



***Quantum cryptography and its
impact on the future of digital
society***

Dr. Luis Adrián Lizama Pérez
Twitter: @luislizama

The background of the slide is a light blue color with a subtle pattern of binary code (0s and 1s). On the left side, there is a vertical strip with a darker blue background, featuring white circuit traces and components, resembling a microchip or a network diagram. The main title 'Presentation plan' is written in a bold, red, serif font at the top right.

Presentation plan

- 1. Preliminaries**
 - Optimization
 - Modeling
 - Sensing
- 2. Post-quantum cryptography**
- 3. Communication**
- 4. Critical Path**



The private Eye

Brian K. Vaughan, Marcos Martin & Muntsa Vicente



1. Preliminaries to Quantum Computation



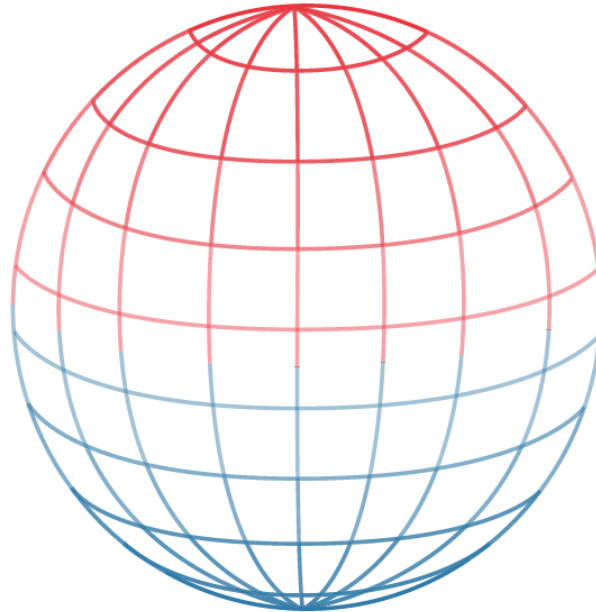
Quantum Computation

Bit

Qubit

0

0



1

1

Quantum Computation

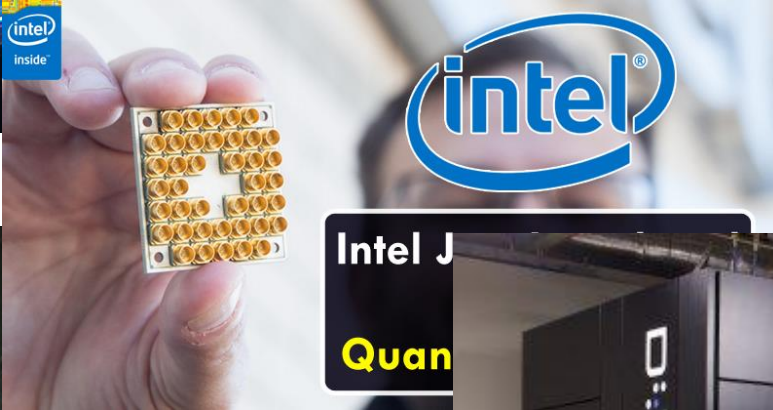
“I think whatever superpower gets that first, it would be like the equivalent of first digital nuclear bomb,”
Rep. Mike McCaul

Beyond
the Limit

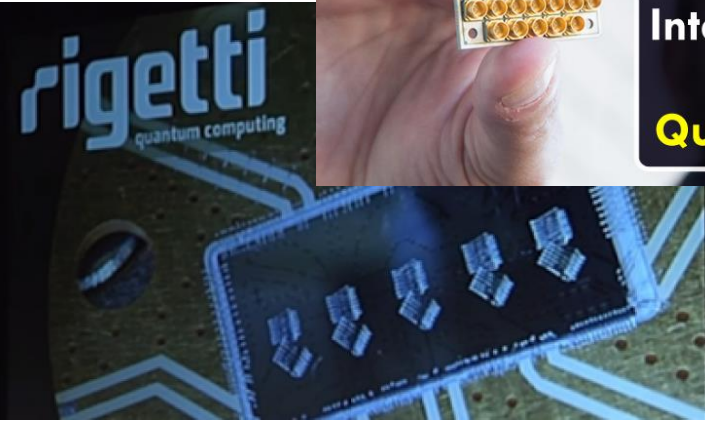
Digital Annealer

FUJITSU Digital Quantum Computing

Meet the future



Intel J
Quan





ST

GOOGLE CLAIMS 'QUANTUM SUPREMACY'

The background image shows a highly complex quantum computing experimental setup. It features a dense array of vertical cylindrical components, likely fiber optic cables or waveguides, arranged in a circular pattern. Numerous bright red laser beams are directed through the setup, creating a vibrant, futuristic scene. The overall lighting is a mix of deep red and cool blue, with a dark, metallic-looking surface. In the top right and bottom right corners, there are decorative elements consisting of white, curved lines and a small rectangular icon, set against a light blue background with faint binary code (0s and 1s) visible.

Chinese Scientists Achieve Quantum Computational Advantage

A research team established a quantum computer prototype, named "Jiuzhang," via which up to 76 photons were detected.

This achievement marks that China has reached the first milestone on the path to full-scale quantum computing -- a quantum computational advantage, also known as "quantum supremacy," which indicates an overwhelming quantum computational speedup.

Optimization algorithms



Optimization algorithms

HOW QUANTUM COMPUTING COULD TRANSFORM LOGISTICS

WITHIN 5-10 YEARS

WHAT ARE QUANTUM COMPUTERS?

