UNIVERSITÀ DEGLI STUDI DI BARI
“ALDO MORO”
Dipartimento Interateneo di Fisica
“Michelangelo Merlin”

THEORETIC GROUP 🎄 CHRISTMAS WORKSHOP 🎅

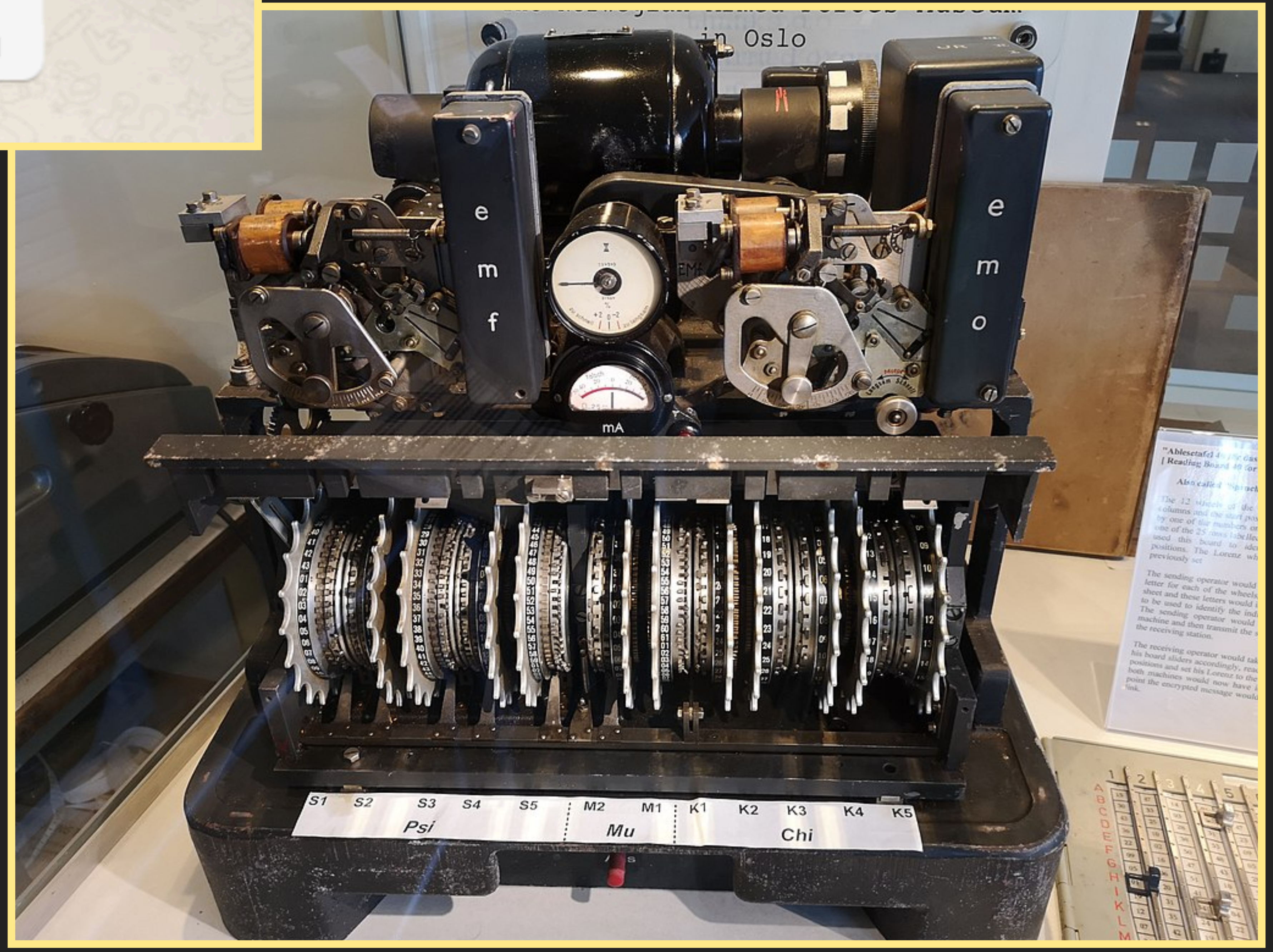
SECURITY OF QUANTUM KEY DISTRIBUTION

Gabriele Staffieri
g.staffieri2@phd.uniba.it

17/12/2024

CRYPTOGRAPHY: WHAT IS IT?

- The study of secure communication techniques in presence of adversarial behavior
- Constructing and analyzing protocols that prevent third parties from reading private messages.
- Applications: electronic commerce, instant messaging, military communications, etc.



HOW DOES IT WORK?

- Protocols and algorithms are implemented to generate a private "key" string
- The key is used by the sender and recipient to encrypt and decrypt the message

Ruleset:

- $0 \longrightarrow$ shift 3 letters backward
- $1 \longrightarrow$ shift 5 letters forward

Plaintext $\longrightarrow$	B	A	B	B	O	N	A	T	A	L	E
Key $\longrightarrow$	0	0	1	0	0	1	1	1	1	0	1
Ciphertext $\longrightarrow$	Z	Y	G	Z	L	S	F	Y	F	I	J

