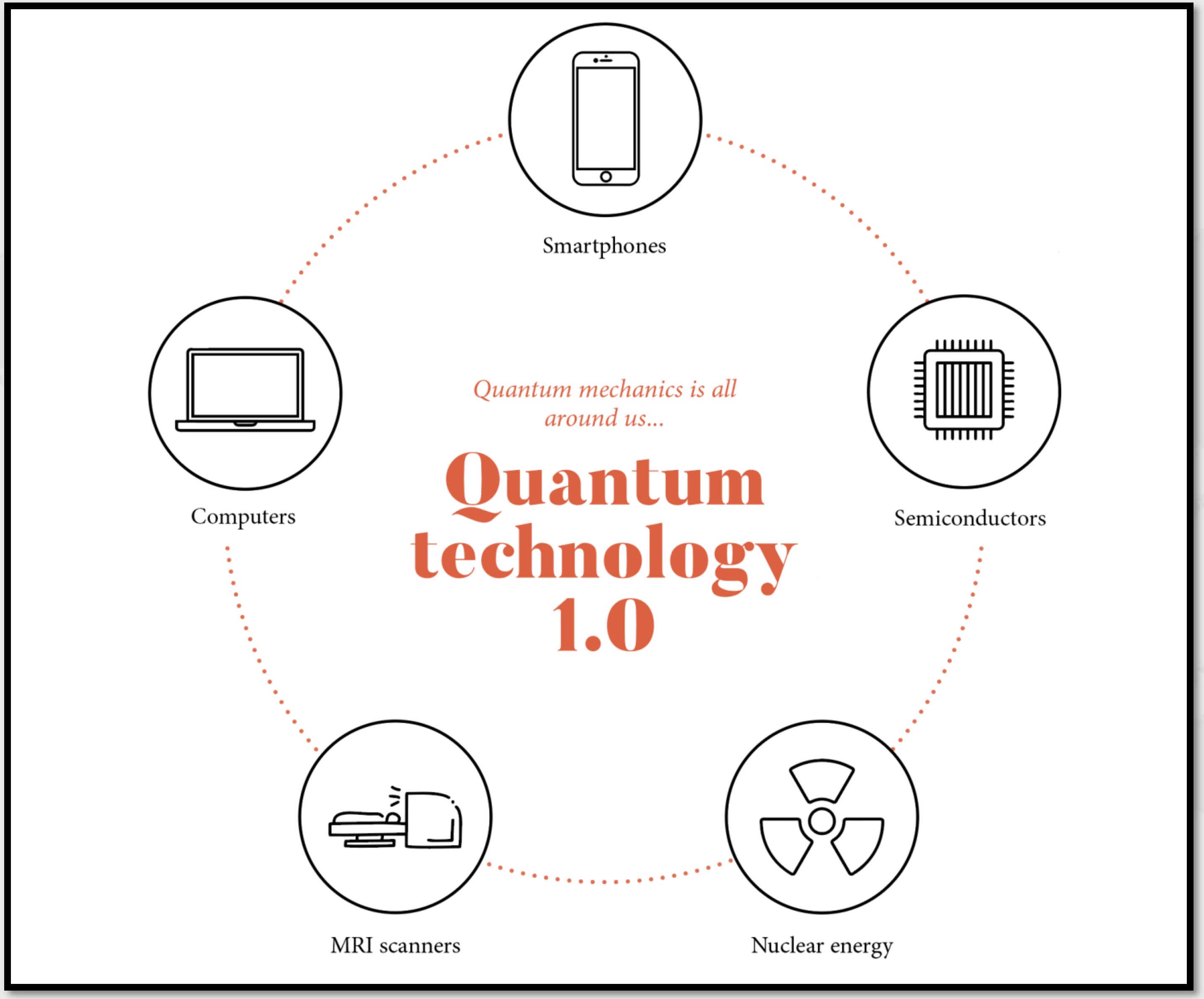
Quantum Cryptography in a nutshell

09/03/2025

Dr. Shashank Gupta
Research Lead, QNu Labs

Quantum Technology

Q→NU



Quantum mechanics is all around us...

