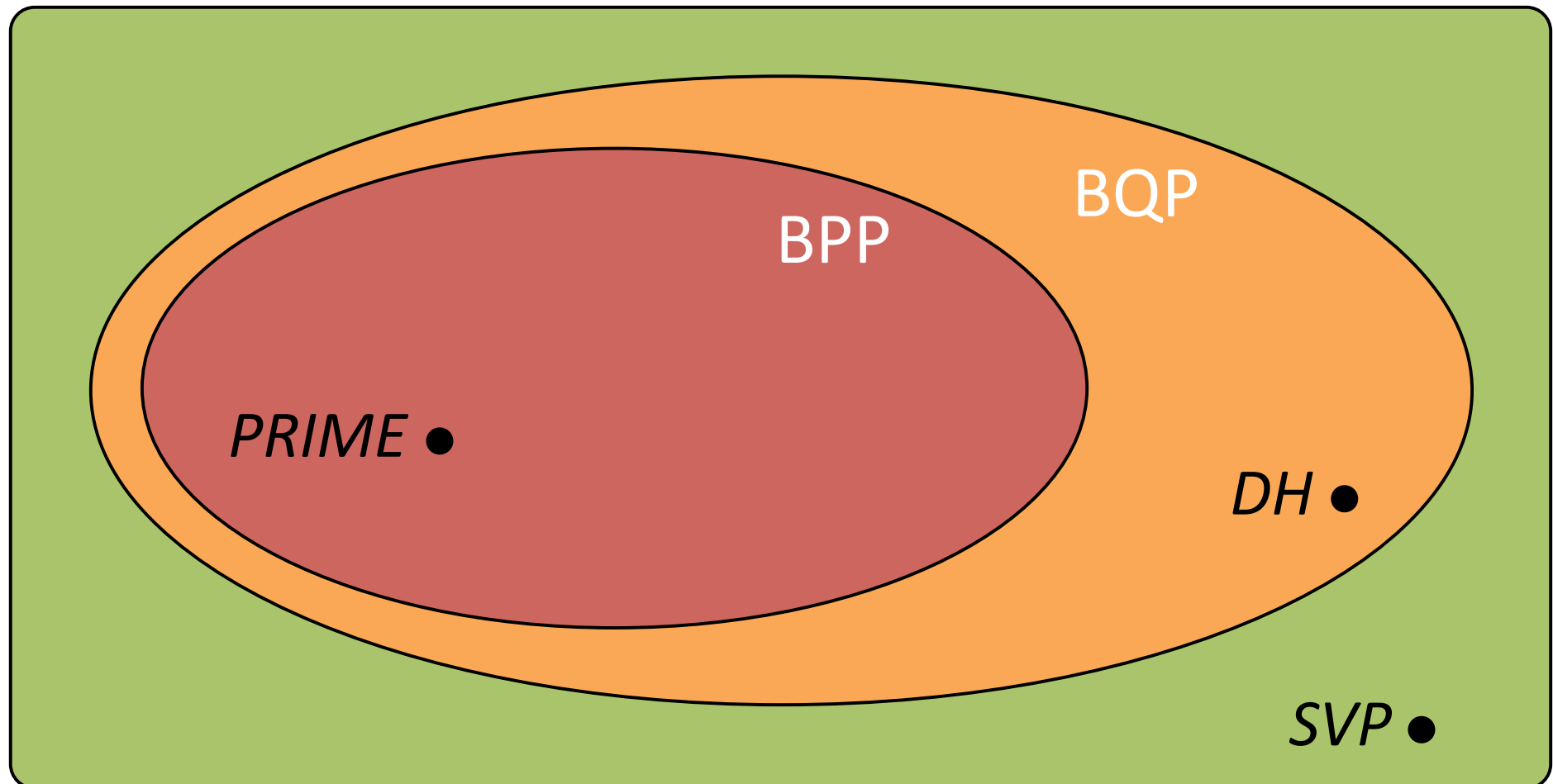
Note that *quantum* information is strictly more general than its “pre-quantum” counterpart.

Why should we care about quantum physics  
when we analyze pre-quantum protocols?



Since we want our analysis to remain valid in  
the presence of post-quantum adversaries.