Computers using quantum bits (qubits) to **organize, process** and **store information**



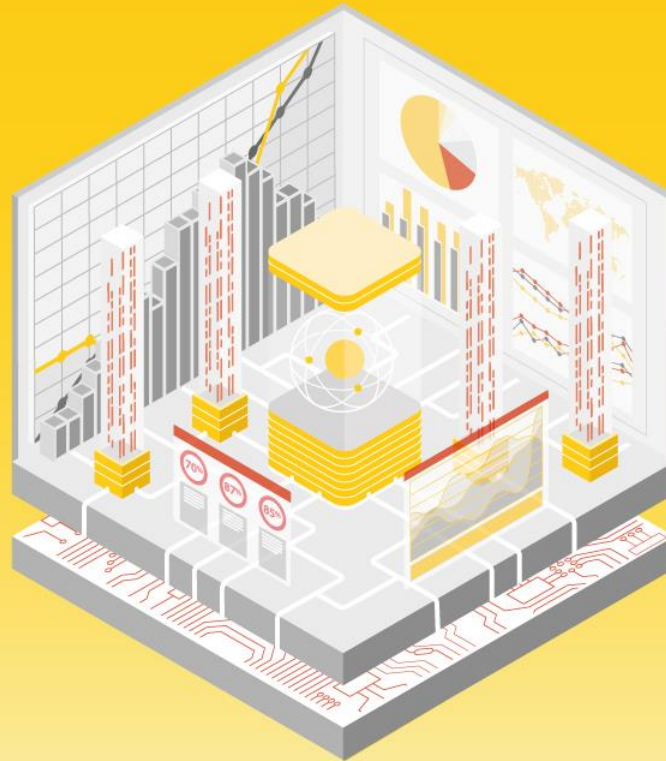
Improved speed



Stores more information



Uses less energy



Enhance dynamic route optimization



Maximize simultaneous packing of parcels



Support adaptive reallocation of assets



Enable rapid testing of designs and materials for logistics use

Optimization algorithms

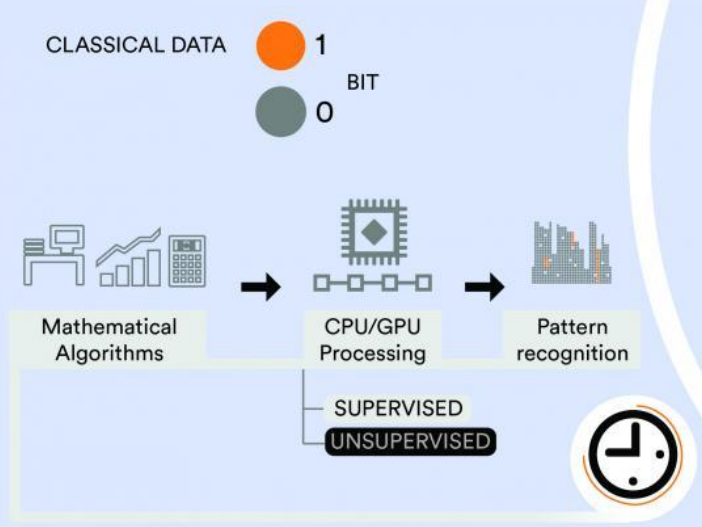


***Data science and mathematical
modeling***

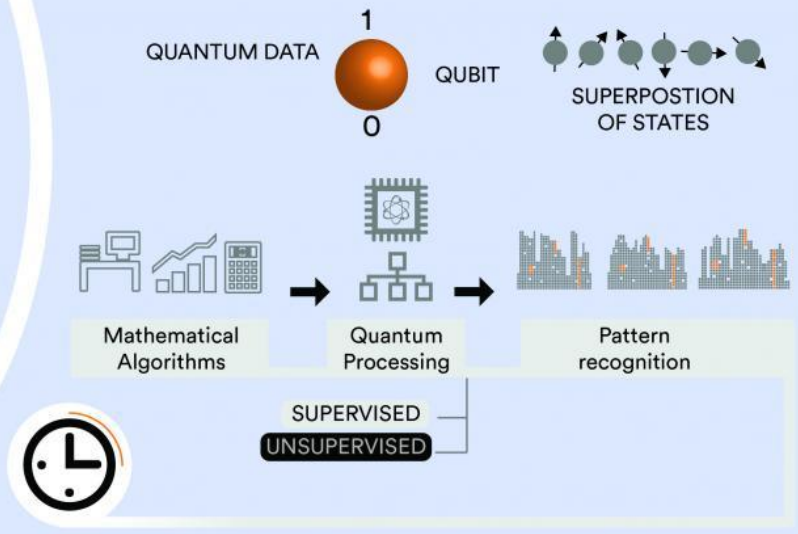


MACHINE LEARNING

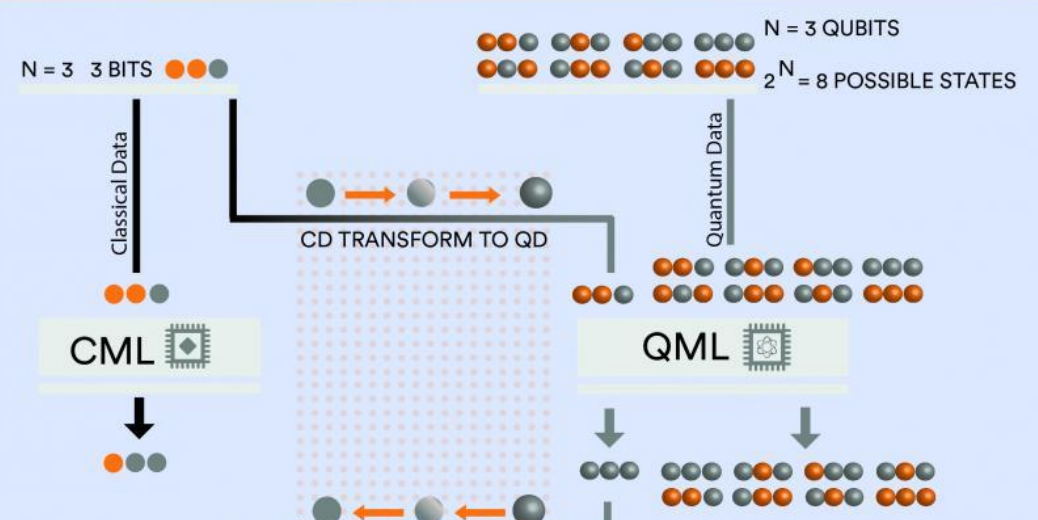
CLASSICAL MACHINE LEARNING - CML



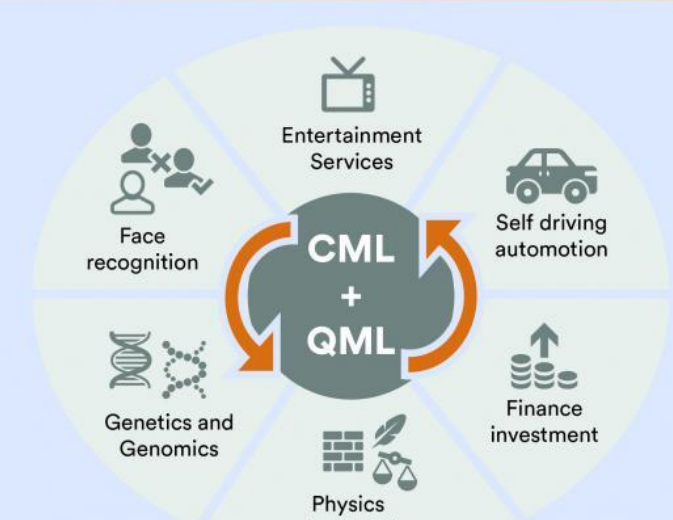
QUANTUM MACHINE LEARNING - QML



PROCESSING METHODS



APPLICATIONS



Quantum sensing



Quantum sensing



2. Post-quantum cryptography

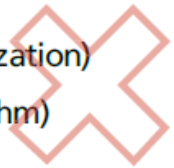


CLASSICAL


POST-QUANTUM

PUBLIC KEY
ENCRYPTION

RSA (integer factorization)
ECC (discrete logarithm)

