Quantum Key Distribution (QKD) Demystified:

From Single Photons to Secure Communication.

Dr. Shashank Gupta
Research Lead, QNu Labs

RSA & ECC are Highly Vulnerable

Classical Encryption build on mathematical complexities are obsolete

Quantum Computers

Powerful algorithms like Shor’s algorithm and Grover’s algorithm running on equally powerful computers can crack these encryption standards.

Q→NU

Harvest Now Decrypt Later

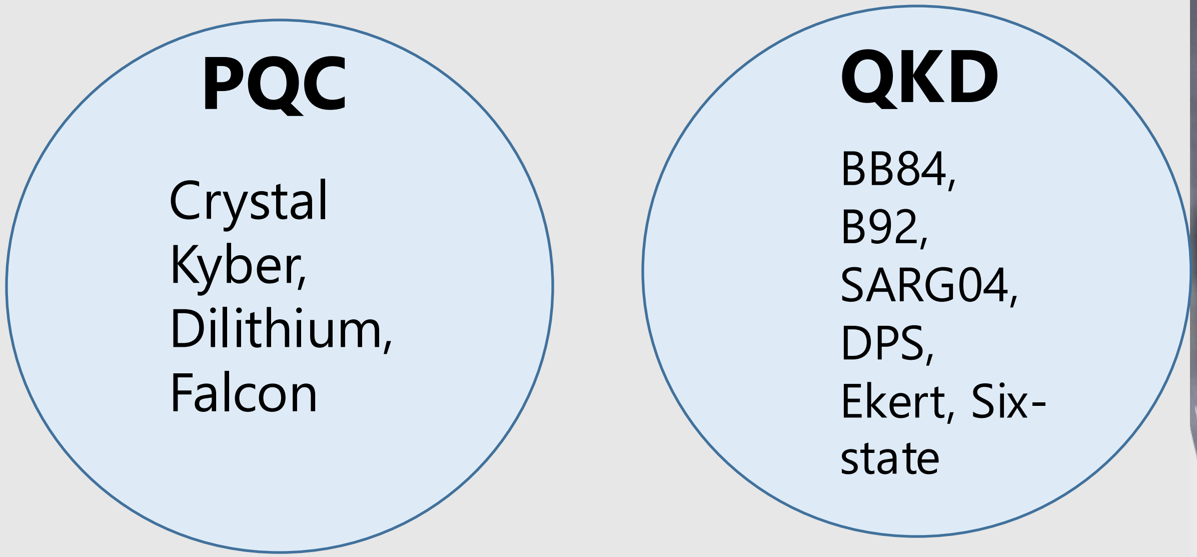
With life of critical data being 10+ years, there is great incentive for hackers to carry out this attack, and crack them later when they have access to larger computing power.