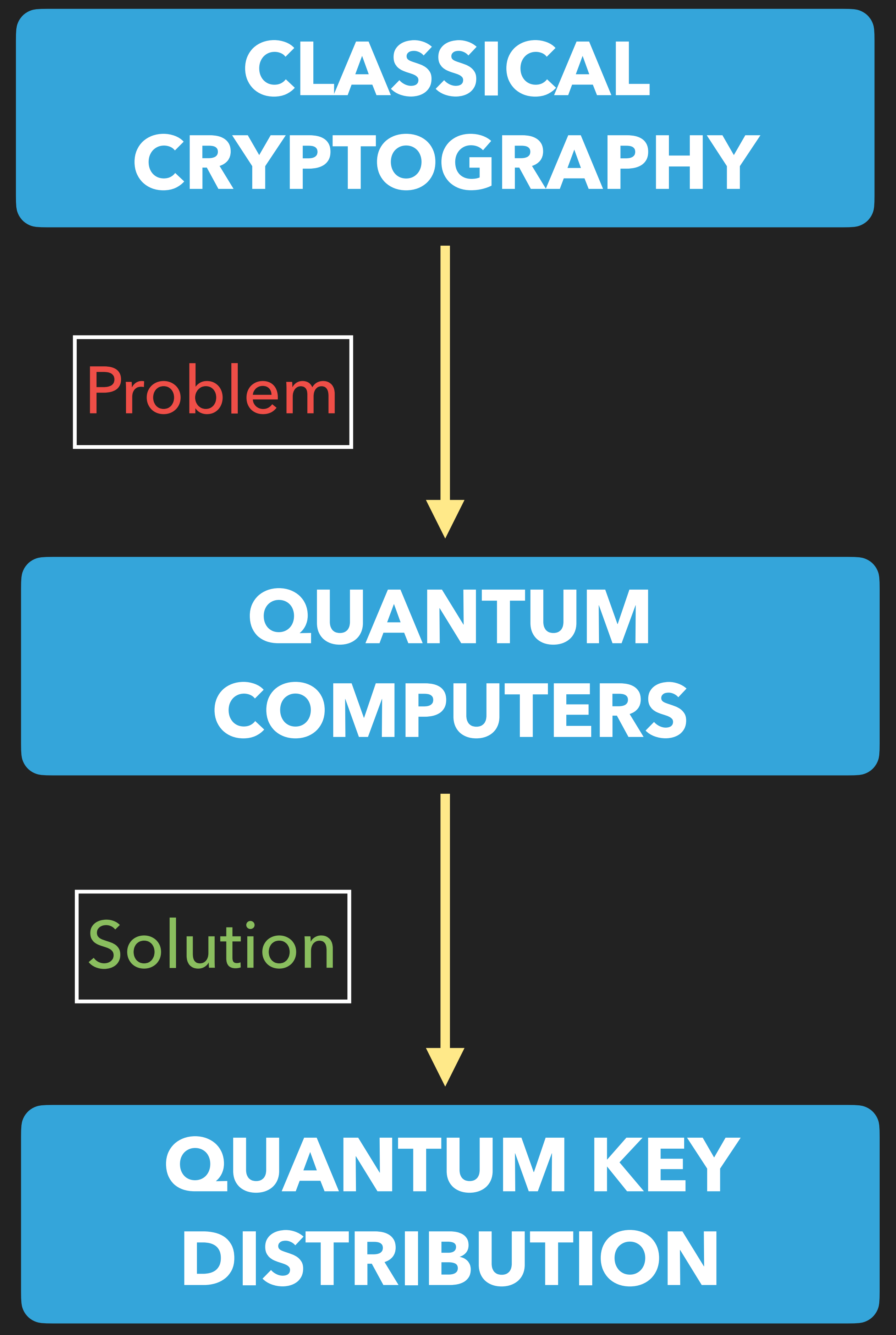
CLASSICAL CRYPTOGRAPHY

- Security based on hard-to-solve mathematical problems (e.g. factorization of large numbers)
- The computational complexity is too great even for most powerful calculators
- Asymmetric cryptography: RSA algorithm (Rivest, Shamir, Adleman 1977)

WHY QUANTUM CRYPTOGRAPHY?

- *Quantum threat*: quantum computers, have higher computational power and can easily break classical cryptosystems (e.g. Shor algorithm)

- Quantum mechanics can be also exploited to build cryptographic protocols: Quantum Key Distribution (QKD)



BB84 PROTOCOL (BENNET, BRASSARD 1984)

- Goal: communicate a random bit of information (0 or 1)
- Alice prepares a pair of entangled qubits

$$|\Phi^+\rangle_{AA'} = \frac{|0\rangle_A|0\rangle_{A'} + |1\rangle_A|1\rangle_{A'}}{\sqrt{2}} = \frac{|+\rangle_A|+\rangle_{A'} + |-\rangle_A|-\rangle_{A'}}{\sqrt{2}}$$

- She sends qubit A' to Bob, then they can measure the qubits in their possession randomly in the (computational) $Z = \{|0\rangle, |1\rangle\}$ or (conjugate) $X = \{|+\rangle, |-\rangle\}$ Pauli basis.

$|\Phi^+\rangle$ can be either written in the X or Z basis: $|\Phi^+\rangle_{AB} = \dfrac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}} = \dfrac{|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B}{\sqrt{2}}$

- Alice measures in the Z basis:

$$50\,\%\text{ prob: } |0\rangle_A \xrightarrow{\text{eigval } +1} |\Phi^+\rangle_{AB} \longrightarrow |0\rangle_A|0\rangle_B$$

$$50\,\%\text{ prob: } |1\rangle_A \xrightarrow[\text{eigval } -1]{} |\Phi^+\rangle_{AB} \longrightarrow |1\rangle_A|1\rangle_B$$

- Alice measures in the X basis:

$$50\,\%\text{ prob: } |+\rangle_A \xrightarrow{\text{eigval } +1} |\Phi^+\rangle_{AB} \rightarrow |+\rangle_A|+\rangle_B$$

$$50\,\%\text{ prob: } |-\rangle_A \xrightarrow[\text{eigval } -1]{} |\Phi^+\rangle_{AB} \rightarrow |-\rangle_A|-\rangle_B$$

- Bob after receiving the qubit $A' \longrightarrow B$ can perform the same kind of measurements
- If Alice and Bob have *randomly* measured in the same basis, they successfully obtain a *random though correlated* result, thus they can associate a random bit:

$$\Longrightarrow \quad \begin{aligned} \{|0\rangle, |+\rangle\} &\longrightarrow \text{eigenvalue } (+1) \longrightarrow 0 \\ \{|1\rangle, |-\rangle\} &\longrightarrow \text{eigenvalue } (-1) \longrightarrow 1 \end{aligned}$$

Pauli eigenstates relation

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \qquad |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

QUBIT PREPARATION AND MEASURE

- To construct a bit string Alice prepares N pairs of qubits

$$|\Psi\rangle = \bigotimes_{j=1}^{N} |\Phi^+\rangle_{AB}^{(j)}$$

- Alice constructs two bit strings a and b

$$a = (a_1 \,, \ldots, \, a_N) \quad \Longrightarrow \quad \begin{array}{lcl} i\text{-th measurement in } Z & \longrightarrow & a_i = 0 \\ i\text{-th measurement in } X & \longrightarrow & a_i = 1 \end{array}$$

$$b = (b_1 \,, \ldots, \, b_N) \quad \Longrightarrow \quad \begin{array}{lcl} \text{eigenvalue } (+1) \text{ in the } i\text{-th measurement} & \longrightarrow & b_i = 0 \\ \text{eigenvalue } (-1) \text{ in the } i\text{-th measurement} & \longrightarrow & b_i = 1 \end{array}$$