The class of (conjectured) hard problems is smaller in the post-quantum world



Is it sufficient to consider  
modified complexity classes?

No.

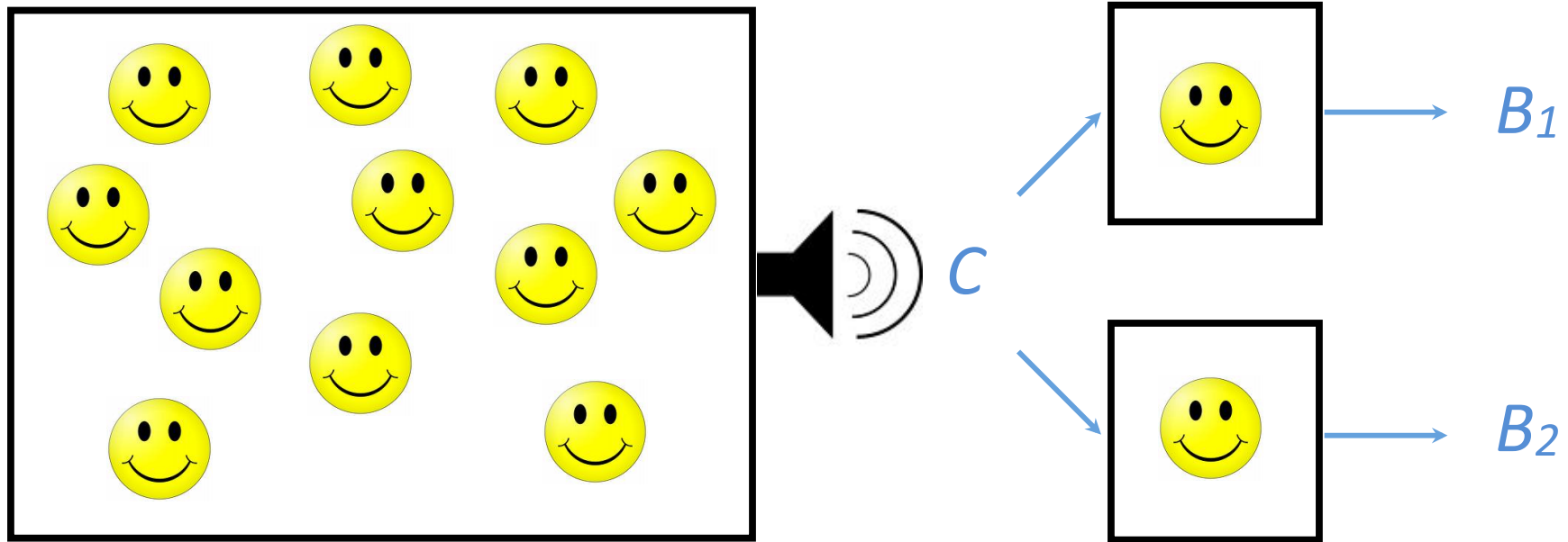
# Various information-theoretic concepts need to be adapted

- Randomness
- Entropy
- Extractors
- Privacy Amplification
- Samplers
- ...

# Observation

- The “classical” theory of information treats information on an abstract level (independent of its physical representation).
- Nevertheless, the classical theory is not general enough to model information stored in quantum systems.

# Toy example



- ①  $N$  collaborating players sitting in a room
- ② 2 of them selected and put in separated rooms
- ③  $N-2$  remaining players announce a bit  $C$  of their choice
- ④ separated players output bits  $B_1$  and  $B_2$

Game is won if  $B_1 \neq B_2$ .

# Analysis

- Each player may choose one of the following four strategies (in case he is selected).

Strategies	$B = 0$	$B = 1$	$B = C$	$B = 1 - C$
------------	---------	---------	---------	-------------

(The strategy defines how the output  $B$  is derived from the input  $C$ .)

- The game cannot be won if the two selected players follow identical strategies.
- This happens with probability  $\approx 1/4$  (for  $N$  large).
- Hence, the game is lost with probability (at least)  $1/4$ .