Quantum technology 1.0

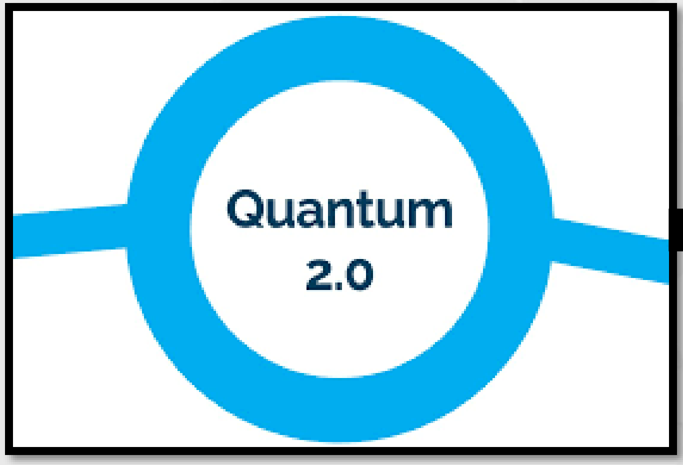
Smartphones

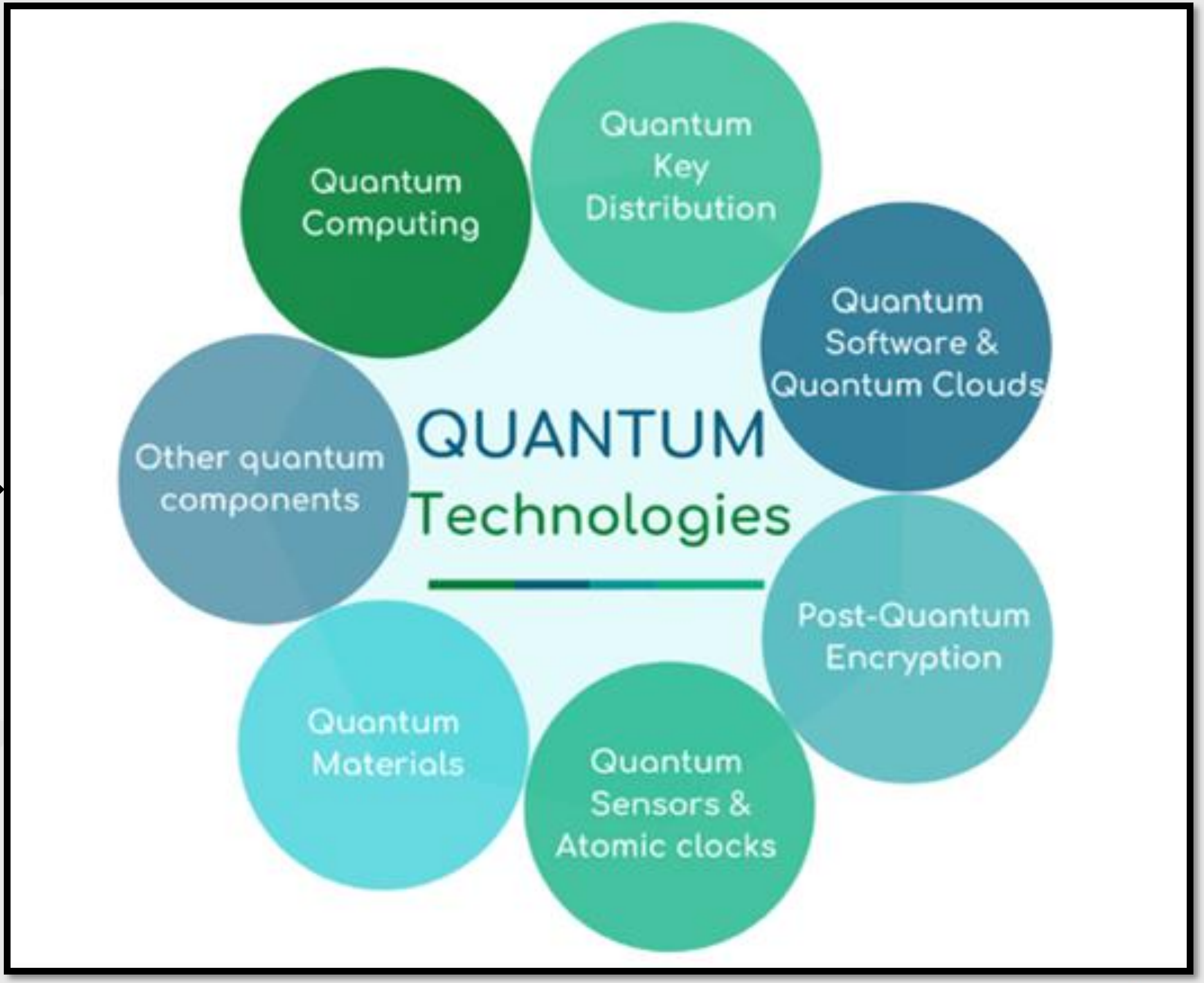
Semiconductors

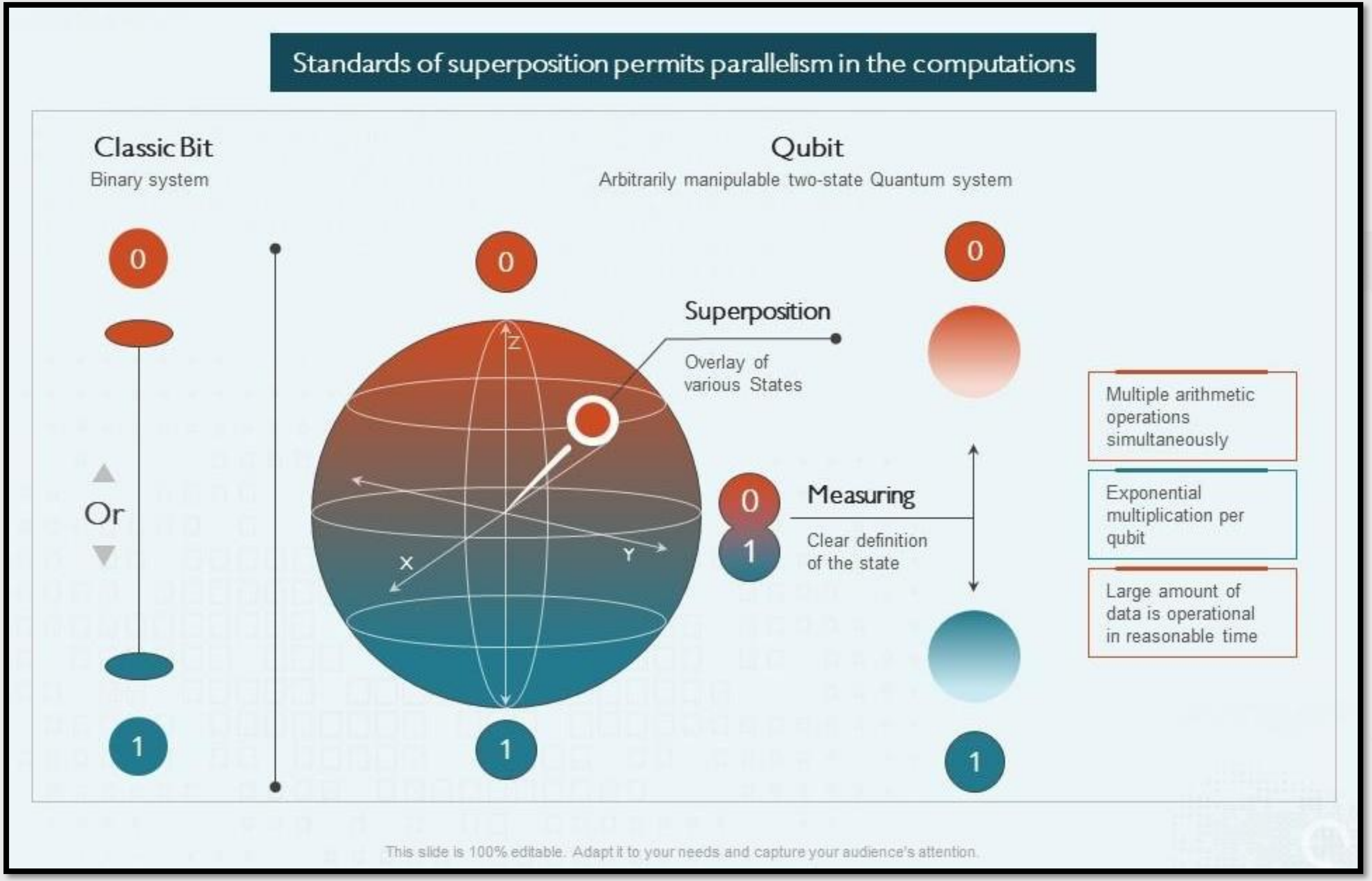
Nuclear energy

MRI scanners

Computers


Quantum
2.0


QUANTUM
Technologies
Quantum Computing
Quantum Key Distribution
Quantum Software & Quantum Clouds
Post-Quantum Encryption
Quantum Sensors & Atomic clocks
Quantum Materials
Other quantum components



Standards of superposition permits parallelism in the computations

Classic Bit

Binary system

Qubit

Arbitrarily manipulable two-state Quantum system

Superposition

Overlay of various States

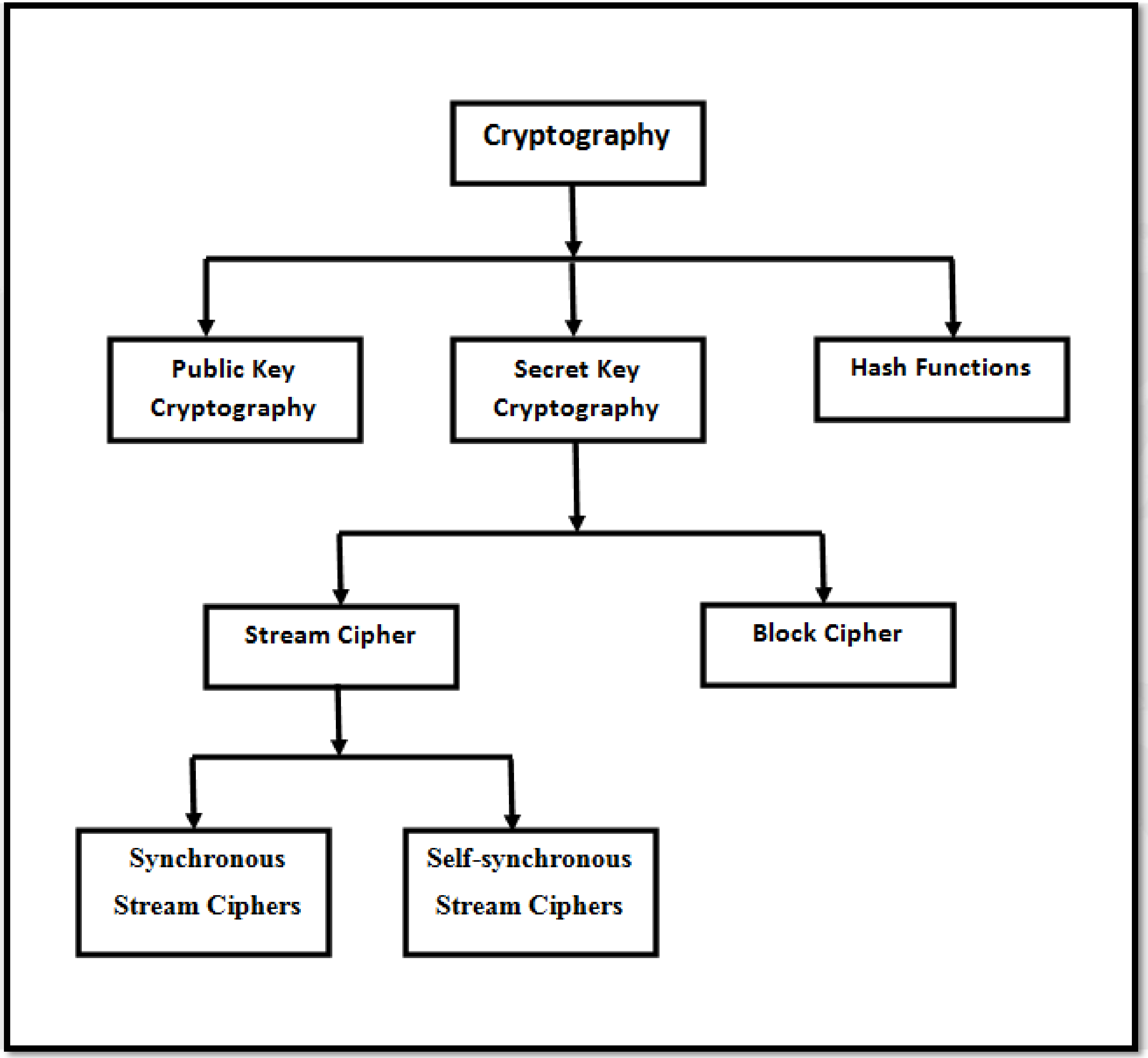
Measuring

Clear definition of the state

- Multiple arithmetic operations simultaneously
- Exponential multiplication per qubit
- Large amount of data is operational in reasonable time