- Bob constructs his own bit strings a' and b' as well

CLASSICAL COMMUNICATION AND POST-PROCESSING

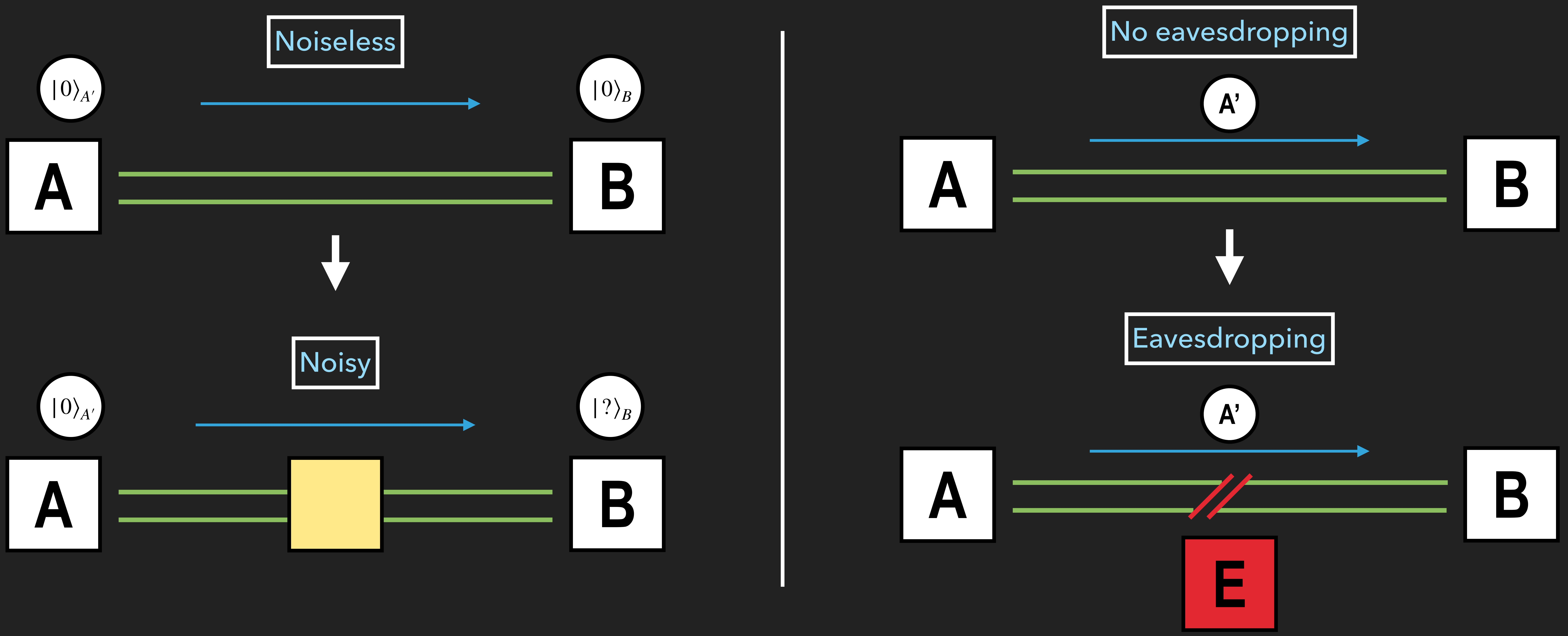
- Alice and Bob publicly announce their choices of measurement a and a'
- If $a_i = a_i'$, Alice and Bob have correlated, despite random, results
  $\Longrightarrow$ They keep $b_i = b_i'$
- If $a_i \neq a_i'$, Alice and Bob have uncorrelated results, in general
  $\Longrightarrow$ They discard b_i and b_i'

	1	2	3	4	5
a_i	0	1	1	0	1
b_i	0	1	0	1	0
Alice's basis	Z	X	X	Z	X
A qubit state	$\vert 0 \rangle$	$\vert - \rangle$	$\vert + \rangle$	$\vert 1 \rangle$	$\vert + \rangle$
a'_i	0	1	0	1	1
Bob's basis	Z	X	Z	X	X
keep/discard	✅	✅	❌	❌	✅
$c_i = c'_i$	0	1	-	-	0

The bits they keep form the secret key string $c = c'$

REAL-WORLD COMPLICATIONS: NOISE AND EAVESDROPPING

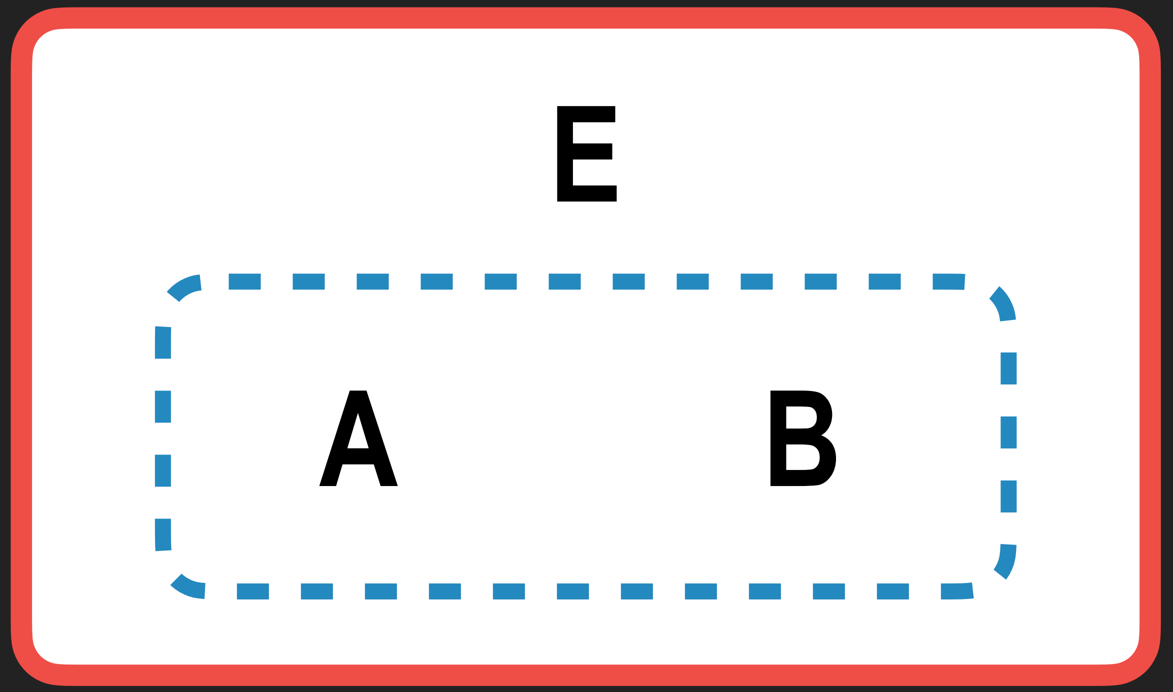
- In reality things are complicated due to the presence of noise and eavesdropping



