Quantum Cryptography 101:

Understanding the Power of Quantum Information

Mina Doosti

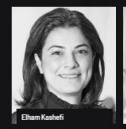
Okinawa School in Physics: From quantum key distribution to the quantum internet (OSP2025)

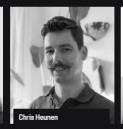
OIST, Okinawa

September 2025

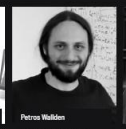
Quantum Software Lab

Faculty

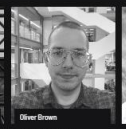

Elham Kashefi
Professor

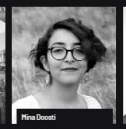

Chris Heunen
Professor

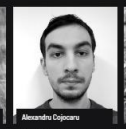

Myrto Arapinis
Reader (Associate Professor)


Petros Wallden
Reader (Associate Professor)


Raul Garcia-Patron Sanchez
Senior Lecturer (Associate Professor)


Oliver Brown
EPCC Chancellor's Fellow

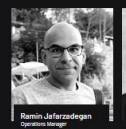

Mina Doosti
Chancellor's Fellow

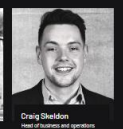

Alexandru Cojocaru
Chancellor's Fellow


Steven Thomson
EPSRC Fellow

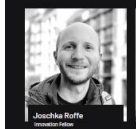

Julien Michel
Professor

Support Team


Ramin Jafarzadegan
Operations Manager


Craig Skeldon
Head of business and operations

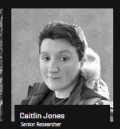
Researchers

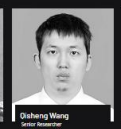

Joschka Roffe
Innovation Fellow

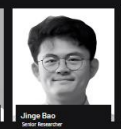

Brian Coyle
Senior Researcher

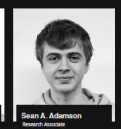

Dominik Leichtle
Senior Researcher

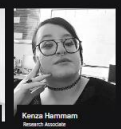

Suchetana Goswami
Senior Researcher

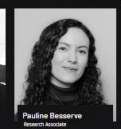

Caitlin Jones
Senior Researcher

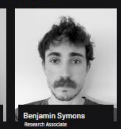

Disheng Wang
Senior Researcher

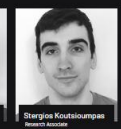

Jinge Bao
Senior Researcher

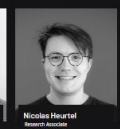

Sean A. Adamson
Research Associate

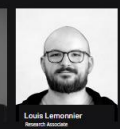

Kenza Hammam
Research Associate

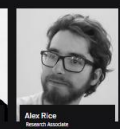

Pauline Besserve
Research Associate

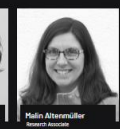

Benjamin Symons
Research Associate


Stergios Koutsioumpas
Research Associate

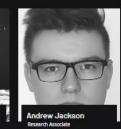

Nicolas Heurtel
Research Associate

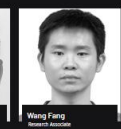

Louis Lemonnier
Research Associate


Alex Rice
Research Associate

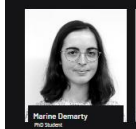

Malin Altenmüller
Research Associate


Kit Battarbee
Research Associate

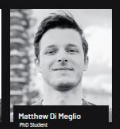

Andrew Jackson
Research Associate

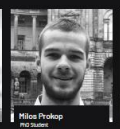

Wang Fang
Research Associate

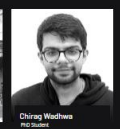

James Mills
PhD Student


Marine Demarty
PhD Student

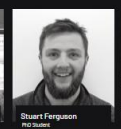

Abbas Poshtvan
PhD Student


Matthew Di Meglio
PhD Student


Milos Prokop
PhD Student


Chirag Wadhwa
PhD Student


Jakub Adamski
PhD Student


Stuart Ferguson
PhD Student

Kengo Hirata
PhD Student

Mateusz Meller
PhD Student

Sean Thrasher
PhD Student

Mario Herrero Gonzalez
PhD Student

Tom Dodd
PhD Student

Adithya Sireesh
PhD Student

Kyle J.S. Campbell
PhD Student

Maria Gragera Garces
PhD Student

Weixi Zhang
PhD Student

Liam Veeder-Sweeney
PhD Student

Laura Lewis
MScR Student

Julia Miklas
Research Intern

Boren Gu
Research Intern

Ben Priestly
Research Intern

Javier Martinez-Cifuentes
Visiting Student

Affiliate Members

Ivan Rungger
Professor

Ross Grassie
QML lead (ISQC)

Majid Safari
Professor, University of Edinburgh

Alessandro Luongo
Research Fellow, National University of Singapore

Eliott Mamon
PhD student,Sorbonne University

Cica Gustiani
Senior Researcher

Harold Olivier
Head of QuantumTech, INRIA

Michael de Oliveira
PhD student,Sorbonne University

Slimane Thabet
PhD student,Sorbonne University

Bo Yang
PhD student,Sorbonne University

Hela Mhiri
Research Intern

James Richings
Applications Consultant

Leo Monbroussou
PhD student,Sorbonne University

Joseph K. L. Lee
Applications Consultant, EPCC

James Perry
Software Architect, EPCC

Paul Hermouet
PhD student,Sorbonne University

Amir Shaikhha
Lecturer, University of Edinburgh

Ava Khamseh
Lecturer, University of Edinburgh

Antonia Mey
Lecturer, University of Edinburgh

Sjoerd Beentjes
Chancellor's Fellow, University of Edinburgh

Michael Bareford
Research Software Engineer,EPCC

Antonio Barbalace Dr
Senior Lecturer, University of Edinburgh

Yuvraj Patel
Lecturer, University of Edinburgh

Luo Mai
Lecturer, University of Edinburgh

Philip J. Camp
Professor , University of Edinburgh

Outline:

- Why quantum cryptography?
- What is quantum cryptography
- Cryptography based on physics: What tools does quantum mechanics give us?
- Quantum information crash course! (Important stuff you need to know)
- Some useful measures

Why do we need a new kind of cryptography?

Quantum Zero Day!

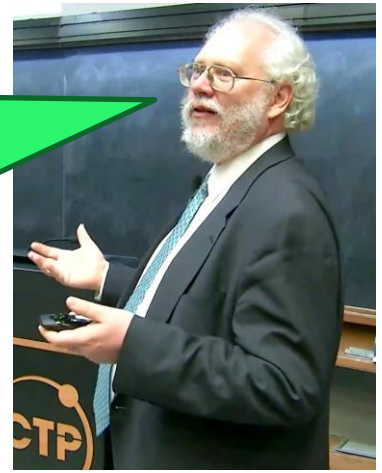
World 1: Panic! No crypto, no security!

World 2: Chill… we still have secure communication

Why can this happen?

Yes, but bro that's exactly the assumption we use for cryptography!
It means your algorithm breaks public key crypto!

I have a quantum algorithm that can factor large numbers efficiently, something we assumed could never be efficient! Yay



Quantum Zero Day!

Why can this happen?

Yes, but bro that's exactly the assumption we use for cryptography!
It means your algorithm breaks public key crypto!

A little history of cryptography: Battle of code makers and code breakers!

Ancient Ciphers (Code Makers and code breaker in even battle)

Caesar Cipher (~50 BCE): Shift letters by 3: simple, but effective in ancient Rome.

Code breakers got smarter and figured it out

Code makers got smarter and made all kinds of hiding and complicated shifts, etc. (Smart code makers thought they won)

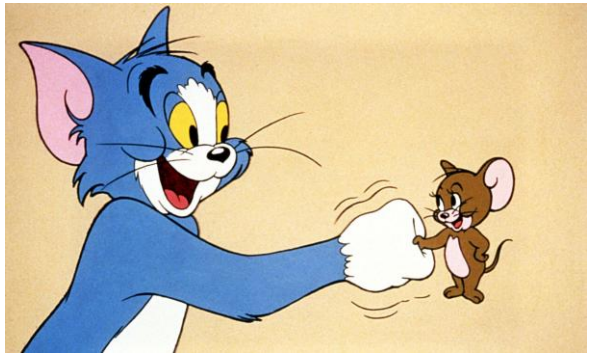
Frequency Analysis (Code Breakers strike back!)

Al-Kindi (~9th century): Cracked substitution ciphers by analyzing letter frequencies: The first general and sophisticated method for cryptanalysis.

World War II: The Crypto Arms Race

Enigma Machine (Code Makers): German military encryption using electromechanical rotors.

Bletchley Park (Code Breakers): Alan Turing and team cracked Enigma, shortening the war by years.



Modern Era: Rise of Mathematical Cryptography

1970s: **Public-key cryptography (RSA, Diffie–Hellman)** changed the game, secrecy without shared keys.

Code Makers win... Until quantum

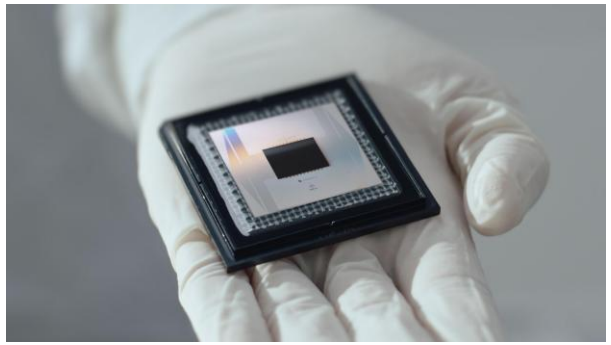
And then code makers had to come up with new ways…

So Quantum Computers… Is it serious?

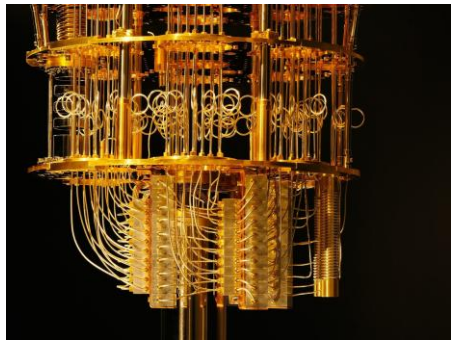
Quantum Computers can solve efficiently factoring and discrete log (and variants of them)

This is what most of public-key cryptography is built on!

And we have the huge progress of quantum hardware today!



Google's Willow, 105 qubits



433-qubit IBM Quantum Osprey processor

Helios 56 qubits

IONQ

XANADU

PsiQuantum

Are we not there yet?

When can this happen?