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Cryptography



Cryptography

Public Key Cryptography

Secret Key Cryptography

Hash Functions

Stream Cipher

Block Cipher

Synchronous Stream Ciphers

Self-synchronous Stream Ciphers

Cryptography after quantum computers comes into picture

Post-Quantum Security

Conjectured

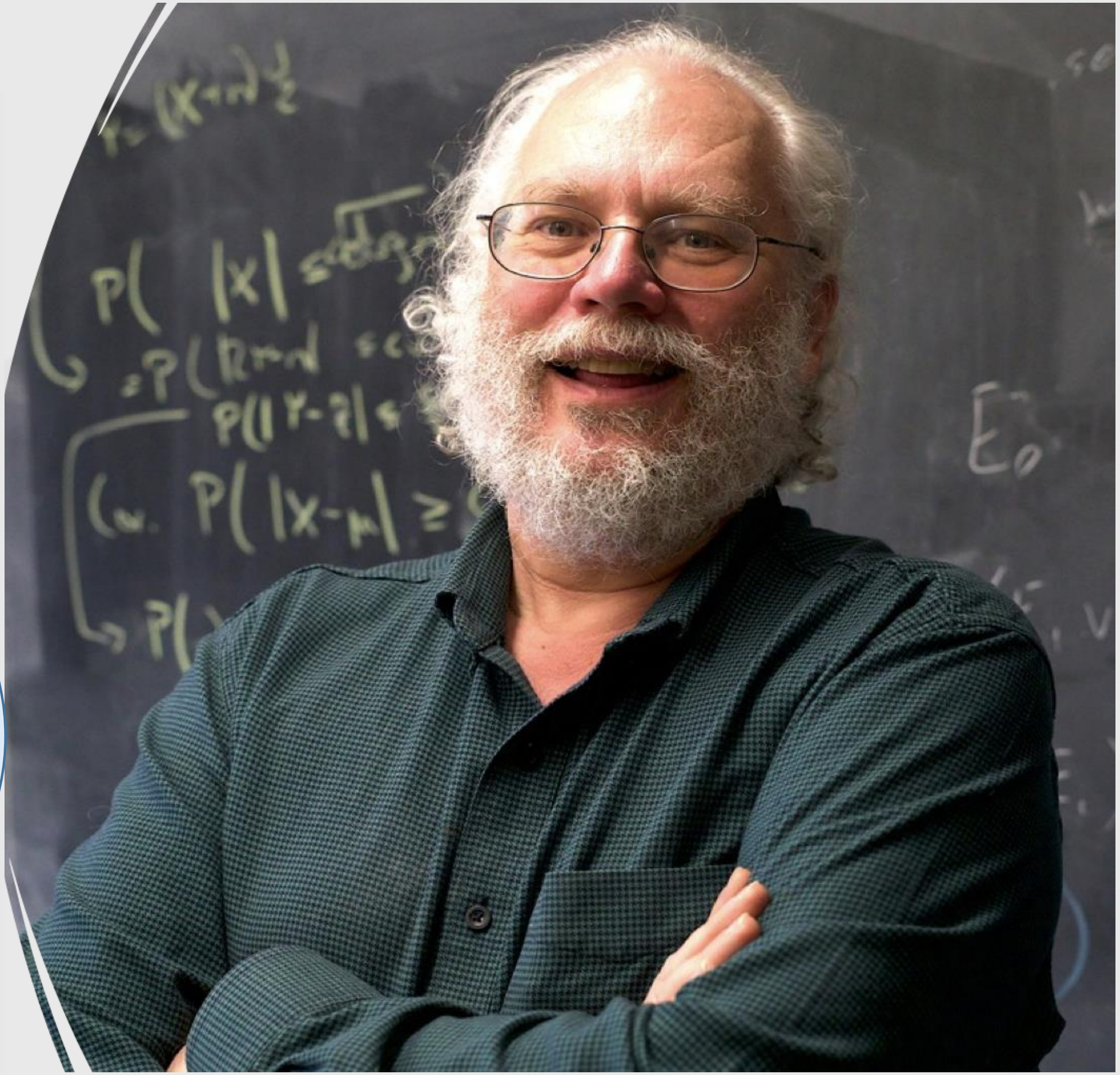
Information theoretic

PQC

Crystal Kyber, Dilithium, Falcon

QKD

BB84, B92, SARG04, DPS, Ekert, Six-state

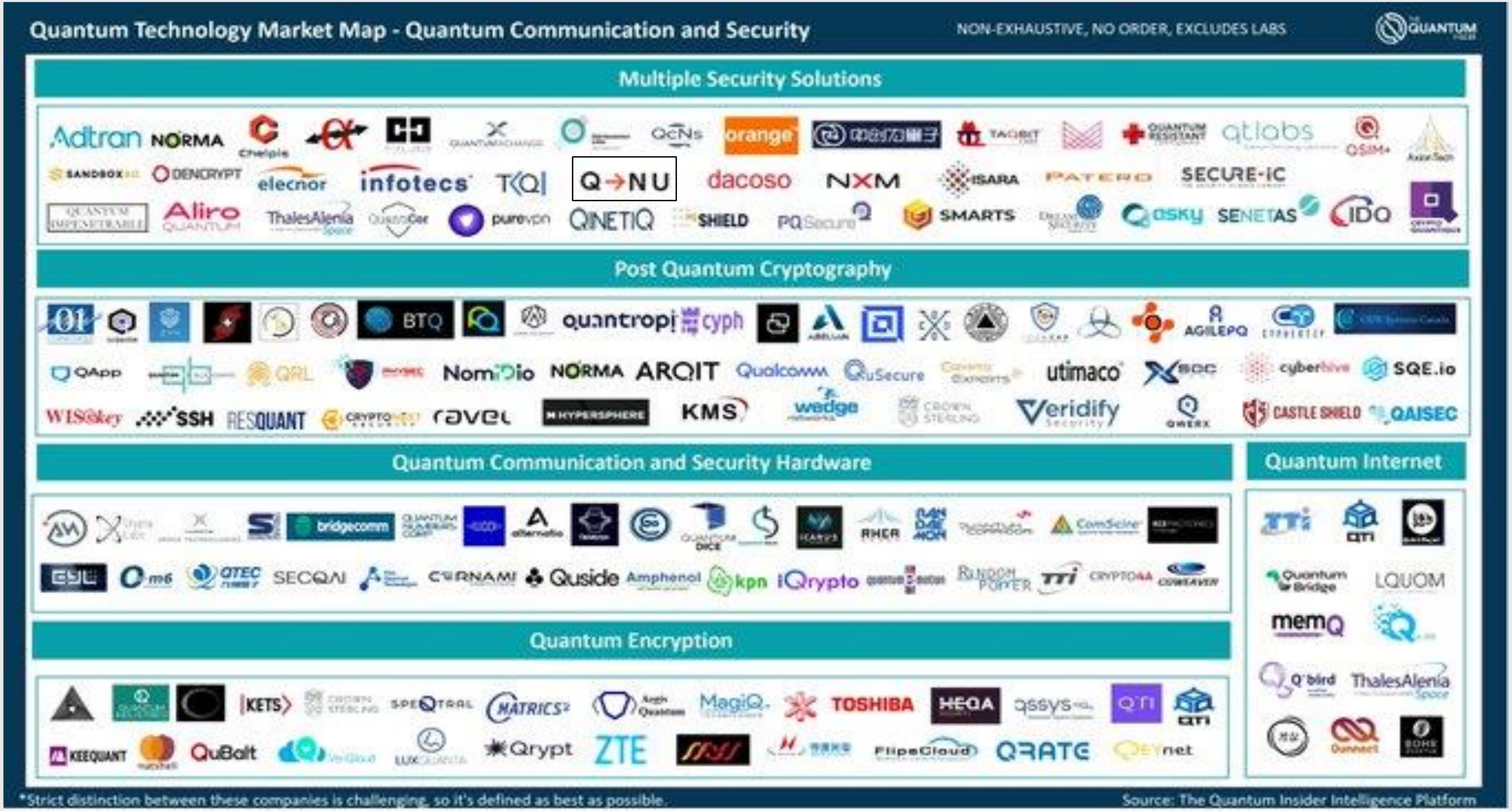


PQC: Post Quantum Cryptography

QKD: Quantum Key Distribution

Q→NU

Quantum security companies



Quantum Technology Market Map - Quantum Communication and Security

NON-EXHAUSTIVE, NO ORDER, EXCLUDES LABS

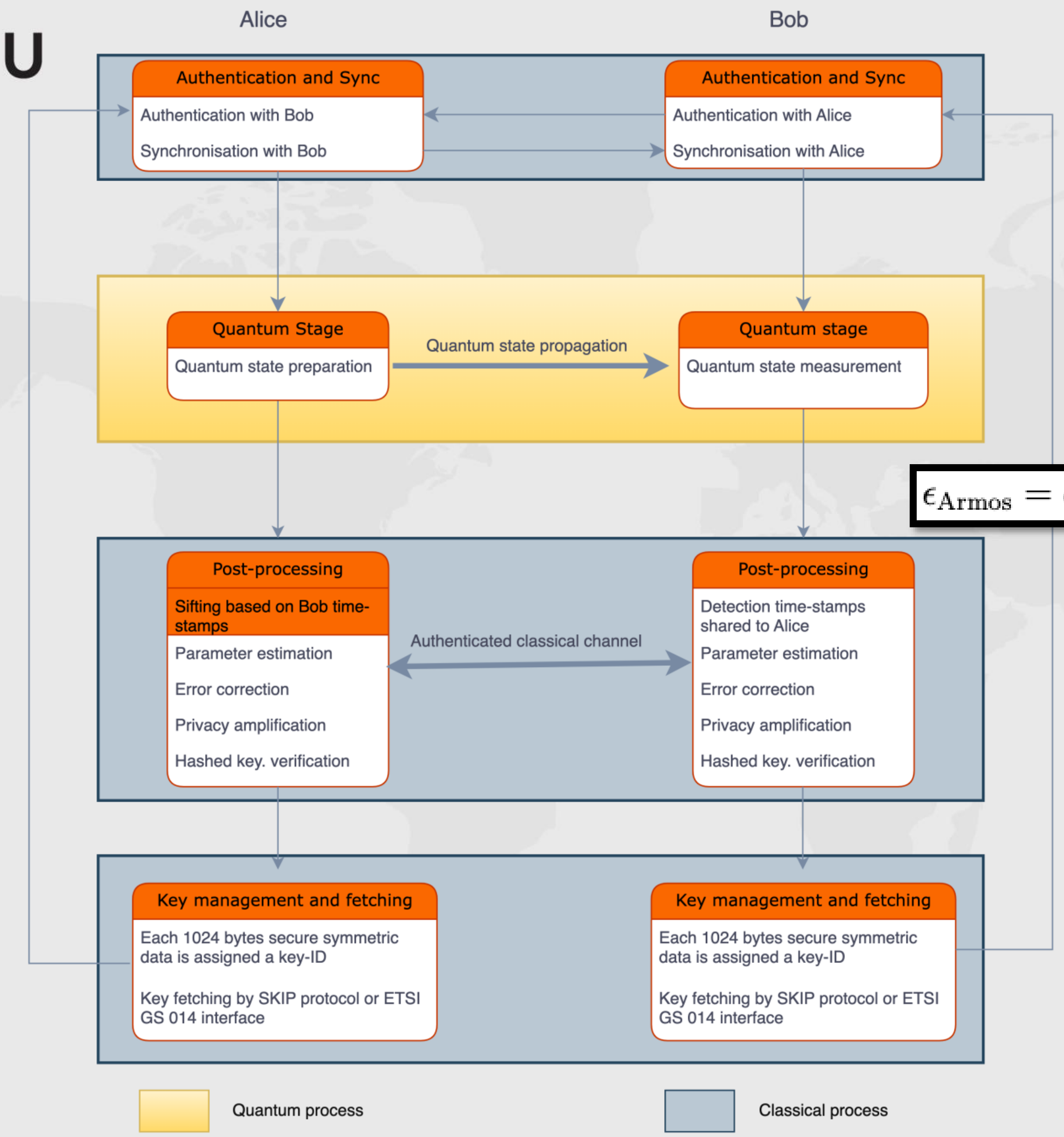
*Strict distinction between these companies is challenging, so it's defined as best as possible.

