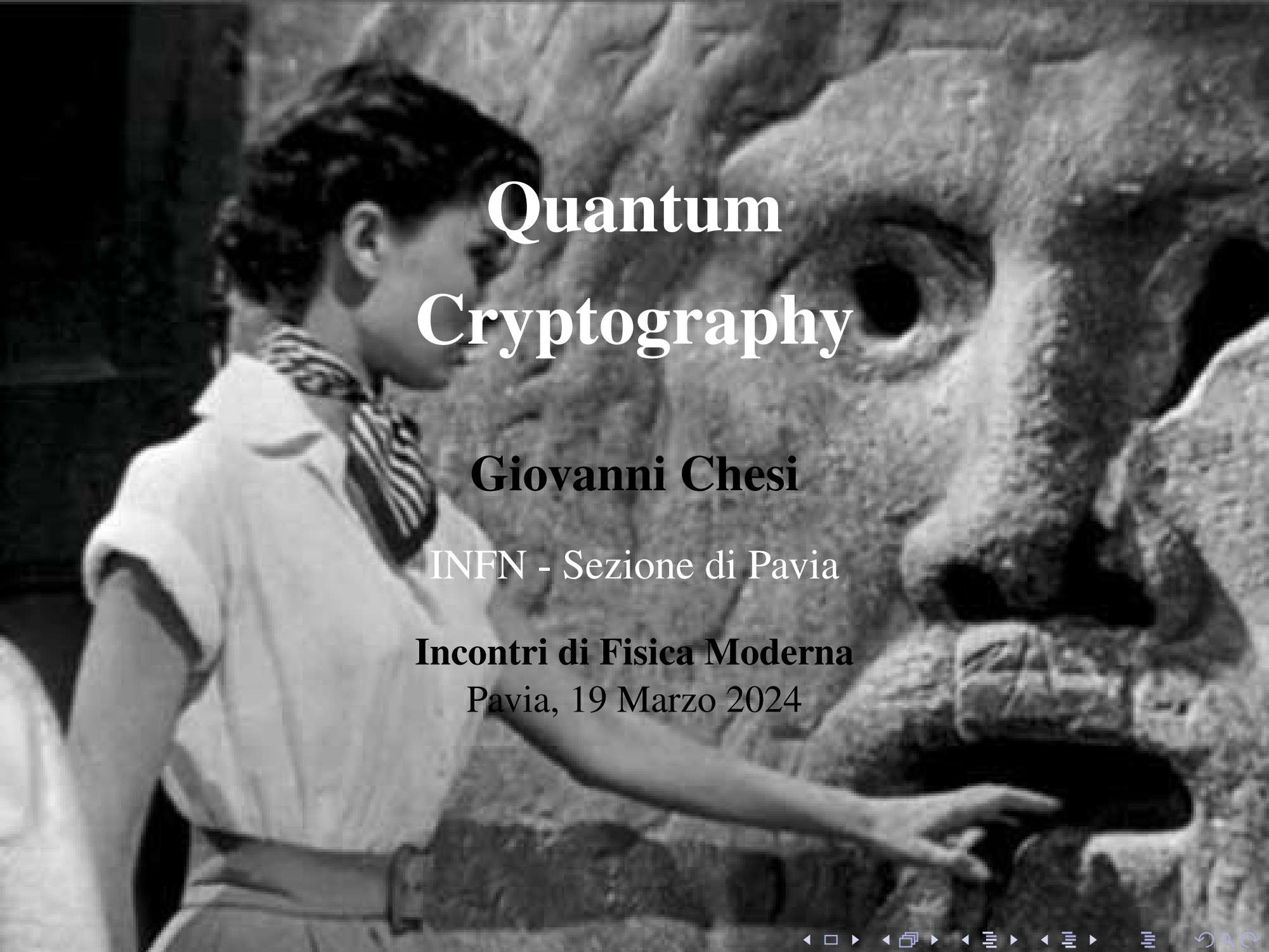


Quantum Cryptography

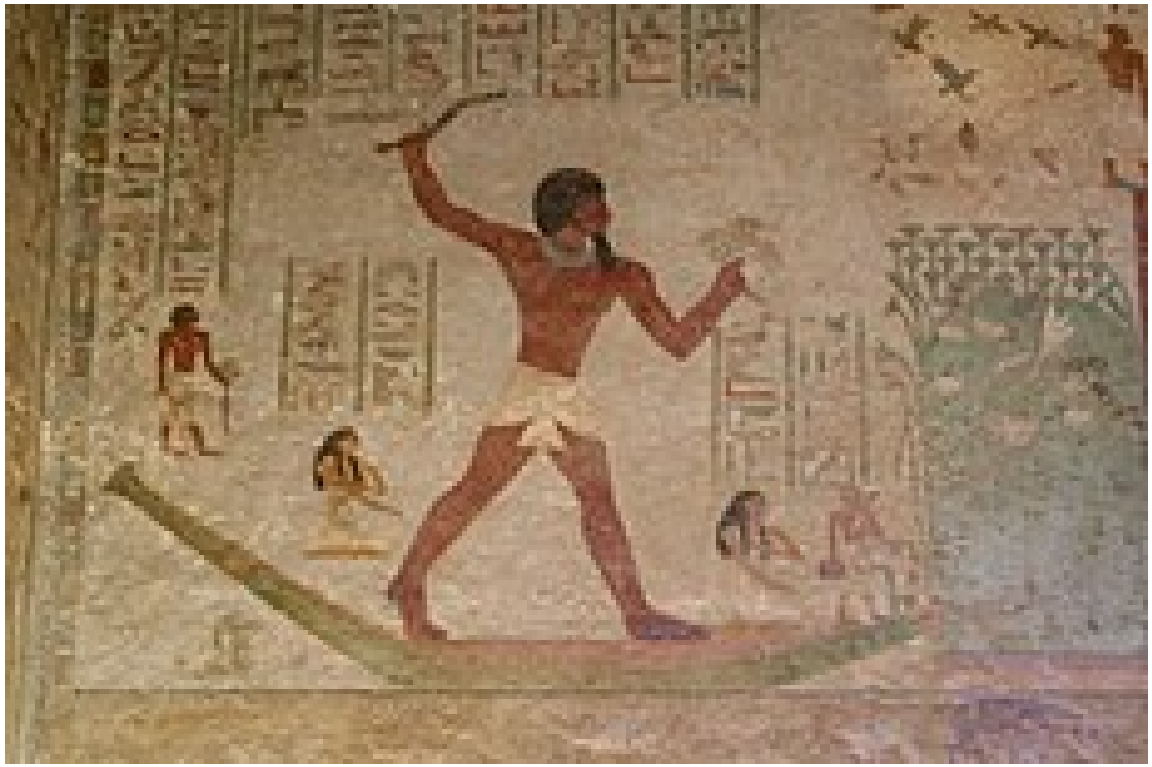
Giovanni Chesi

INFN - Sezione di Pavia

Incontri di Fisica Moderna
Pavia, 19 Marzo 2024

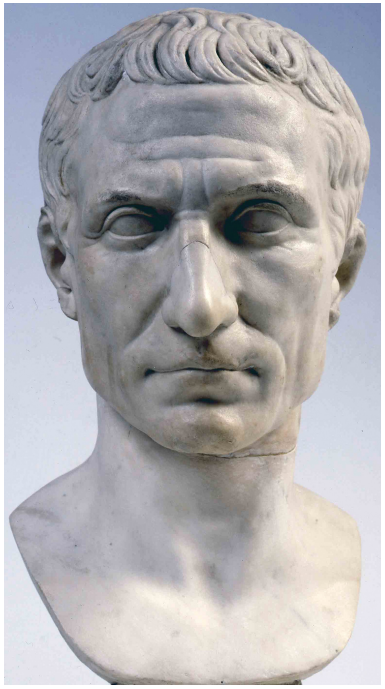
Brevissima storia della crittografia

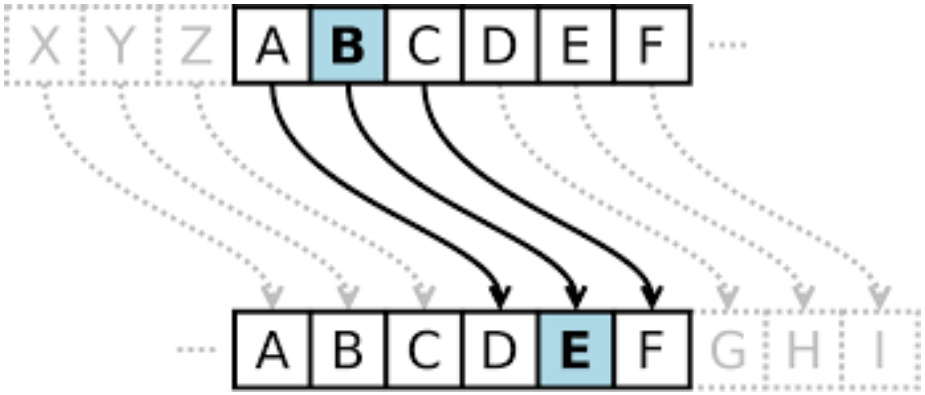
Khnumhotep II



Breve storia della crittografia

Il cifrario di Cesare

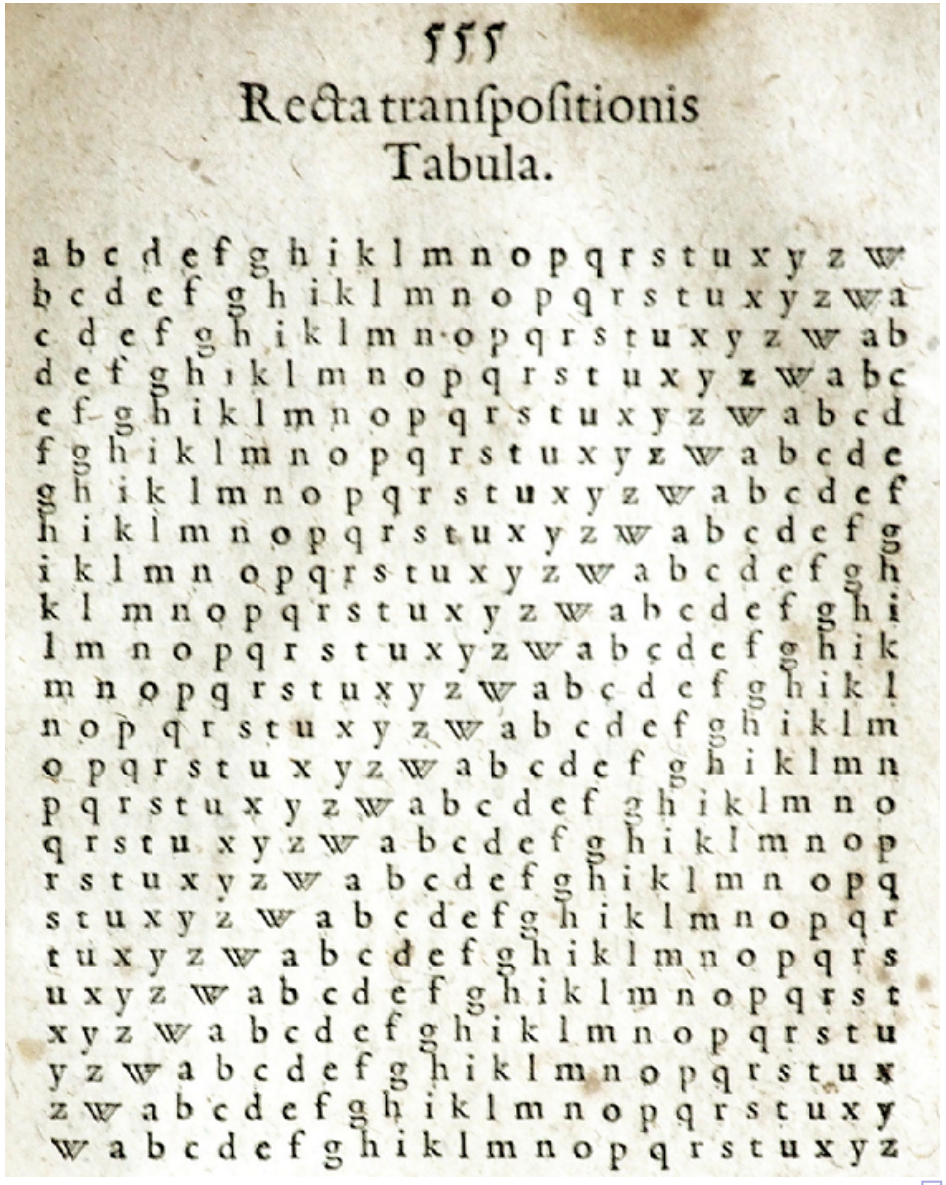




Istituto Nazionale di Fisica Nucleare

Non così breve storia della crittografia

Il cifrario di Vigenere



fff

Recta tranſpoſitionis
Tabula.

a b c d e f g h i k l m n o p q r s t u x y z w
b c d e f g h i k l m n o p q r s t u x y z w a
c d e f g h i k l m n o p q r s t u x y z w a b
d e f g h i k l m n o p q r s t u x y z w a b c
e f g h i k l m n o p q r s t u x y z w a b c d
f g h i k l m n o p q r s t u x y z w a b c d e
g h i k l m n o p q r s t u x y z w a b c d e f