# This analysis can be made rigorous

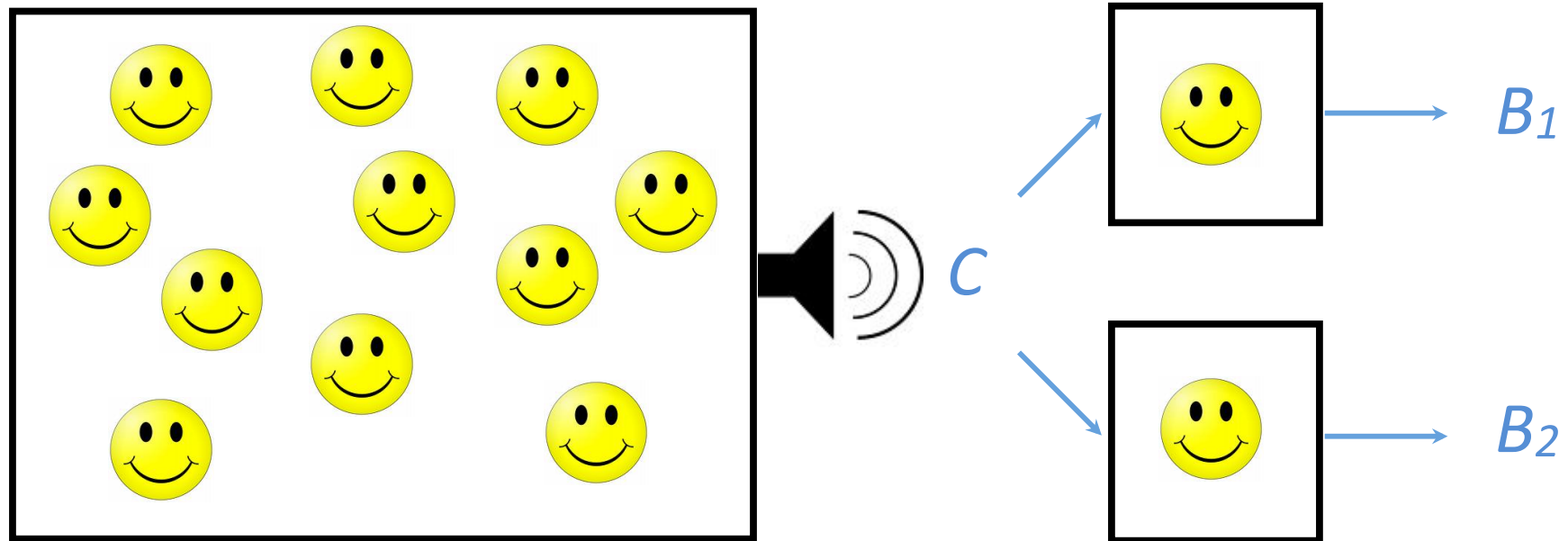
## Theorem

- for any possible strategy, the game is lost with probability at least  $\approx 1/4$ .

## Implicit Assumption

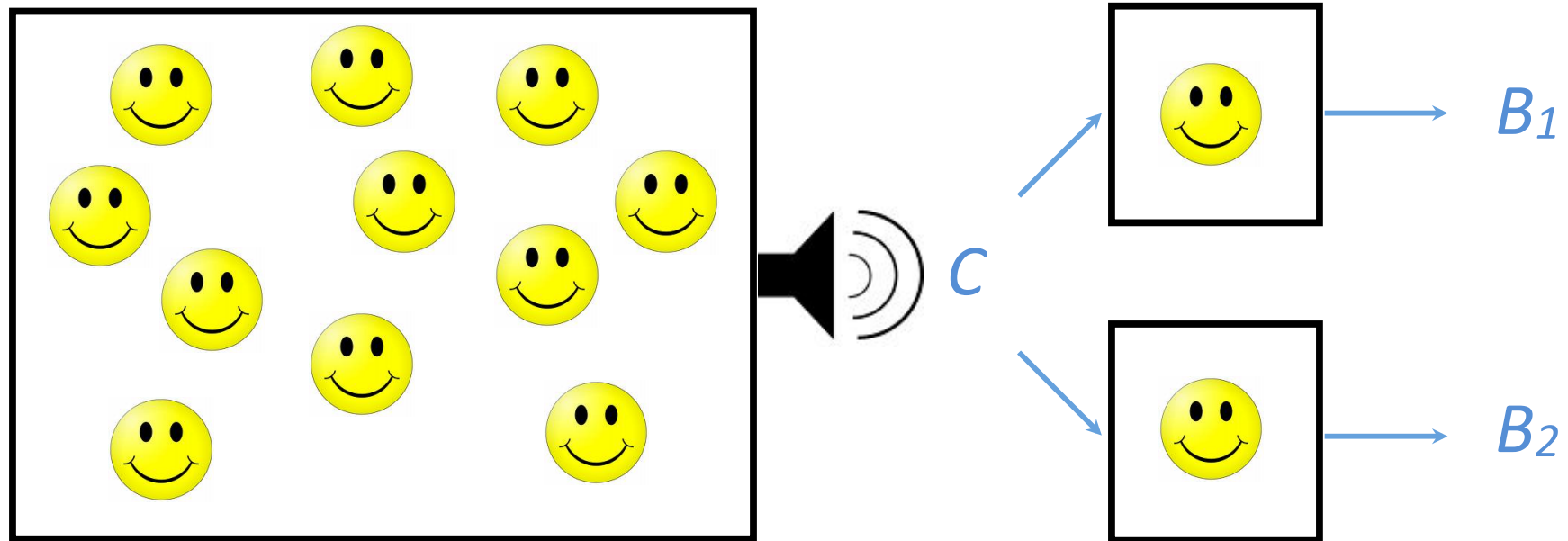
- Players do not hold any quantum information.