Source: The Quantum Insider Intelligence Platform

Ref. https://x.com/QuantumDaily/status/1767881188771799436

Quantum Key Distribution

QKD Stages



Alice

Bob

Authentication and Sync

Authentication with Bob

Synchronisation with Bob

Authentication and Sync

Authentication with Alice

Synchronisation with Alice

Quantum Stage

Quantum state preparation

Quantum state propagation

Quantum stage

Quantum state measurement

Post-processing

Sifting based on Bob time-stamps

Parameter estimation

Error correction

Privacy amplification

Hashed key. verification

Authenticated classical channel

Post-processing

Detection time-stamps shared to Alice

Parameter estimation

Error correction

Privacy amplification

Hashed key. verification

Key management and fetching

Each 1024 bytes secure symmetric data is assigned a key-ID

Key fetching by SKIP protocol or ETSI GS 014 interface

Key management and fetching

Each 1024 bytes secure symmetric data is assigned a key-ID

Key fetching by SKIP protocol or ETSI GS 014 interface

Quantum process

Classical process

$\varepsilon_{\mathrm{AUT}} \leq 10^{-13}$.

$$\epsilon_{\mathrm{Armos}} = \epsilon_{\mathrm{VIS}} + \epsilon_{\mathrm{Smooth}} + \epsilon_{\mathrm{PA}} + 2\epsilon_{\mathrm{VER}} + \epsilon_{\mathrm{MAC}} \lesssim 3 \times 10^{-12}$$

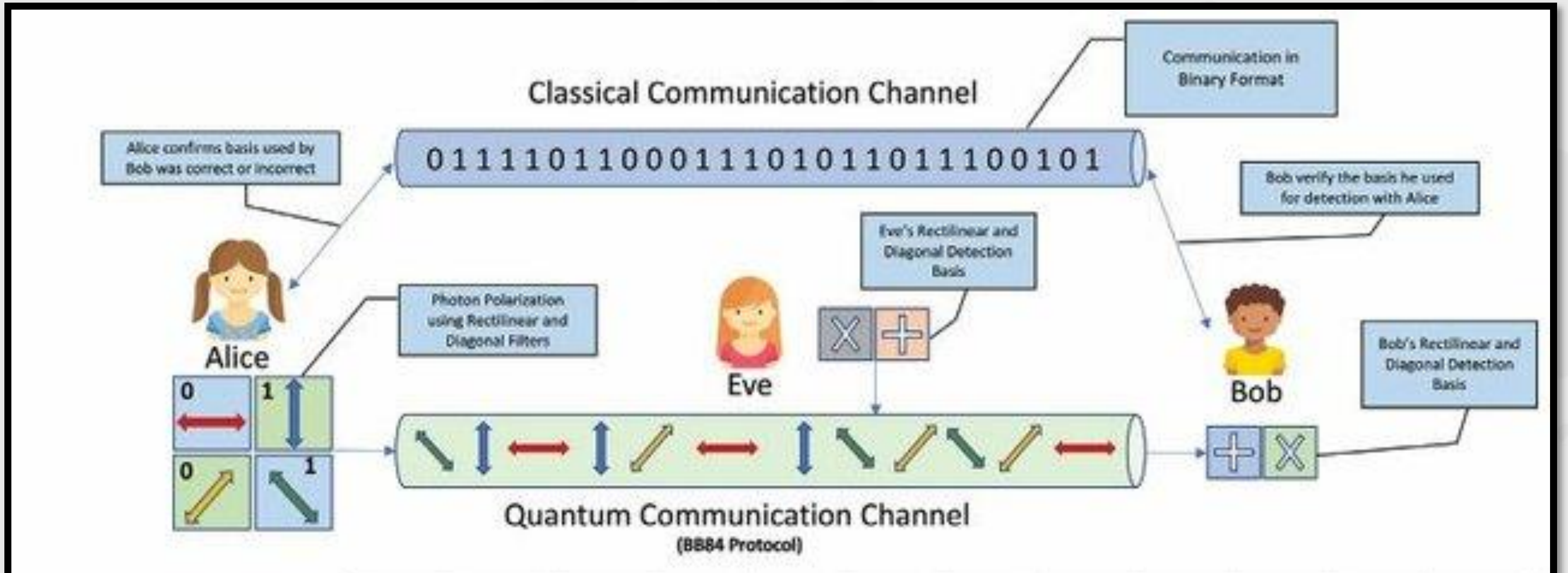
$\varepsilon_{\mathrm{PE}} \leq 9 \times 10^{-13}$.

$\varepsilon_{\mathrm{VER}} \leq 9 \times 10^{-13}$.

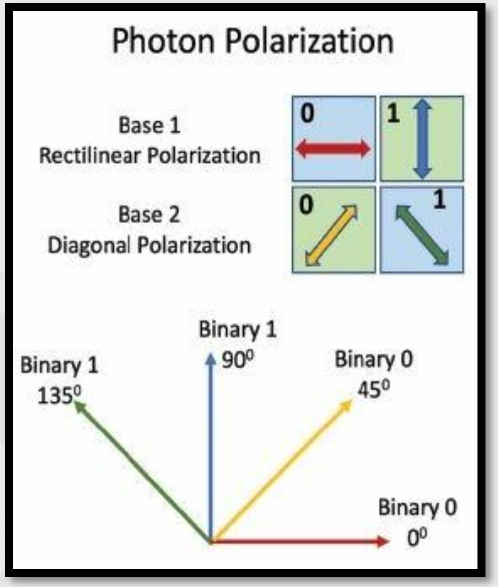
Point-to-Point QKD

Protocol: BB84

Q→NU


Classical Communication Channel
Communication in Binary Format
0 1 1 1 1 0 1 1 0 0 0 1 1 1 0 1 0 1 1 0 1 1 1 0 0 1 0 1
Alice confirms basis used by Bob was correct or incorrect
Bob verify the basis he used for detection with Alice
Eve's Rectilinear and Diagonal Detection Basis
Photon Polarization using Rectilinear and Diagonal Filters
Alice
Eve
Bob
Bob's Rectilinear and Diagonal Detection Basis
0
1
0
1
Quantum Communication Channel
(BB84 Protocol)

Alice's bit sequence	1	1	0	1	0	0	1	1	0	1	0	0
Alice's Photon Polarization	⤡	↕	↔	↕	⤢	↔	↕	⤡	⤢	⤡	⤢	↔
Bob's detection basis	X	+	X	+	+	+	+	X	+	X	X	X
Bob's measurement	1	1	1	1	1	0	1	1	0	1	0	1
Key	1	1	-	1	-	0	1	1	-	1	0	-



https://www.researchgate.net/publication/359228217_Quantum_Computing_and_the_Future_Internet/figures?lo=1

Protocol: Decoy-DPS

Armos protocol - Decoy-DPS

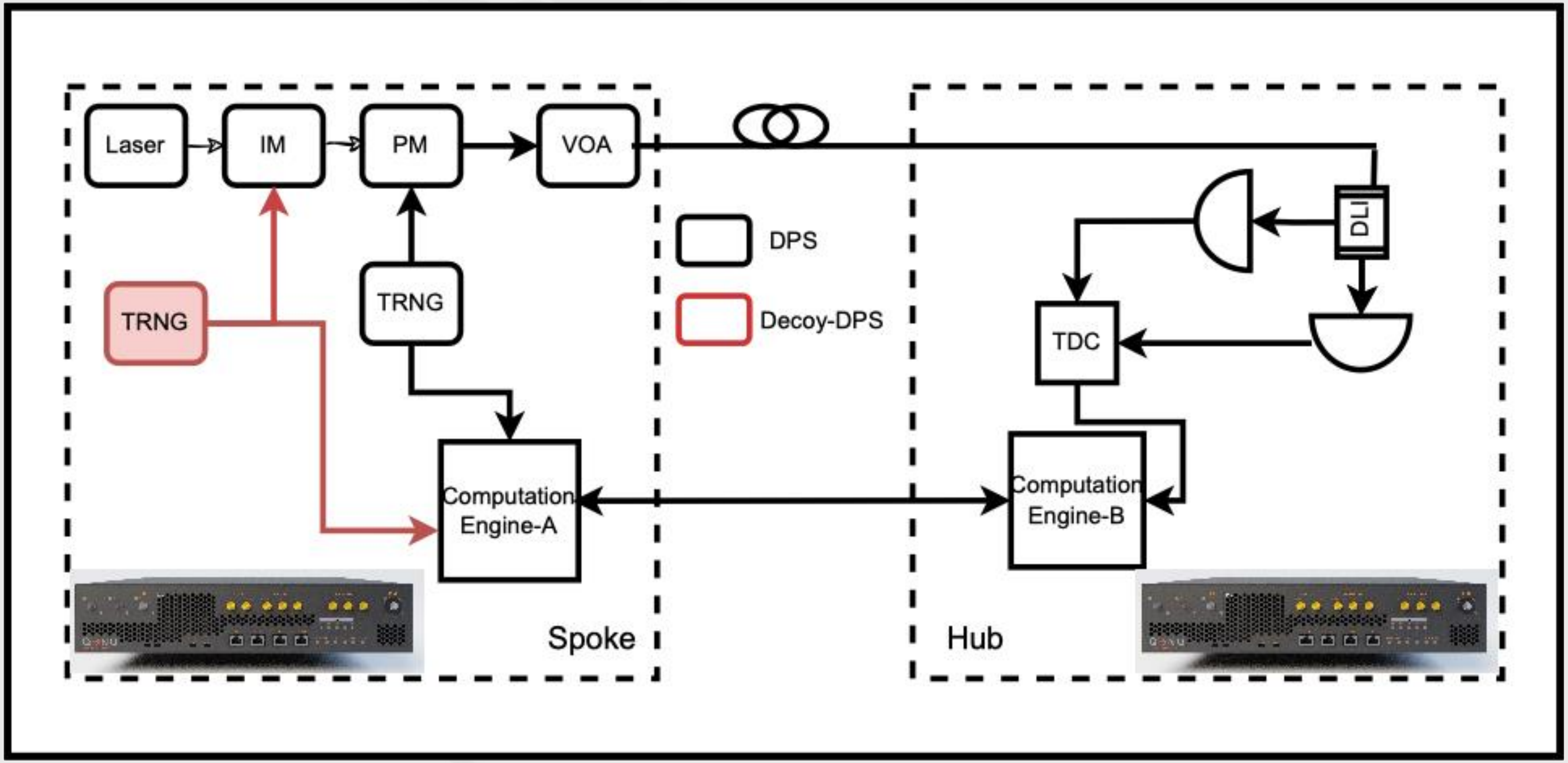


Fig. Block diagram of the QKD systems constituting ChaQra.