h i k l m n o p q r s t u x y z w a b c d e f g
i k l m n o p q r s t u x y z w a b c d e f g h
k l m n o p q r s t u x y z w a b c d e f g h i
l m n o p q r s t u x y z w a b c d e f g h i k
m n o p q r s t u x y z w a b c d e f g h i k l
n o p q r s t u x y z w a b c d e f g h i k l m
o p q r s t u x y z w a b c d e f g h i k l m n
p q r s t u x y z w a b c d e f g h i k l m n o
q r s t u x y z w a b c d e f g h i k l m n o p
r s t u x y z w a b c d e f g h i k l m n o p q
s t u x y z w a b c d e f g h i k l m n o p q r
t u x y z w a b c d e f g h i k l m n o p q r s
u x y z w a b c d e f g h i k l m n o p q r s t
x y z w a b c d e f g h i k l m n o p q r s t u
y z w a b c d e f g h i k l m n o p q r s t u x
z w a b c d e f g h i k l m n o p q r s t u x y
w a b c d e f g h i k l m n o p q r s t u x y z

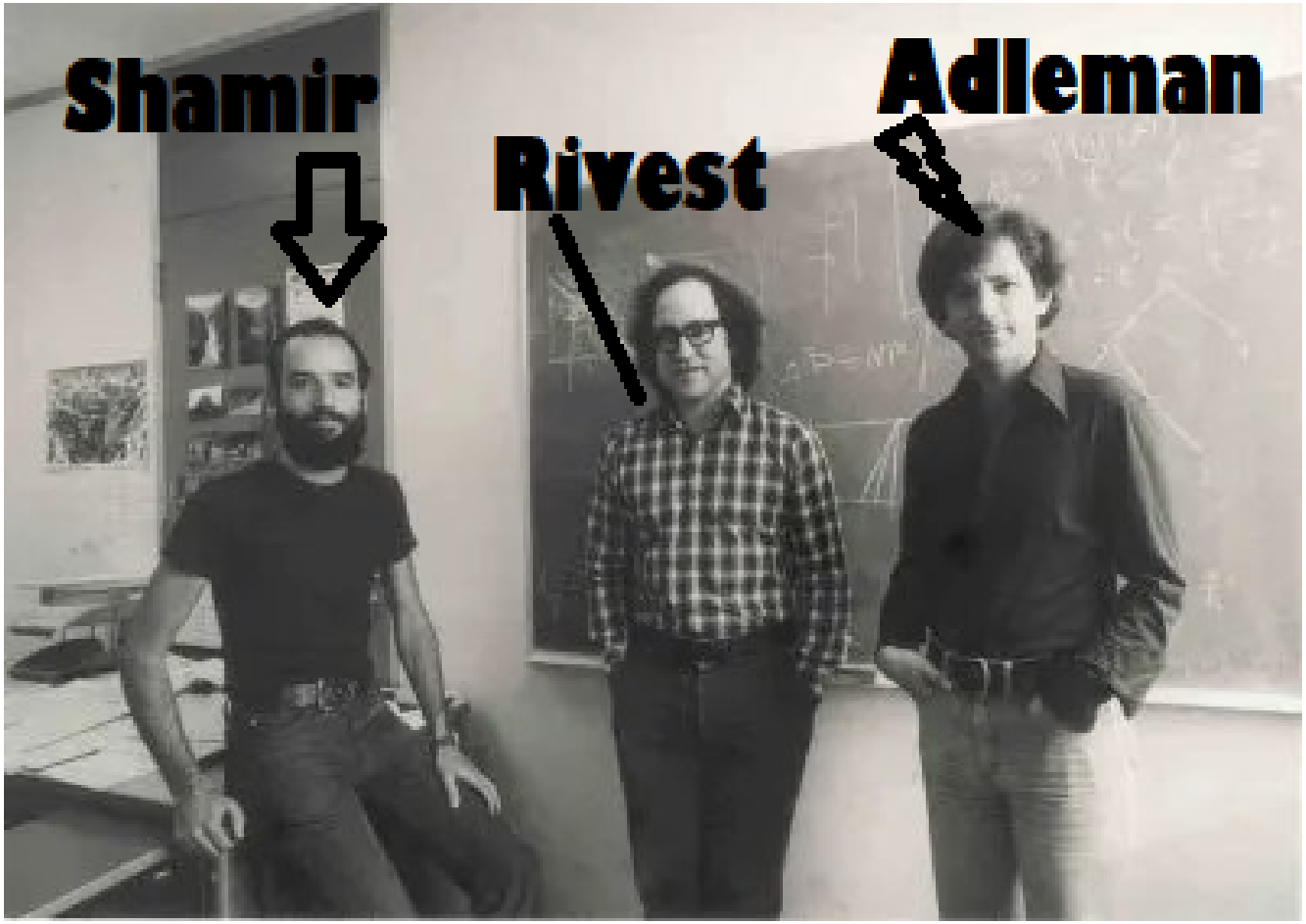
INFN
Istituto Nazionale di Fisica Nucleare