# Toy example



- The game can be won with probability **1** if the players use an **internal** quantum device.
- **Note:** all communication during the game is still **purely classical**.

# Toy example



- ①  $N$  players start with an  $N$ -partite GHZ state
- ② keep state stored
- ③ all remaining players measure in diagonal basis and choose  $C$  as the **xor** of their measurement results
- ④ separated players determine  $B_1$  and  $B_2$  by measuring in either the diagonal or the circular basis, depending on  $C$ .

# What do we learn from this example?

- Quantum mechanics allows us to win games that cannot be won in a classical world (examples known as “pseudo telepathy games”).
- Note that there is no physical principle that allows us to rule out quantum attacks.

Even proofs that are entirely based on probability theory may be invalid in a post-quantum world.

# Underlying reason for the failure of the “classical” proof

The concept of probabilities is not general enough to model knowledge.

## This is problematic in cryptography

For example, we are used to say that a key  $S$  is uniform if its distribution  $P_S$ , from an adversary's point of view, is (close to) uniform.

# General scenario



Knowledge of observer characterized by distribution  $P_X$ .

# General scenario



We may model the observer's knowledge explicitly as a random variable  $E$  specified by a joint distribution  $P_{XE}$ .

If the observer's knowledge has a specific (classical) value  $E=e$ , his knowledge about  $X$  is given by  $P_{X|E=e}$ .

# What about a quantum observer?

Random value  
 $X$

Quantum Observer  
 $E$

If  $E$  is encoded in the state of a quantum system, we need to consider the *cq*-state  $\rho_{XE}$ .

We say that  $X$  is *uniform w.r.t.*  $E$  if  $\rho_{XE} \sim \text{id}_X \otimes \rho_E$ .

# Extractors

**Definition** (standard version)

A  $(k, \varepsilon)$ -*extractor* is a function

$$\text{ext}: (X, S) \rightarrow Z$$

whose output  $Z$  is  $\varepsilon$ -close to uniform whenever  $S$  is uniform and

$$H_{\min}(X) \geq k .$$

$$H_{\min}(X) := -\log_2 p_{\text{guess}}(X),$$

where  $p_{\text{guess}}(X)$  is the prob. of correctly guessing  $X$ .

# A slightly extended version

**Definition** (version with explicit knowledge)

A  $(k, \varepsilon)$ -*extractor* is a function

$$\text{ext}: (X, S) \rightarrow Z$$

whose output  $Z$  is  $\varepsilon$ -close to uniform w.r.t.  $E$   
whenever  $S$  is uniform and

$$H_{\min}(X|E) \geq k .$$

$$H_{\min}(X|E) := -\log_2 p_{\text{guess}}(X|E),$$

where  $p_{\text{guess}}(X|E)$  is the prob. of guessing  $X$  given  $E$ .