- There has been many recent progress in Quantum Error Correction, making the algorithms like Shor more possible
- Quantum hardware is getting better every year, hence studying the **practical viability** of quantum threats is becoming more vital

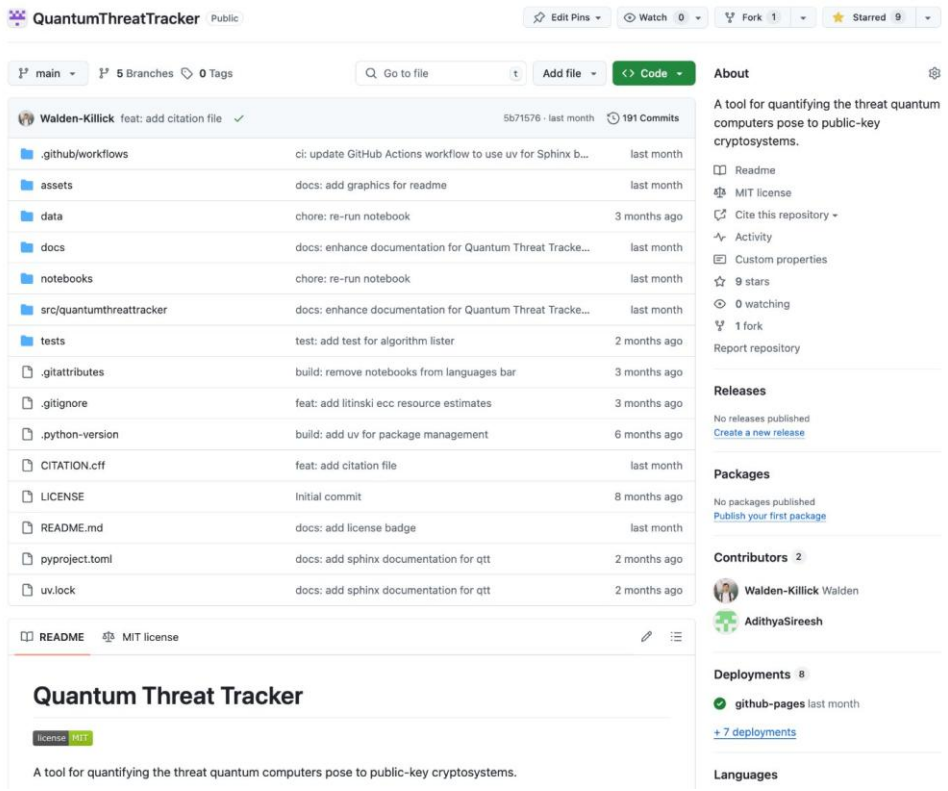
Can we understand when currently deployed cryptographic protocols will become vulnerable to quantum attacks?

There is an open-source project called “Quantum Threat Tracker”

https://github.com/qec-codes/QuantumThreatTracker

Adithya Sireesh

Petros Wallden



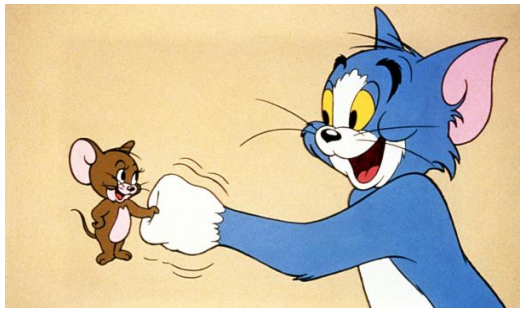
The burden of knowledge!

Now that we know all this, we can't wait till everything breaks! We need to act now!

1. We need to find new ways to maintain security in the quantum world and it's not an easy theoretical problem.
2. Cryptography is not just theoretical; it needs to be deployable and efficient.
3. Even if we find good solutions it will take time to adjust the infrastructure and change the standards, etc.

Which is why everyone started looking for new solutions: Governments, Standard Agencies (NIST), Companies, …

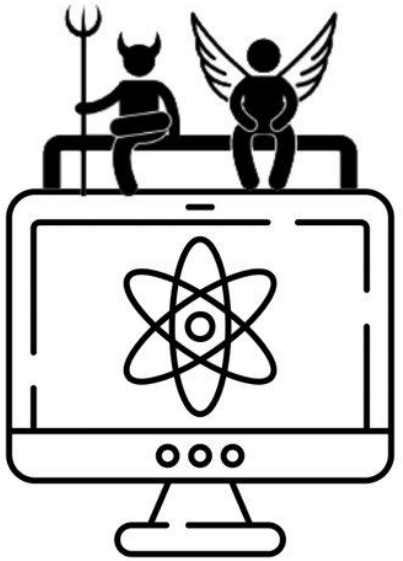
Finding new mathematical assumptions: Problems that are also hard to solve for quantum computers!



Nature breaks and nature makes!

Quantum Cryptography: Cryptography enabled by physics

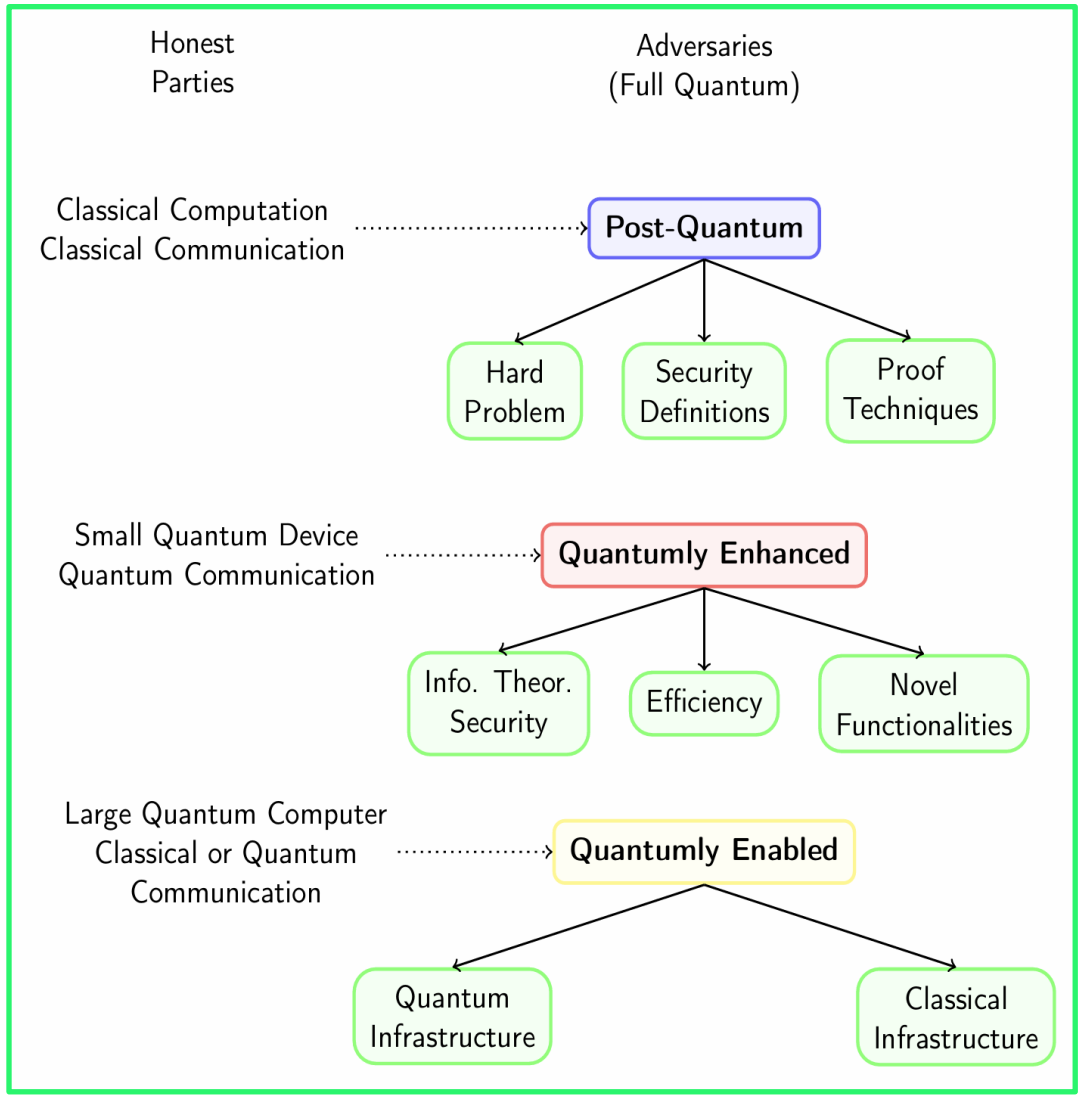
Finding the balance between the power and limitations of a quantum adversary!



Quantum Cryptanalysis & Quantum Cryptography

Quantum systems have very interesting non-classical properties…
Can we use them for cryptography?

The landscape of Quantum Cyber Security



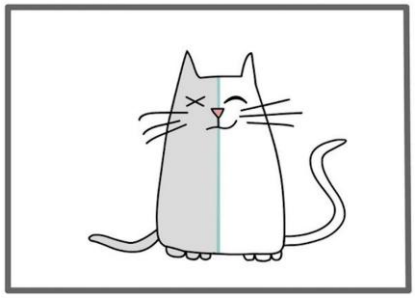
What new things we need in the quantum era?

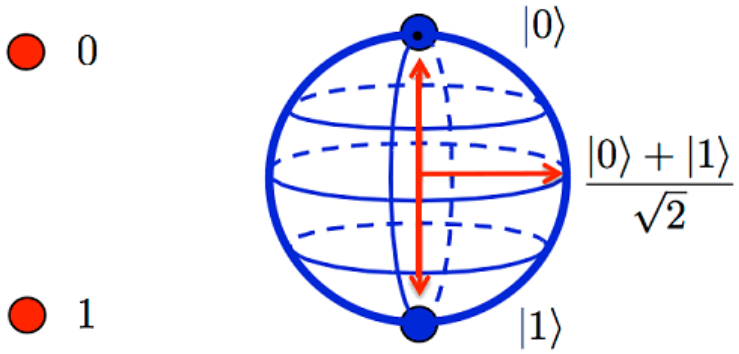
- New definitions (for instance for encryption's security, or unforgeability, etc)
- New primitives
- New protocols
- New quantum algorithms that explores the full power of quantum adversary (for instance Quantum Machine Learning)

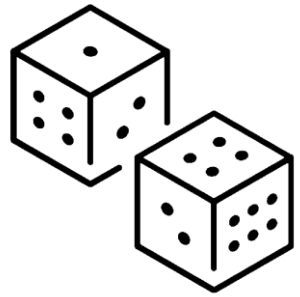
Wallden, Petros, and Elham Kashefi. "Cyber security in the quantum era." *Communications of the ACM* 62.4 (2019): 120-120.

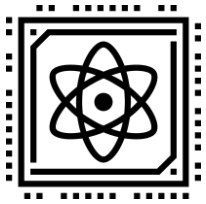
What does nature have to offer? (Properties of Quantum Information)

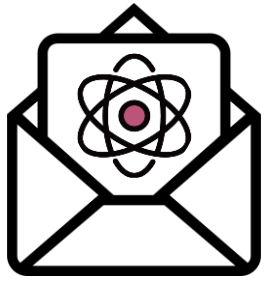
Quantum Superposition and Measurements

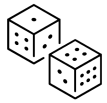




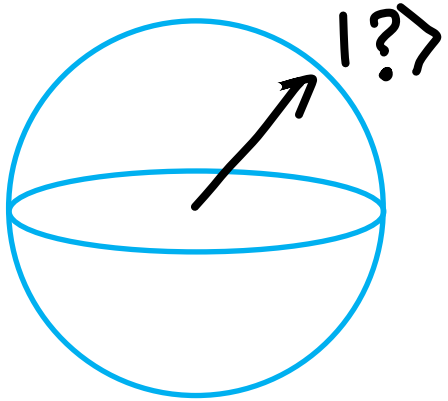


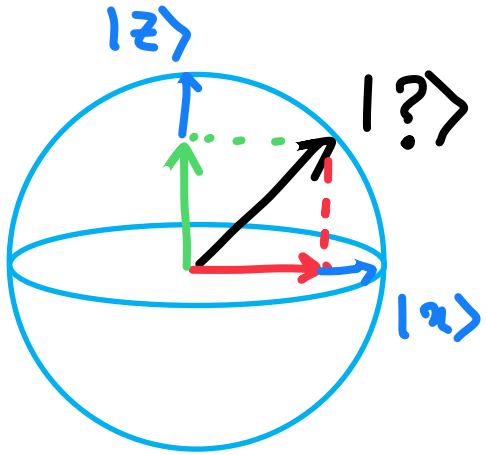






1. Probabilistic
2. Destructive



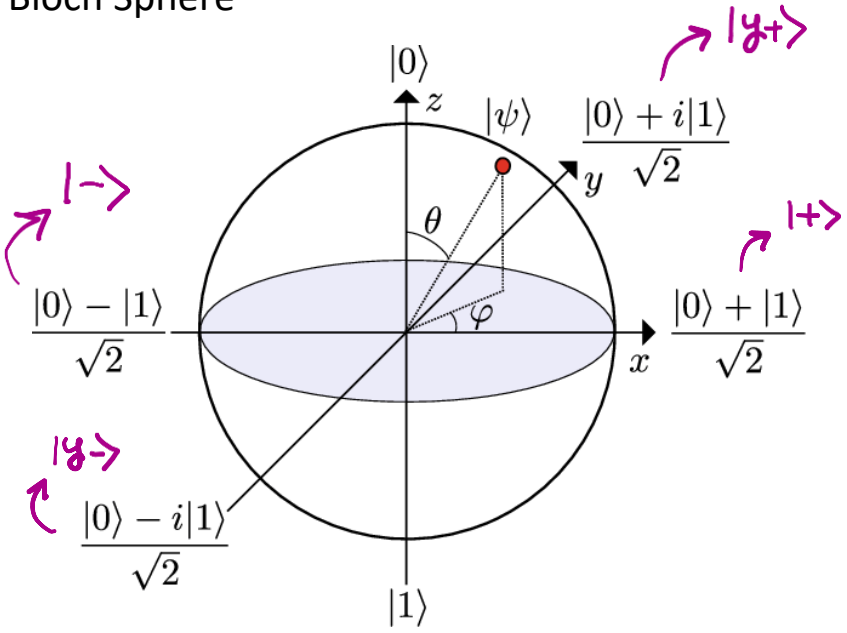


So
Is that good for us
(crypto) or bad for us?