Q→NU

Post-Quantum Security

Conjectured

Information theoretic

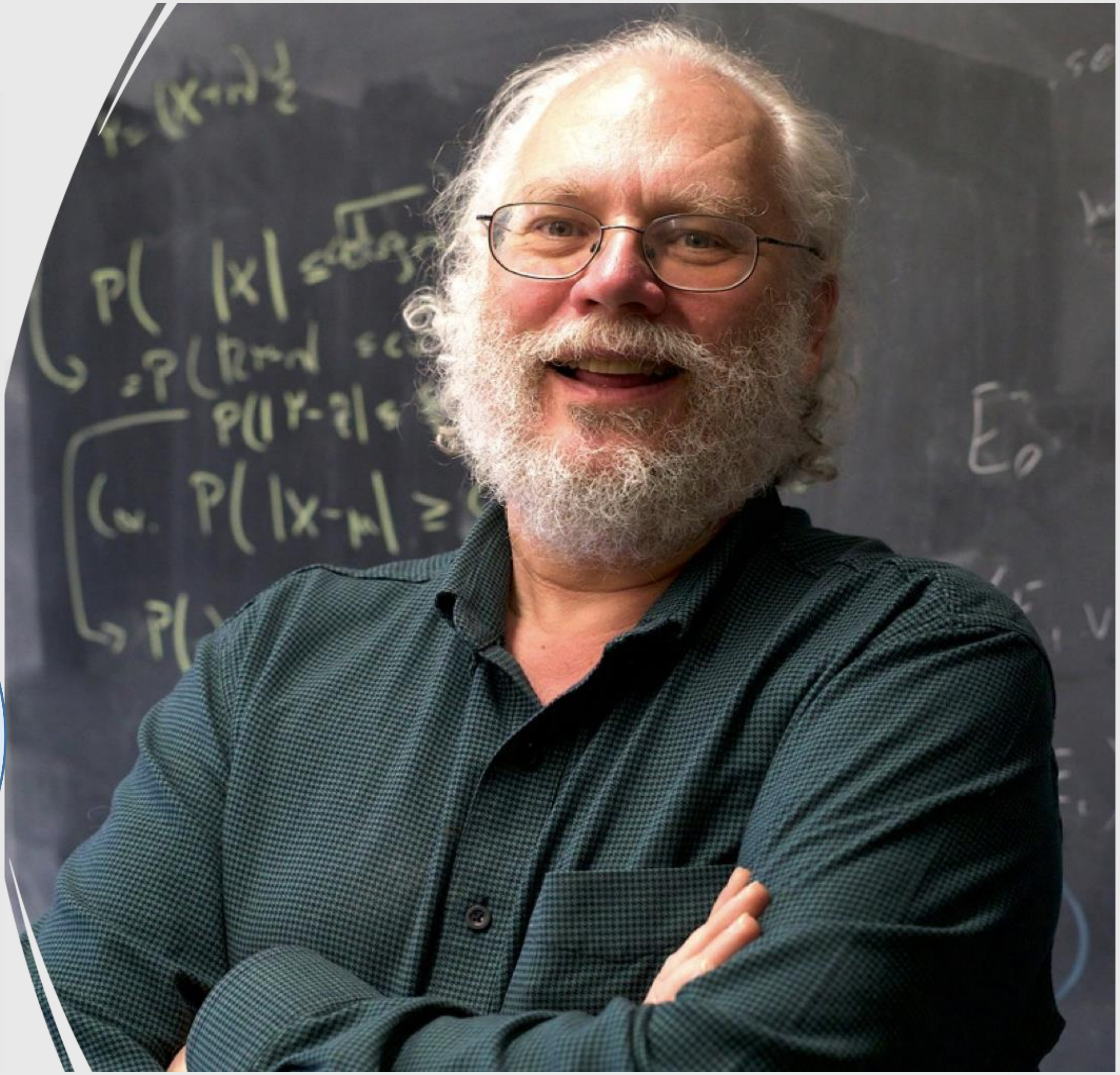


PQC

Crystal Kyber, Dilithium, Falcon

QKD

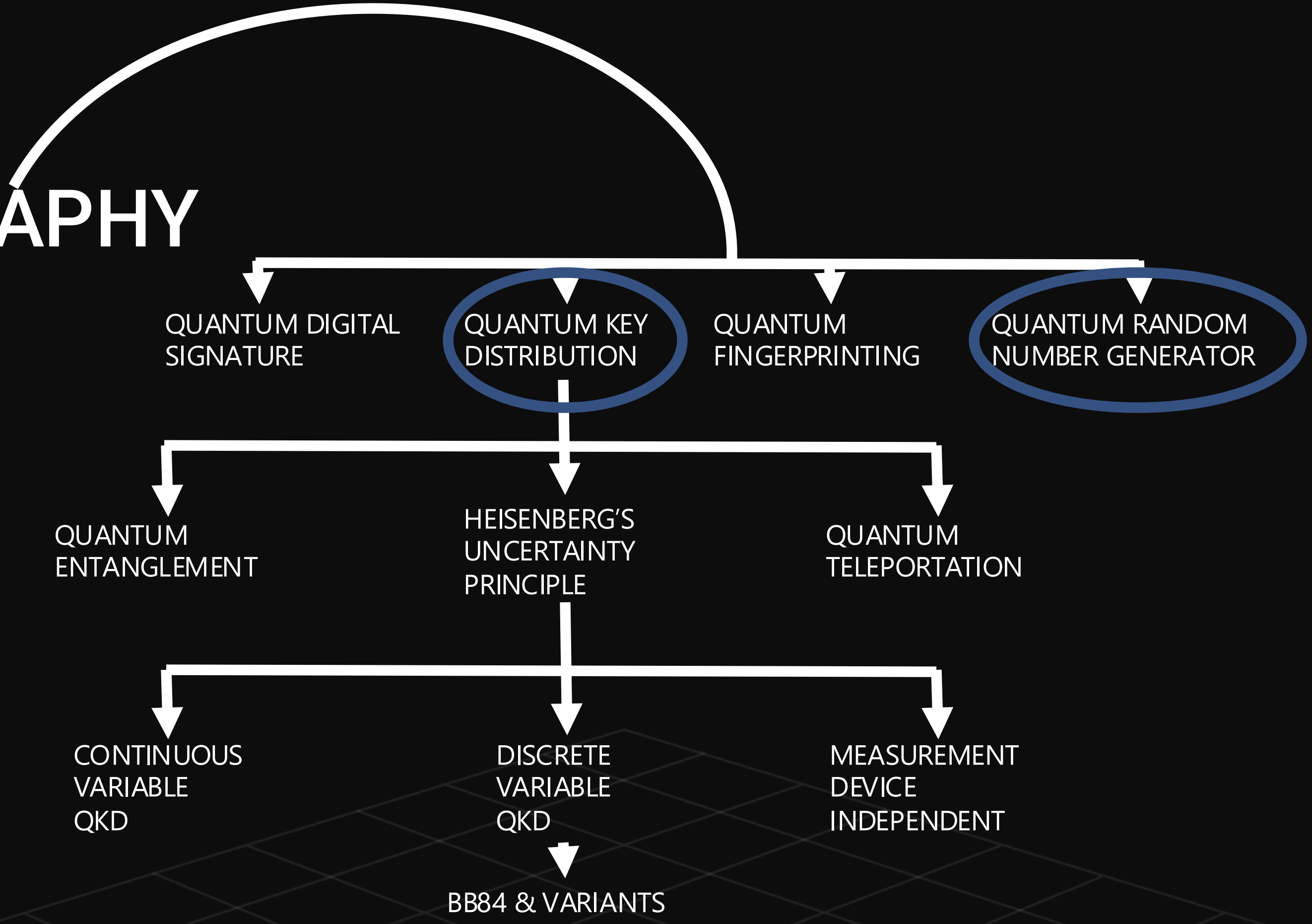
BB84, B92, SARG04, DPS, Ekert, Six-state