La lunga storia della crittografia

Il cifrario di Vernam, ovvero il One Time Pad

Basta con la storia della crittografia

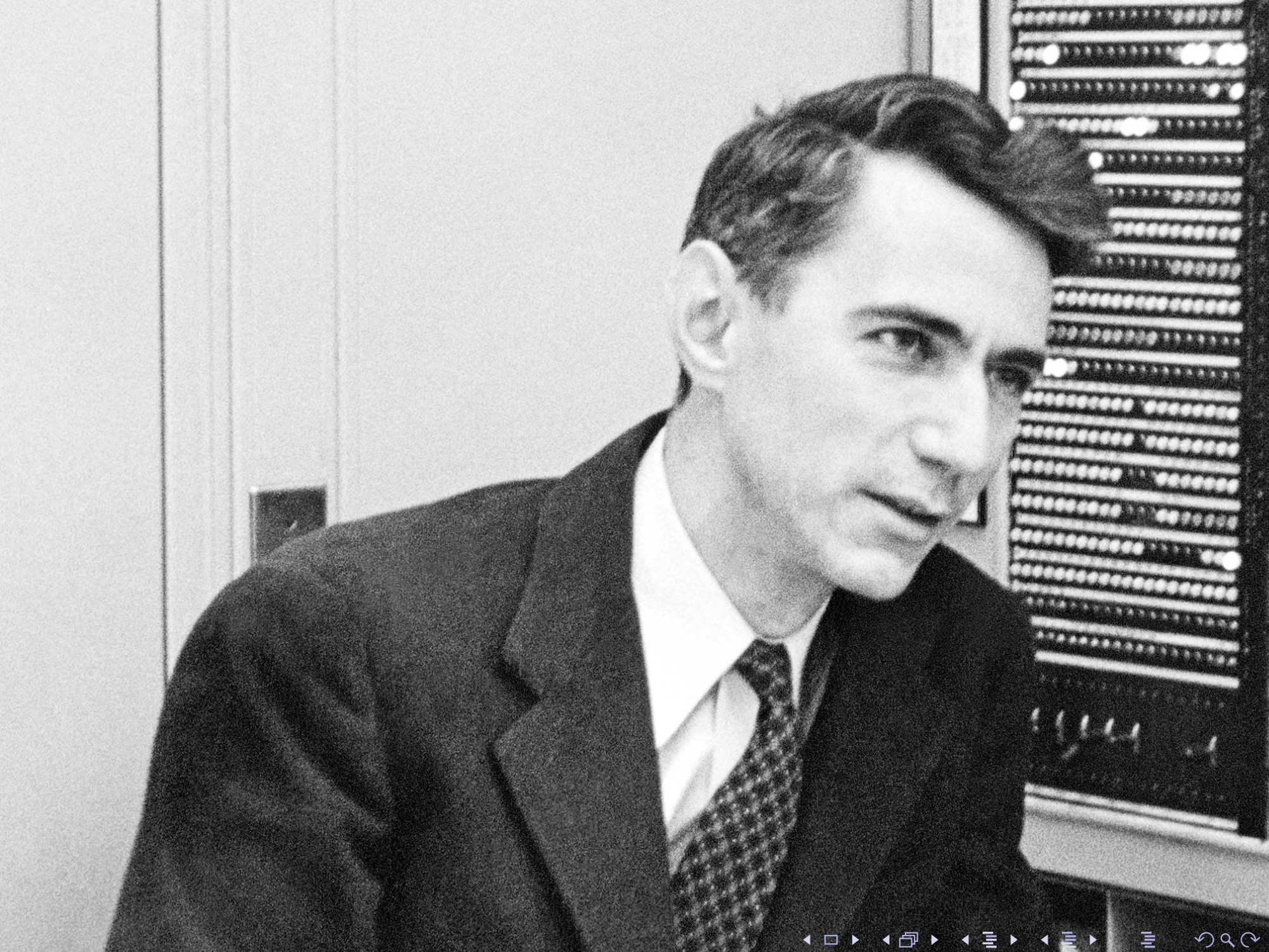
Crittografia a chiave pubblica e asimmetrica: il protocollo RSA



Crittografia

A. Ekert, Phys. Rev. Lett. **67**, 661 (1991)

Today, one can briefly define cryptography as a mathematical system of transforming information so that it is unintelligible and therefore useless to those who are not meant to have access to it. However, as the computational process associated with transforming the information is always performed by physical means, one cannot separate the mathematical structure from the underlying laws of physics that govern the process of computation.



Teoria dell'informazione

Teoria dell'informazione

C. E. Shannon, *A Mathematical Theory of Communication*, Bell Syst. Tech. J. *27* (1948)

Teoria dell'informazione

C. E. Shannon, *A Mathematical Theory of Communication*, Bell Syst. Tech. J. *27* (1948)

- Come posso ingegnerizzare codifica, trasmissione e decodifica dell'informazione

Teoria dell'informazione

C. E. Shannon, *A Mathematical Theory of Communication*, Bell Syst. Tech. J. *27* (1948)

- Come posso ingegnerizzare codifica, trasmissione e decodifica dell'informazione
- Come posso misurare l'informazione contenuta in un messaggio

Teoria dell'informazione

C. E. Shannon, *A Mathematical Theory of Communication*, Bell Syst. Tech. J. *27* (1948)

- Come posso ingegnerizzare codifica, trasmissione e decodifica dell'informazione
- Come posso misurare l'informazione contenuta in un messaggio
- Come si può comprimere un messaggio senza perdere informazione

Teoria dell'informazione

C. E. Shannon, *A Mathematical Theory of Communication*, Bell Syst. Tech. J. *27* (1948)

- Come posso ingegnerizzare codifica, trasmissione e decodifica dell'informazione
- Come posso misurare l'informazione contenuta in un messaggio
- Come si può comprimere un messaggio senza perdere informazione
- Che cosa succede se c'è rumore nel canale

Teoria dell'informazione

C. E. Shannon, *A Mathematical Theory of Communication*, Bell Syst. Tech. J. *27* (1948)

- Come posso ingegnerizzare codifica, trasmissione e decodifica dell'informazione
- Come posso misurare l'informazione contenuta in un messaggio
- Come si può comprimere un messaggio senza perdere informazione
- Che cosa succede se c'è rumore nel canale

