

From PKI to Quantum-Secure Networks: Where Does QKD Fit?

Harinee Natarajan

Co-founder & CEO, Qrypta Comm

Invited talk • Q-Entangle 2026 • Bengaluru



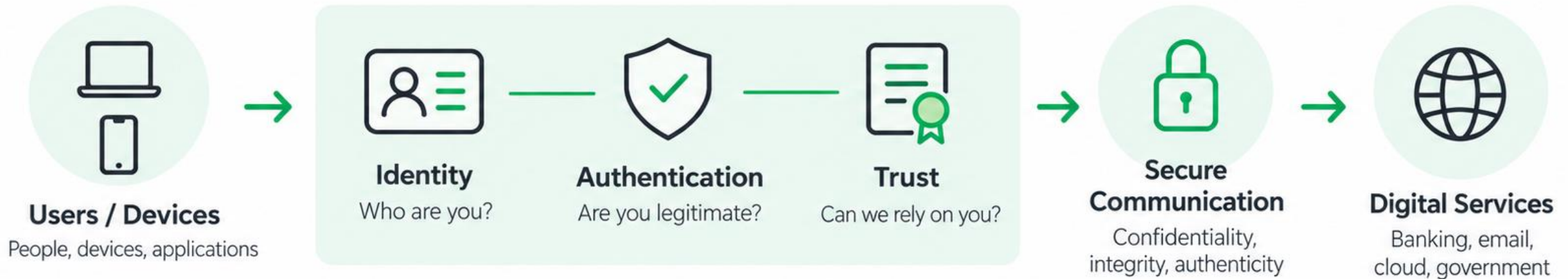
ABSOLUTE TIMING. UNBREAKABLE TRUST.



Indian Institute
of Science, Bengaluru

We already have an infrastructure for **digital trust**

Every time we go online, an invisible trust infrastructure works together to keep communication secure.



UNDERPINNED BY



PKI

Certificates & trust frameworks



Cryptography

Protocols & algorithms



Key Management

Generation, storage, rotation



Trust Infrastructure

CAs, standards, policies

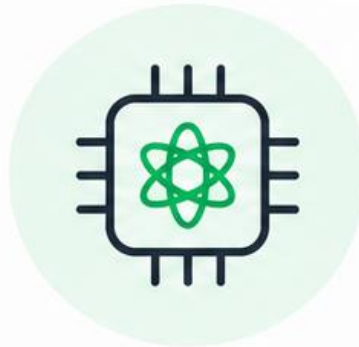
The security we rely on today is at risk tomorrow

Quantum computers threaten widely used public-key cryptography, putting today's digital trust model at risk.



Classical Cryptography

Secures digital communication today
Examples: RSA, ECC



Quantum Computers

Sufficiently powerful quantum
computers threaten RSA and ECC



We need new solutions

To keep data and communications
secure in a post-quantum world.



Web
browsing



Banking &
payments



Email &
communication



What is hard
to break today...

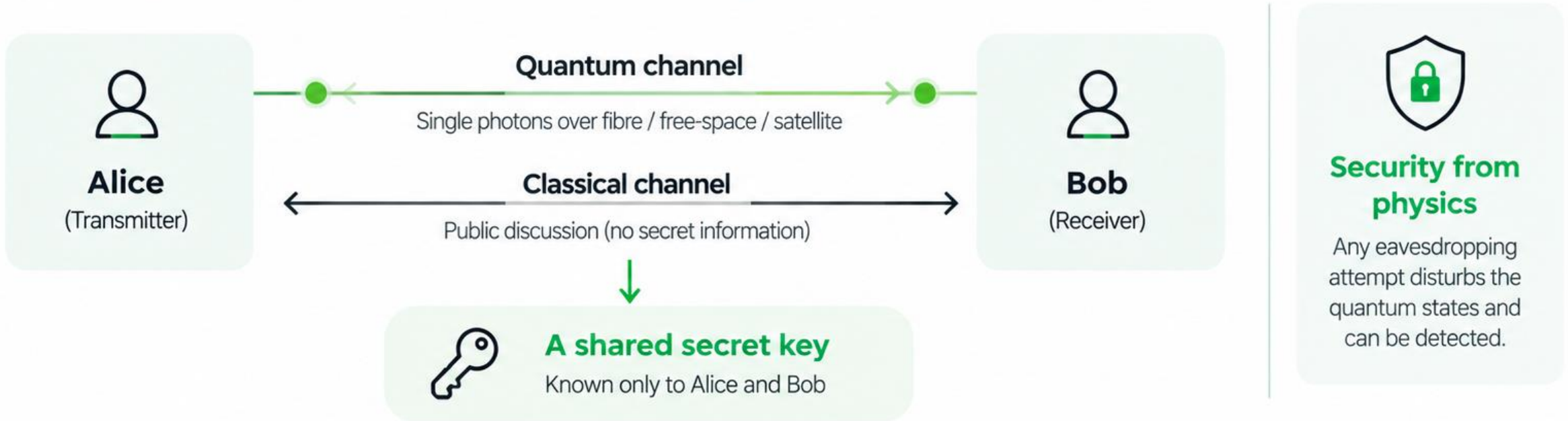


...may not remain
secure in the future.

This is why both **PQC** and **QKD** enter the conversation.

My world: Quantum Key Distribution (QKD)

QKD uses the laws of quantum physics to enable two distant parties to establish a shared, secret key, with the ability to detect eavesdropping.



Confidentiality

Generates shared random keys with information-theoretic security.