Point-to-Multipoint QKD (ChaQra)

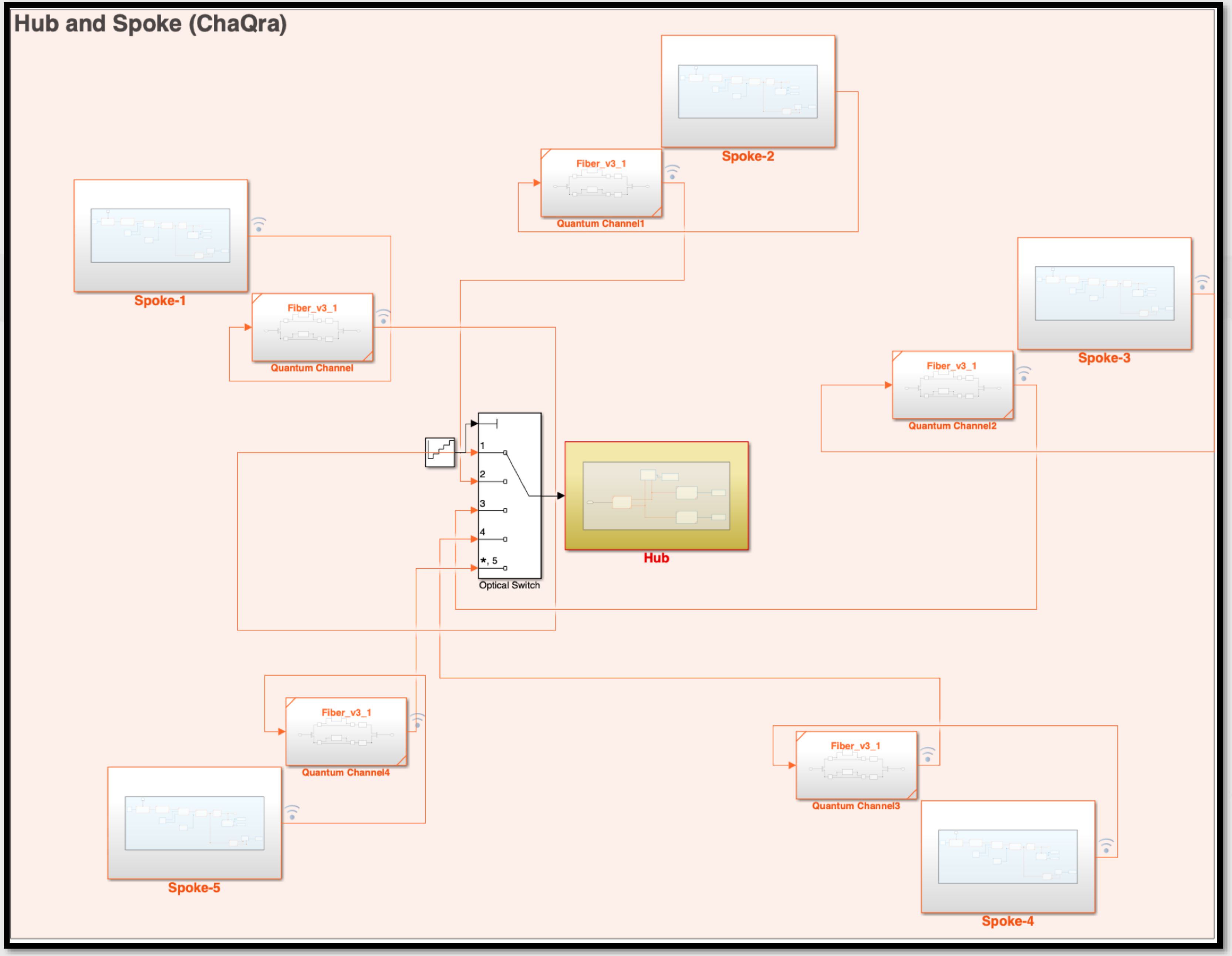


Fig. Simulink block diagram of ChaQra.

Q→NU

Quantum secured Indian Subcontinent

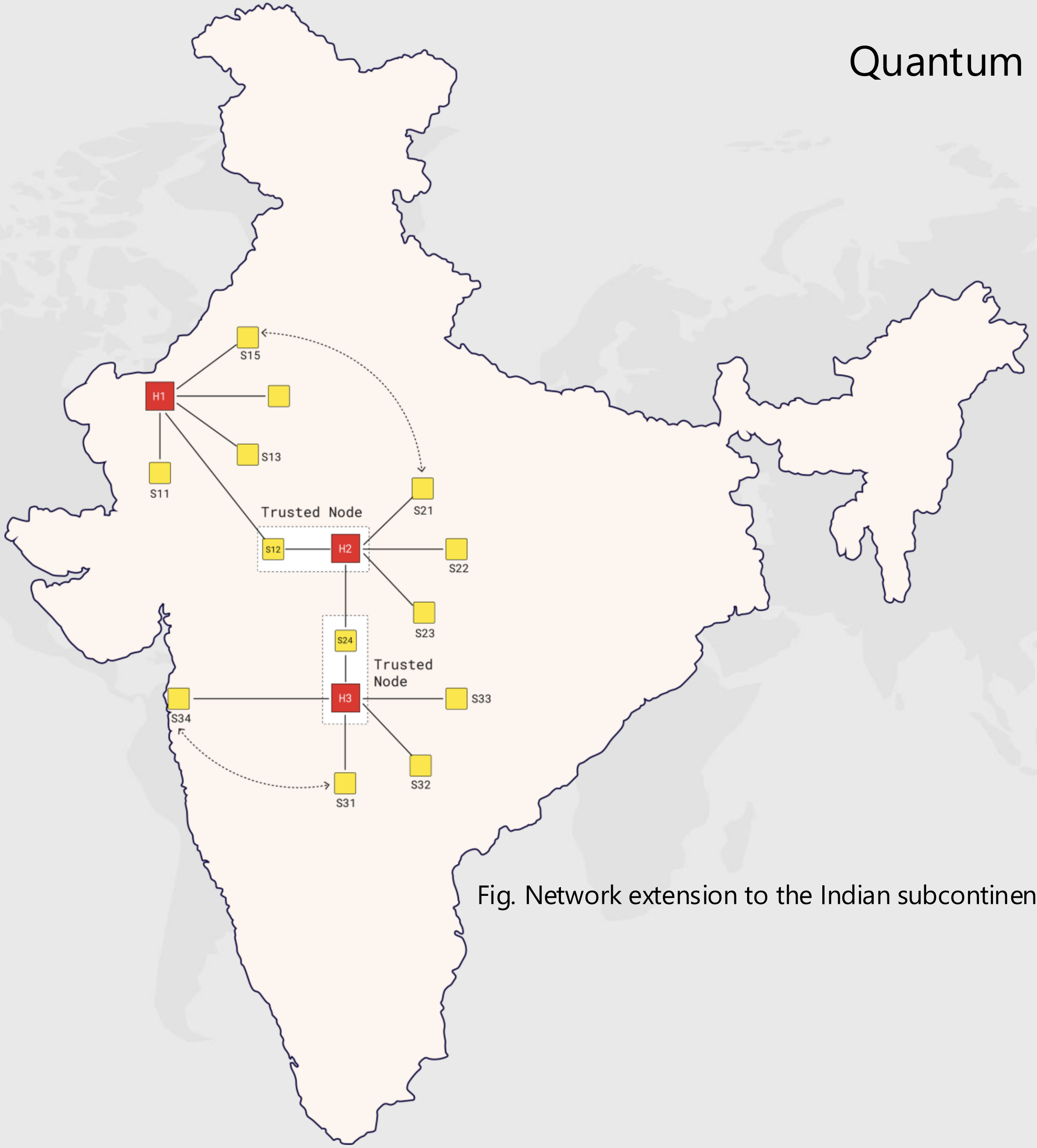
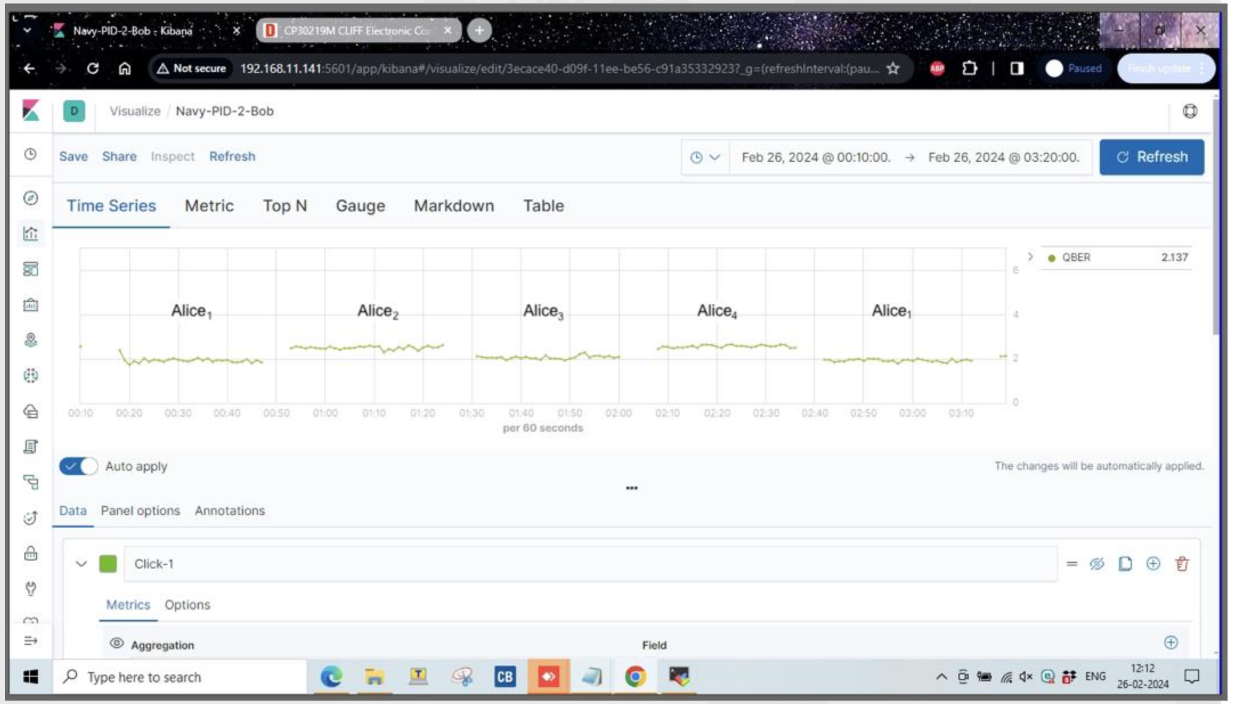


Fig. Network extension to the Indian subcontinent using ChaQra as a cellular unit.