- In the real case Eve can intercept the qubit A'. The quantum system that Eve can control is the entire environment E

$\Longrightarrow$ System ABE is isolated

$\Longrightarrow$ The overall evolution is unitary



$$|\Psi\rangle_{AA'} \otimes |\phi\rangle_E \longrightarrow \left(\mathbf{1}_A \otimes U_{[A' \to B]E}\right) |\Psi\rangle_{AA'} \otimes |\phi\rangle_E = |\Theta\rangle_{ABE}$$

- The final state of the system AB

$$\rho_{AB} = \mathrm{Tr}_E \left(|\Theta\rangle_{ABE}\langle\Theta| \right)$$

ρ_{AB} can be characterized by some constraints

- $Qber$ (Quantum bit error rate)

$$Qber^{(Z)} = \mathrm{Tr}\Big(|0\rangle_A\langle 0| \otimes |1\rangle_B\langle 1| \rho_{AB} \Big) + \mathrm{Tr}\Big(|1\rangle_A\langle 1| \otimes |0\rangle_B\langle 0| \rho_{AB} \Big)$$

$$Qber^{(X)} = \mathrm{Tr}\Big(|+\rangle_A\langle +| \otimes |-\rangle_B\langle -| \rho_{AB} \Big) + \mathrm{Tr}\Big(|-\rangle_A\langle -| \otimes |+\rangle_B\langle +| \rho_{AB} \Big)$$

- $|\Phi^+\rangle_{AA'}$ is maximally entangled and qubit A does not evolve

$\Longrightarrow$ The reduced density matrix of A is completely mixed

$$\rho_A = \frac{1}{2}\mathbf{1}_A$$

SECURITY PROOF - SECRET KEY RATE

$$\boxed{r_N = \eta\left(\frac{l - l_{leak}}{N}\right)}$$

- l number of secret bits
- l_{leak} number of bits leaked for error correction
- η transmittance of the channel
- N total number of rounds (block size)

- At the end of the protocol Alice and Bob share a bit string Z^N and while E^N is Eve's system
- The problem: estimate how many bits in Z^N are *secret* w.r.t. Eve

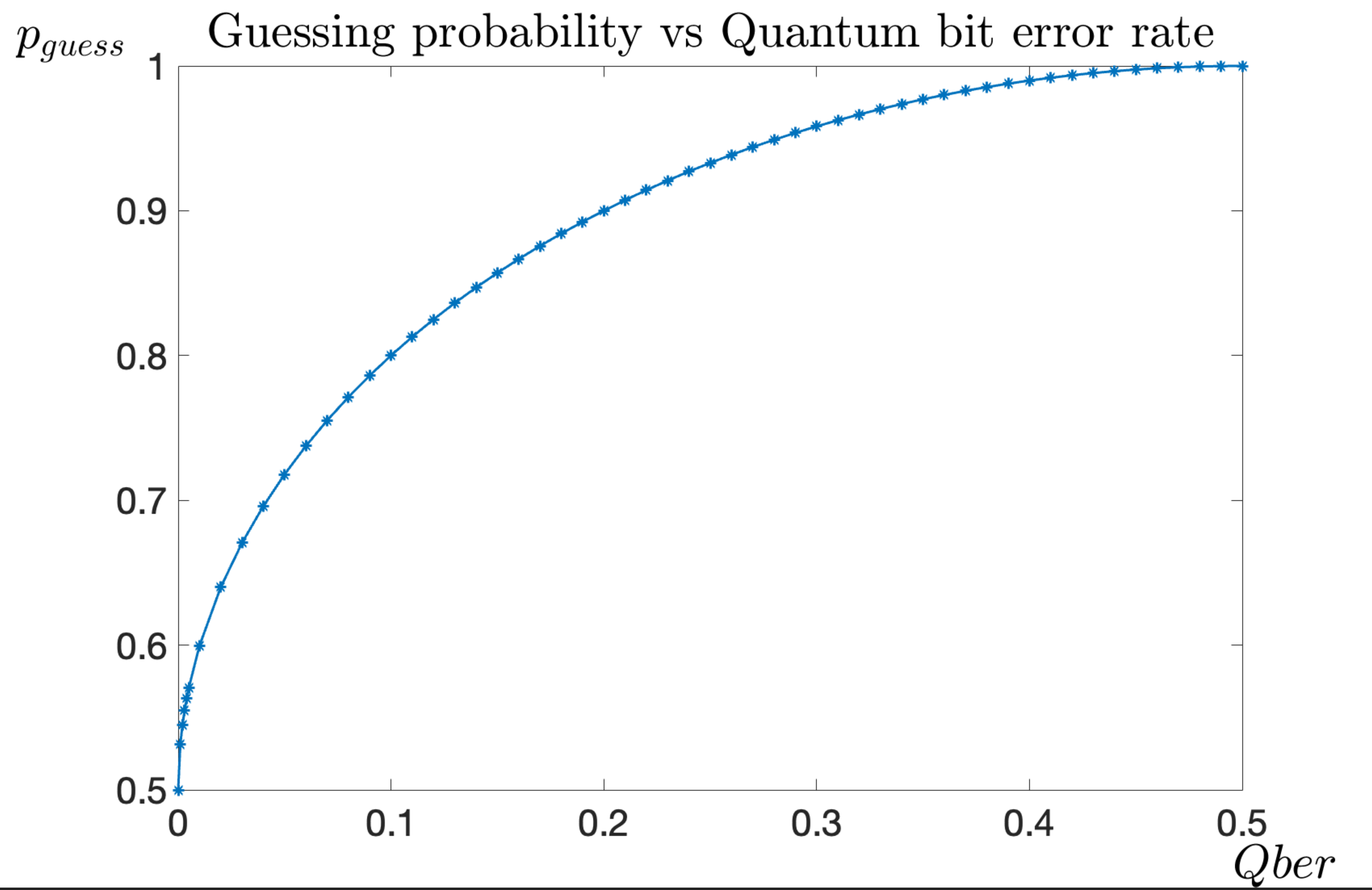
GUESSING PROBABILITY

- The idea: if Eve's probability $p_{guess}(Z^N | E^N)$ to guess Z^N conditioned to her side information E^N is low, the protocol is secure against her attacks.
- Left-over hash lemma