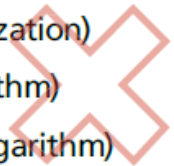


McEliece (code-based)
Kyber (KEM) (lattice-based)




SIGNATURES

RSA (integer factorization)
DSA (discrete logarithm)
ECDSA (discrete logarithm)

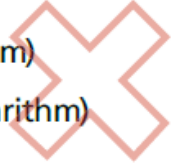


XMSS (hash-based)
HVEv- (multivariate)



KEY EXCHANGE

DH (discrete logarithm)
ECDH (discrete logarithm)




NewHope (lattice-based)




SYMMETRIC KEY
ENCRYPTION

AES-128




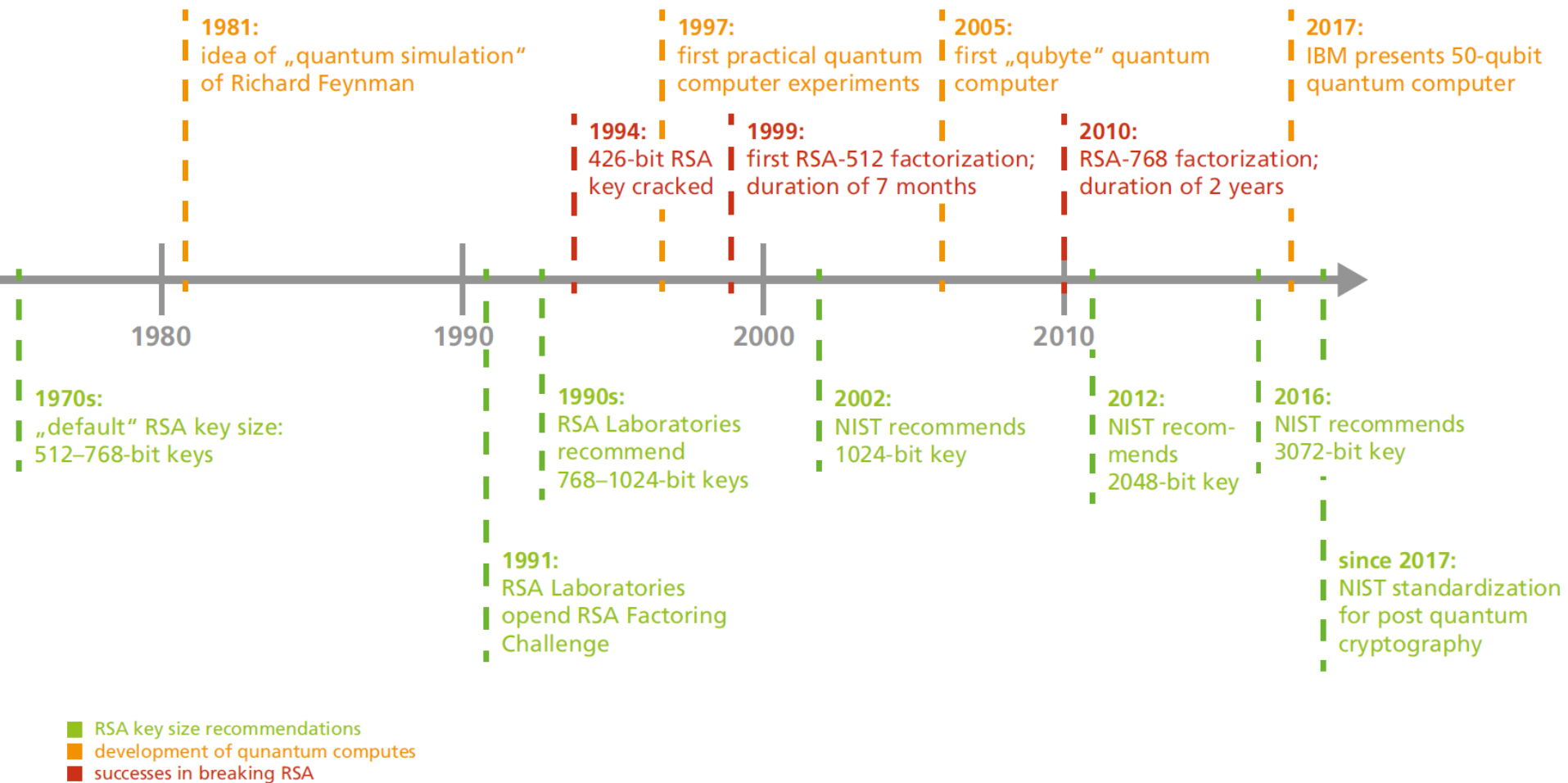
AES-256



HASH FUNCTIONS

SHA2
SHA3





Austria, March 2016: "A quantum machine factors the number 15" using Shor's algorithm.
 New largest number factored on a quantum device is 56,153