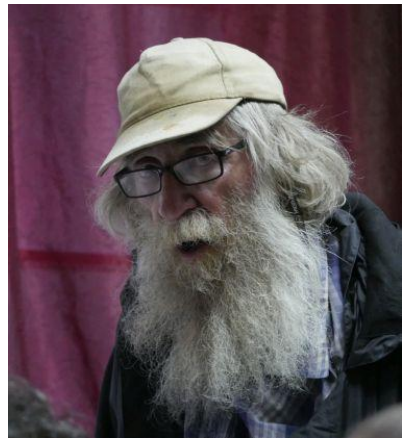
1. Superposition is one of the most important components of most quantum algorithm with speedup (bad)
2. If someone measures a quantum states, it can disturb or destroy it (good/bad)
3. Superposition + Measurement gives us the notion of conjugate basis/coding! (super good)

Conjugate basis

Bloch Sphere



Pauli Matrices: I, X, Y, Z
A basis for qubit operations
Their eigenvectors, are a basis for qubit state



Stephen Wiesner (1942-2021)

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$

↳ in Z basis

$\begin{cases} Z|0\rangle = |0\rangle \\ Z|1\rangle = -|1\rangle \end{cases}$ $\begin{cases} X|+\rangle = |+\rangle \\ X|-\rangle = -|-\rangle \end{cases}$ But $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$

$|\psi\rangle = \alpha'|+\rangle + \beta'|-\rangle$

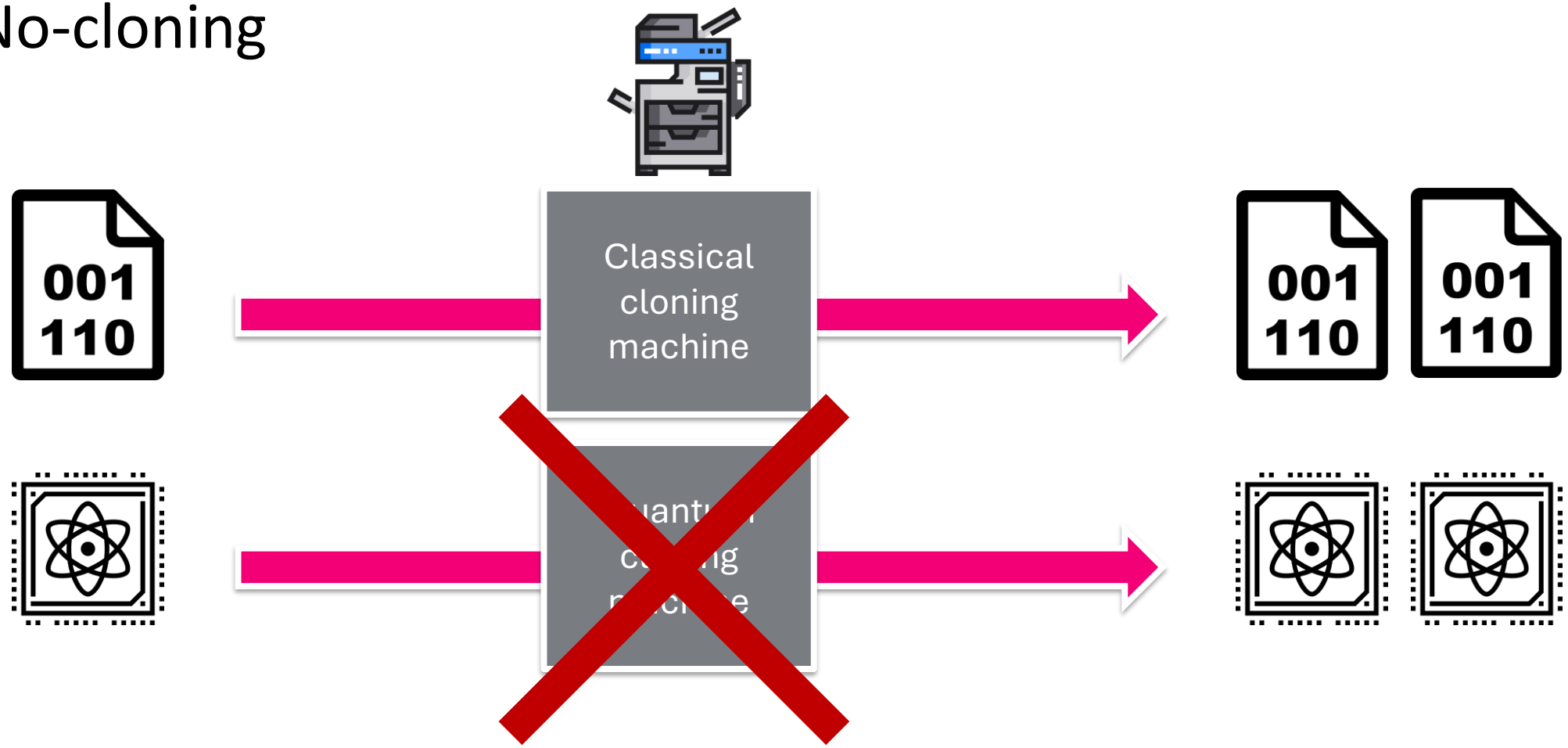
$|\psi\rangle = |+\rangle$ → Measure in X → $P_+ = 1$, $P_- = 0$ ⇝ $|+\rangle$ ✓

→ in Z → $P_0 = 1/2$, $P_1 = 1/2$ ⇝ $|0\rangle/|1\rangle$

Encode in Z basis, Measure in Z basis
Encode in X basis, Measure in X basis
↝ Deterministic!

Encode in X Measure in Z (or the other way) ↝ Uniform Dist

No-cloning



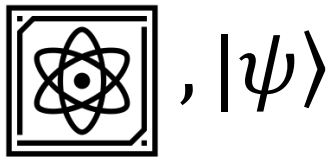
No cloning theorem Discovered in 1982 by Wootters and Zurek (some say 1970 by J. L. Park):
There is no quantum process that can create two perfect copies of an unknown quantum state

Wootters, William K., and Wojciech H. Zurek. "A single quantum cannot be cloned." *Nature* 299.5886 (1982): 802-803.

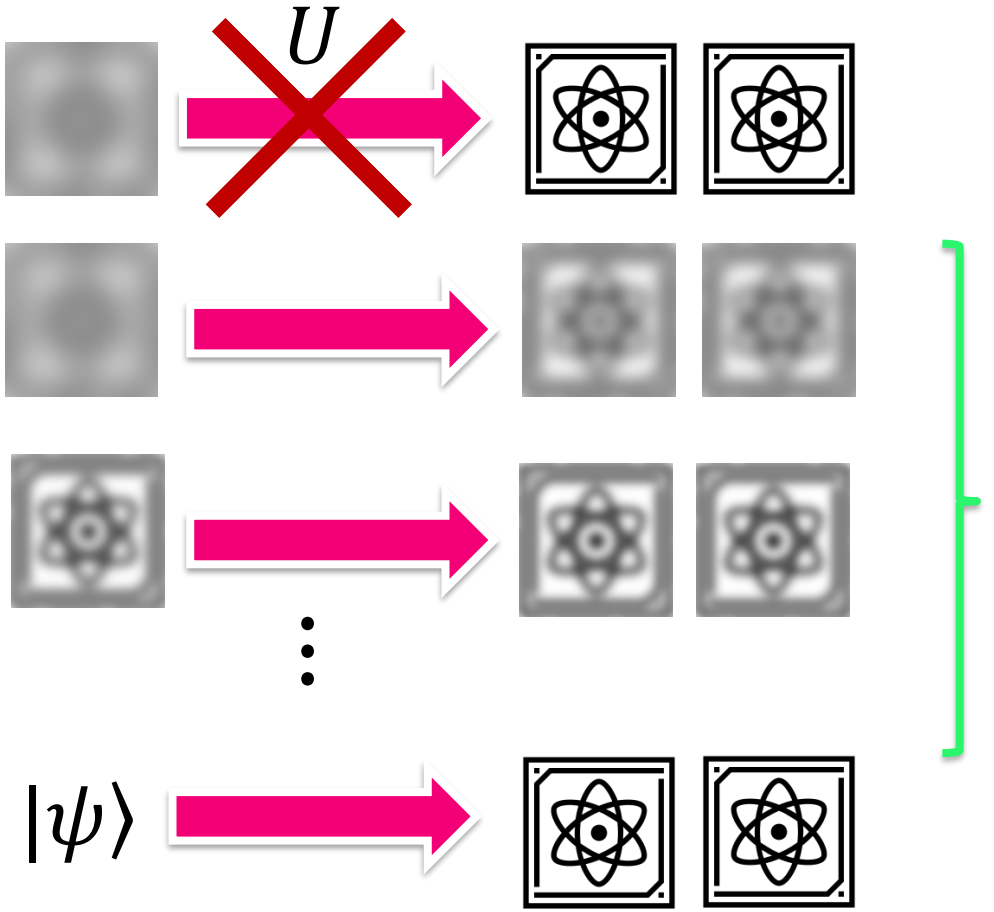
1. Very good! Because it means that an adversary can't copy states and tries to learn the secret we hide in them? (Many quantum crypto protocols rely on no-cloning directly or indirectly)
2. Sometimes this property makes proofs and definitions more difficult (Like transcripts, oracles, …)

Other flavours of cloning and relation to learning

For quantum states

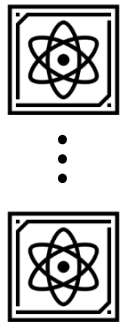


$, |\psi\rangle$



Approximate cloning

Tomography is a notion of learning for quantum states



$|\psi\rangle$

Relation between state estimation (state tomography) and approximate cloning [1,2]

[1] Bruß, D., Ekert, A., & Macchiavello, C. (1998). Optimal universal quantum cloning and state estimation. *Physical review letters*, *81*(12), 2598.