If Z^N is Alice and Bob's string and Eve owns side information E^N about it, the number l of random bits in Z^N on which Eve is completely ignorant about is given by: $l \simeq -\log_2 p_{guess}(Z^N | E^N)$

- Collective attacks: if each qubit attack is identical and statistically independent, every qubit measurement is represented by a i.i.d. random variable and the guessing probability factorizes: $p_{guess}(Z^N | E^N) = \left[p_{guess}(Z | E)\right]^N$

GUESSING PROBABILITY AND QBER

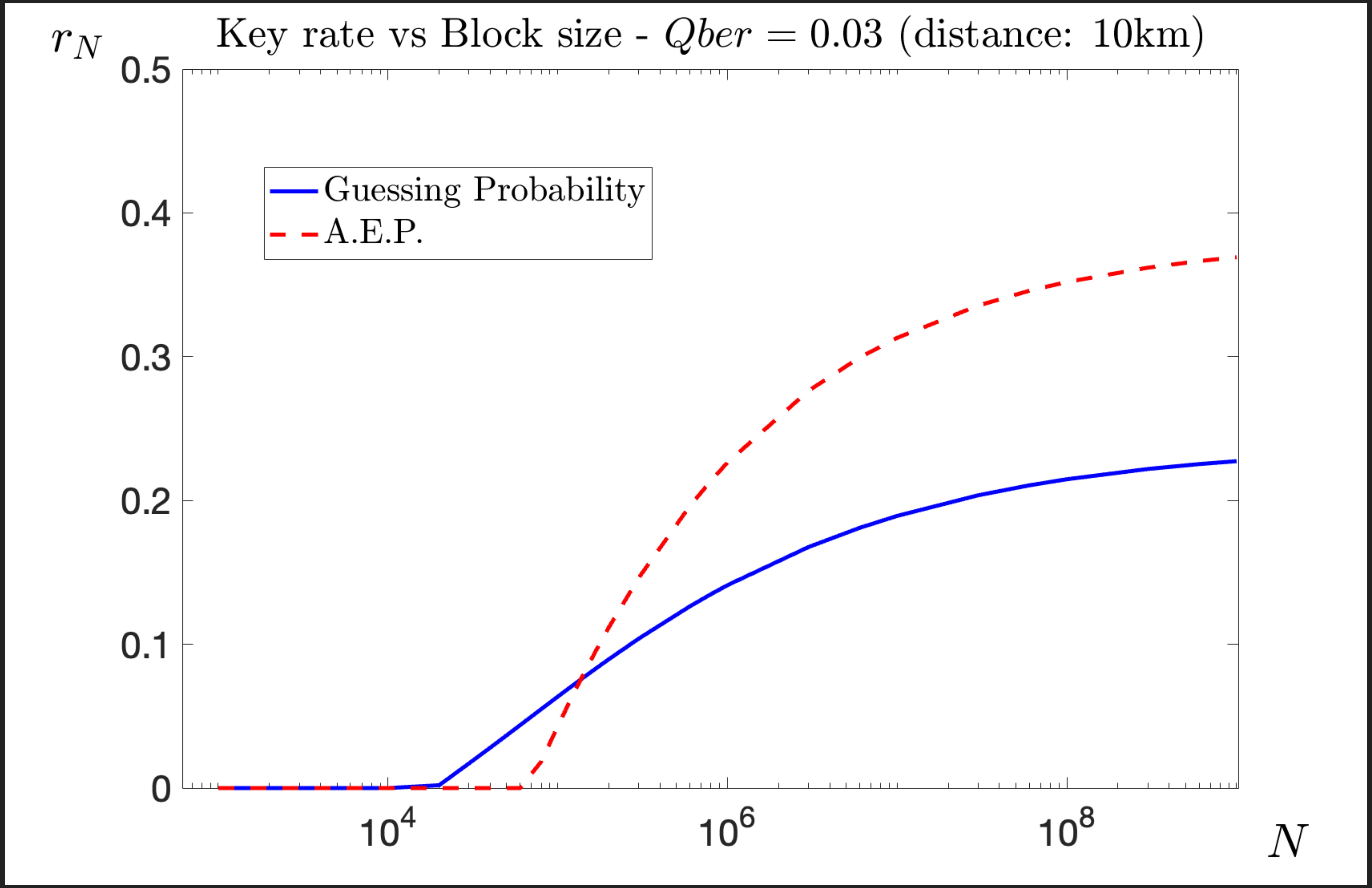


- Analytic form of the guessing probability in terms of the $Qber$ (1 qubit):

$$p_{guess}(Qber) = \frac{1}{2} + \sqrt{Qber(1 - Qber)}$$

- $p_{guess} \geq 0.5$
- Information-disturbance trade-off

GUESSING PROBABILITY VS ASYMPTOTIC EQUIPARTITION PROPERTY



- Guessing probability is better w.r.t. A.E.P. when one studies the security at finite-size
- For $N \leq 10^5$ one still manages to have non-vanishing key rate

CONCLUSION

- Quantum Key Distribution represents the quantum answer to the "quantum threat"
- Quantum cryptography aims to be everlasting i.e. no more depending on the technological advance, being founded on inviolable laws of physics
- Guessing probability outperforms traditional approaches in studying the security of QKD at finite size

THANK YOU FOR YOUR ATTENTION!

BACKUP SLIDES

TOOLS OF QUANTUM INFORMATION THEORY: ENTROPY

- Y random variable, $Y \sim P_Y$

  Shannon Entropy: $$H(Y)_{P_Y} = -\sum_{y \in \mathcal{Y}} P_Y(y) \cdot \log_2 [P_Y(y)]$$

- A quantum system, ρ_A state

  Von Neumann Entropy: $$H(Y)_{P_Y} = -\,\mathrm{Tr}\left(\rho_A \log \rho_A\right)$$

Shannon: if an event occurs with probability p, then its surprisal is $-\log_2 p$. The entropy is the average surprisal of an event

$\Longrightarrow$

$H(Y)_{P_Y}$ measures the uncertainty (in bit) about the value of a r.v. Y, distributed as P_Y

ERROR CORRECTION LEAKAGE

- The outcome of Bob's measurement on one qubit can be seen as a binary random variable Y, distributed as $Qber$

e.g. Alice measures $|\Phi^+\rangle_{AB}$ in $\{|0\rangle, |1\rangle\}$ and finds $|0\rangle$. Then Bob will find:

- with probability $p = Qber$ state $|1\rangle$ (error occurred)
- with probability $q = 1 - Qber$ state $|0\rangle$ (error not occurred)