Entropia di Shannon

$X = \{X_x\}_{x=0}^{N} = \{X_0, X_1, \ldots, X_N\}$

$$\mathrm{H}(X) \equiv -\sum_{x=0}^{N} \mathrm{p}_x \log_2 \mathrm{p}_x$$

$$= \sum_{x=0}^{N} \mathrm{p}_x (-\log_2 \mathrm{p}_x)$$

INFN
Istituto Nazionale di Fisica Nucleare

Teoria fisica dell'informazione - Fotoni viaggiatori

Istituto Nazionale di Fisica Nucleare

Teoria fisica dell'informazione - Fotoni viaggiatori

Fotoni come *flying qubits*

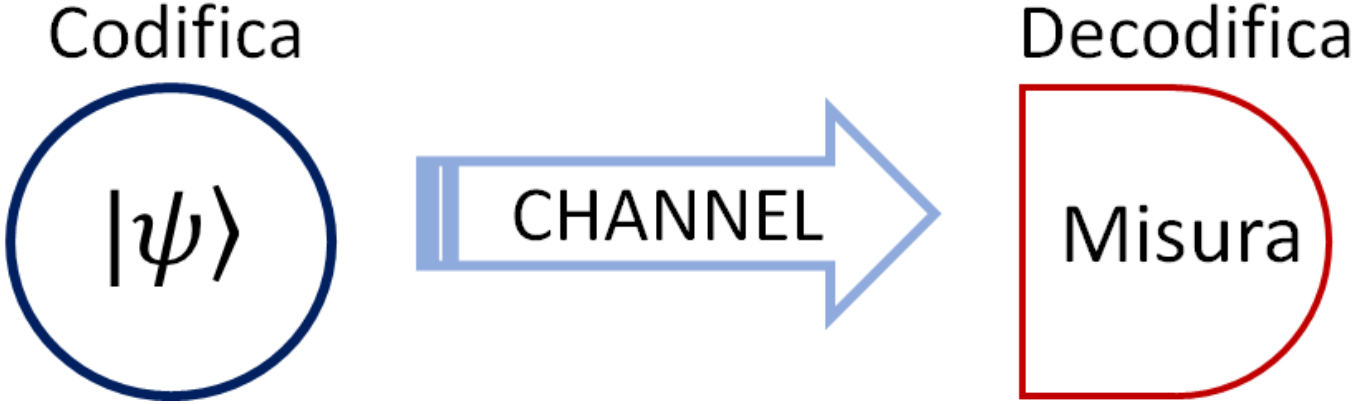
I fotoni si prestano alla trasmissione di informazione perché interagiscono molto poco fra loro e con l'ambiente esterno.

Teoria fisica dell'informazione - Fotoni viaggiatori

Fotoni come *flying qubits*

I fotoni si prestano alla trasmissione di informazione perché interagiscono molto poco fra loro e con l'ambiente esterno.

Teoria quantistica dell'informazione



INFN
Istituto Nazionale di Fisica Nucleare

Quantum Key Distribution (QKD)

Crittografia quantistica

La crittografia quantistica è un approccio alla crittografia che ridefinisce la nozione di *sicurezza* attraverso le leggi della meccanica quantistica.

Quantum Key Distribution (QKD)

Crittografia quantistica

La crittografia quantistica è un approccio alla crittografia che ridefinisce la nozione di *sicurezza* attraverso le leggi della meccanica quantistica.

Sicurezza classica

Un sistema crittografico classico ad oggi è sicuro se la decriptazione della chiave richiede un potenza computazionale non accessibile (RSA) e/o se la chiave è usata solo una volta (one-time pad). All'atto di generazione della chiave, l'informazione può sempre essere copiata.

Quantum Key Distribution (QKD)

Sicurezza quantistica

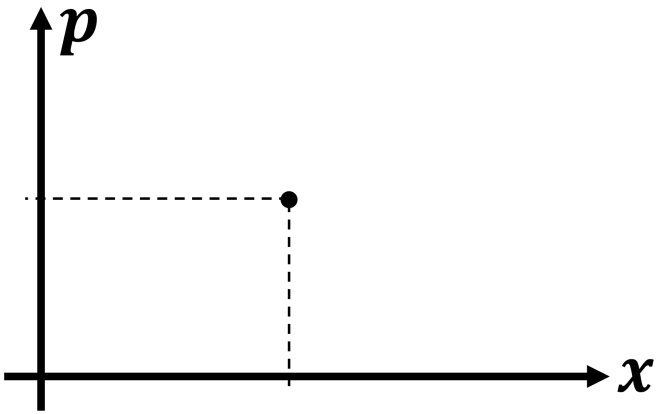
Un sistema crittografico quantistico è sicuro perché l'informazione scambiata all'atto di generazione della chiave non può essere letta o copiata senza che questo sia scoperto da mittente e ricevente.

QKD

Un protocollo di Quantum Key Distribution permette a due parti di generare e condividere una chiave segreta attraverso un canale quantistico insicuro, operazioni locali e comunicazione classica (LOCC).

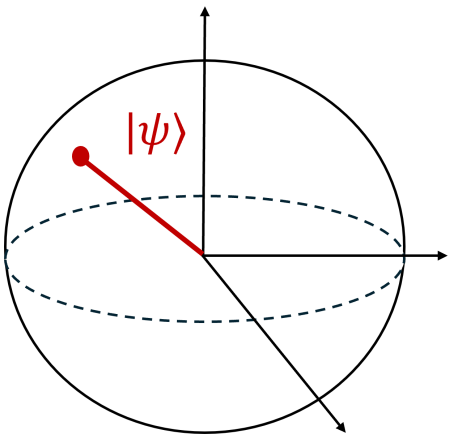
Stato di un sistema fisico

Meccanica Newtoniana



$$\mathbf{x} = x, y, z$$
$$\mathbf{p} = p_x, p_y, p_z$$

Meccanica Quantistica



$$\langle\psi| = (|\psi\rangle)^*, \langle\psi| \cdot |\psi\rangle = \langle\psi|\psi\rangle = 1,$$
$$\langle\psi_\perp|\psi\rangle = 0$$
$$A|a\rangle = a|a\rangle$$

$$|\langle\psi|a\rangle|^2 = \Pr(a|\psi)$$

INFN
Istituto Nazionale di Fisica Nucleare

Stati di sovrapposizione

Prendiamo due grandezze fisiche $A \to \{|a_0\rangle, |a_1\rangle\}$ e $B \to \{|b_0\rangle, |b_1\rangle\}$.
$A|a_0\rangle = a_0|a_0\rangle$, $A|a_1\rangle = a_1|a_1\rangle$
$B|b_0\rangle = b_0|b_0\rangle$, $B|b_1\rangle = b_1|b_1\rangle$

$|a_0\rangle \equiv |0\rangle, \quad |a_1\rangle \equiv |1\rangle$
$|b_0\rangle \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle,$
$|b_1\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$

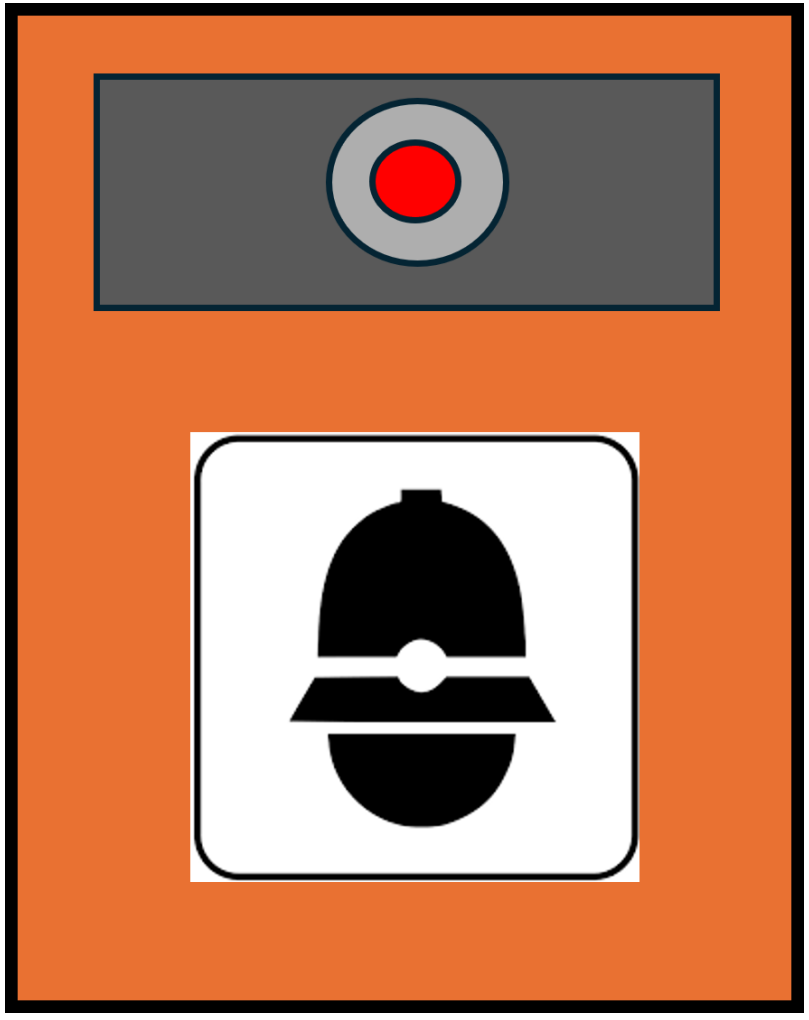
- Preparo il sistema in uno degli stati di A, diciamo $|0\rangle$
- Misuro la grandezza fisica B
- Qual è la probabilità di vedere uno dei due possibili risultati di B?

$$\Pr(b_0|a_0) = |\langle -|0\rangle|^2 = \Pr(b_1|a_0) = |\langle +|0\rangle|^2 = 1/2$$

INFN
Istituto Nazionale di Fisica Nucleare

Relazioni di incertezza

(principio di indeterminazione)



Istituto Nazionale di Fisica Nucleare

Teorema del No-Cloning

Teorema del No-Cloning

Teorema del No-Cloning

Istituto Nazionale di Fisica Nucleare

Protocollo BB84

"When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachievable with traditional transmission media, e.g. a communication channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected."