PQC: Post Quantum Cryptography

QKD: Quantum Key Distribution

QUANTUM CRYPTOGRAPHY



QUANTUM DIGITAL SIGNATURE

QUANTUM KEY DISTRIBUTION

QUANTUM FINGERPRINTING

QUANTUM RANDOM NUMBER GENERATOR

QUANTUM ENTANGLEMENT

HEISENBERG'S UNCERTAINTY PRINCIPLE

QUANTUM TELEPORTATION

CONTINUOUS VARIABLE QKD

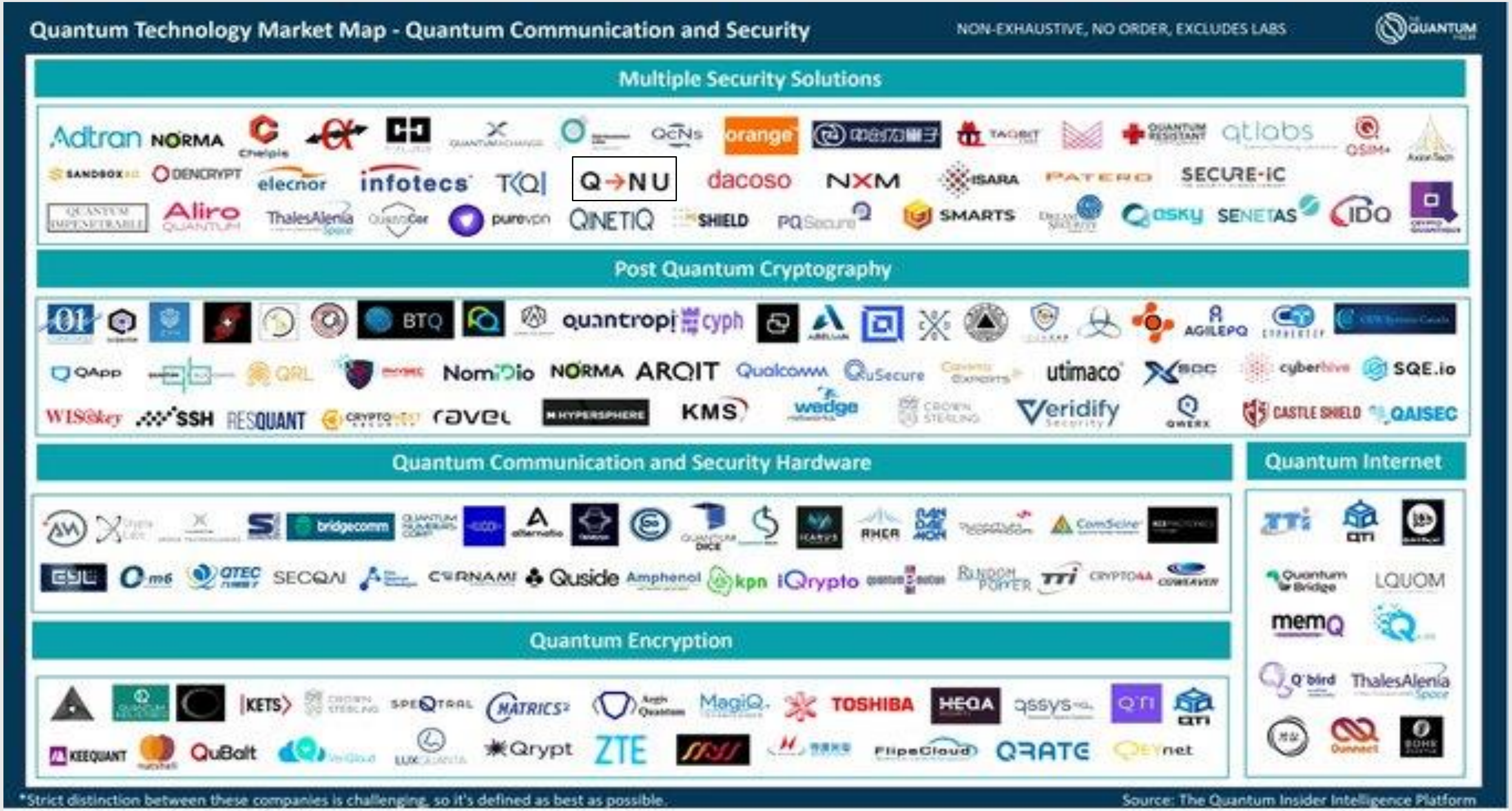
DISCRETE VARIABLE QKD

MEASUREMENT DEVICE INDEPENDENT

BB84 & VARIANTS

Q→NU

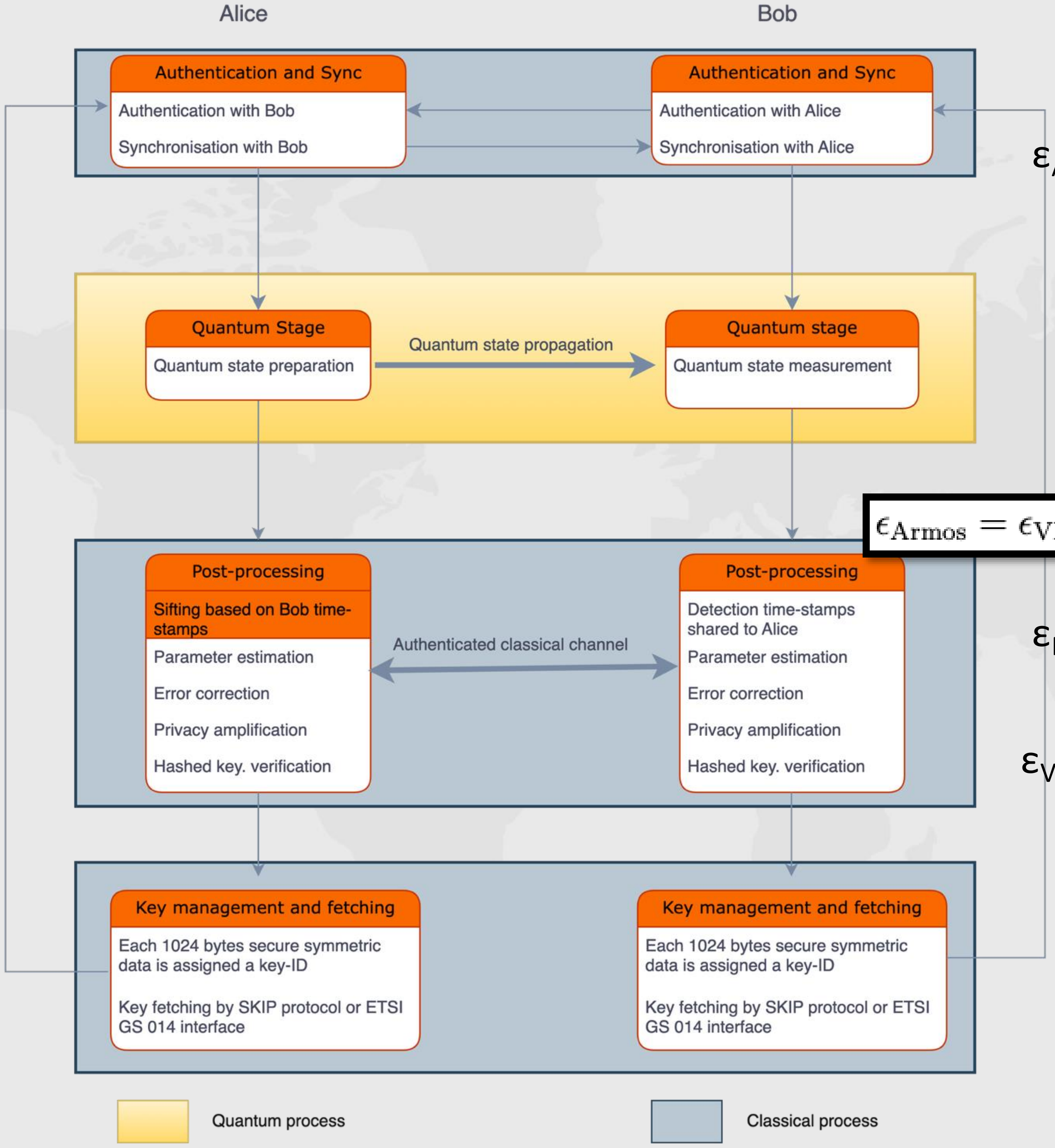
Quantum security companies



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

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

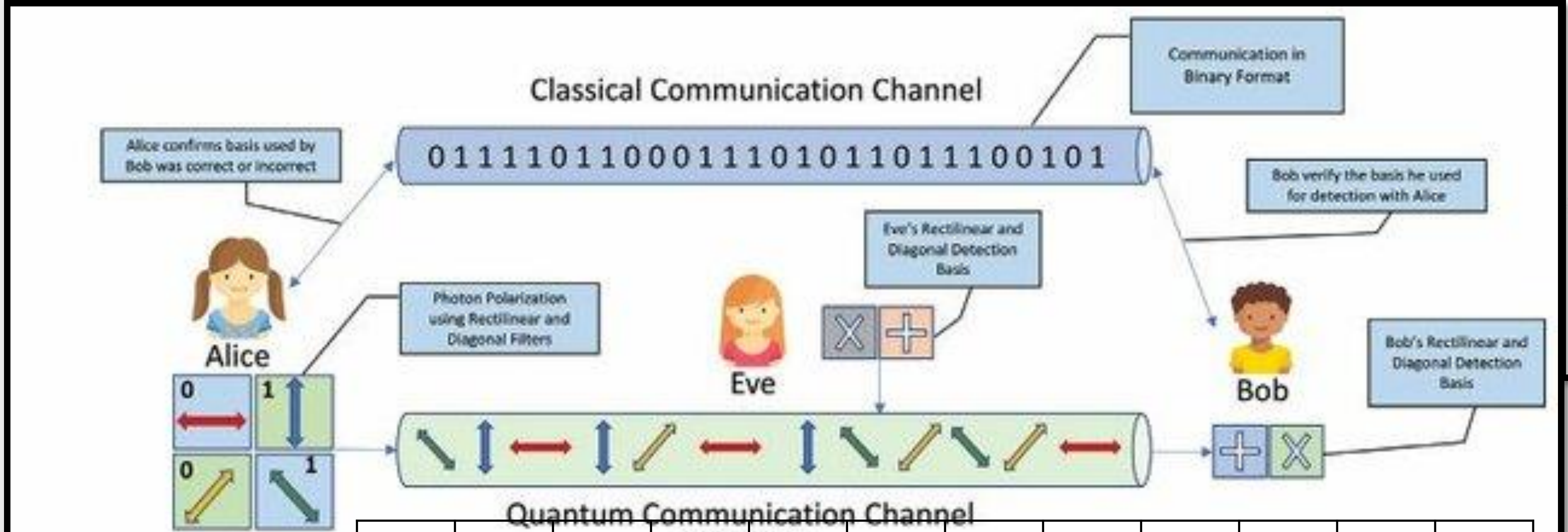