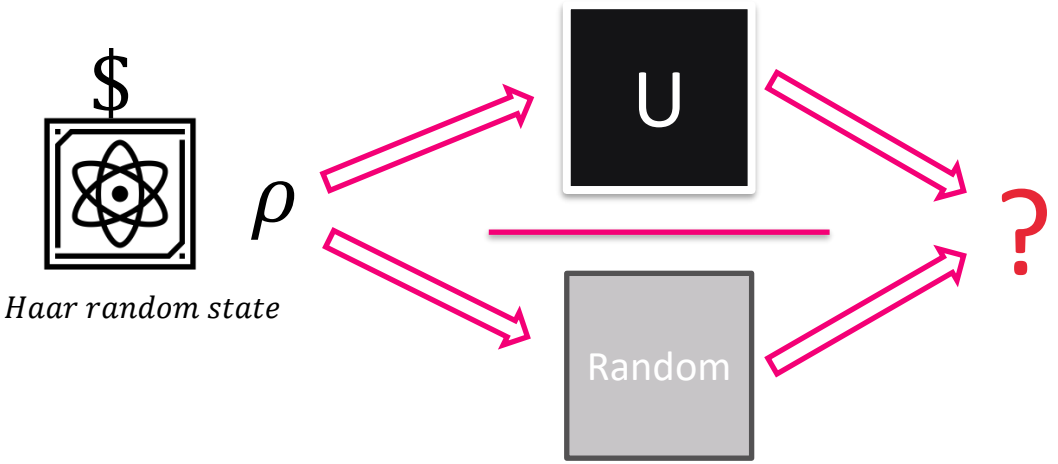
[2] Bruß, Dagmar, et al. "Optimal universal and state-dependent quantum cloning." *Physical Review A* 57.4 (1998): 2368.

From unclonability of quantum states to processes

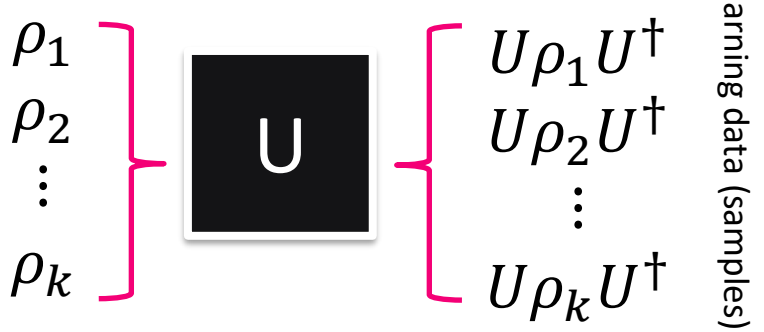
? What does “unclonability of a quantum process” mean?

First attempt [Chiribella et. al. 08]: Two black boxes O_1 and O_2 cannot be perfectly cloned by a single-use.

What about multiple-use?



“Black-box” or “Unknown” Unitary



$$\rho \sim \mathcal{D} \Longrightarrow U\rho U^\dagger$$

$$x_\rho \Longrightarrow f(x_\rho)$$

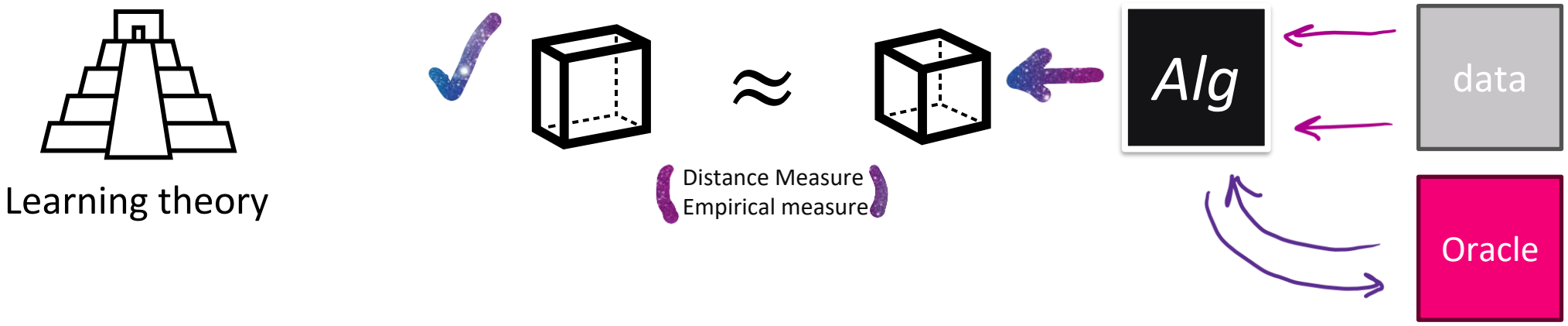
[3] Chiribella G, D’Ariano GM, Perinotti P. Optimal cloning of unitary transformation. Physical review letters. 2008 Oct 30;101(18):180504.

Unclonability and learnability

The extended notion of unclonability can be defined through the notion of “learnability”

***Richard Feynman**: "What I cannot create, I do not understand."*

***Mina/QM:** "What I cannot learn, I do not clone."*



Take home message: Different flavors of unclonability can be defined based on different formal learning models.

Before I tell you other properties, we need to know some more quantum information

Quantum systems beyond qubit

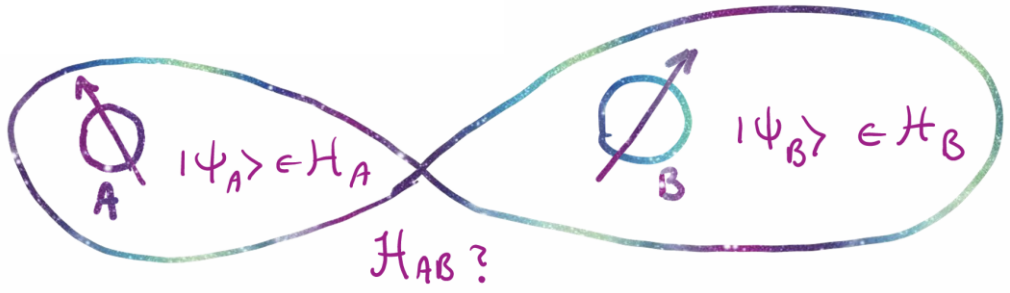
One qubit state lives in a Hilbert space of dimension 2

Higher dimension: You can also have a d-dimensional vector in a d-dimensional Hilbert space $\mathcal{H}^d$

We can also have n qubits The state of a n-qubit system lives in 2^n dimensional Hilbert space ($d = 2^n$).
But if we have n qubit (let's say n=2) they each have their own quantum state as well…
so how do we talk about them?

Composite Systems: Two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ can form a new Hilbert space $\mathcal{H}_{AB}$ which includes vectors that describes both system A and B

$$\dim \mathcal{H}_{AB} = \dim \mathcal{H}_A \times \dim \mathcal{H}_B$$



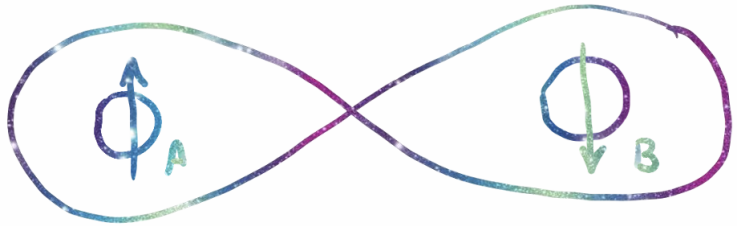
Its basis is built from basis of $\mathcal{H}_A$ and $\mathcal{H}_B$
How? By tensor product

$$\mathcal{H}_A \otimes \mathcal{H}_B = \mathcal{H}_{AB}$$

General quantum states

The vector representation of the states you saw (bra-ket notation) might not be enough to describe the state of all systems!

Why?



$\in \mathcal{H}_{AB}$ → Any vector here!

The other side of the first postulate!

1. Sub-systems

What else is there in $\mathcal{H}_{AB}$?

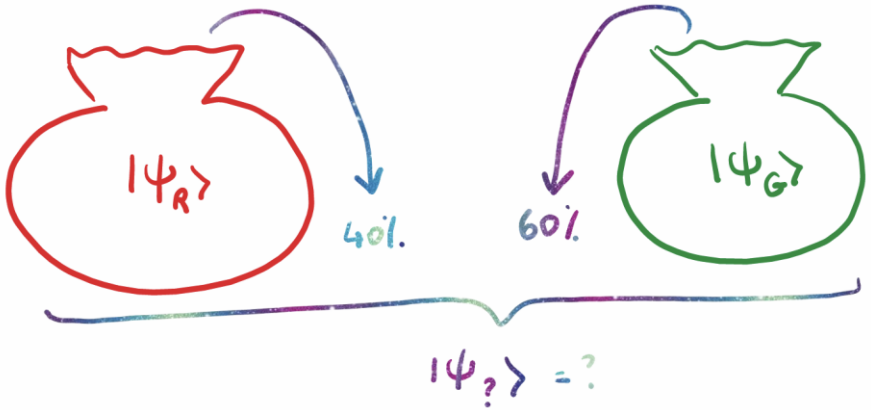
$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left[|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle\right] \in \mathcal{H}_{AB}$$

$|\Psi_A\rangle \neq |\uparrow\rangle$ $|\Psi_A\rangle \neq |\downarrow\rangle$

$|\Psi_B\rangle \neq |\uparrow\rangle$ $|\Psi_B\rangle \neq |\downarrow\rangle$

We need a way to describe the state of subsystems!

2. Ensemble of states



We need a way to describe mixtures!

$$\rho = p_1 |\Psi_R\rangle\langle\Psi_R| + p_2 |\Psi_G\rangle\langle\Psi_G|$$

p_1: 40%, p_2: 60%

General quantum states: Density Matrix Formalism

A density operator is a linear operator $\rho \in \mathcal{L}(\mathcal{H}^d)$: $\mathcal{H}^d \rightarrow \mathcal{H}^d$ with the following properties:

ρ is Hermitian (or self-adjoint) i.e: $\rho = \rho^\dagger$

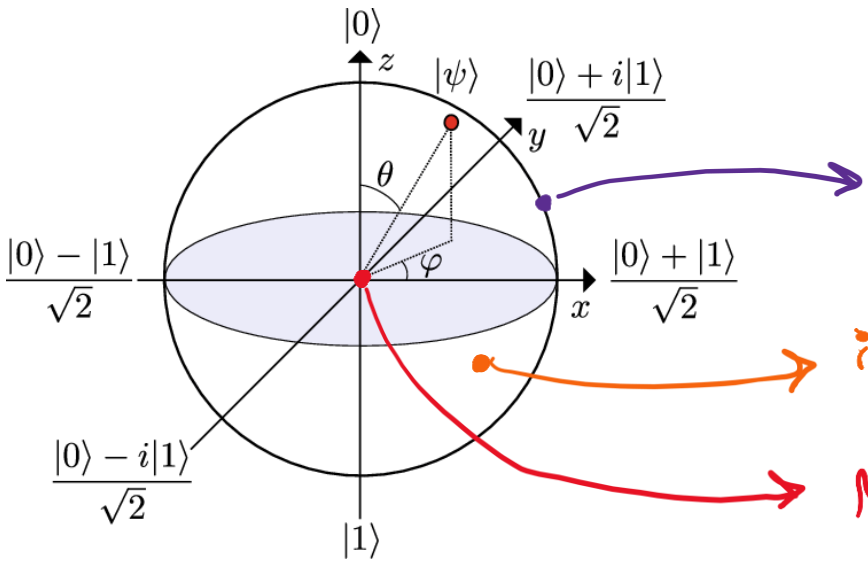
$Tr[\rho] = 1$: ρ is normalised

ρ is positive (or more precisely positive semidefinite): $\rho \geq 0$

↪ Eigenvalues being real, positive and normalised

ρ can be represented by a $d \times d$ matirx

$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \rho = |00\rangle\langle 00| = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}(1\ 0\ 0\ 0) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