# A slightly extended version

**Definition** (including quantum knowledge)

A  $(k, \varepsilon)$ -*extractor* is a function

$$\text{ext}: (X, S) \rightarrow Z$$

whose output  $Z$  is  $\varepsilon$ -close to uniform w.r.t.  $E$   
whenever  $S$  is uniform and

$$H_{\min}(X|E) \geq k .$$

**Note:** This is almost identical to the classical version, but  $H_{\min}(X|E)$  is now a quantum entropy.

# Entropy in the presence of quantum knowledge

## **Definition** (operational version)

The *min-entropy*  $H_{\min}(X|E)$  is defined by

$$H_{\min}(X|E) := -\log_2 p_{\text{guess}}(X|E),$$

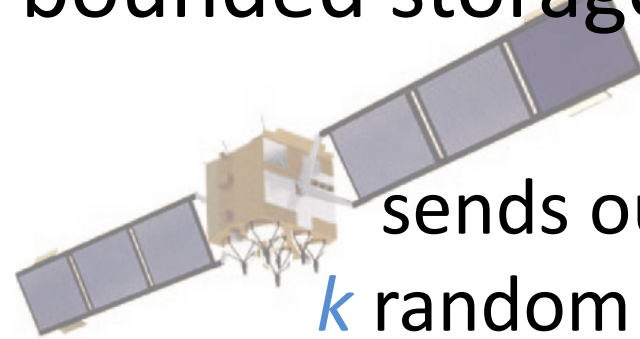
where  $p_{\text{guess}}(X|E)$  is the probability of correctly guessing  $X$  given  $E$ .

# Remarks

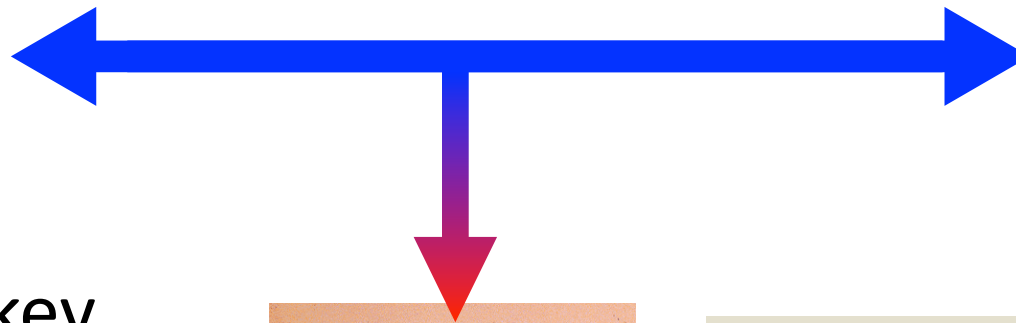
- Classical extractors do not necessarily satisfy the quantum definition
- An explicit example of such a separation has been constructed [Gavinsky, Kempe, Kerenidis, Raz, de Wolf, 2007]
- However, many known constructions of extractors still satisfy the post-quantum definition
  - Two-universal hashing [RR, 2005]
  - Sample-and-hash approach [König, RR, 2007]
  - $\delta$ -biased masking [Fehr, Schaffner, 2008]
  - Trevisan's extractor [De, Portmann, Vidick, RR, 2009]
  - Almost two-universal hashing [Tomamichel, Smith, RR, 2010]