$$\boxed{\epsilon_{\text{Armos}} = \epsilon_{\text{VIS}} + \epsilon_{\text{Smooth}} + \epsilon_{\text{PA}} + 2\epsilon_{\text{VER}} + \epsilon_{\text{MAC}} \lesssim 3 \times 10^{-12}}$$

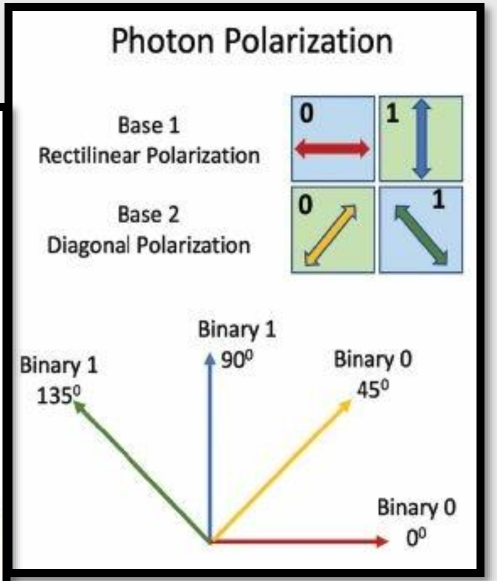
$\varepsilon_{\mathrm{PE}} \leq 9 \times 10^{-13}$.

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

Point-to-Point QKD

Protocol: BB84


Classical Communication Channel
0111101100011101011011100101
Communication in Binary Format
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 basis sequence	1	0	0	0	1	0	0	1	1	1	1	0
Alice's bit sequence	1	1	0	1	0	0	1	1	0	1	0	0
Alice's Photon Polarization	⤡	↕	↔	↕	⤢	↔	↕	⤡	⤢	⤡	⤢	↔
Bob's detection basis	☒	⊞	☒	⊞	⊞	⊞	⊞	☒	⊞	☒	☒	☒
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