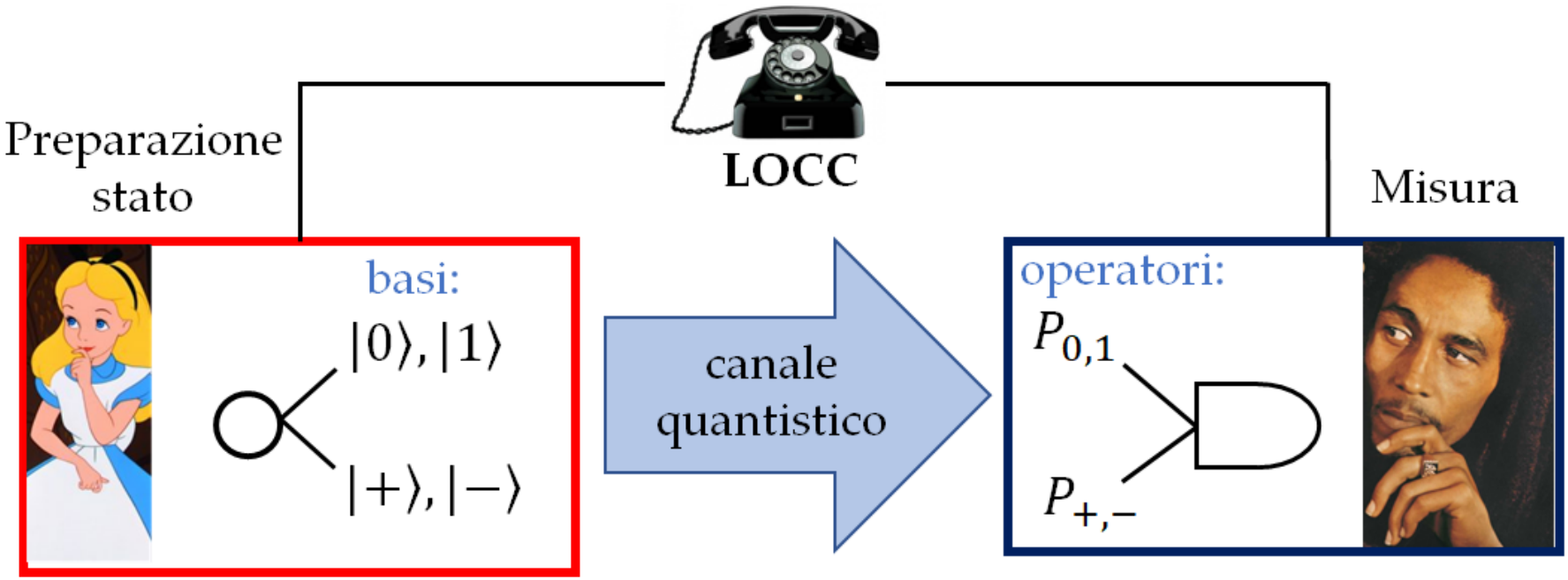
C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175

INFN
Istituto Nazionale di Fisica Nucleare

Protocollo BB84 - P&M

Protocollo BB84 - P&M

1) Prepare and measure



Protocollo BB84 - P&M

2) Sifting 

Protocollo BB84 - P&M

2) Sifting 

Protocollo BB84 - P&M

2) Sifting

Alice	Bob
1. $\{0,1\}$	1. $\{0,1\}$
2. $\{+,-\}$	2. $\{+,-\}$
3. $\{0,1\}$	3. $\{+,-\}$
4. $\{0,1\}$	4. $\{+,-\}$
5. $\{+,-\}$	5. $\{0,1\}$
6. $\{0,1\}$	6. $\{+,-\}$
7. $\{+,-\}$	7. $\{0,1\}$
8. $\{+,-\}$	8. $\{+,-\}$
9. ...	9. ...

INFN
Istituto Nazionale di Fisica Nucleare

Protocollo BB84 - P&M

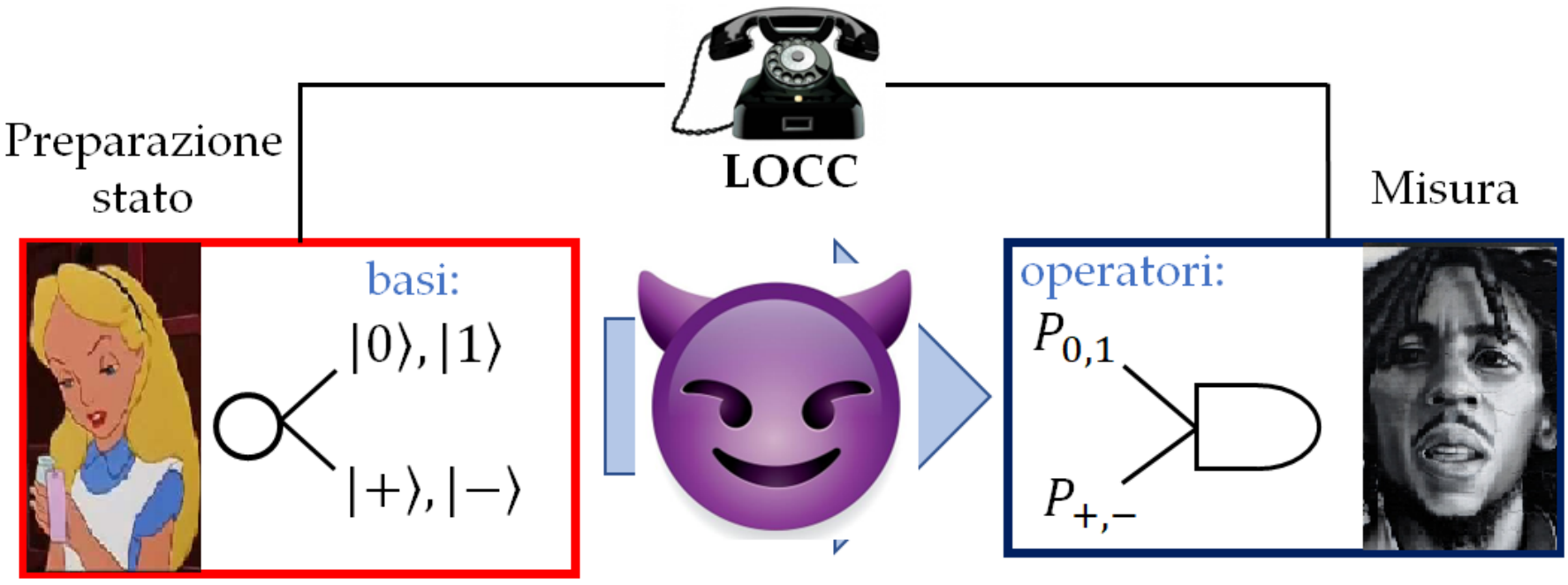
2) Sifting

Alice	Bob
1. $\{0,1\}$	1. $\{0,1\}$
2. $\{+,-\}$	2. $\{+,-\}$
3. $\{0,1\}$	3. $\{+,-\}$
4. $\{0,1\}$	4. $\{0,1\}$
5. $\{+,-\}$	5. $\{0,1\}$
6. $\{0,1\}$	6. $\{+,-\}$
7. $\{+,-\}$	7. $\{0,1\}$
8. $\{+,-\}$	8. $\{+,-\}$
9. ...	9. ...