# Example

## Maurer's bounded storage model



$S_{\text{initial}}$   
short initial key

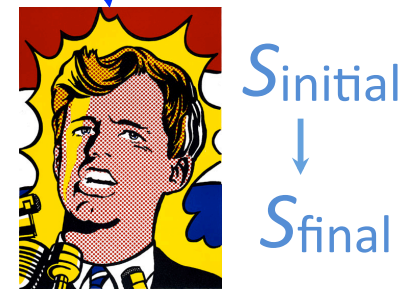
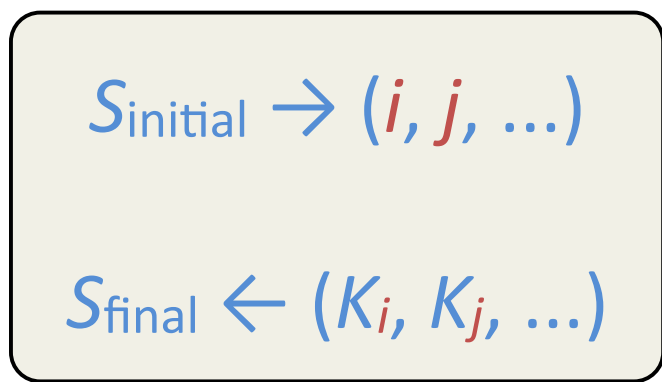
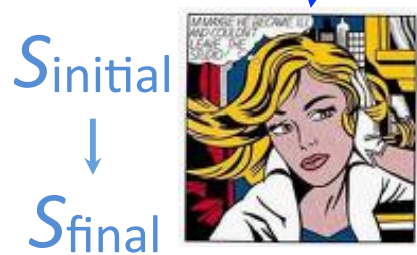
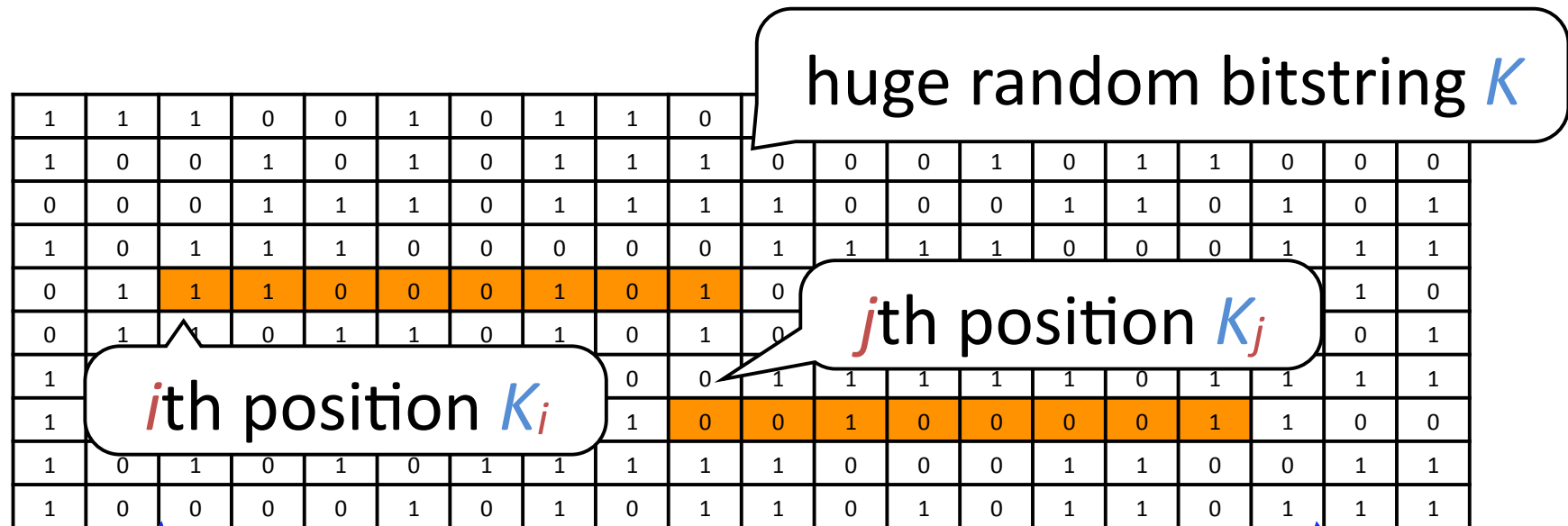


$S_{\text{initial}}$



**Assumption:**  
adversary  
can store at most  
 $m < k$  bits

# Key agreement in the bounded storage model



# Security analysis of the bounded storage model

- If Eve has **only classical memory**, information-theoretically secure key agreement is possible.
- In general, the security is compromised if Eve in addition has (even a small) quantum device.  
[Gavinsky, Kempe, Kerenidis, Raz, de Wolf, 2007]
- The protocol can be adapted (by using “quantum-proof” extractors) to make it secure against adversaries with quantum memory.  
[Ben-Aroya, Regev, de Wolf, 2007],  
[König, RR, 2007]

# Implication

When proving the security of a cryptographic scheme (in the post-quantum world), it is generally unavoidable to take into account quantum physics.