Q→NU

Protocol: Decoy-DPS

Armos protocol - Decoy-DPS

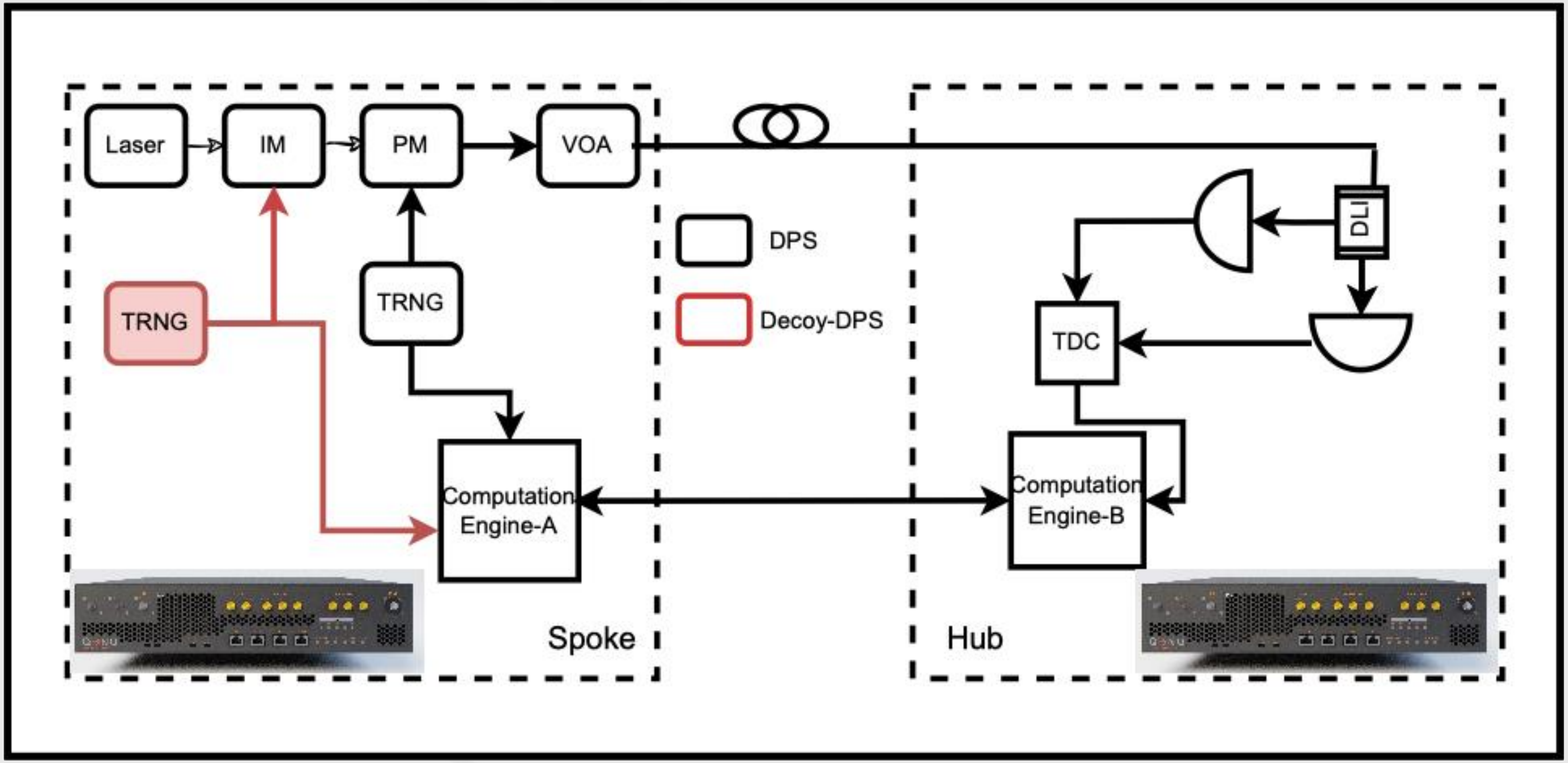


Fig. Block diagram of the QKD systems constituting ChaQra.

Point-to-Multipoint QKD (ChaQra)