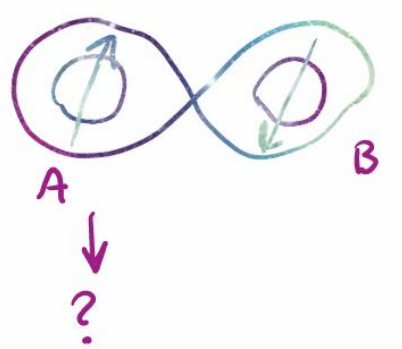


surface : pure states

inside : mixed states

Maximally mixed state ! $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{I}{2}$

Subsystems



Pure

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right] \qquad \rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$$

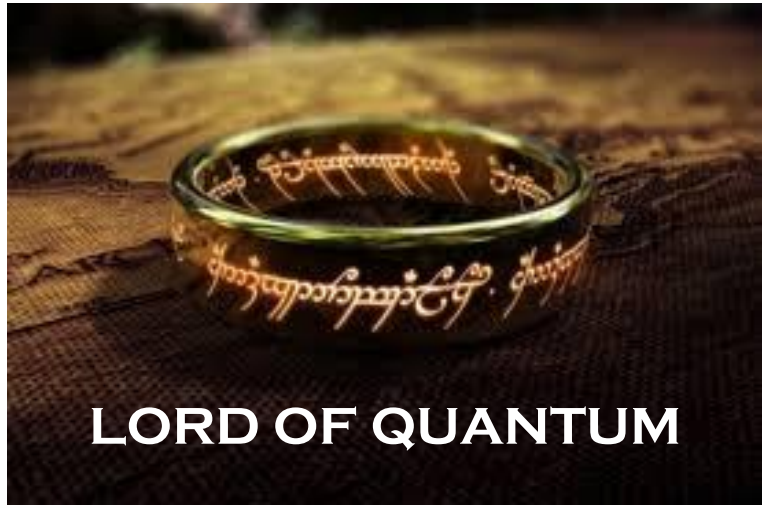
$$\rho_A = \mathrm{Tr}_B\left[|\psi_{AB}\rangle\langle\psi_{AB}|\right] \qquad \rho_B = \mathrm{Tr}_A\left[\rho_{AB}\right] \rightarrow$$ Reduced density matrix

→ Trace out subsystem B!

For a separable state we have: $\rho_{AB} = \rho_A \otimes \rho_B$

This is not the case for entangled states

One density operator to rule them all!



ρ

Pure state

$|\psi\rangle\langle\psi|$

rank 1

Mixed state

$\sum_x p_x |\psi_x\rangle\langle\psi_x|$

Separable state

$|\psi_i\rangle \otimes |\psi_j\rangle$

$|\psi_{ij}\rangle\langle\psi_{ij}|$

Entangled state

$|\psi_{ij}\rangle \neq |\psi_i\rangle \otimes |\psi_j\rangle$

$\rho_i = Tr_j[|\psi_{ij}\rangle\langle\psi_{ij}|]$

What about measurements? (POVMs)

You have seen simple one qubit measurements, which also generalises for observable O

Born Rule:
The measured result for an observable O, on a quantum system $|\psi\rangle$ is given by its eigenvalues λ
The probability of getting a specific eigenvalue λ_i is equal to $\mathrm{p(i)} = \langle\psi|P_i|\psi\rangle$
or more generally for a density matrix ρ is given by $p(i) = Tr[P_i \rho P_i^\dagger]$
Where P_i is the projection onto the eigenspace of O corresponding to λ_i

We can define more general measurements that are non-projective.

POVM (Positive Operator-Valued Measurement) is the most general class of measurements in quantum mechanics

Definition: A POVM on $\mathbb{C}^d$ is a set of positive semidefinite ($M_j \geq 0$) matrices $\{M_j\}_j$ such that:

$$\sum_j M_j = \mathbb{I}_d$$

The probability p_j of obtaining the outcome j when performing the measurement $\{M_j\}_j$ is given by:

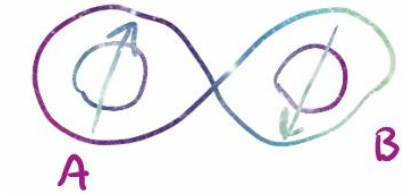
$$p_j = Tr[M_j \rho]$$

Generalisation of Born Rule

POVM Measurements

What can you do with POVMs?

1. You can measure sub-systems:



Let's say you only want to measure qubit A:

$M_0 = |0\rangle\langle 0| \otimes I_B$

$M_1 = |1\rangle\langle 1| \otimes I_B$

2. You can also define other interesting measurement scenarios:

Case 1: It's outcome 1 → $|\psi_1\rangle$ Case 2: It's outcome 2 → $|\psi_2\rangle$ Case 3: I don't know!

$M_1 + M_2 + M_3 = I$

$\alpha\, |\psi_2^\perp\rangle\langle\psi_2^\perp|$ $\beta\, |\psi_1^\perp\rangle\langle\psi_1^\perp|$ $I - M_1 - M_2$

Then we can optimise the parameters to minimize the "I don't know" probability!

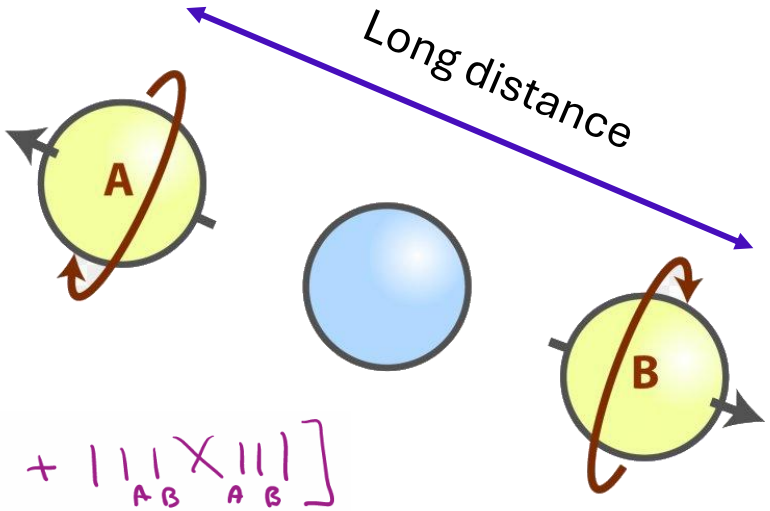
This is a cool problem in QI called "unambiguous state discrimination" problem!

Now the rest of the properties…

Entanglement and its properties

Maximally Entangled states (Like Bell-pair or EPR Pair or GHZ state) have some interesting properties!

1. There are non-local correlations between them. These properties exists in the statistics of the measurements



2. Let's look at the states of the subsystems:

$$\rho_{AB} = |EPR\rangle\langle EPR| = \frac{1}{2}\left[|00\rangle_{AB}\langle 00| + |00\rangle_{AB}\langle 11| + |11\rangle_{AB}\langle 00| + |11\rangle_{AB}\langle 11|\right]$$

$$\rho_A = Tr_B(\rho_{AB}) = \frac{1}{2}\left[|0\rangle\langle 0|_A \langle 0|0\rangle_B + |0\rangle\langle 1|_A \langle 0|1\rangle_B + |1\rangle\langle 0|_A \langle 1|0\rangle_B + |1\rangle\langle 1|_A \langle 1|1\rangle_B\right]$$

$$= \frac{1}{2}\left[|0\rangle\langle 0| + |1\rangle\langle 1|\right]_A$$

$$\rho_B = Tr_A(\rho_{AB}) = \frac{1}{2}\left[|0\rangle\langle 0| + |1\rangle\langle 1|\right]_B$$

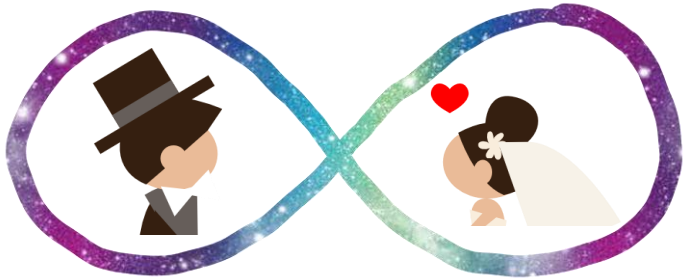
This is the maximally mixed state!
Has no information!

Entanglement and its properties continued…

3. EPR states (Bell-pairs) have always maximal correlation, no matter in which local basis you look:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] = \frac{1}{\sqrt{2}}[|++\rangle + |--\rangle]$$

4. Maximally entangled states are monogamous!



Monogamy of Entanglement: If two qubits are maximally entangled, then they are separable with respect to any third qubit

$$\rho_{AB} = Tr_E(\rho_{ABE}) = |\phi^+\rangle\langle\phi^+|_{AB} \Rightarrow \rho_{ABE} = |\phi^+\rangle\langle\phi^+| \otimes \rho_E$$

By knowing A and B are strongly (quantum) correlated, we know that A and B are not correlated with anything else, like E!

This is very useful in security proofs!

Measuring properties of quantum states

Measures of distances for quantum states

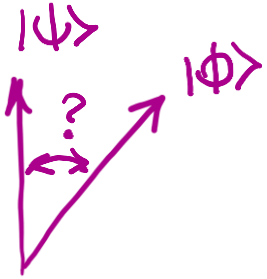
There are different ways to quantify the distance between quantum states:

1. Trace distance: (think of quantum states as distributions) It's a generalisation of total variation distance.

Also a measure of distinguishability of quantum states (we'll see this)

$$d_{tr}(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_1 = \frac{1}{2}Tr\left[\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}\right] = \frac{1}{2}\sum_i^r |\lambda_i|$$

the eigenvalues of ρ−σ, and r is its rank



2. Fidelity: (think of quantum states as vector/matrix), and look at their overlap

Pure States: It depends on the angle between the two vectors:

$$F(|\psi_1\rangle,|\psi_2\rangle) = |\langle\psi_1|\psi_2\rangle|^2$$

One pure State:

$$F(|\psi_1\rangle\langle\psi_1|,\rho_2) = |\langle\psi_1|\rho_2|\psi_1\rangle|$$

Two general states:

$$F(\rho_1,\rho_2) = \left(Tr[\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}]\right)^2$$

Distinguishability of quantum states

Distinguishing game:
Assume a fixed set of possible states $\{|\psi_1\rangle, \cdots, |\psi_n\rangle\}$
Alice chooses one of these states $|\psi_i\rangle$ and sends it to Bob
Challenge: Bob to find the index $i \in \{1, \cdots, n\}$ (Bob can make any measurement)

Theorem: Non-orthogonal pure states cannot be distinguished with certainty

Let's take two non-orthogonal states and any desired POVM measurements, and see why

$\{|\psi\rangle, |\phi\rangle\}$ $\quad \langle\psi|\phi\rangle \neq 0$ $\quad E_1 = M_1 M_1^\dagger$ $\quad E_2 = M_2 M_2^\dagger$

Assume distinguishing is perfect: if $|\psi_i\rangle = |\psi\rangle \rightarrow P_1 = \langle\psi|E_1|\psi\rangle = 1$ $\quad$ if $|\psi_i\rangle = |\phi\rangle$ $\quad P_2 = \langle\phi|E_2|\phi\rangle = 1$

But also $\sum_i E_i = I \Rightarrow \langle\psi|E_2|\psi\rangle = 0$ $\quad$ Let' write $|\psi\rangle = \alpha|\phi\rangle + \beta|\phi^\perp\rangle \rightarrow (\bar{\alpha}\langle\phi| + \bar{\beta}\langle\phi^\perp|)E_2(\alpha|\phi\rangle + \beta|\phi^\perp\rangle) = 0$

$\alpha^2\langle\phi|E_2|\phi\rangle + \beta^2\langle\phi^\perp|E_2|\phi^\perp\rangle = 0 \Rightarrow \alpha^2 = 0$!