INFN
Istituto Nazionale di Fisica Nucleare

Protocollo BB84 - P&M

1) Prepare and measure



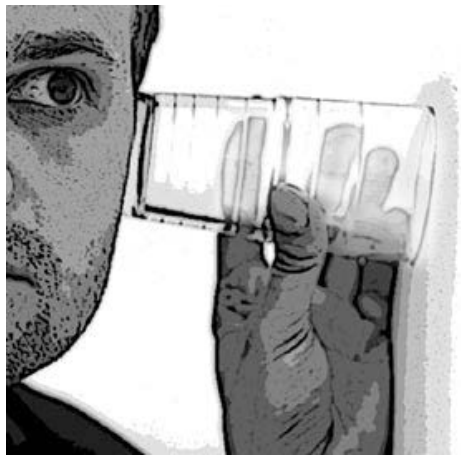
Protocollo BB84 - P&M

3) Parameter estimation

Protocollo BB84 - P&M

3) Parameter estimation

Un sottoinsieme casuale dei bit sopravvissuti (stati preparati da Alice e risultati di Bob) viene confrontato pubblicamente e vengono calcolati i *rate di errore* (QBER) relativi ad ogni base. Alice e Bob decidono se proseguire o abortire il protocollo.



Protocollo BB84 - P&M

3) Parameter estimation

Un sottoinsieme casuale dei bit sopravvissuti (stati preparati da Alice e risultati di Bob) viene confrontato pubblicamente e vengono calcolati i *rate di errore* (QBER) relativi ad ogni base. Alice e Bob decidono se proseguire o abortire il protocollo.

4) Error correction and Privacy amplification

Viene eseguito un algoritmo di correzione degli errori al termine del quale Alice e Bob condividono la stessa chiave. La chiave viene infine compressa e messa in sicurezza.

INFN
Istituto Nazionale di Fisica Nucleare

Entanglement

Entanglement

$\mathscr{H}_A, \mathscr{H}_B, \mathscr{H}_A \otimes \mathscr{H}_B = \mathscr{H}_{AB}$

$|\alpha\rangle_A \in \mathscr{H}_A, |\beta\rangle_B \in \mathscr{H}_B \rightarrow |\alpha\rangle_A \otimes |\beta\rangle_B \in \mathscr{H}_{AB}$

$$|\psi\rangle_{AB}^{(\text{entangled})} \neq |\alpha\rangle_A \otimes |\beta\rangle_B \quad \wedge \quad |\psi\rangle_{AB}^{(\text{entangled})} \in \mathscr{H}_{AB}$$

$$|\psi\rangle_{AB}^{(\text{entangled})} = \sum_j \lambda_j |j\rangle_A |j\rangle_B$$

Entanglement

$\mathscr{H}_A, \mathscr{H}_B, \mathscr{H}_A \otimes \mathscr{H}_B = \mathscr{H}_{AB}$

$|\alpha\rangle_A \in \mathscr{H}_A, |\beta\rangle_B \in \mathscr{H}_B \rightarrow |\alpha\rangle_A \otimes |\beta\rangle_B \in \mathscr{H}_{AB}$

$$|\psi\rangle_{AB}^{(\text{entangled})} \neq |\alpha\rangle_A \otimes |\beta\rangle_B \quad \wedge \quad |\psi\rangle_{AB}^{(\text{entangled})} \in \mathscr{H}_{AB}$$

$$|\psi\rangle_{AB}^{(\text{entangled})} = \sum_j \lambda_j |j\rangle_A |j\rangle_B$$

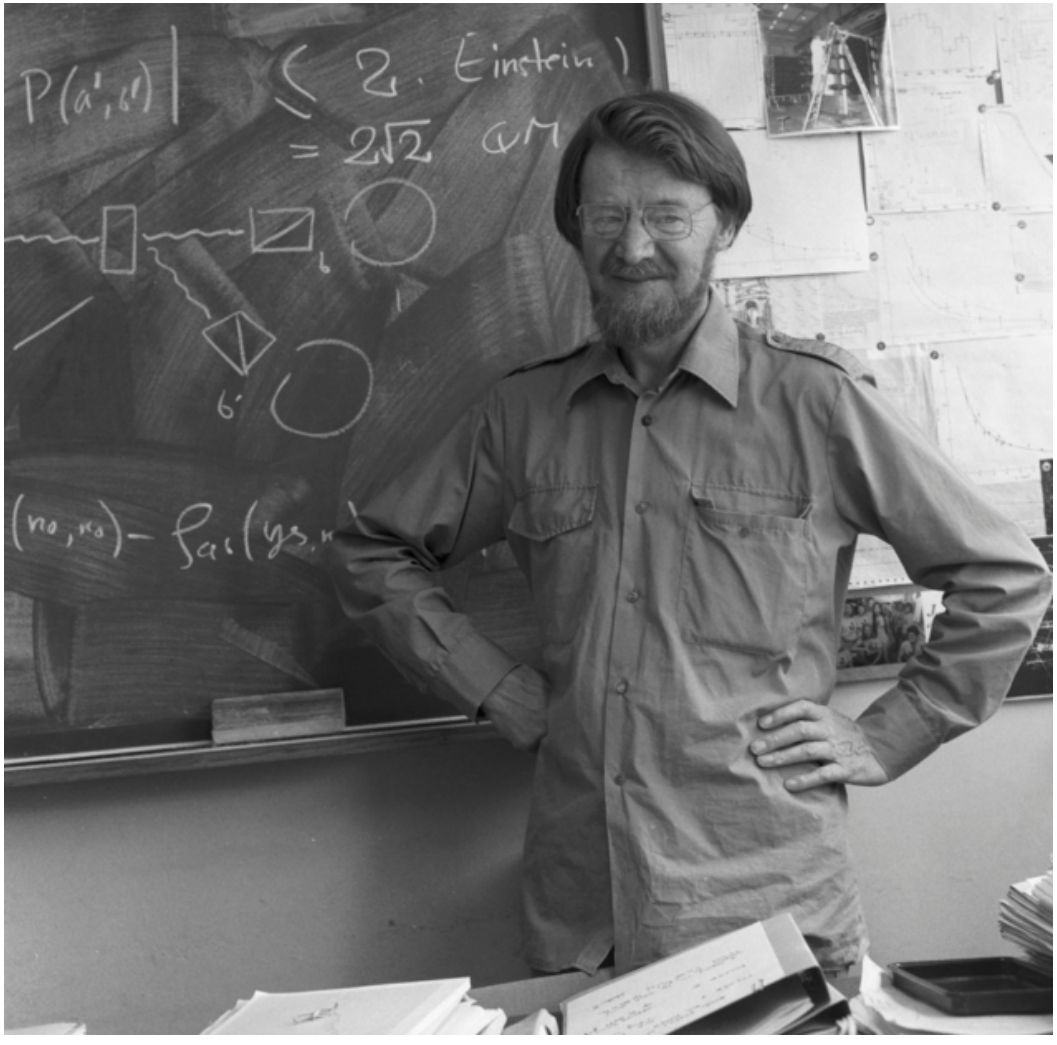
Stati di Bell

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Phi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

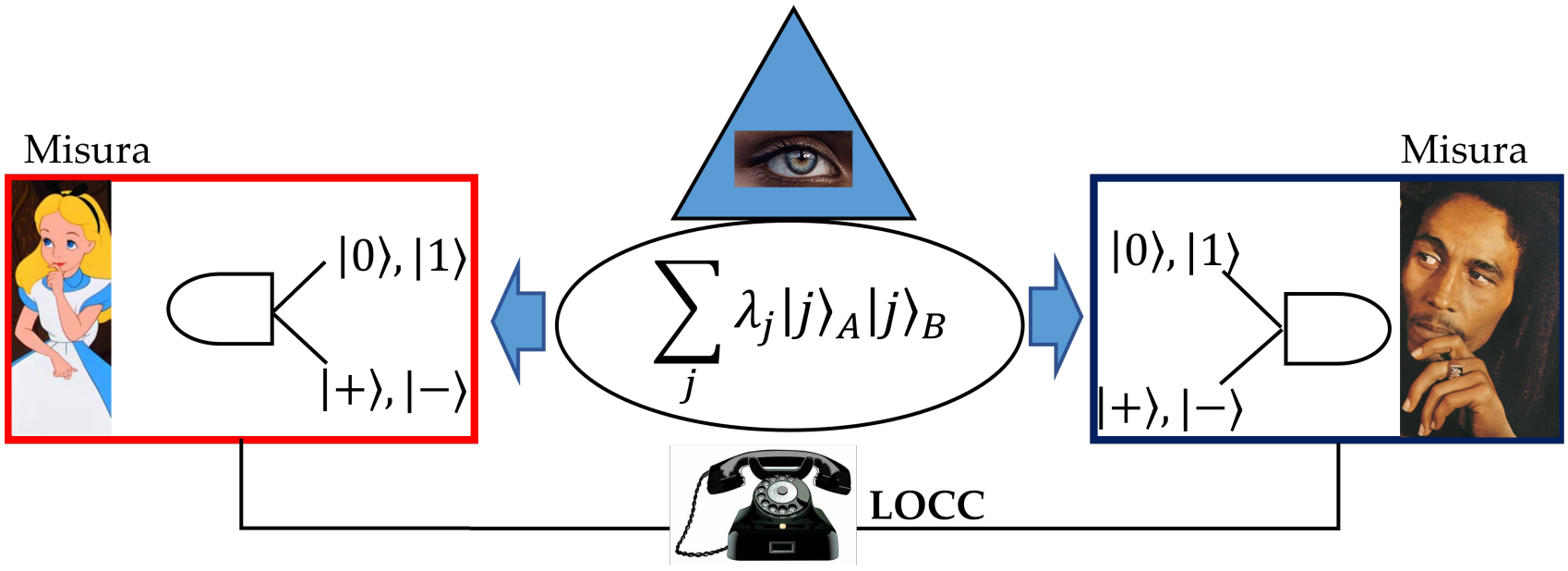
$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Entanglement