Eavesdropper detection

Security comes from the laws of quantum mechanics.



Technology platforms

Implemented over optical fibre, free-space and satellite links.

But a QKD link **isn't a network**

Moving from a point-to-point QKD link to a real, scalable quantum-secure network brings new challenges.

1. Point-to-point link



Demonstrates QKD and generates shared keys.

2. Multi-node network



Connect multiple users across a network.

3. Real-world infrastructure



Fibre, free-space or satellite links integrated with telecom networks.

Towards a quantum-secure network



A resilient, scalable network delivering quantum-secure keys in real environments.

Key practical challenges



Distance & loss

Photon loss limits range and key rate.



Key rate

Trade-off between rate, distance and security.



Hardware

High-performance and stable sources and detectors.



Network architecture

Trusted vs. untrusted nodes, routing and key management.



Timing & stability

Precise synchronization and long-term operation.

But who are **Alice and Bob**?

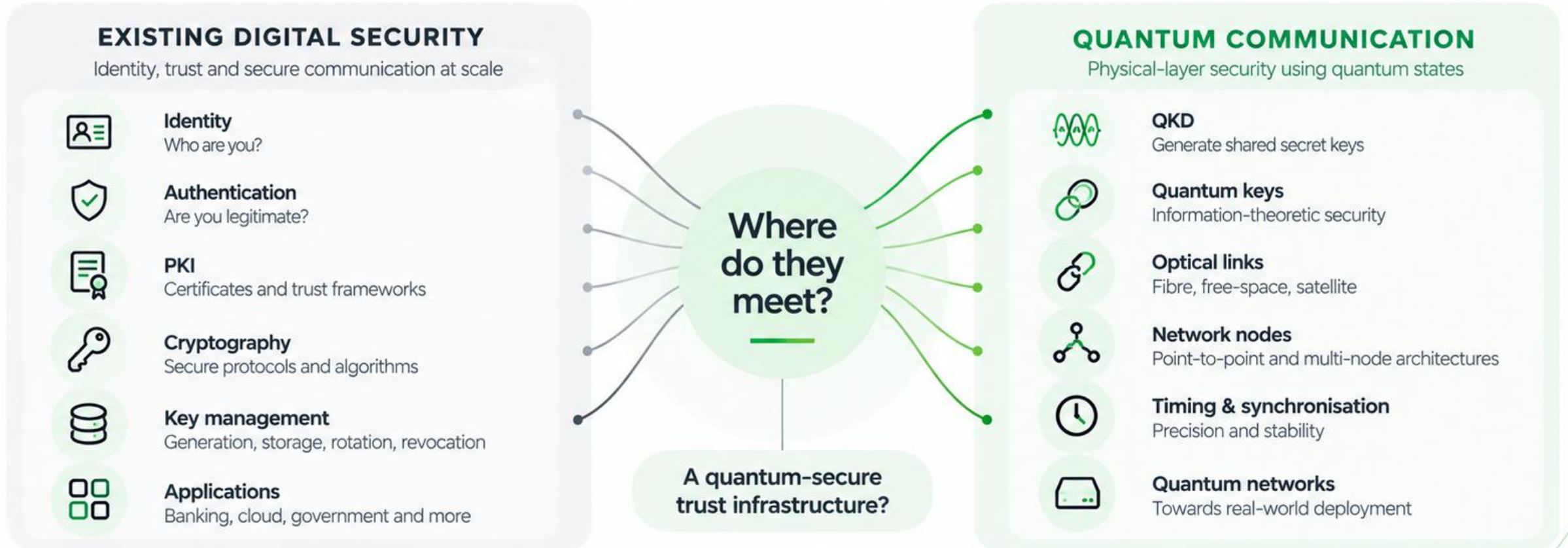
Generating a quantum key is not the same as knowing who you are communicating with.



**A quantum key link gives us security at the physical layer.
Building a trusted communication system requires much more.**

Two worlds. One question.

Existing digital security and quantum communication solve different parts of the problem.
The real opportunity lies in how they come together.



How do we integrate quantum-generated keys into today's security infrastructure?

What does the **bridge** actually need?

If QKD enters an existing security infrastructure, the physics is only one part of the story.



QKD may generate the keys, but trust infrastructure makes them usable.

Where this question becomes **practical**

What we're building at Qrypta Comm

Qrypta Comm is building QryptOS to make quantum-secure networks scalable, deployable and economically viable for critical networks.



We started by trying to make **QKD scalable**. In doing so, we ran directly into the **integration questions** discussed today.

Two paths forward. Likely one hybrid transition.

PKI + PQC + QKD, or a more quantum-native trust layer?

1 Extend today's trust stack



PKI

Identity & trust



PQC

Algorithm upgrade



QKD

High-assurance links



KMS / Apps

Mostly familiar systems

Evolutionary path

Likely answer:
Hybrid



Keep PKI where it works



Deploy PQC broadly



Use QKD where it matters



Redesign gradually

Practical transition = hybrid

2 Rethink the architecture



Trust + keys

Designed together



Quantum network

First-class infrastructure



Identity / policy

May evolve



Apps

Consume a new trust layer

Transformational path



The destination may be new. The transition will likely be **hybrid**.

Where Does QKD Fit?

An open question for a quantum-secure future



What should we **preserve**?



What needs to **change**?



What should a **quantum-secure trust** architecture become?

I'd like to **learn** from this community.



Contact us at:
ceo@qryptacomm.com



QRYPTA COMM

ABSOLUTE TIMING. UNBREAKABLE TRUST.