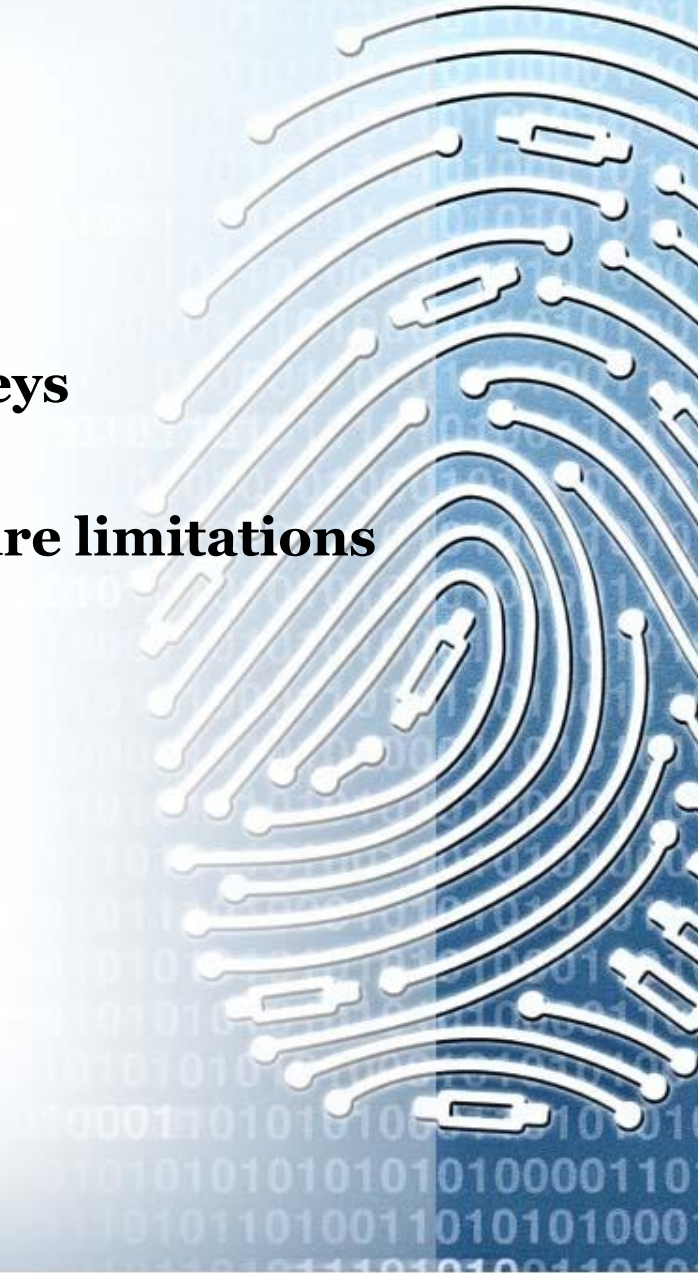


COURTESY: UNIVERSITY OF MARYLAND



Prevention measures

- **Audit data and cryptographic assets**
- **Identify the types of cryptographic keys**
- **Identify potential future infrastructure limitations**
- **Maintain situational awareness**