Disuguaglianze di Bell



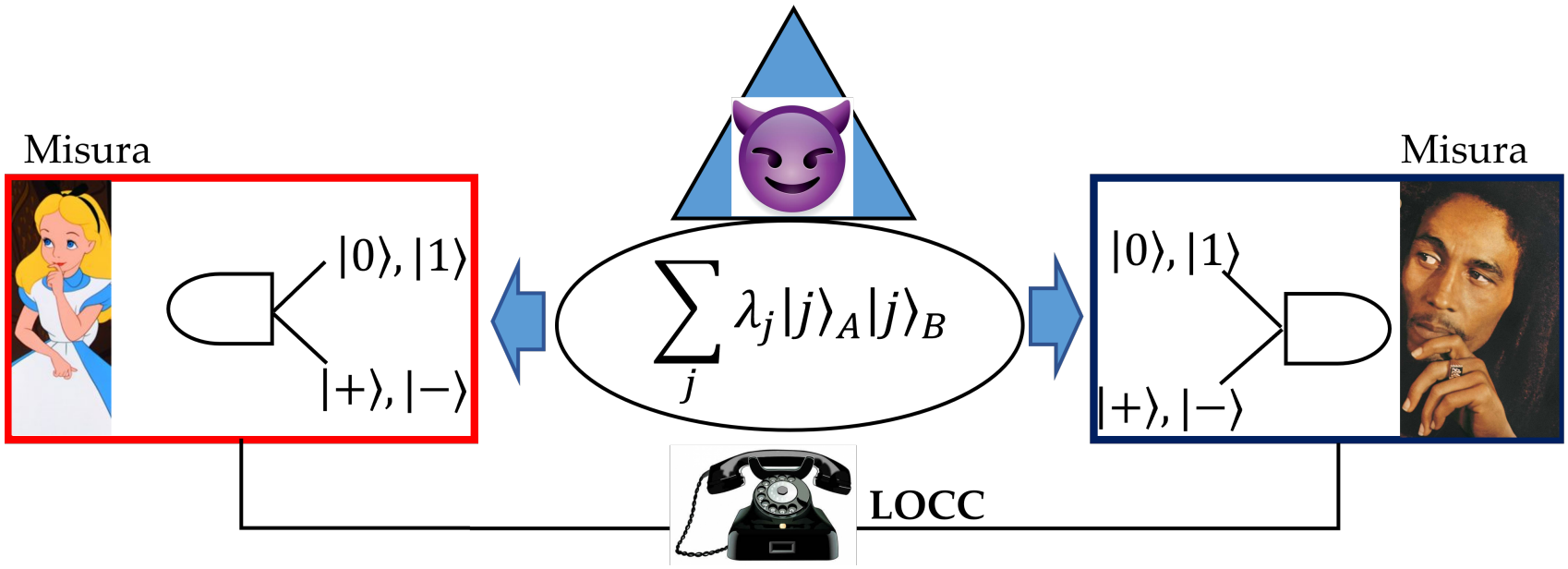
BB84 entanglement-based



- 1) Misura
- 2) Sifting
- 3) Parameter estimation
- 4) Error correction e Privacy amplification

INFN
Istituto Nazionale di Fisica Nucleare

BB84 entanglement-based



- 1) Misura
- 2) Sifting
- 3) Parameter estimation
- 4) Error correction e Privacy amplification

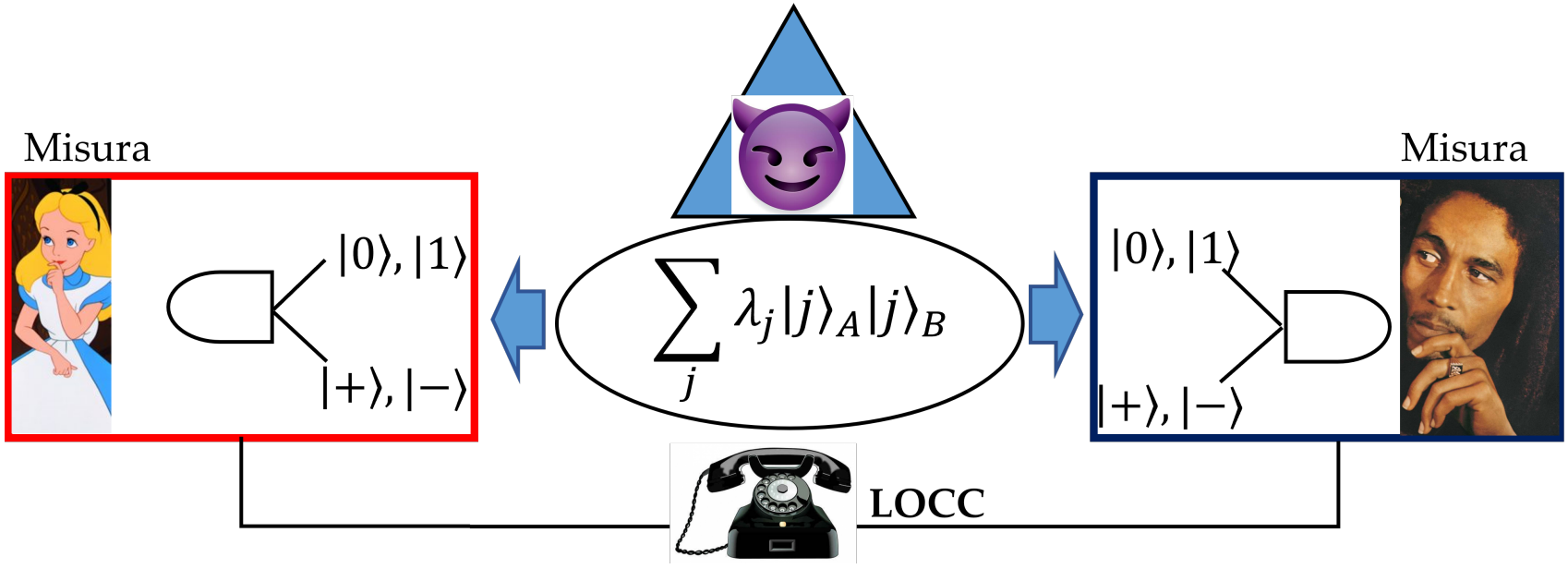
INFN
Istituto Nazionale di Fisica Nucleare