Q→NU

Software Defined Networking (SDN)



Navy-PID-2-Bob - Kibana

CP30219M CLIFF Electronic Co

Not secure 192.168.11.141:5601/app/kibana#/visualize/edit/3ecace40-d09f-11ee-be56-c91a35332923?_g=(refreshInterval:(pau...

Visualize / Navy-PID-2-Bob

Save Share Inspect Refresh

Feb 26, 2024 @ 00:10:00. → Feb 26, 2024 @ 03:20:00.

Refresh

Time Series Metric Top N Gauge Markdown Table

Auto apply

The changes will be automatically applied.

Data Panel options Annotations

Click-1

Metrics Options

Aggregation Field

Type here to search

ENG 12:12 26-02-2024

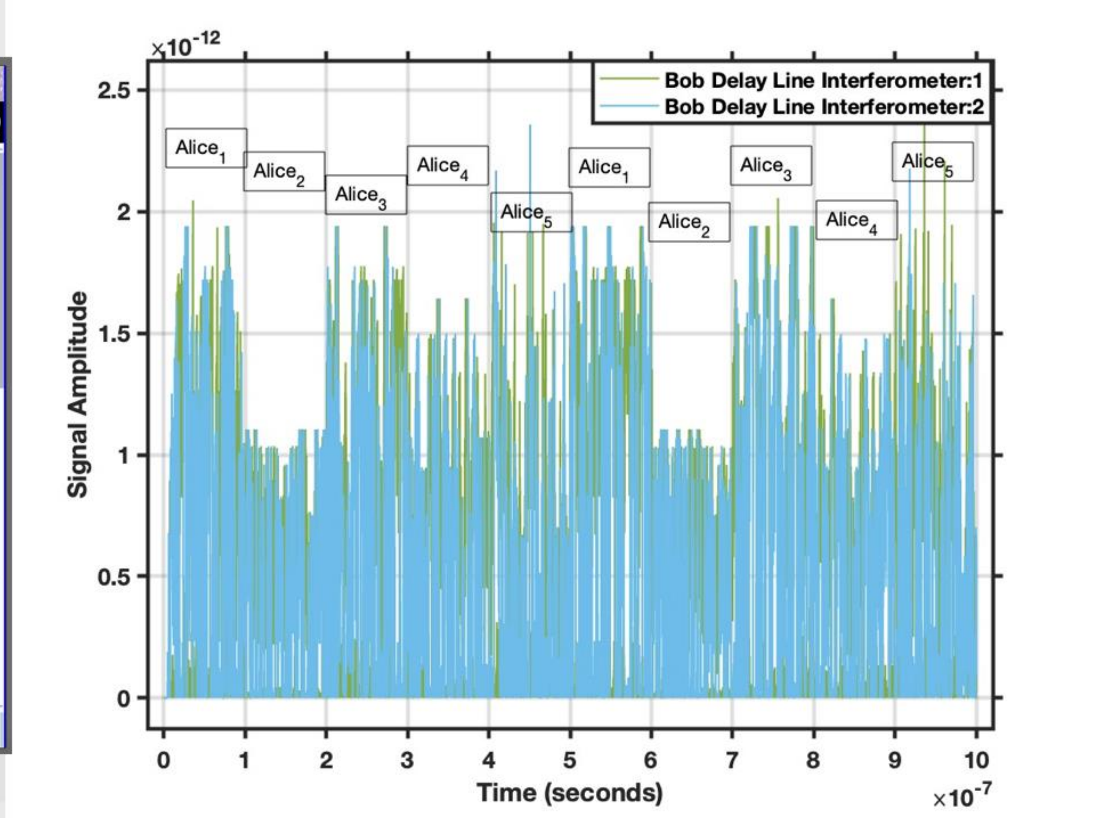
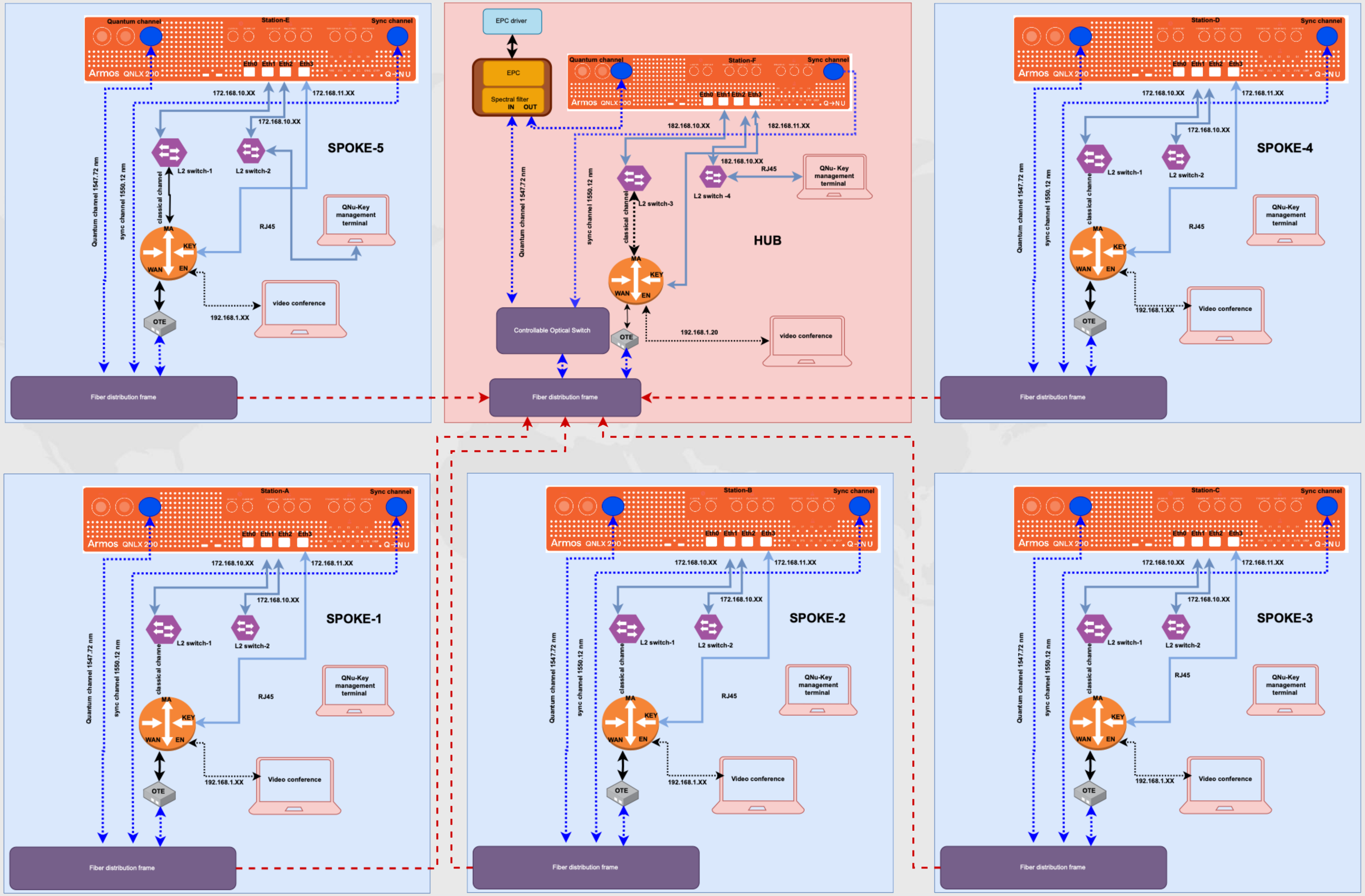


Fig. Dynamical switching mechanism in ChaQra.