New Hope Algorithm

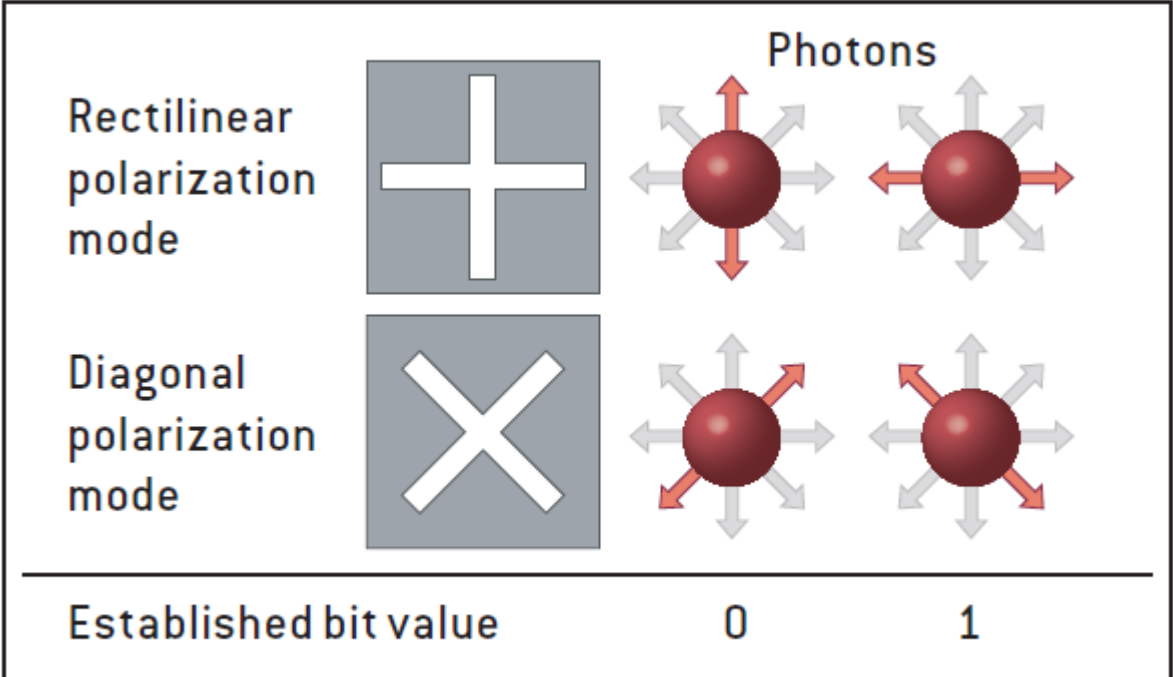


Google

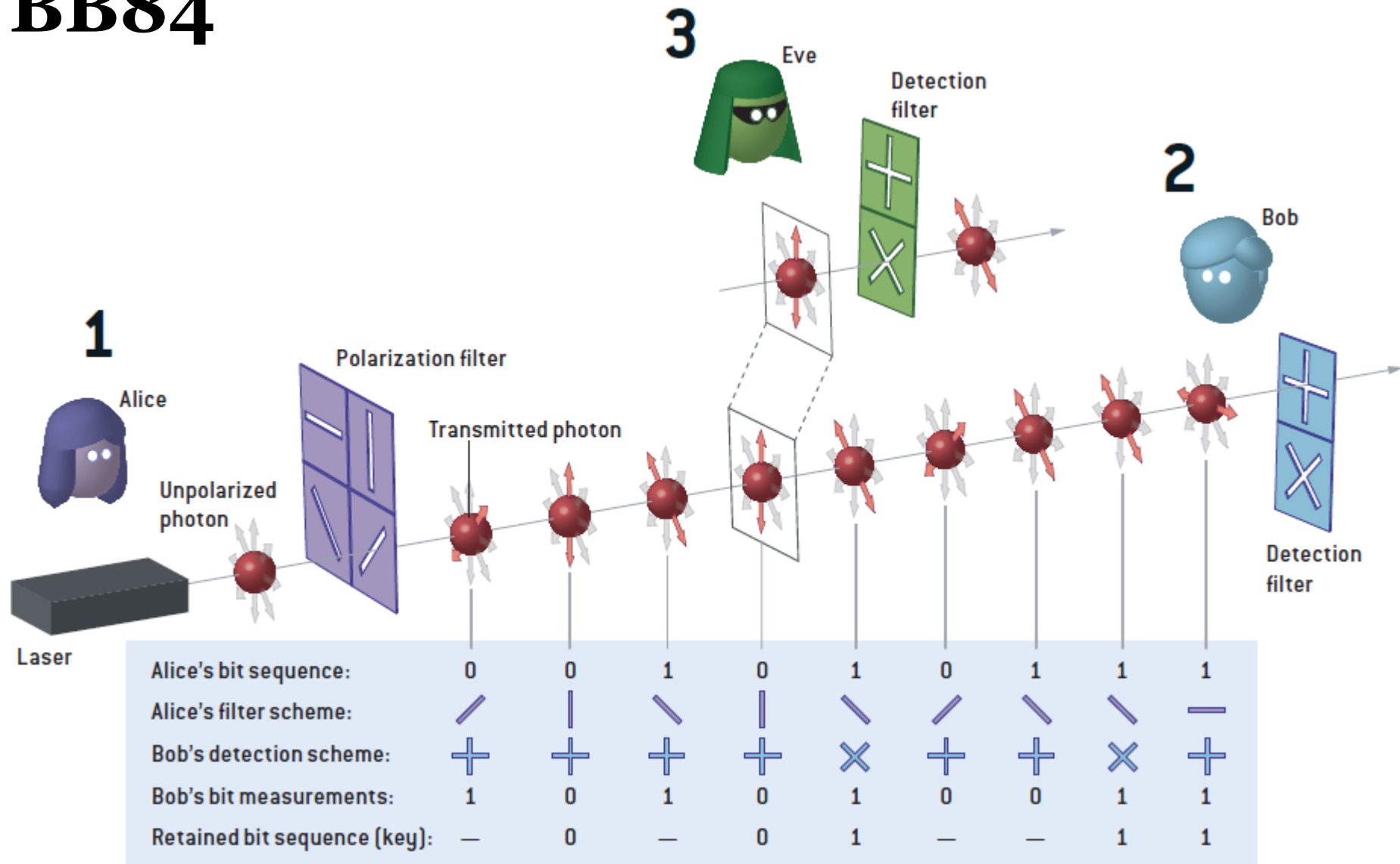
3. Quantum communication



BB84



BB84



National Quantum Communication Backbone Project

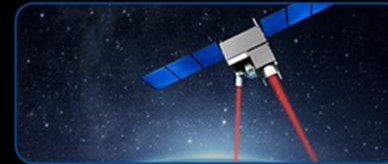
- ▶ Inter-city quantum communication backbone with 32 trusted relays (~2000km)
- ▶ For financial applications, public affairs, etc.
- ▶ Test-bed for quantum foundations (e.g. frequency dissemination)
- ▶ Established in the end of 2016



The World's First Quantum Science Experiment Satellite "Micius" Was Successfully Launched

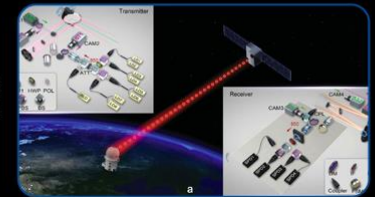
Satellite-based Entanglement Distribution Over 1200 Kilometers and Test of Non-locality at Space Scale

01



Quantum Key Distribution from the Satellite to Ground Over 1200 Kilometers

02



Quantum Teleportation from Ground to the Satellite Over 1400 Kilometers

03

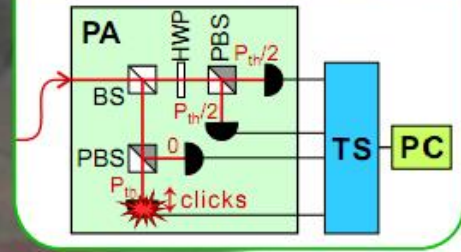
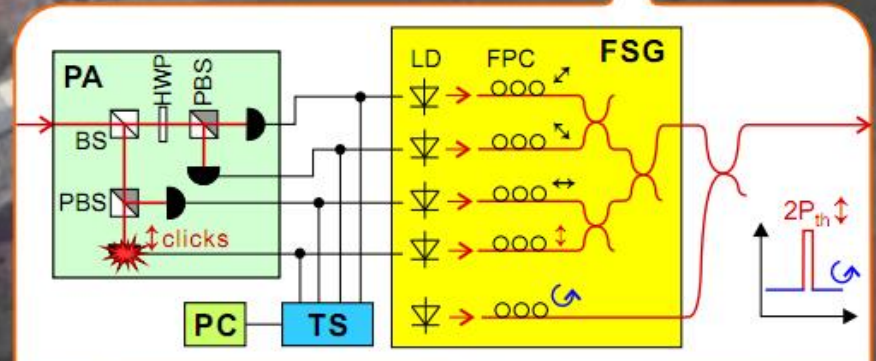
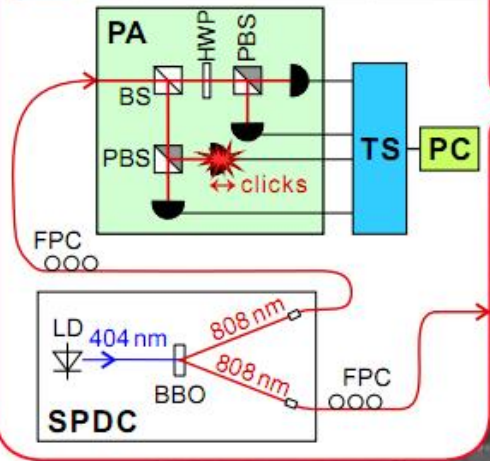


2017-08-10

Congratulations to "Micius" Quantum Satellite for Successfully Completing Three Major Scientific Experiments

China Becomes the First Country Mastering the Satellite-ground Wide-area Quantum Communication Network Technology

Perfect eavesdropper on a quantum cryptography system (2011)



Quantum Eve



Quantum Hacking Group

4. Critical Path



Critical Path

- **Understand industry impact.**
- **Develop a strategy.**



Critical Path

- **Monitor technology and industry developments.**
- **Improve your crypto-agility.**