Protocollo E91

A. Ekert, Phys. Rev. Lett. **67**, 661 (1991)

Istituto Nazionale di Fisica Nucleare

Protocollo E91

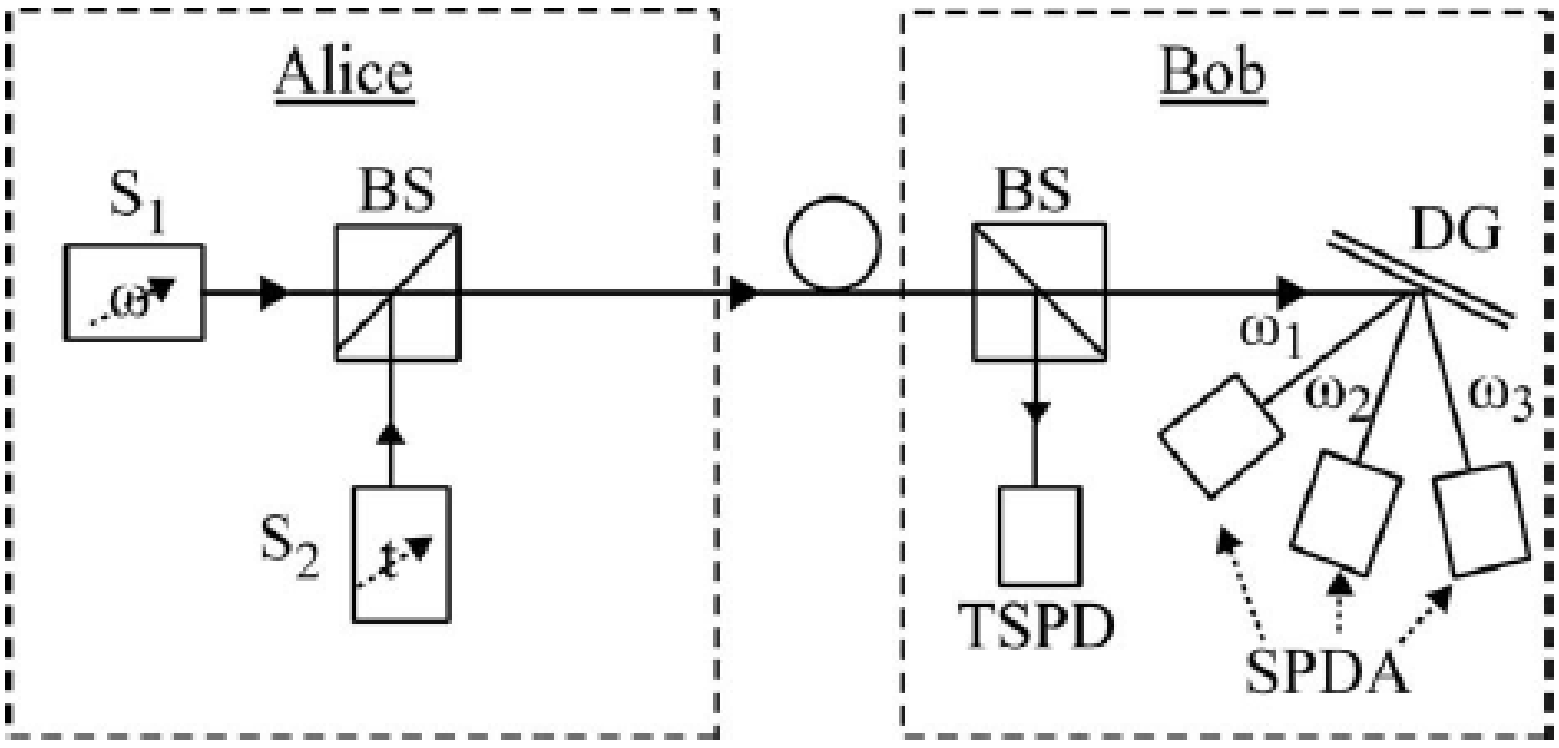


- 1) Misura
- 2) Sifting
- 3) Stima e valutazione delle correlazioni via disuguaglianze di Bell
- 4) Error correction e Privacy amplification

INFN
Istituto Nazionale di Fisica Nucleare

Sviluppi: QKD a variabili continue

B. Qi, Opt. Lett. **31**, 2795 (2006)



Sviluppi: Italian Quantum Backbone (IQB)

A. Meda et al., "QKD and frequency distribution cooperation: the Twin-field QKD case," 2022 IEEE 15th Workshop on Low Temperature Electronics (WOLTE), Matera, Italy, 2022, pp. 1-4

Sviluppi: High dimensional QKD

Sviluppi: High dimensional QKD

Codifichiamo l'informazione su stati a dimensione $d > 2$:

Sviluppi: High dimensional QKD

Codifichiamo l'informazione su stati a dimensione $d > 2$:

$$\text{quBits} \rightarrow \text{quDits}$$

Sviluppi: High dimensional QKD

Codifichiamo l'informazione su stati a dimensione $d > 2$:

$$\text{quBits} \rightarrow \text{quDits}$$

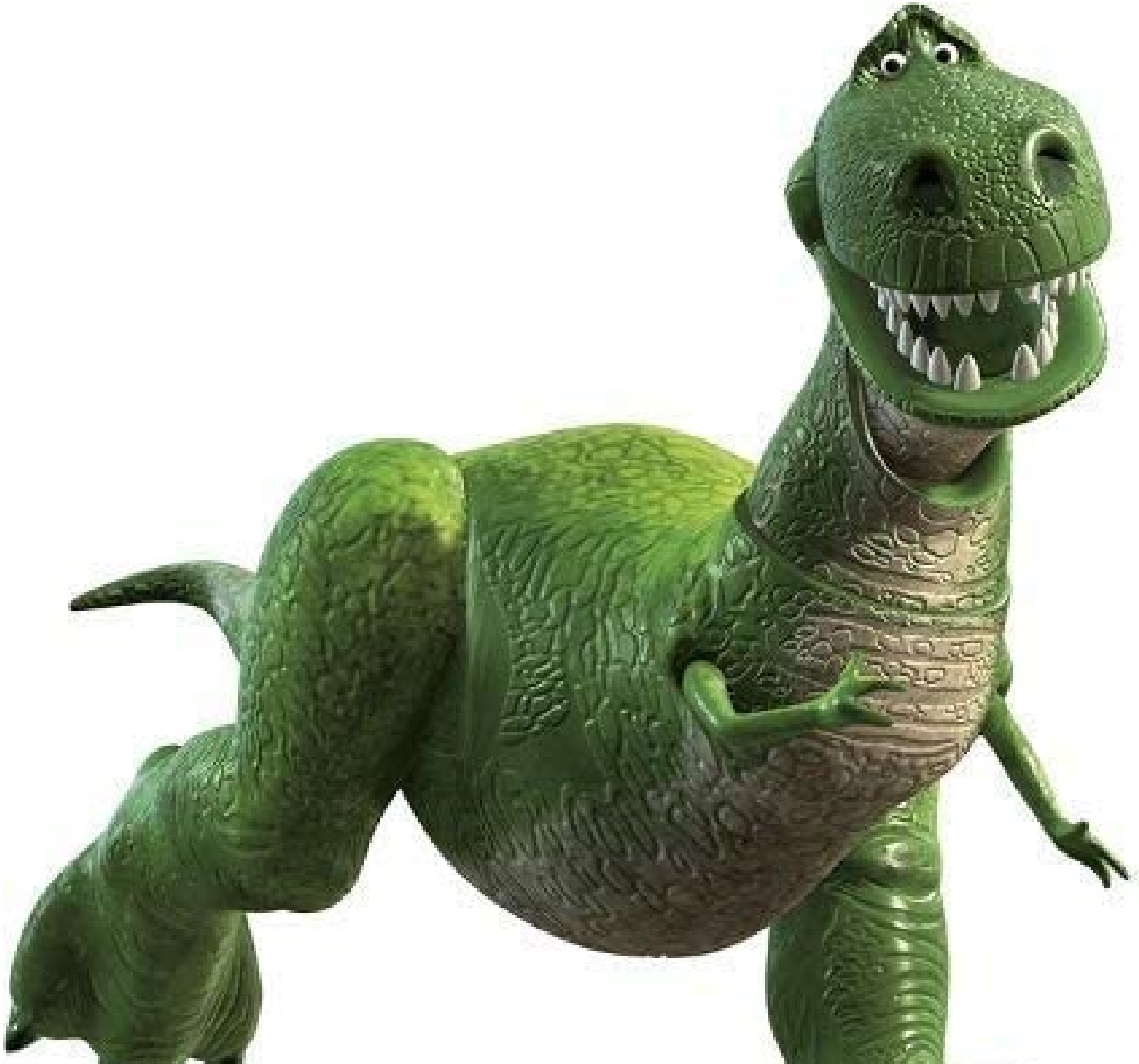
Vantaggi:

- protocolli più robusti
- rate di trasmissione maggiori

D. Bruss and C. Macchiavello, *Phys. Rev. Lett.* **88** (2002)

N.J. Cerf, M. Bourennane, A. Karlsson and N. Gisin, *Phys. Rev. Lett.* **88** (2002)

The end



Istituto Nazionale di Fisica Nucleare