Quantum secured Indian Subcontinent

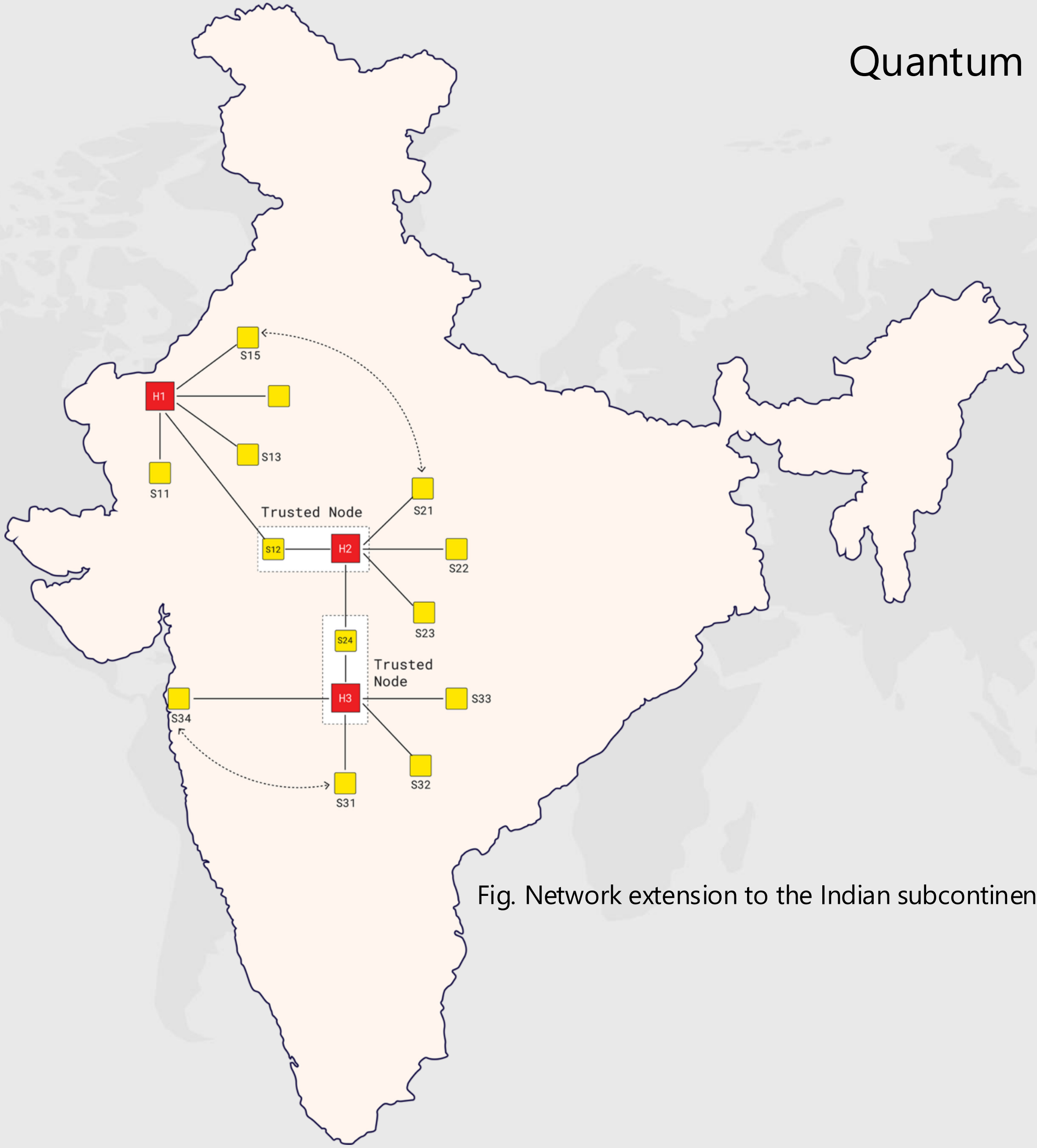
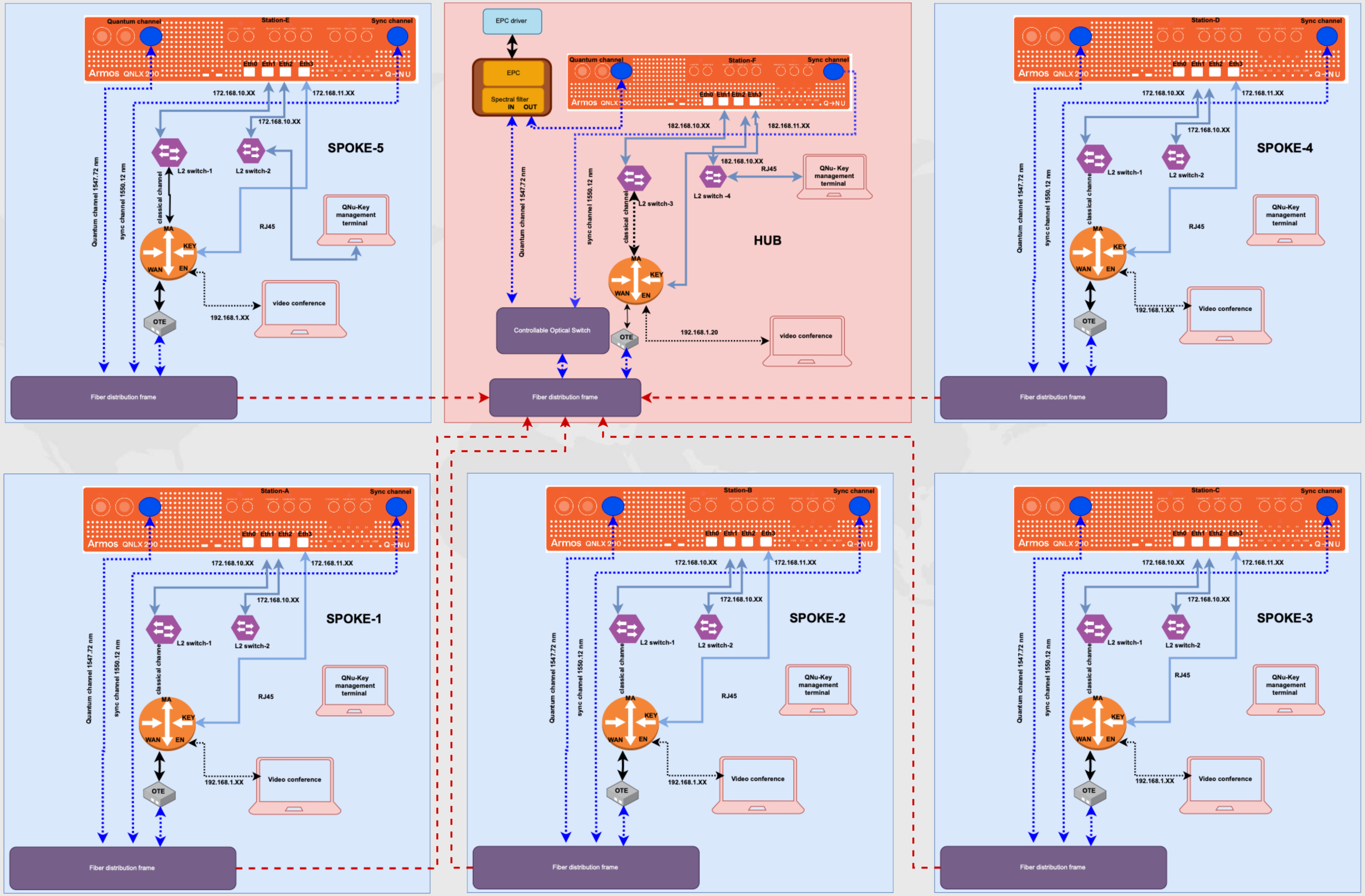


Fig. Network extension to the Indian subcontinent using ChaQra as a cellular unit.