Q#

```
/// A qubit initially in the  $|0\rangle$  state that we want to send
/// the state of msg to.
operation Teleportation(msg : Qubit, receiver : Qubit) : () {
    body {
        using (resources in Reset[0]) {
            // Ask for an auxiliary qubit that we can use to prepare
            // for teleportation.
            let aux = Prepare(|0>);

            // Create some entanglement that we can use to send
            H(aux);
            CNOT(aux, receiver);

            // Move our message into the entangled pair.
            CNOT(msg, aux);
            H(msg);

            // Measure out the entanglement.
            if (M(msg) == One) { Z(receiver); }
            if (M(aux) == One) { X(receiver); }

            // Reset our "here" qubit before releasing it.
            Reset(here);
        }
    }
}
```





New QKD protocol

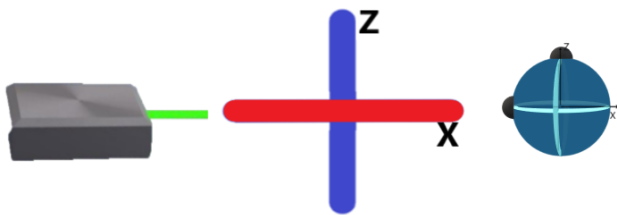
Alice



Bob



1.-Alice prepares and sends Bob a random string of non-orthogonal quantum states.



2.-Bob measures Alice's non-orthogonal state pairs with random bases (X or Z).

Base en Z



Base en X



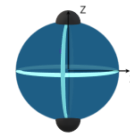
3.-Bob announces Double Matching events to Alice.

Event: Double Matching (DM).



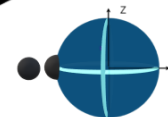
Getting: ($| - \rangle$, $|0z\rangle$)

Event: No-Double Matching (DM).



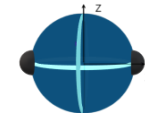
Getting: ($|0z\rangle$, $|1z\rangle$)

Event: Double Matching (DM).



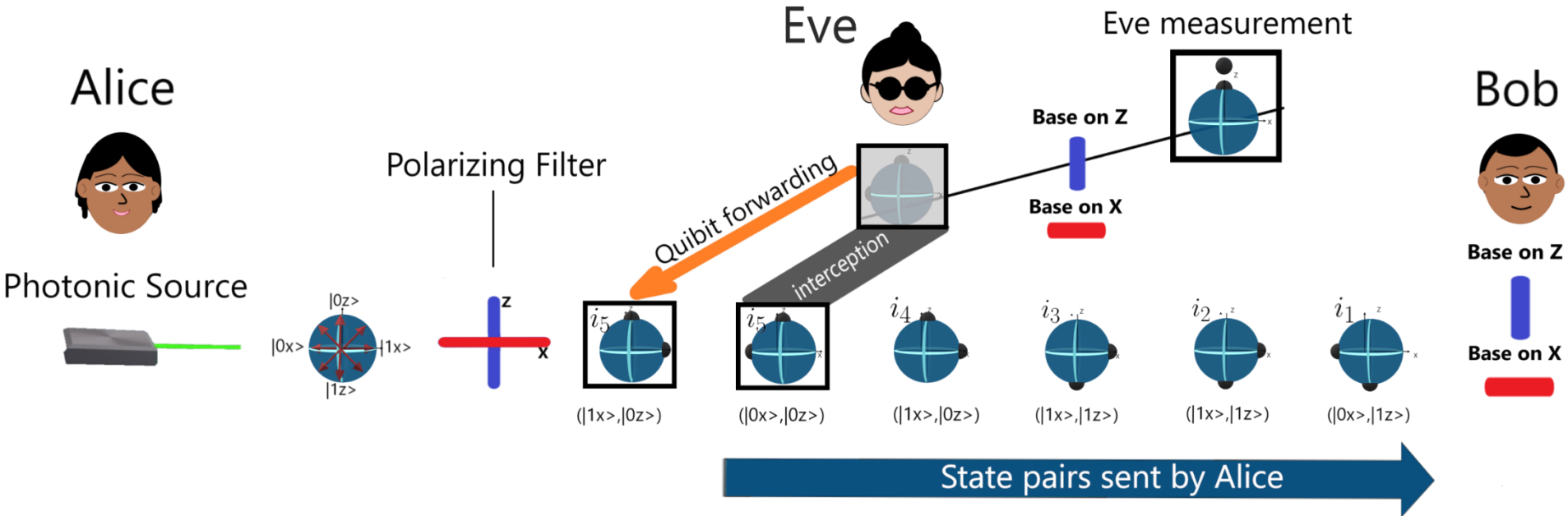
Getting: ($|0x\rangle$, $| - \rangle$)

Event: No-Double Matching (DM).



Getting: ($|0x\rangle$, $|1x\rangle$)