Distinguishability of quantum states continued…

In general, for mixed states, there is a limit on how well you can distinguish them

This is a fundamental bound in quantum information known as the "Holevo Bound"

Holevo-Helstrom bound: The optimal probability of distinguishing between two density matrices which have been picked with equal probability, is given by this bound:

$$P_{disc}^{opt} = \frac{1}{2} + \frac{1}{4}\|\rho_1 - \rho_2\|_{tr}$$

The trace-distance between the states

Shannon entropy vs Von Neumann entropy

Shannon Entropy: Average information produced by a random variable:

$$H(X) = -\sum_i p_i \log p_i$$

Binary entropy

$$H(X) := h(p) = -p \log p - (1-p) \log(1-p)$$

$= 0$ iff the random variable is deterministic

$= \log N$ if it comes from a uniform distribution (maximum randomness)

Von Neumann Entropy: measuring uncertainty/randomness of having a specific quantum states

$$S(\rho) = -\sum_{i=1}^{N} \lambda_i \log \lambda_i$$

$= 0$ iff the state is pure (I know with certainty what state I have)

$= \log N$ if it's a maximally mixed state (least pure state)

More classical information theory:

Shannon Entropy: Average information produced by a random variable:

$$H(X) = -\sum_i p_i \log p_i$$

Conditional Entropy: The amount of randomness of variable Y given the variable X:

$$H(Y|X) = H(X,Y) - H(X)$$

Mutual Information: The amount of information obtain from one variable X by observing another one Y:

$$I(X:Y) = H(X) + H(Y) - H(X,Y)$$

Relative Entropy: Measure of how one prob distribution P(x) differs from another Q(xi):

$$H(P||Q) = \sum_i P(x_i) \log\left(\frac{P(x_i)}{Q(x_i)}\right)$$

Everything I just told you has a consequence!
Don’t believe me?
See the rest of the lectures!

Quantum Software Lab

THE UNIVERSITY of EDINBURGH informatics

Quantum Cryptography 102:

Secure Communication Using Quantum Information

Mina Doosti

Okinawa School in Physics: From quantum key distribution to the quantum internet (OSP2025)

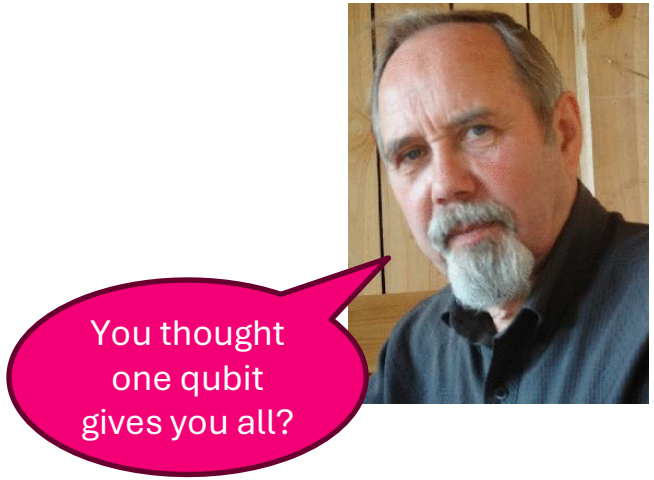
OIST, Okinawa

September 2025

Outline:

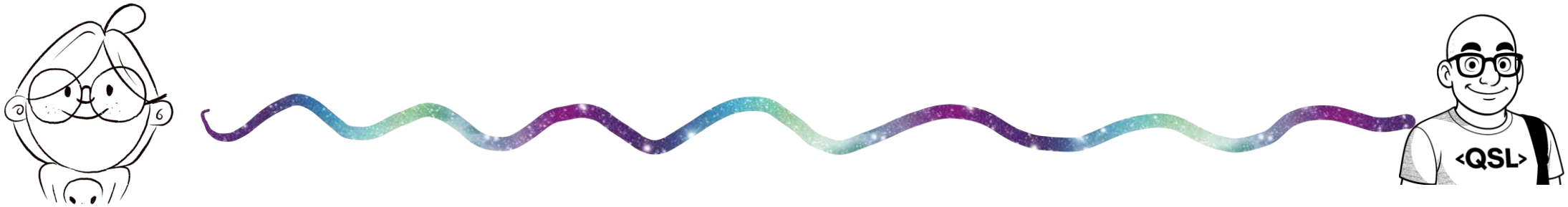
- Communication with quantum information
- QKD
- Simple proofs of QKD
- Ideas for modern proofs of QKD
- Other QKD protocols

Superdense coding



Remember the distinguishing problem?
One consequence of that is that it is impossible to extract more than one classical bit of information from a single qubit. (Holevo Bound)

But what if Alice and Bob share an EPR pair?



Alice can perform an operation ONLY on her own qubit and then send it to Bob to convey two bits of information!

How?

That's what we do in Teleportation too!

QKD

Types of security:

1. Computational Security: Security guaranteed when adversaries do not have the computational power/time to "break" it

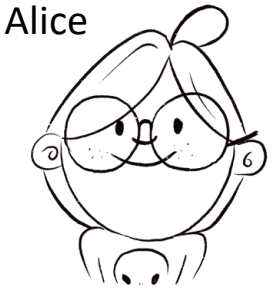
a) Usually relies on assuming that certain problems are hard to solve (need exponential time)
b) Security may break if better (classical) algorithms are found, or new devices (quantum computers), or much faster (classical) computers, or given sufficient time.
c) Security could break retrospectively (revealing past secrets)

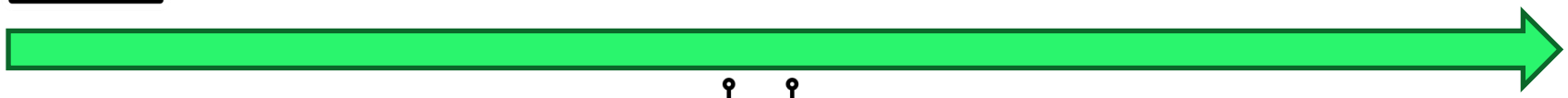
2. Information Theoretic Security (ITS): Cannot be broken irrespective of the computational power of the adversary ("Perfect Security"): The adversary is unbounded

One-Time Pad (OTP)

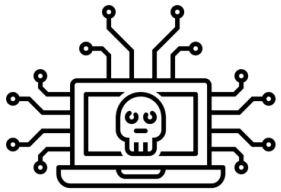
Before we go to QKD, let's look at a famous classical protocol called OTP!

Alice





Bob



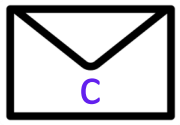
Eve

m = "OIST"

=01001111010010010101001101010100

k = 10001010100001010100101010101010

1. Random
2. As long as the message



$= m \oplus k$

c = 110…010

$$Dec_k(c) = c \oplus k = m \oplus k \oplus k = m$$

k

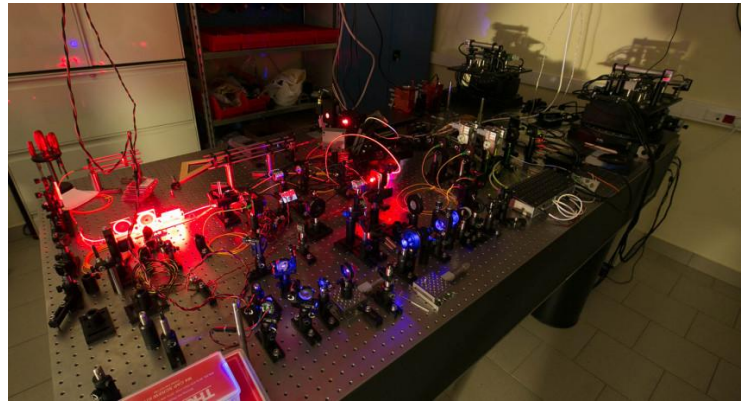
c leaks no information of m (doesn't matter what Eve does)
The protocol is information theoretically secure

Do you see any problems?

How do they share the key?

Quantum Key Distribution (QKD)

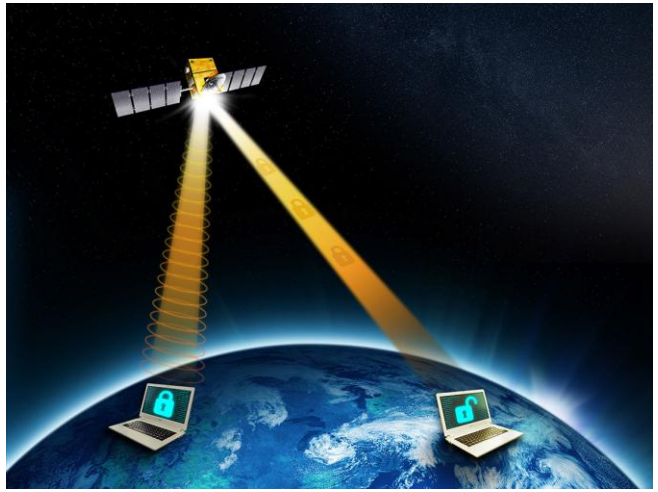
What if I told you can share long keys relying on quantum mechanics with an information theoretic security against any quantum adversary?



QKD doesn't need full quantum computers (just small/minimal) quantum devices

QKD is available today.

You can even do QKD with satellite today!



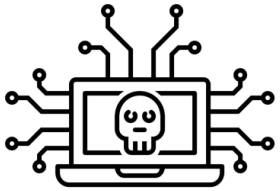
QKD has forward secrecy

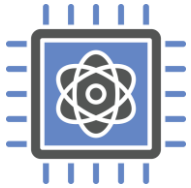
Ingredients of QKD:

What do we need to do (the simplest version of) QKD?

1. Quantum Mechanics!
2. Ability to prepare qubit states $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$
3. Ability to measure qubits in Z and X basis
4. A quantum (insecure) channel to send qubits
5. A classical authenticated channel (but also insecure)

Remember here we trust the devices of Alice and Bob's labs
There are protocols (device independent) where you don't need to assume that! (Artur's lectures)





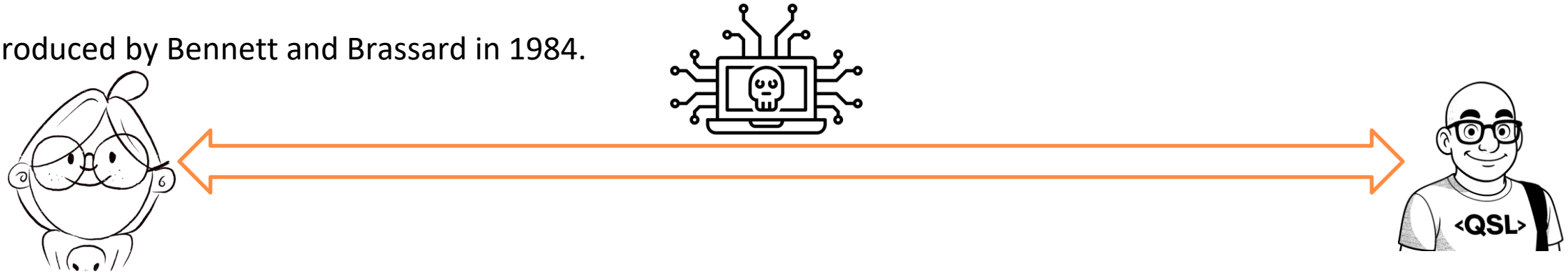
Eve can perform any quantum operation and measurement they want and have unbounded computational power

So how does it work?