ChaQra is live

Q→NU

ChaQra – 1 Hub and 5 Spokes



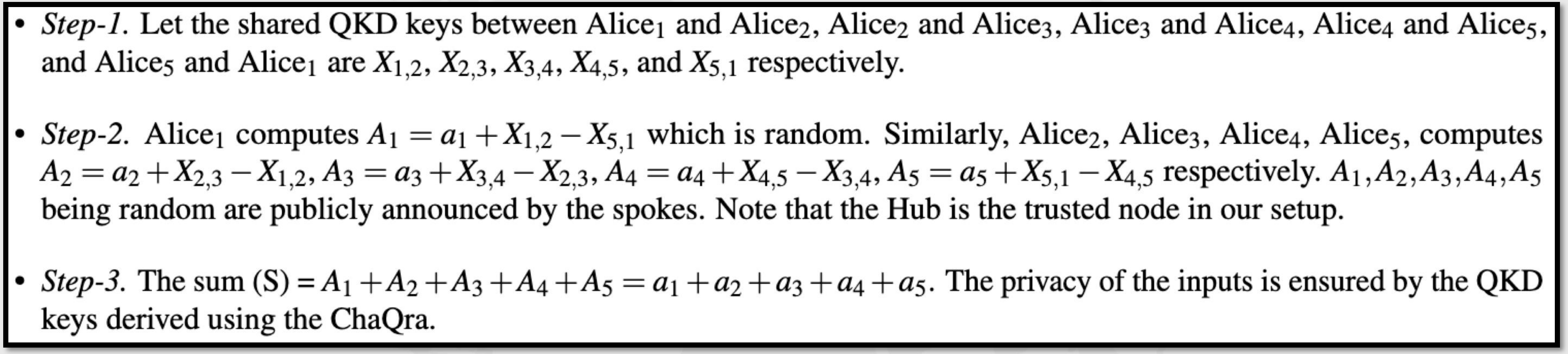
Results – Field tested system

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.

Beyond QKD

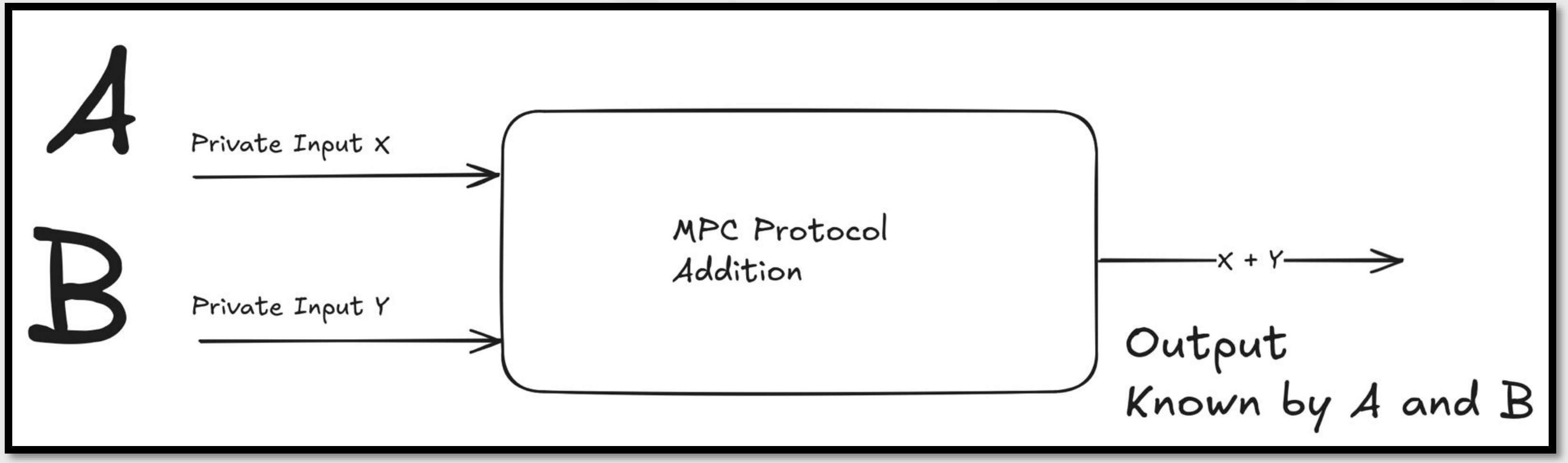
Quantum Multiparty computation



- *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.

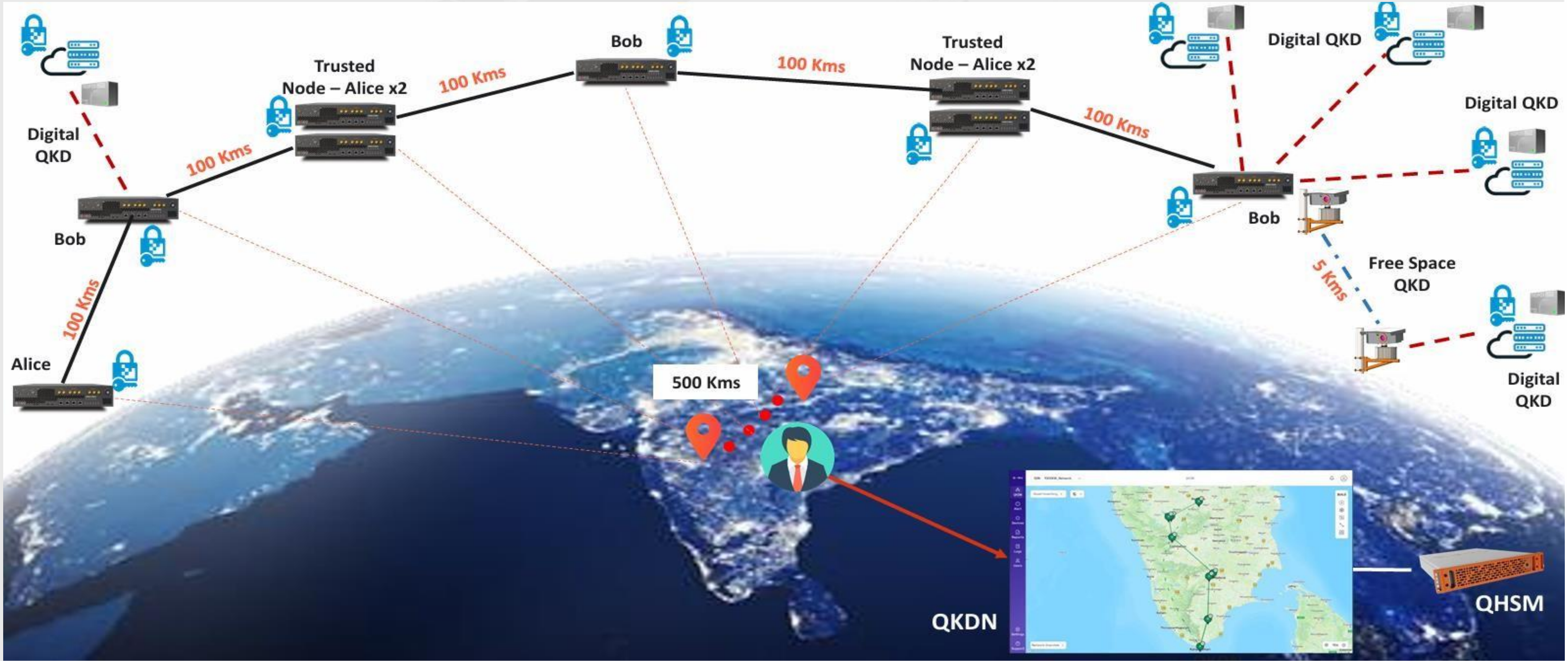
- *Step-3*. The sum (S) = $A_1 + A_2 + A_3 + A_4 + A_5 = a_1 + a_2 + a_3 + a_4 + a_5$. The privacy of the inputs is ensured by the QKD keys derived using the ChaQra.