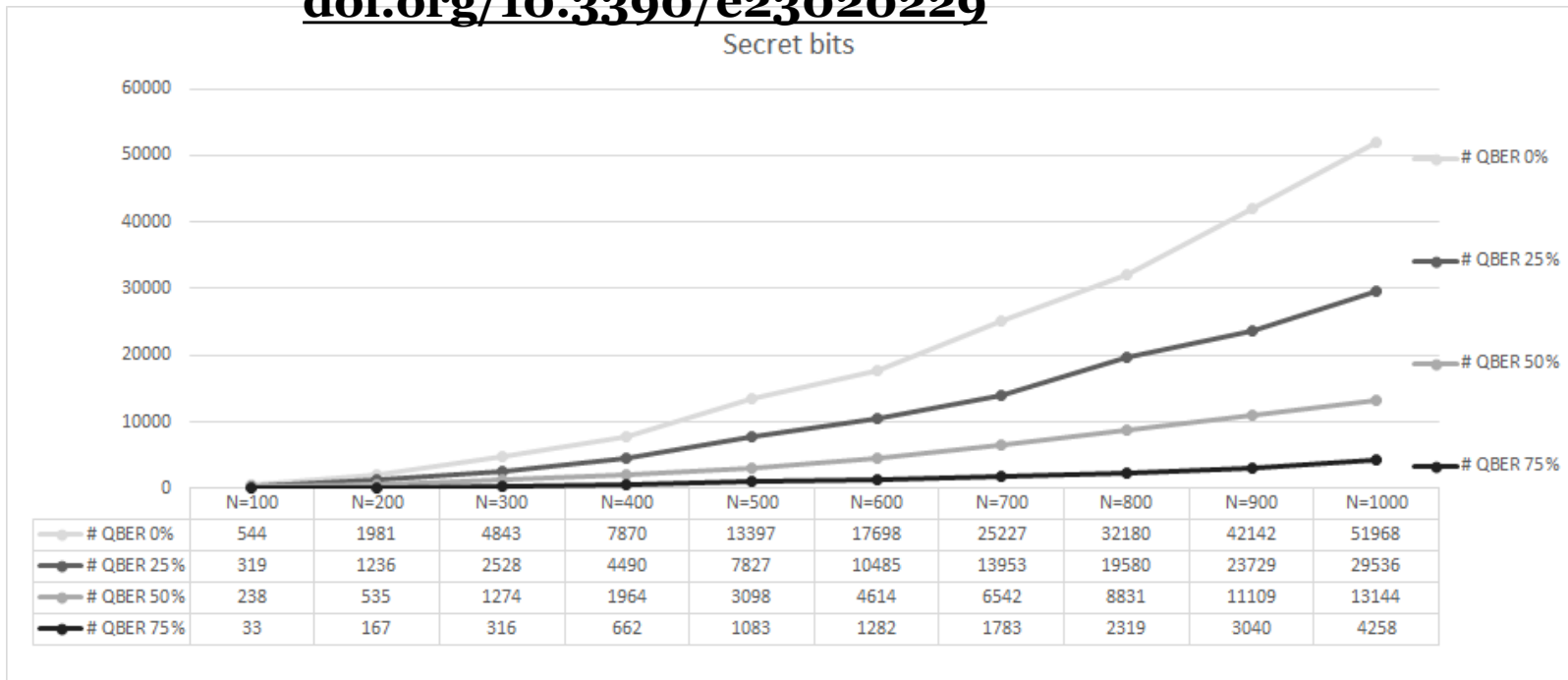
New QKD protocol



Bob Measurement	$i_1 = (-, 1z\rangle);$	$i_2 = (1x\rangle, -);$	$i_3 = (-, 1z\rangle);$	$i_4 = (1x\rangle, -)$
Alice Frames	1. $f_3 = (i_1, i_2),$	2. $f_3 = (i_1, i_3),$	3. $f_6 = (i_2, i_4),$	4. $f_6 = (i_3, i_4)$
Bob's Frames and SS	1. $\begin{pmatrix} - & 1z\rangle \\ 1x\rangle & - \end{pmatrix} f_3$ $SS = 11, 11$	2. $\begin{pmatrix} - & 1z\rangle \\ 1x\rangle & - \end{pmatrix} f_3$ $SS = 00, 11$	3. $\begin{pmatrix} 1x\rangle & - \\ 1x\rangle & - \end{pmatrix} f_6$ $SS = 00, 11$	4. $\begin{pmatrix} - & 1z\rangle \\ 1x\rangle & - \end{pmatrix} f_6$ $SS = 11, 11$
Secret bit	0	1	0	0

doi.org/10.3390/sym12061053

doi.org/10.3390/e23020229



- **Distance**
- **Speed**
- **Key length**

Post-quantum KEP

$$P = k u k^{-1} \rightarrow P^x = k u^x k^{-1}$$

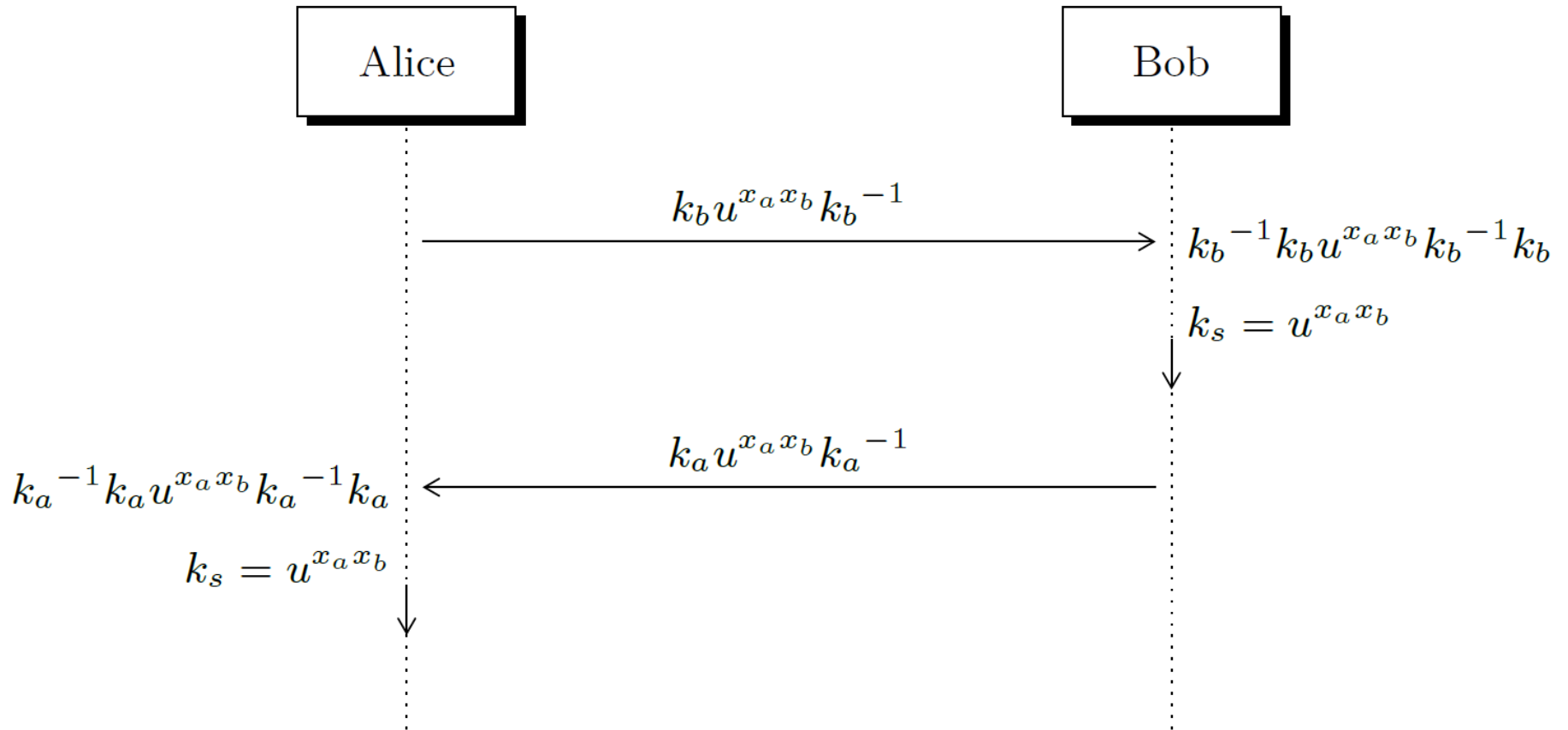
Public Key	Private Key
$P_a = k_a u^{x_a} (k_a)^{-1}$	$R_a = \{k_a, x_a\}$
$P_b = k_b u^{x_b} (k_b)^{-1}$	$R_b = \{k_b, x_b\}$