Remember conjugate coding?

First QKD: BB84 Protocol

Introduced by Bennett and Brassard in 1984.



1. Alice picks random pairs of bits: $\{(a_i, x_i)\}$
   x_i chooses the basis: if $x_i = 0$ it's Z basis or $\{|0\rangle, |1\rangle\}$, if $x_i = 1$ it's Z basis or $\{|+\rangle, |-\rangle\}$
   a_i chooses the state within each basis: if $a_i = 0$ it's $\{|0\rangle, |+\rangle\}$, if $a_i = 1$ it's $\{|1\rangle, |-\rangle\}$
2. Alice sends the stream of states to Bob according to above encoding.

3. Bob for each qubit i, picks a random bit y_i that selects a random basis (if 0: Z basis, if 1: X basis), and measure each qubit in y_i basis separately and records b_i
   Bob has pairs $\{(b_i, y_i)\}$
4. Alice/Bob announce ONLY the basis x_i and y_i over the classical authenticated channel
5. They only keep the bits (a_i and b_i), in the positions that $x_i = y_i$. These bits will be the shared raw key
6. Parameter Estimation
7. They do some classical post-processing to get the very secure key from the raw key.

Let’s see an example:

Key value a_i	0	0	1	1	0
Encoding (basis) x_i	0	1	1	0	1
BB84 state sent by Alice	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$
Bob’s Measurement basis y_i	0	0	1	1	0
Bob’s measurement outcome b_i	0	1	1	1	1
Raw key					

Let’s see an example:

Key value a_i	0	0	1	1	0
Encoding (basis) x_i	0	1	1	0	1
BB84 state sent by Alice	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$
Bob’s Measurement basis y_i	0	0	1	1	0
Bob’s measurement outcome b_i	0	1	1	1	1
Raw key	0	✗	1	✗	✗

Why is it correct?

Because whenever the basis match, the measurement outcome is deterministic, Alice and Bob both get the same value!

Why doesn’t Eve know it?

Eve knows the bases too, but not the values (values and bases are independent): 50-50 probability

Parameter Estimation Phase

Alice and Bob do some check, to see if there's an Eve, this is called "Parameter Estimation":

They choose fraction f of the raw key randomly and announce the bits itself: a_i, b_i to estimate the correlation of their strings called Quantum-Bit Error Rate (QBER)
This can bound the correlation Eve might have too.

$$QBER = \frac{e_t}{t}$$

e_t: # errors in the test bits

t: # bits revealed for test

If QBER ≤ threshold: proceed to classical post-processing
If QBER > threshold: abort the protocol, there is too much noise/eavesdropping

This threshold for BB84 is usually 11%.

Why is it secure? (some intuitions)

What Eve can do?

1. Measure the qubits on her own and tries to guess the bits

BUT: Measurements affect the quantum state, and we can detect amount of eavesdropping and abort if QBER is high

2. Copy the qubits, keep a copy and use it later to reveal the bits and learn the key

BUT: no-cloning prevents that!
Even if Eve tries to do approximate cloning, the QBER will be the same

3. Measures the qubit, but send another one instead so it's not detected: Intercept-resend Attack

Still the success probability is low: Analysing this attack gives a QBER of 25%

Intercept-resend attack analysis

Eve does this:

1. **Eve** intercepts each qubit sent by Alice.
2. She **measures** it in a randomly chosen basis (either Z or X, just like BB84).
3. Then she **resends** a new qubit to Bob, prepared in the state she observed.

- Eve chooses the **correct basis** with probability ½ : In this case, Bob receives the correct state.
- Eve chooses the **wrong basis** with probability ½.

-- Her measurement gives a **random outcome**, she sends a random BB84 state, but when Bob's measure there's still a ½ probability to get the correct outcome

$$P_{win}^{Eve} = \Pr[\text{correct basis}] \times 1 + \Pr[\text{wrong basis}] \times \Pr[\text{Bob gets correct outcome}]$$

↳ for each bit

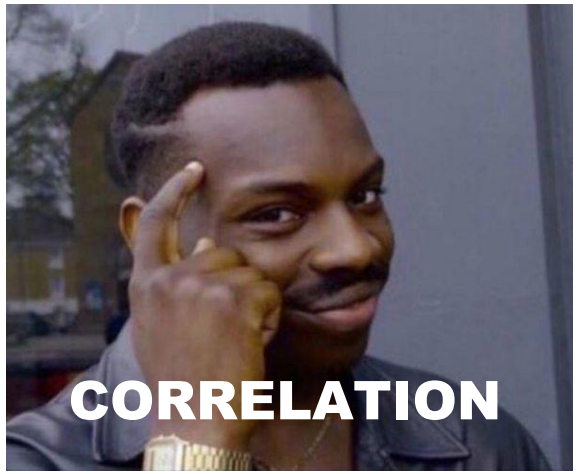
$$= \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}$$

Or in another words, they can detect with 25% probability, QBER = 25%

But should we go over all possible attack scenarios for Eve?

There should be a better way!

What was the key concept here between the bits of Alice, Bob and Eve?



Proof of QKD

Alice: bit-string A; Bob: bit-string B Eve: bit-string E for any attack she wants to do

We want to quantify correlations. We want:

$$I(A:B) > I(A:E)$$

Mutual information

So, if QBER low then A,B are more correlated than A,E or B,E.
And Alice and Bob can increase their advantage in the final post-processing

The classical post-processing steps:

Information Reconciliation (IR): Exchange information (classical error-correcting codes) to make A' = B'

Privacy Amplification (PA): Distil shorter key completely secret from Eve (use universal hash functions to amplify privacy)

Proof of QKD: continued

We are going to bound the error by a quantity called secret key rate, R which will be:

$$R_{\mathrm{BB84}} = \frac{1}{2}\left(1 - h(e_b) - h(e_p)\right)$$

Average error in the Z basis

Average error in the X basis

Note: I made a few simplification assumptions here, the actual expression is more complicated (ideal detection, post-processing, asymptotic limit)

If we assume symmetric error: the errors in different bases equal and equal to the QBER ($e_b = e_p = D$) we get:

$$R_{\mathrm{BB84}} = \frac{1}{2}\left(1 - 2h(D)\right)$$

What's the largest D that protocol doesn't abort? $R \leq 0 \Rightarrow h(D) = \frac{1}{2} \Rightarrow D = 0.11 \rightarrow 11\%$

Proof of QKD: continued

To get this expression we use mutual information and Holevo bound:

$$R_{\mathrm{BB84}} = \frac{1}{2}\left(1 - h(e_b) - h(e_p)\right)$$

$$R = \frac{1}{2}\left(I(A:B) - S(A:E)\right)$$

Eve has a quantum state and a classical random variable, we need to construct quantum-classical ensembles
Then quantify how much information is accessible through such quantum-classical states

$$I_{acc}(F) \leq \chi(F)$$ Holevo quantity

The maximum amount of information extractable from a single qubit!

The full chain of bounds:

$$S(A:E) \leq I_{acc}(F) \leq \chi(F) = S(\sigma_E) - \frac{1}{2}(h(e_b) + h(e_p))$$

Proof of QKD: shortcomings

This is an old proof, first really formal security proof of QKD
But it has potential issues:

1. We made some assumptions to simplify (perfect measurement and preparation)
2. The proof doesn't exactly work in finite-key regime (asymptotic relations)
3. It's not composable (composability is a nice cryptographic property, especially important for QKD)
4. We consider the best attack to be i.i.d, one can also consider collective (coherent) attacks
5. There are some physical attacks we didn't take into account (lossy channel, dark count, double-splitting)

There are more novel proofs of QKD, that solve most of these problems

More QKD Protocols

There are several QKD Protocols: Six-state protocol, E91 protocol, B92 protocol, …

There are also QKD protocols that you don't need to trust the devices (Device-independent protocols)

We want to look at BBM92 protocol (by Bennett, Brassard, Mermin): Also known as Entangled-based QKD

Alice and Bob share n copies of maximally entangled states (EPR pairs)

1. Alice measures her qubits in a random basis x_i
2. She obtains measurement outcome a_i $\begin{cases} =0 & |0\rangle, |+\rangle \\ =1 & |1\rangle, |-\rangle \end{cases}$
3. Stores the pairs $\{(x_i, a_i)\}$

1. Bob measures her qubits in a random basis y_i
2. He obtains measurement outcome b_i
3. Stores the pairs $\{(y_i, b_i)\}$

The rest is like BB84…

BB92: Intuition and ideas

Remember properties of maximally entangled states?

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle_A |0\rangle_B + |1\rangle_A |1_B\rangle \right] = \frac{1}{\sqrt{2}}\left[|+\rangle_A |+\rangle_B + |-\rangle_A |-\rangle_B \right]$$

The maximally entangled state produces the same correlation as conjugate encoding-decoding

Also, monogamy of entanglement ensures that Eve can't get also maximally entangled with Bob

How does this help with the security proof of QKD?

From the point of view of an adversary, the protocol's data and information is indistinguishable to normal BB84

So to do the proof of BB84, we first prove the security of BB92, and then we make a reduction to BB84

But this sounds more complicated… how is this better for the proof?

Composable security and Abstract Cryptography

There are different frameworks for doing crypto proofs:

1. Game-based framework
2. Composable framework: (composable: if you combine the QKD with something else, it remains secure. You don't need to redo the proof!)

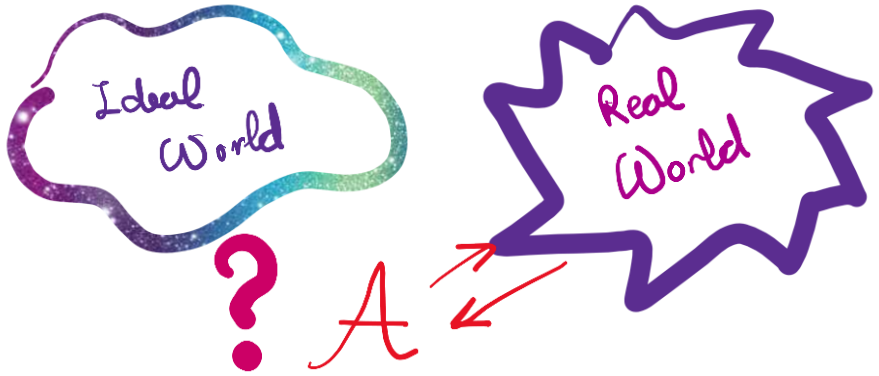
One can use Abstract Cryptography (AC) or Universal Composability (UC): AC is nicer in quantum

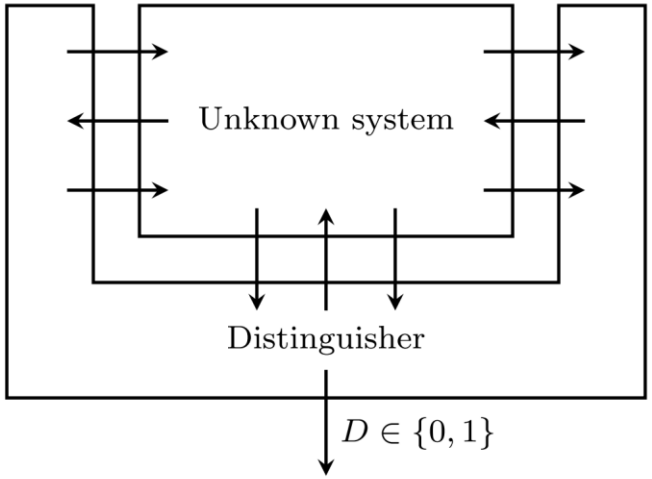
Innovations in Computer Science 2011

Abstract Cryptography

Ueli Maurer[1] Renato Renner[2]
[1]Department of Computer Science, ETH Zurich, Switzerland
[2]Institute for Theoretical Physics, ETH Zurich, Switzerland
maurer@inf.ethz.ch renner@phys.ethz.ch

Abstract: In the spirit of algebraic abstraction, this paper advocates the definition and use of higher levels of abstraction in cryptography (and beyond). If contrasted with the standard bottom-up approach to defining models of computation, algorithms, complexity, efficiency, and then security of cryptographic schemes, our approach is top-down and axiomatic, where lower abstraction levels inherit the definitions and theorems (e.g. a composition theorem) from the higher level, but the definition or concretization of low levels is not required for proving theorems at the higher levels. The goal is to strive for simpler definitions, higher generality of results, simpler proofs, improved elegance, possibly better didactic suitability, and to derive new insights from the abstract viewpoint.