Uncertainty about Y:

$$H_2(Qber) = -Qber \cdot \log_2\left(Qber\right) - (1 - Qber) \cdot \log_2\left(1 - Qber\right)$$

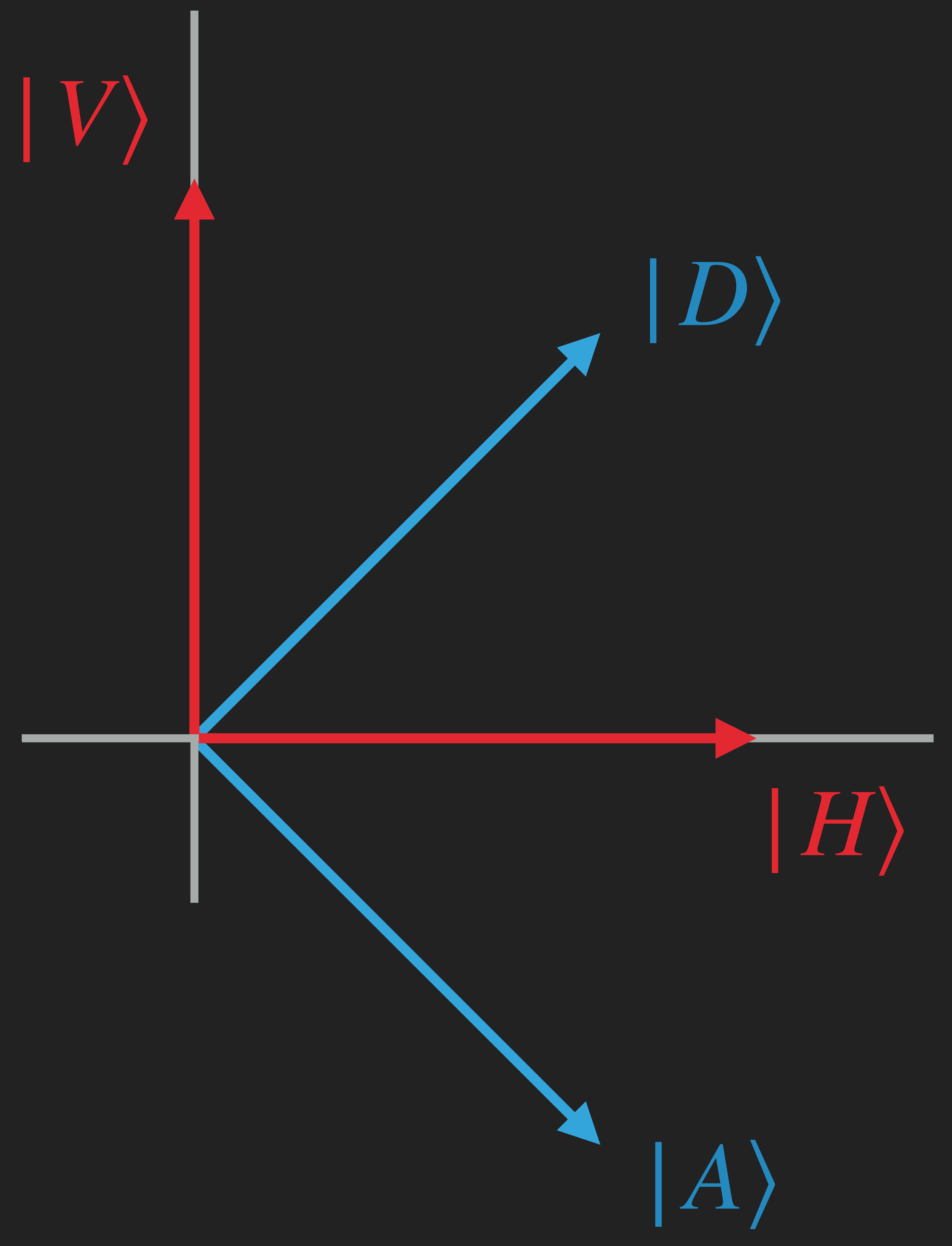
- Bob has to communicate $l_{leak} = H_2(Qber)$ bits of information to Alice to help her correct her string

PHOTONS AS QUBITS

- Qubits are photons in QKD protocols
- Polarization is the observable that is measured

$$\sigma_x : \quad \{|+\rangle, |-\rangle\} \longleftrightarrow \{|D\rangle, |A\rangle\}$$
$$\sigma_z : \quad \{|0\rangle, |1\rangle\} \longleftrightarrow \{|H\rangle, |V\rangle\}$$

$$|D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}} \qquad |A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}$$



GUESSING PROBABILITY AS FIDELITY ($N = 1$ QUBIT PAIR)

- Guessing probability can be obtained optimizing quantum fidelity on systems A and B

[1] $$p_{guess}(Z|E) = \max_{\rho_{AB}\,,\,\sigma_{AB}} F^2\left(\rho_{AB}\,,\, \sum_j Z_j\, \sigma_{AB}\, Z_j \right)$$

Fidelity

$$F(\rho,\sigma) = \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} = ||\sqrt{\rho}\sqrt{\sigma}||_1$$

- Collective attacks: $\rho_{AB}^{(N)} = \rho_{AB}^{\otimes N}$

Z completely positive map ⟶ Kraus-Sudarshan operators

$$Z\{\sigma_{AB}\} = \sum_j Z_j\, \sigma_{AB}\, Z_j \qquad Z_j = \mathbf{1}_A \otimes |j\rangle_B\langle j| \qquad j = 0,1$$

[1] Coles, Patrick J. "Unification of different views of decoherence and discord." Physical Review A 85.4 (2012): 042103.