Post-quantum KEP

User	Operation	Result
Alice	$(\mathbf{k}_b \mathbf{u}^{x_b} \mathbf{k}_b^{-1})^{x_a} =$	$\mathbf{k}_b \mathbf{u}^{x_a x_b} \mathbf{k}_b^{-1}$
Bob	$(\mathbf{k}_a \mathbf{u}^{x_a} \mathbf{k}_a^{-1})^{x_b} =$	$\mathbf{k}_a \mathbf{u}^{x_a x_b} \mathbf{k}_a^{-1}$

doi: 10.20944/preprints202105.0174.v1

Post-quantum KEP



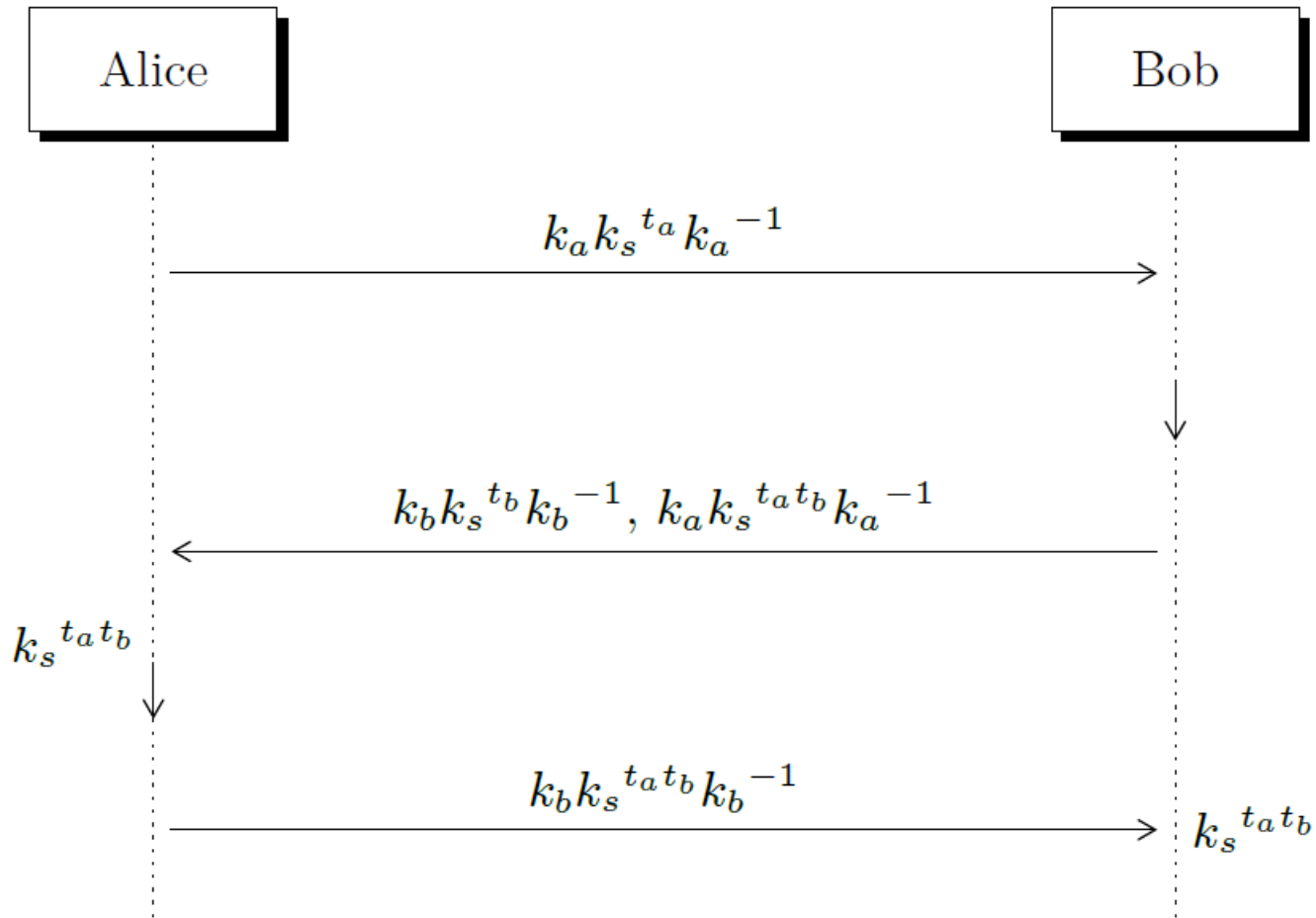
doi: 10.20944/preprints202105.0174.v1

Post-quantum KEP

User	Public key	Certified key
CA	$\mathbf{k}_{ca} \mathbf{u}^{x_{ca}} \mathbf{k}_{ca}^{-1}$	-
Alice	$\mathbf{k}_a \mathbf{u}^{x_a} \mathbf{k}_a^{-1}$	$\mathbf{k}_a \mathbf{u}^{x_a x_{ca}} \mathbf{k}_a^{-1}$
Bob	$\mathbf{k}_b \mathbf{u}^{x_b} \mathbf{k}_b^{-1}$	$\mathbf{k}_b \mathbf{u}^{x_b x_{ca}} \mathbf{k}_b^{-1}$

doi: 10.20944/preprints202105.0174.v1

Post-quantum KEP



doi: 10.20944/preprints202105.0174.v1

Conclusions

- **Understand industry impact.**
- **Develop a quantum strategy.**
- **Monitor technology and industry developments.**
- **Improve your crypto-agility.**



Thanks for your attention!