## Remarks

- This warning also applies to **purely classical** cryptographic schemes.
- It is relevant for both **information-theoretically** and **computationally** secure cryptosystems.

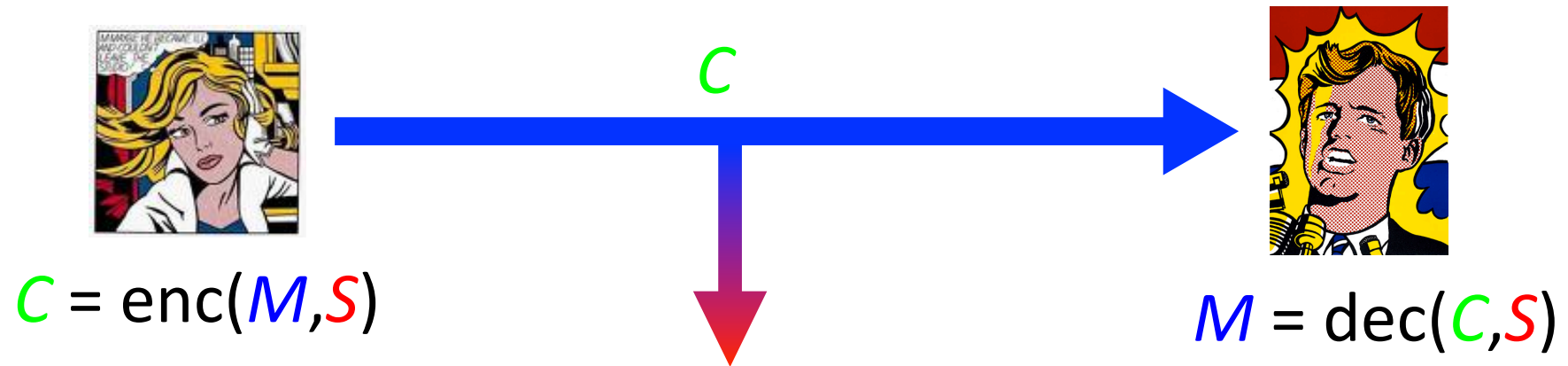
# Information-theoretic proofs in cryptography

- one-time-pad encryption
- key agreement based on physical assumptions (bounded storage, noise)
- some multi-party computation protocols
- impossibility results ...

# The positive side of the post-quantum world

The incompleteness of classical information-theoretic arguments also affects “impossibility proofs”.

# Shannon's "impossibility result"



## Theorem

For information-theoretically secure encryption, the key  $S$  needs to be at least as long as the message  $M$ .

In particular, *One-Time-Pad encryption* is optimal.

# Proof of Shannon's theorem

Let  $M$  be a uniformly distributed  $n$ -bit message,  $S$  a secret key, and  $C$  the ciphertext.

## Requirements

- $H(M | SC) = 0$ , since  $M$  determined by  $S, C$ .
- $H(M | C) = H(M) = n$ , since  $M$  indep. of  $C$ .

## Hence

- $H(S) \geq I(M : S | C) = H(M | C) - H(M | SC) = n$ .

# How general is Shannon's result?

## Observations

- Quantum key distribution (QKD) can be used to transmit arbitrarily long messages starting with only a short initial key.
- Hence, Shannon's impossibility theorem is invalid in the post-quantum world.

## Question

- What is wrong with the proof?

# Proof of Shannon's theorem

Let  $M$  be a uniformly distributed  $n$ -bit message,  $S$  a secret key, and  $C$  the ciphertext.

## Requirements

$$H(M | SC_{Bob})$$

- $H(M | SC) = 0$ , since  $M$  determines  $C$ .
- $H(M | C) = H(M) = n$ , since  $M$  is uniformly distributed.

No cloning:

$C_{Bob} \neq C_{Eve}$  in general

## Hence

$$H(M | C_{Eve})$$

- $H(S) \geq I(M : S | C) = H(M | C) - H(M | SC) = n$ .

# Conclusion

- In a post-quantum world, we need to reconsider our notion of “knowledge” and adapt information-theoretic concepts accordingly.
- This is an enormous task ...

Thanks for your attention