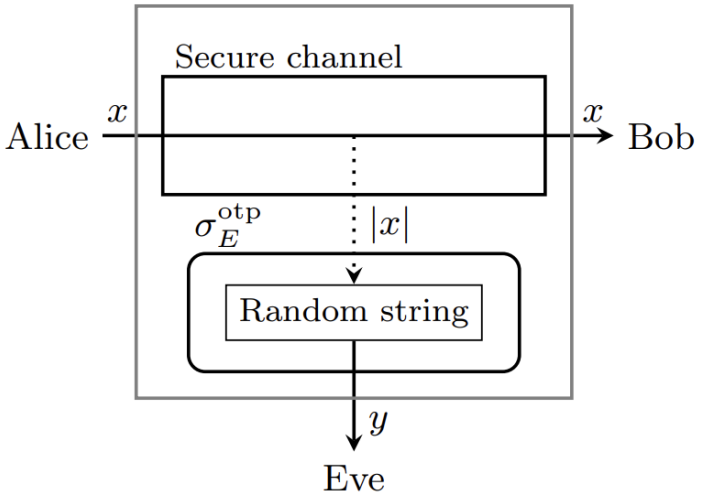
A bit more formal…

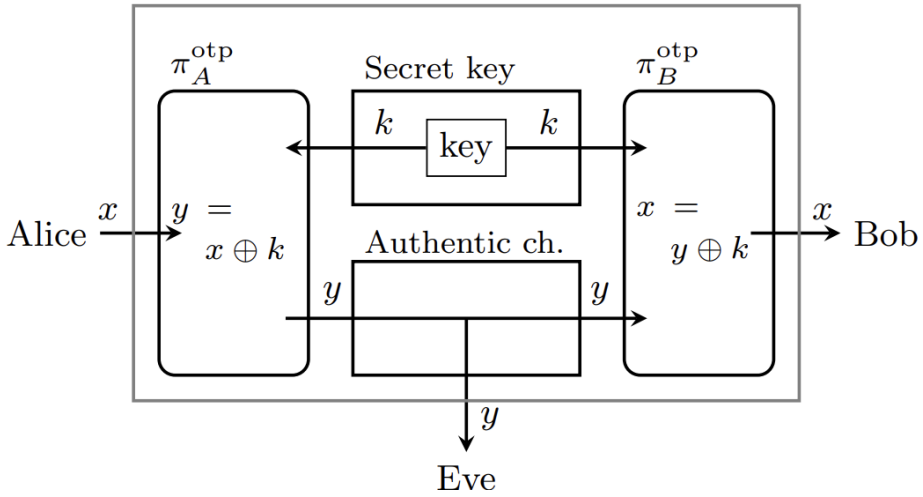
In AC, these ideal/real boxes that abstract the functionality of a protocol are called Resources
Security in AC is formalized via resource construction:

We say that a protocol π, ϵ-constructs an ideal resource $\mathcal{S}$ from a real resource (or collection of resources) $\mathcal{R}$, written as:

$$\pi\mathcal{R} \approx_\epsilon \mathcal{S}$$

Let's look at OTP as a simple example





Want to learn more AC?

Someone told me in the break that there was recently this summer school, where Maurer gave a nice lecture about AC, so if you want to learn more, you can hear it from the source ;)

https://swissmaprs.ch/videos/quantum-key-distribution-summer-school/

Composable proofs of QKD

- They do the proof based on entropic-uncertainty inequalities
- That will allow them to use composable security framework
- Some specific entropic quantity allows them to go around the asymptotic problem and have a proof for finite-key-size regime
- They really capture all the assumptions they can (nothing has been put under the rug!)

A largely self-contained and complete security proof for quantum key distribution

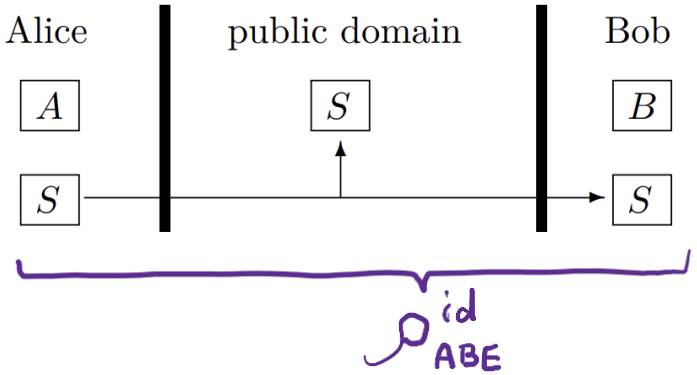
Marco Tomamichel[1] and Anthony Leverrier[2]

[1]Centre for Quantum Software and Information, University of Technology Sydney, Australia
[2]Inria Paris, France

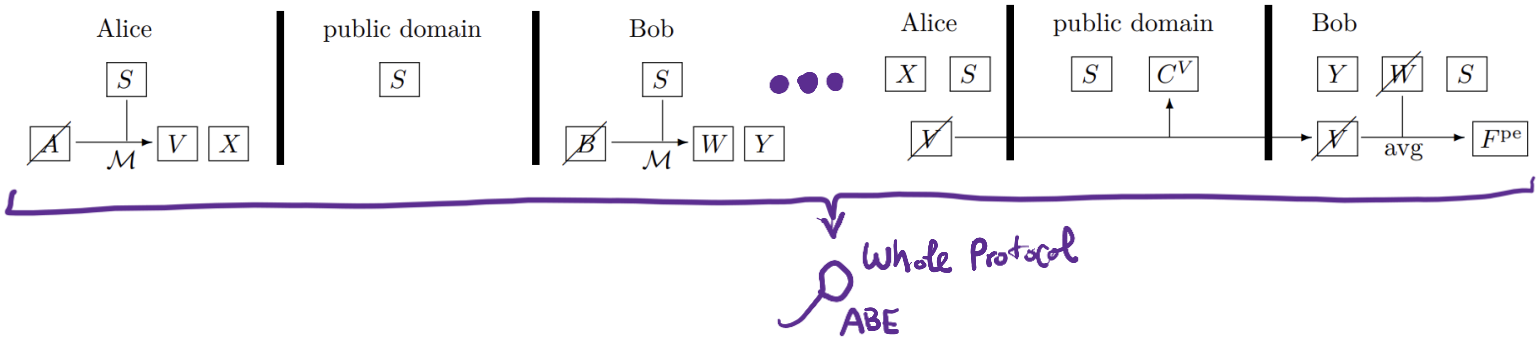
Published: 2017-07-14, volume 1, page 14
Eprint: arXiv:1506.08458v3
Doi: https://doi.org/10.22331/q-2017-07-14-14
Citation: Quantum 1, 14 (2017).

You start with the entanglement-based protocol (We do the AC proof here)

Then you show the prepare-and-send version "reduces" to the entanglement one (it's basically statistically indistinguishable)



≈



A note on the “Authentication”

Quantum Key Distribution (QKD) and Quantum Cryptography (QC)

HOME > CYBERSECURITY > QUANTUM KEY DISTRIBUTION (QKD) AND QUANTUM CRYPTOGRAPHY QC

Synopsis
NSA continues to evaluate the usage of cryptography solutions to secure the transmission of data in National Security Systems. NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations below are overcome.

What are Quantum Key Distribution (QKD) and Quantum Cryptography (QC)?
Quantum key distribution utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology. Quantum cryptography uses the same physics principles and similar technology to communicate over a dedicated communications link. Published theories suggest that physics allows QKD or QC to detect the presence of an eavesdropper, a feature not provided in standard cryptography.

Quantum-resistant algorithms are implemented on existing platforms and derive their security through mathematical complexity. These algorithms used in cryptographic protocols provide the means for assuring the confidentiality, integrity, and authentication of a transmission—even against a potential future quantum computer. The National Institute of Standards and Technology (NIST) is presently conducting a rigorous selection process to identify quantum-resistant (or post-quantum) algorithms for standardization[1]. Once NIST completes its selection process, NSA will issue updated guidance through CNSSP-15.

Understanding the QKD/QC story
Quantum key distribution and Quantum cryptography vendors—and the media—occasionally state bold claims based on theory—e.g., that this technology offers "guaranteed" security based on the laws of physics. Communications needs and security requirements physically conflict in the use of QKD/QC, and the engineering required to balance these fundamental issues has extremely low tolerance for error. Thus, security of QKD and QC is highly implementation-dependent rather than assured by laws of physics. Although we refer to QKD only to simplify discussion below, similar statements can be made for QC.

Technical limitations
1. **Quantum key distribution is only a partial solution.** QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e. entity source authentication). QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or preplaced keys to provide that authentication. Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better understood risk profile.

- Authentication is very important!
- It’s not just QKD, everything needs authentication!
- Authentication comes with a price!

The debate over QKD: A rebuttal to the NSA’s objections

Renato Renner[1,2] and Ramona Wolf[1,2]

[1]Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland
[2]Quantum Center, ETH Zurich, 8093 Zurich, Switzerland

A recent publication by the NSA assessing the usability of quantum cryptography has generated significant attention, concluding that this technology is not recommended for use. Here, we reply to this criticism and argue that some of the points raised are unjustified, whereas others are problematic now but can be expected to be resolved in the foreseeable future.

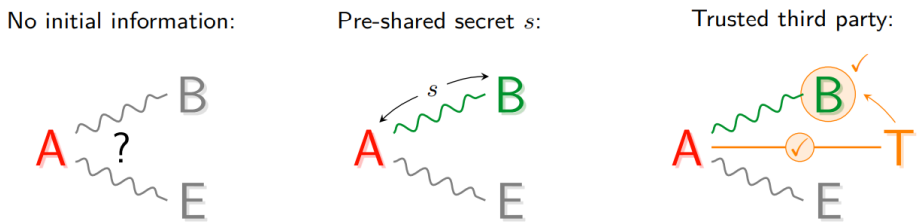


Figure 1: **Authentication.** Without any initial information about Bob (B), there is no way for Alice (A) to distinguish whether a message she receives is from him or from an adversary Eve (E) who pretends to be B (left figure). Any authentication scheme (classical or quantum) must rely on something that breaks the symmetry between B and E (from A’s viewpoint). This could be a pre-shared secret s held by A and B (middle figure). Alternatively, A could rely on a trusted third party (T) who can distinguish B from E, which requires some initial authenticated connection between A and T (right figure).

Authentication for QKD

There are several ways to do Authentication for QKD (and other quantum protocols):

1. Using secret-key methods: Message Authentication Codes (MACs)
   - You need a share key (but small) 😐
   - You only need it once! If you do QKD once you can use part of the key for next authentication ✓
   - You can still get IT security ✓
2. Using public-key methods: Signature schemes
   - No need for extra key ✓
   - But the security is computational, so it will reduce the security of QKD to computational as well! (authentication will be the weak link) 😐
3. Having a trusted third party
4. Using alternative assumptions! We'll see that later 😊

And now you know QKD!

Thank you!