BLOCK CHARACTERIZATION OF FIDELITY

- A particular characterization of Fidelity for $P, Q \in P(\mathscr{H})$ can be exploited to write an SDP [2]

$$F(P,Q) = \max_X \left\{ |\mathrm{Tr}\,(X)| \quad : \quad X \in L(\mathscr{H}), \quad \begin{pmatrix} P & X \\ X^\dagger & Q \end{pmatrix} \in P(\mathscr{H} \oplus \mathscr{H}\} \right\}$$

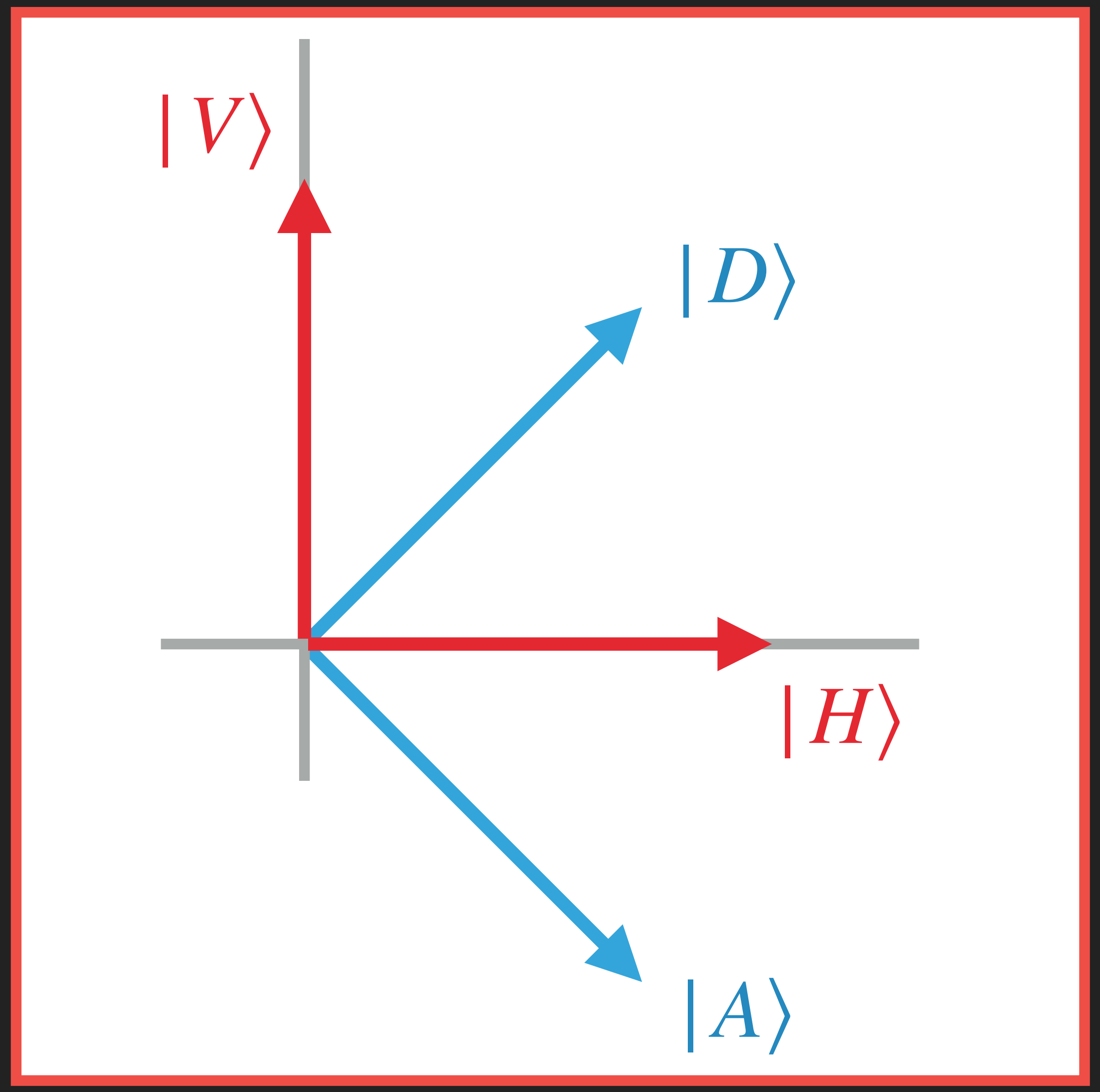
$$\begin{pmatrix} P & X \\ X^\dagger & Q \end{pmatrix} \in P(\mathscr{H} \oplus \mathscr{H}) \iff X = \sqrt{P}K\sqrt{Q}, \quad ||K||_\infty \leq 1$$

$$|\mathrm{Tr}\,(X)| \longrightarrow Re[\mathrm{Tr}\,(X)] = \frac{1}{2}\mathrm{Tr}\,(X) + \frac{1}{2}\mathrm{Tr}\,(X^\dagger)$$

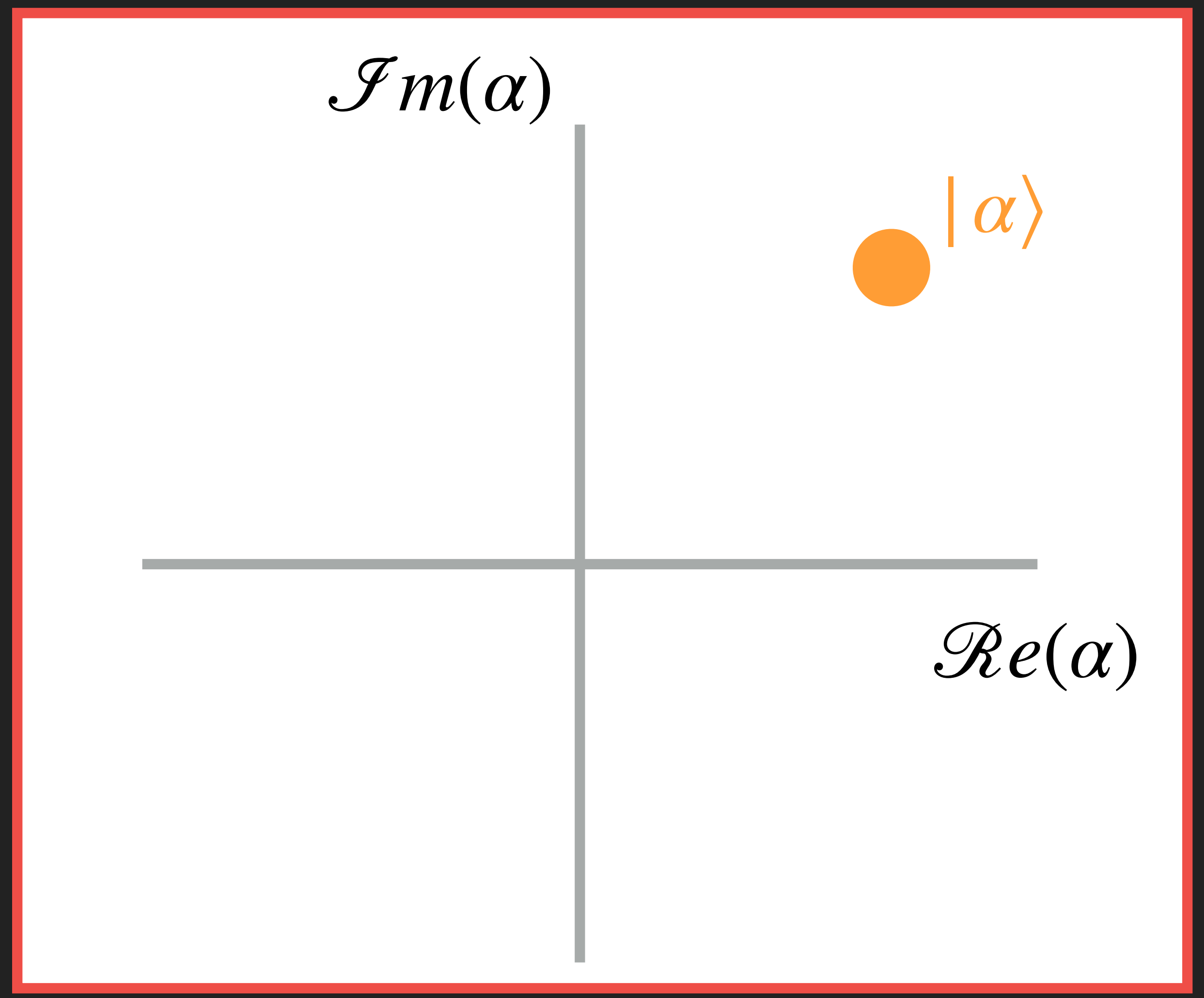
[2] Watrous, John. *The theory of quantum information*. Cambridge university press, 2018.