ChaQra is live

ChaQra –
1 Hub and
5 Spokes

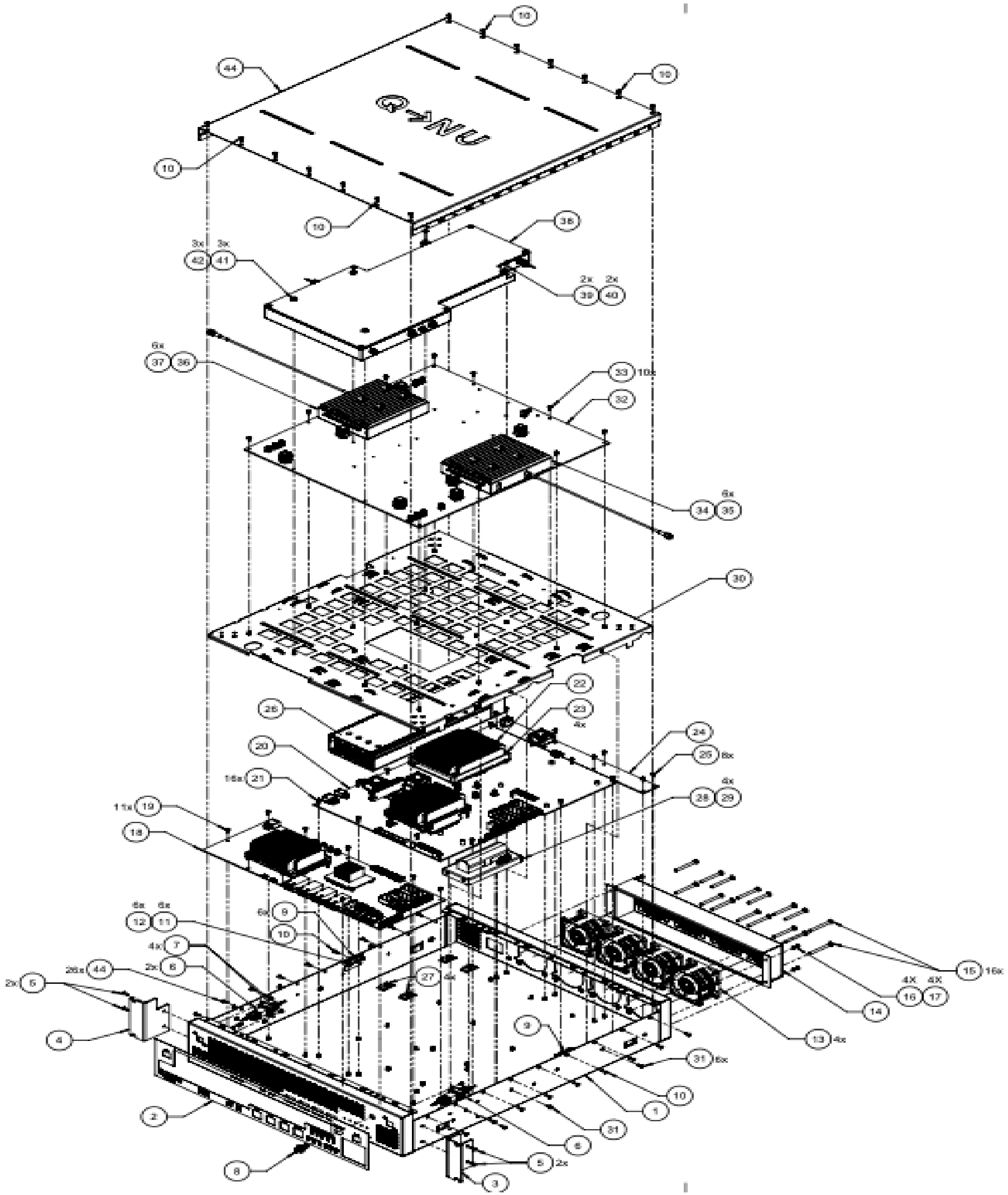


Results – Field tested system

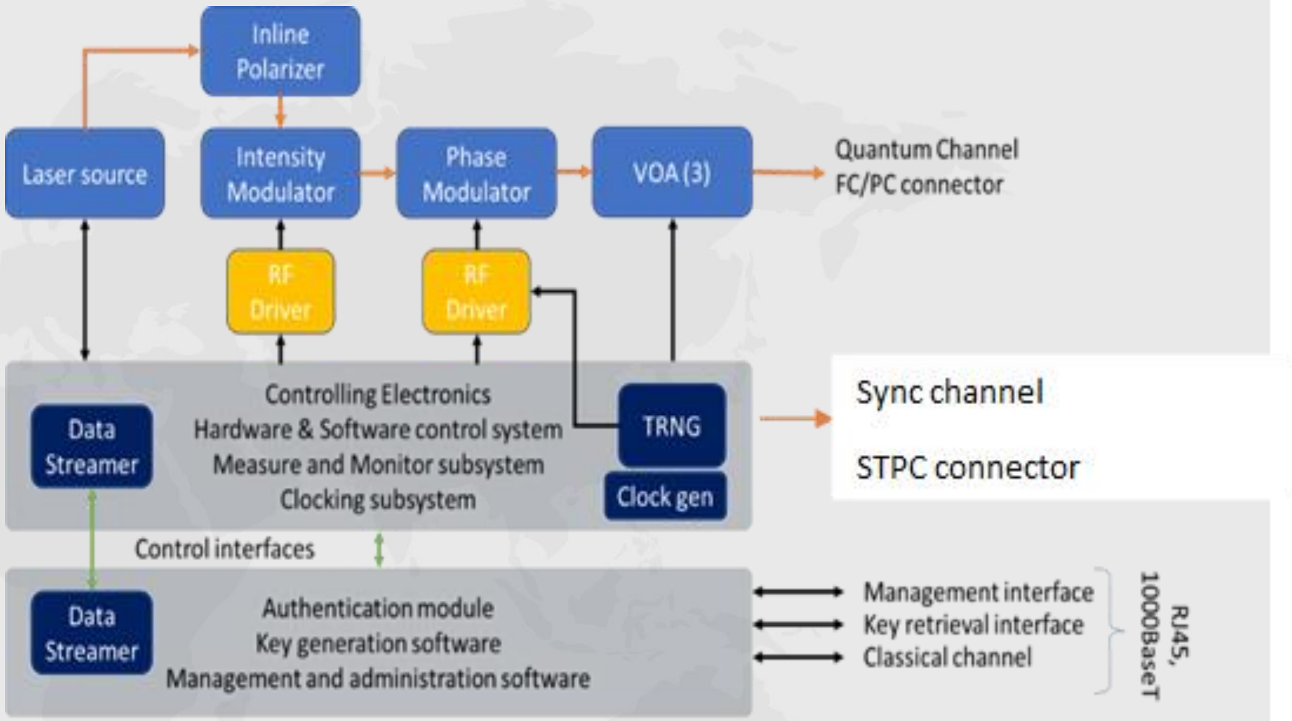
S.No.	Spoke no.	Distance (Km)	Loss (dB)	Key rate (kbps)	QBER (%)
1	A1	100	28	3.2	3.66
2	A2	90	25	6.4	3.34
3	A3	75	18	9.8	3.2
4	A4	65	15	16.2	2.34
5	A5	100	30	1.8	3.5

Table-1. Key specifications of ChaQra. Key rate at lesser loss is limited by the dead time of the single photon detector.

Implementation security



Hardware architecture – Alice node



Inline Polarizer

Laser source

Intensity Modulator

Phase Modulator

VOA (3)

Quantum Channel
FC/PC connector

RF Driver

RF Driver

Controlling Electronics
Hardware & Software control system
Measure and Monitor subsystem
Clocking subsystem