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

QNu Labs serving National Quantum Mission

National Quantum Mission Deliverables



Q→NU

Quantum Cryptography

Armos (QKD) With Trusted Node in P2P and P2MP

Tropos (QRNG)

Post-Quantum Cryptography

QOSMOS

ENTROPY AS A SERVICE

Q-VPN

QVault

Qverse

mCARP

YOUR OWN QUANTUM LAB

QKDN

Quantum Sensing

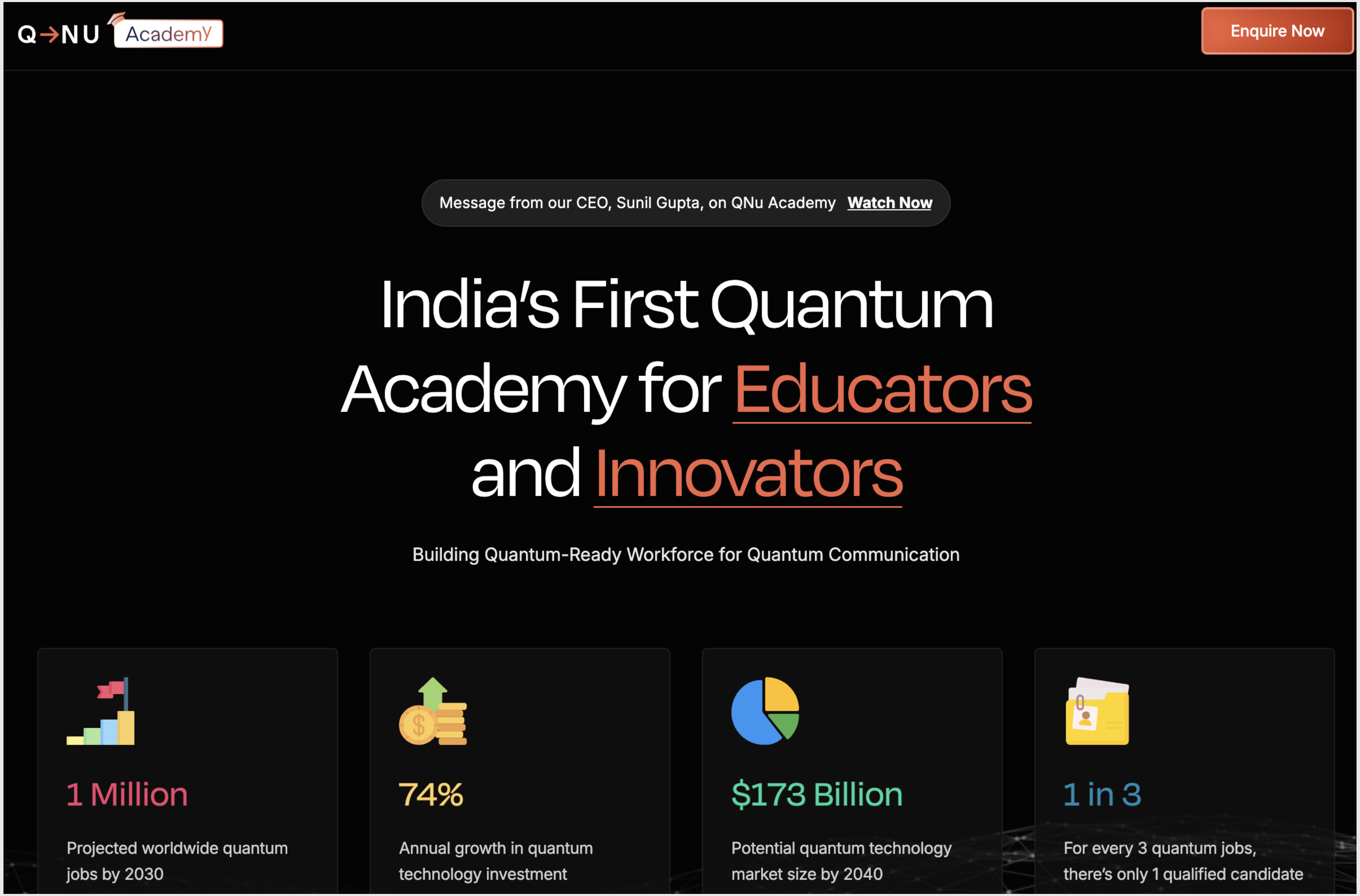
QGuru*

QMag*

* Product under R&D Industry Leading Products and Solutions

Q→NU

Q-->Nu Academy



Message from our CEO, Sunil Gupta, on QNu Academy **Watch Now**

India's First Quantum Academy for Educators and Innovators

Building Quantum-Ready Workforce for Quantum Communication

1 Million

Projected worldwide quantum jobs by 2030

74%

Annual growth in quantum technology investment

$173 Billion

Potential quantum technology market size by 2040

1 in 3

For every 3 quantum jobs, there's only 1 qualified candidate

Q→NU

Q→NU

Thank You

qnulabs.com

SparQ Summer Internship - 2025