DISCRETE-VARIABLE AND CONTINUOUS-VARIABLE QKD PROTOCOLS

- Discrete-variable (DV)
  - Long range ($\lesssim 1200km$)
  - Non-trivial detection (high-efficiency photon detectors, expansive cooling systems required)

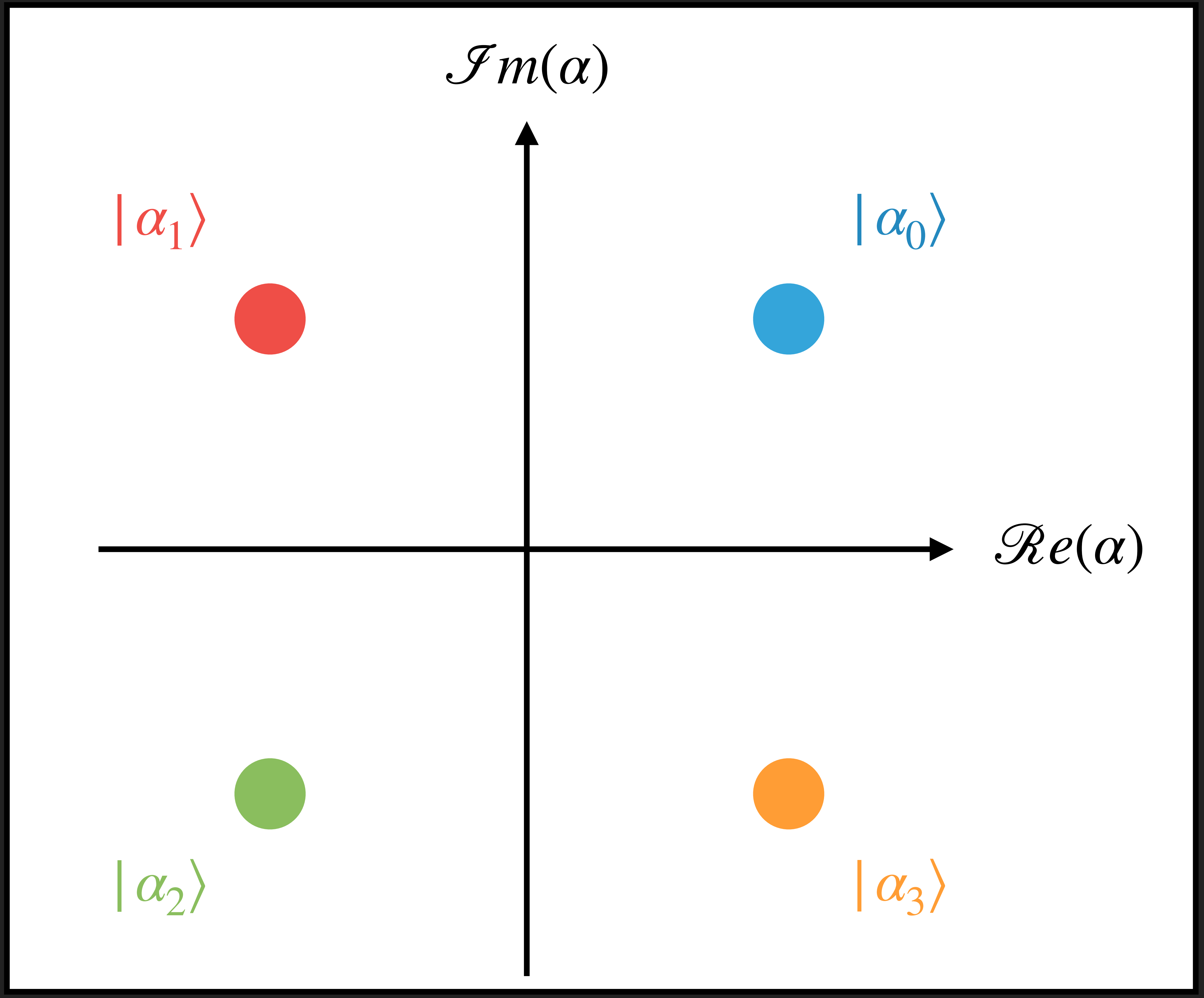


- Continuous-variable (CV)
  - Metropolitan range ($\lesssim 100km$)
  - Mature detection techniques (Coherent detection)



CV PROTOCOLS WITH DISCRETE MODULATION (DM-CV-QKD)

- Quadrature Phase Shifting Key (QPSK)
- $\alpha_j = |\alpha| \exp\left[i\left(\frac{\pi}{4} + \frac{\pi}{2} j\right)\right] \qquad j = 0,1,2,3$
- $|\alpha_j\rangle = e^{-|\alpha|^2/2} \sum_{k=0}^{\infty} \frac{\alpha_j^k}{\sqrt{k!}} |k\rangle$
- Homodyne and Heterodyne detection



CLASSICAL CRYPTOGRAPHY

- Based on hard-to-solve mathematical problems (e.g. factorization of large numbers)
- Asymmetric cryptography: RSA algorithm (Rivest, Shamir, Adleman 1977)