Data Streamer

TRNG

Clock gen

Sync channel

STPC connector

Control interfaces

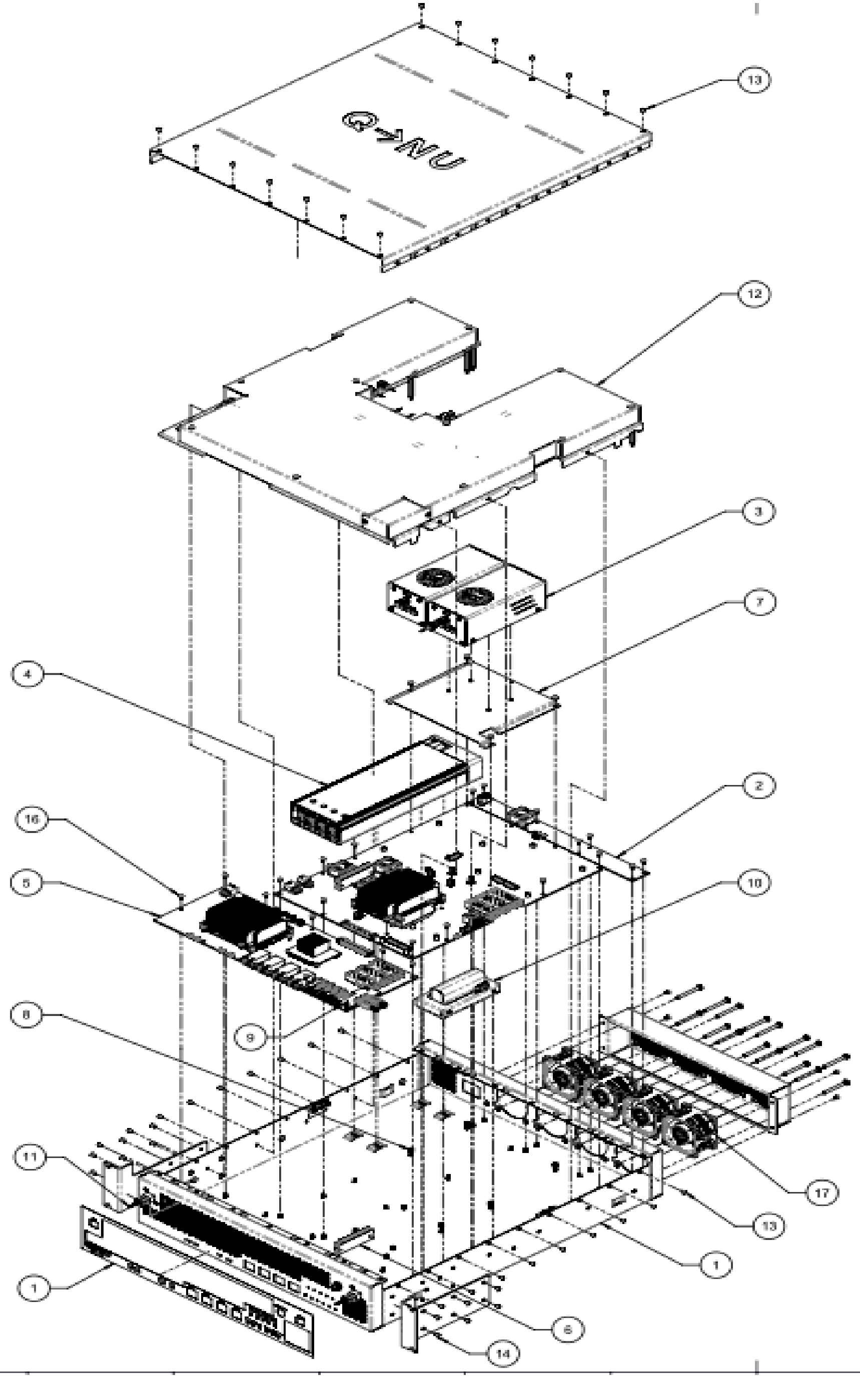
Data Streamer

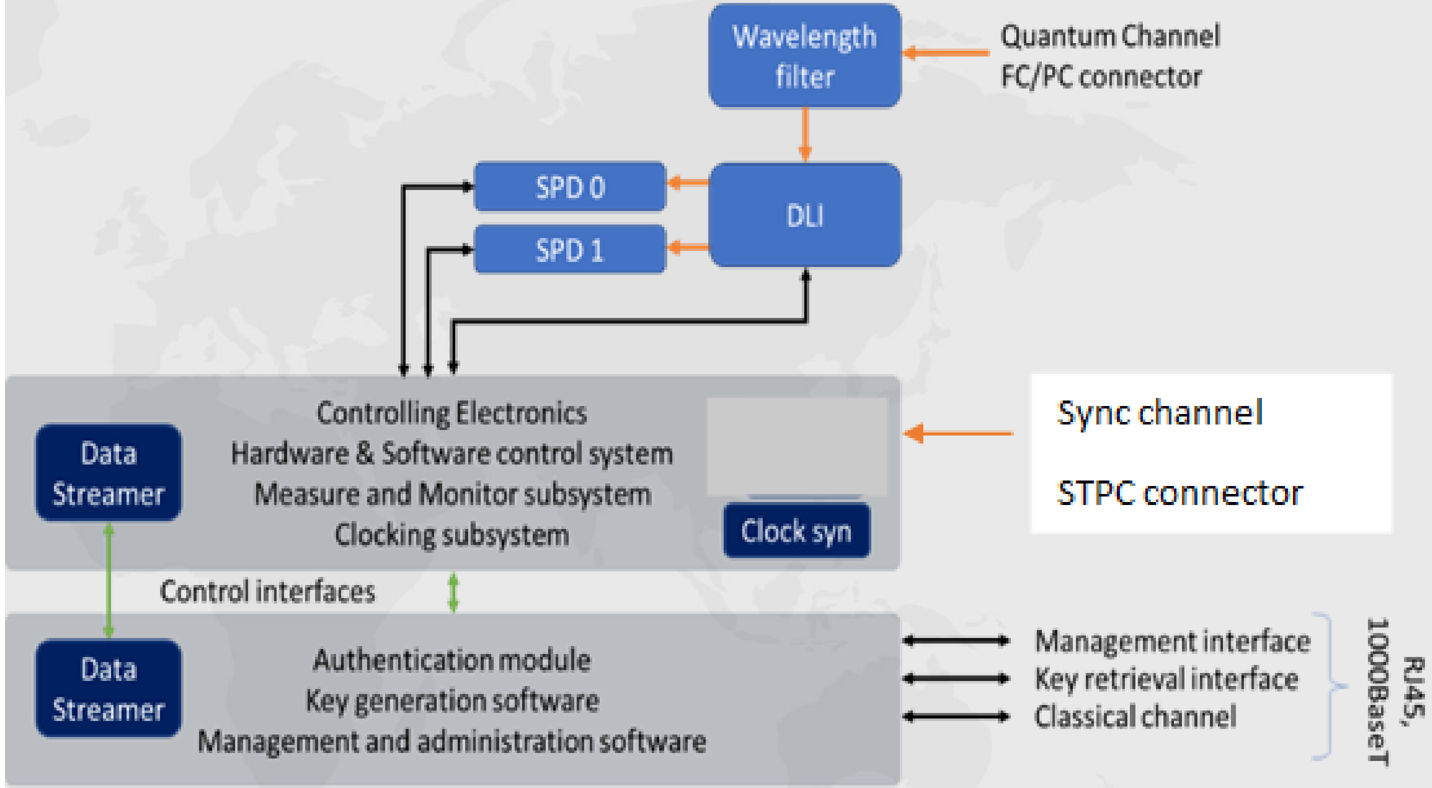
Authentication module
Key generation software
Management and administration software

Management interface
Key retrieval interface
Classical channel

RJ45, 1000BaseT

Hardware architecture – Bob node





Wavelength filter

Quantum Channel
FC/PC connector

SPD 0

SPD 1

DLI

Data Streamer

Controlling Electronics
Hardware & Software control system
Measure and Monitor subsystem
Clocking subsystem

Clock syn

Sync channel

STPC connector

Control interfaces

Data Streamer

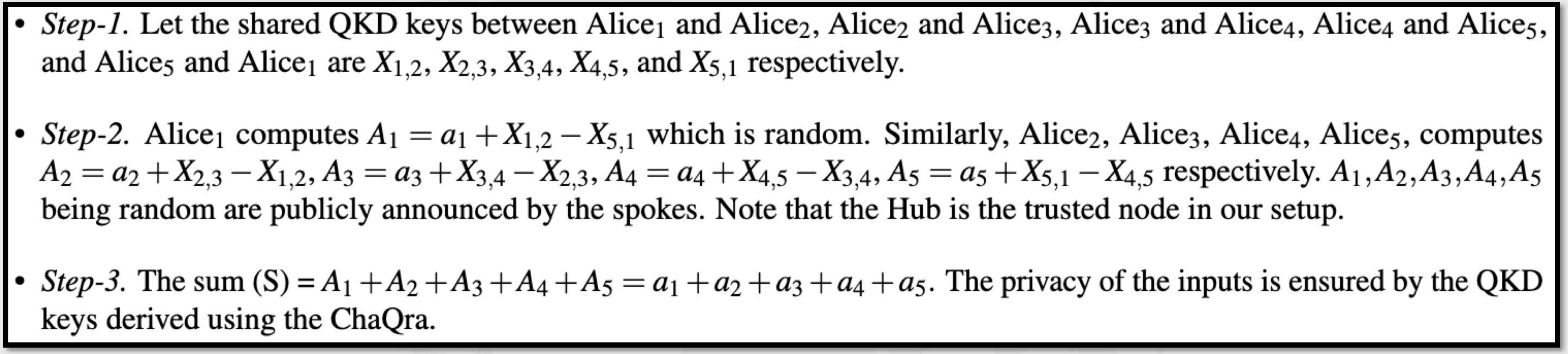
Authentication module
Key generation software
Management and administration software

Management interface
Key retrieval interface
Classical channel

RJ45,
1000BaseT

Beyond QKD

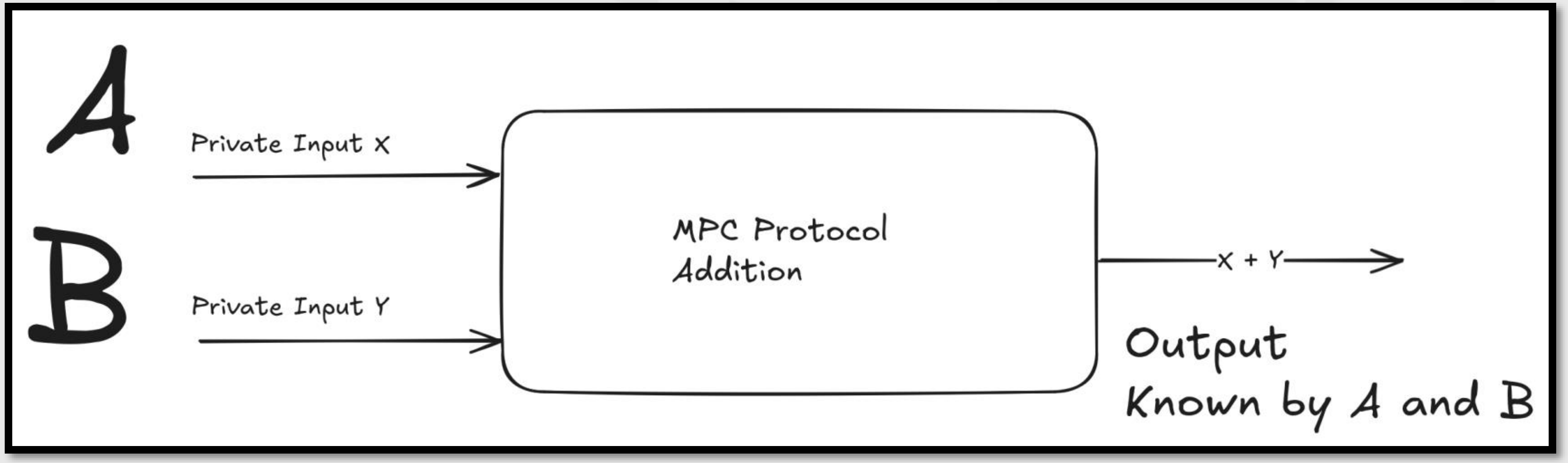
Quantum Multiparty computation



- *Step-1.* Let the shared QKD keys between Alice$_1$ and Alice$_2$, Alice$_2$ and Alice$_3$, Alice$_3$ and Alice$_4$, Alice$_4$ and Alice$_5$, and Alice$_5$ and Alice$_1$ are $X_{1,2}$, $X_{2,3}$, $X_{3,4}$, $X_{4,5}$, and $X_{5,1}$ respectively.

- *Step-2.* Alice$_1$ computes $A_1 = a_1 + X_{1,2} - X_{5,1}$ which is random. Similarly, Alice$_2$, Alice$_3$, Alice$_4$, Alice$_5$, computes $A_2 = a_2 + X_{2,3} - X_{1,2}$, $A_3 = a_3 + X_{3,4} - X_{2,3}$, $A_4 = a_4 + X_{4,5} - X_{3,4}$, $A_5 = a_5 + X_{5,1} - X_{4,5}$ respectively. A_1, A_2, A_3, A_4, A_5 being random are publicly announced by the spokes. Note that the Hub is the trusted node in our setup.

- *Step-3.* The sum (S) = $A_1 + A_2 + A_3 + A_4 + A_5 = a_1 + a_2 + a_3 + a_4 + a_5$. The privacy of the inputs is ensured by the QKD keys derived using the ChaQra.



QKD network is a platform for the shared randomness that will support distributed computing, threshold computation, authentication and lot more

Thank You

qnulabs.com

SparQ Summer Internship - 2025