

QUANTUM KEY DISTRIBUTION.



Quantum key distribution uses the physics of single photons, not computational difficulty, to exchange encryption keys — **any attempt to intercept the key measurably disturbs it, but everything else in the network still depends on ordinary security discipline.**

- PHOTON KEY EXCHANGE
- EAVESDROPPING DETECTION
- TRUSTED-NODE RELAYS
- DISTANCE LIMITATIONS

01 THE MECHANISM

No-Cloning & Disturbance

An unknown quantum state cannot be copied perfectly, so **any attempt to intercept and read the photons in transit measurably disturbs them** — a physical law, not a computational assumption an attacker might one day break.

Encoding & Basis Sifting

Key bits are encoded into photon properties — typically polarization — using randomly chosen bases (as in BB84). Sender and receiver compare basis choices over a public channel and **keep only the bits measured in a matching basis.**

Error Correction & Privacy Amplification

The sifted key still carries channel noise and any partial information an eavesdropper may have gained. **Error correction and privacy amplification distill it down** to a shorter key with a bounded, quantifiable security margin.

02 THE FLOW

The Correctly Deployed QKD Link

CONTAINED

1

Photons cross a dedicated fiber or free-space link; a statistical sample is measured for an elevated quantum bit error rate (QBER) **before any key material is trusted.**

2

Sifting, error correction, and privacy amplification run over a classical channel that is **already authenticated with a pre-shared or PQC-derived credential**, so a substituted session is rejected.

3

The distilled key is consumed immediately by a standard symmetric cipher — QKD hands off **key material, not a general-purpose secure channel.**

The Naive / Unhardened Deployment

EXPOSED

1

The classical channel's authentication relies on a weak or reused pre-shared secret, letting an attacker run a full man-in-the-middle **against both channels, undetected.**

2

Because photon loss caps direct fiber links around 100–200km, key material passes through **trusted-node relays that decrypt and re-encrypt it in the clear** at every hop.

3

Downstream systems treat "quantum-secure key exchange" as a blanket guarantee, while **endpoint malware or a weak cipher implementation** undoes it entirely.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Quantum Channel Integrity	The physical link — fiber or free-space — carrying single-photon states, engineered to keep loss and noise inside the bound where eavesdropping detection stays statistically valid.
Authenticated Classical Channel	The public channel carrying sifting, error-correction, and privacy-amplification traffic; it must already be authenticated before a QKD session starts, since QKD cannot bootstrap that trust itself.
Key Distillation & Management	Error correction, privacy amplification, and secure handoff of the resulting symmetric key into a standard cipher such as AES, IPsec, or MACsec.
Network Topology	How range is extended past direct fiber-loss limits — trusted-node relays today, with quantum repeaters and satellite-to-ground links still largely experimental.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
QKD Hardware Alone, No Prior Authentication	No	Without an already-authenticated classical channel, an attacker can man-in-the-middle both the quantum and classical legs from session one.
Trusted-Node Relay, Unhardened Hops	No	Decrypts key material in the clear at every intermediate node; compromising a single relay compromises every key that passes through it.
QKD as a Drop-In PKI Replacement	No	Distributes symmetric key material point-to-point — no digital signatures, no PKI-style identity, no internet-scale reach.
Treating QKD as Interchangeable With PQC	No	Different problems: PQC swaps in quantum-resistant math via a software update; QKD needs new optical hardware and dedicated links.
QKD + Authenticated Channel + Hardened Relays + Standard Crypto Downstream	Yes	Combines physical-layer eavesdropping detection with the conventional controls for everything QKD itself does not cover.

QUANTUM KEY DISTRIBUTION.

DETECT · DISTILL · DEPLOY

05 PROGRAM OPERATIONS

QKD secures key distribution over a physical link, not application-layer trust.

The distilled key still has to be consumed correctly by symmetric cryptography and ordinary application security controls.

Range is fundamentally limited by photon loss,

roughly 100–200km over standard fiber — real deployments need trusted-node relays or satellite links, each with its own operational and physical security requirements.

The classical authentication channel is a hard dependency, not an afterthought.

QKD cannot bootstrap its own authentication and depends on pre-shared or PQC-derived credentials, managed like any other key material.

Detection is statistical, not retroactive.

An elevated QBER flags likely eavesdropping and the session's key is discarded — it does not undo any exposure that occurred on classical infrastructure around the quantum link.

06 CONTROL MAPPING

ETSI GS QKD

Industry Specification Group standards for QKD system architecture and application interfaces, aimed at interoperability between vendor implementations.

ITU-T Y.3800 SERIES

Network-level framework and requirements for integrating QKD into telecom infrastructure, including key-management interfaces and functional architecture.

ISO/IEC 23837-1/-2

Security requirements and standardized test/evaluation methods for QKD modules — the closest thing to a certifiable security baseline for QKD hardware.

NSA CNSA 2.0 GUIDANCE

Explicitly does not endorse QKD for national security systems, citing unresolved implementation risk, and directs agencies toward post-quantum cryptography instead.

07 WHAT THIS DOES NOT SOLVE

Authentication & Identity

QKD does not authenticate the parties on a link; it needs **pre-existing trusted credentials** — classical PKI, pre-shared keys, or PQC signatures — to know who it's actually talking to.

Digital Signatures & Non-Repudiation

QKD produces symmetric key material only. **Signing documents, code, or transactions** still requires public-key cryptography, increasingly PQC-based.

Endpoint & Implementation Security

A quantum-secure key is only as strong as the classical systems around it — **malware, weak cipher implementations, or detector side-channels** undercut the theoretical guarantee.

Internet-Scale, Software-Only Deployment

QKD needs purpose-built optical hardware and dedicated links. Unlike PQC, **it cannot be rolled out as a software update.**

08 MYTHS VS. REALITY

MYTH	REALITY
“QKD makes a network unhackable.”	It secures only the key-exchange step on one link — it does nothing for compromised endpoints or attacks on the surrounding classical infrastructure.
MYTH	REALITY
“QKD and post-quantum cryptography solve the same problem.”	PQC swaps in quantum-resistant math via software; QKD distributes keys via physics over dedicated hardware — most near-term migration plans center on PQC.
MYTH	REALITY
“Quantum key distribution has unlimited range.”	Single-photon signals attenuate in fiber, capping direct links around 100–200km; longer distances need trusted-node relays or experimental quantum repeaters.
MYTH	REALITY
“Detected eavesdropping means the attacker learned nothing.”	Detection means the compromised key is discarded before use — it says nothing about attacks on the classical infrastructure around the link.
MYTH	REALITY
“QKD removes the need for authentication.”	QKD depends on an already-authenticated classical channel to stop a substituted session — it cannot bootstrap that initial trust itself.

09 SPEAK THE PROGRAM — KEY TERMS

BB84 PROTOCOL

The original QKD protocol (Bennett & Brassard, 1984), encoding key bits into **photon polarization across two conjugate bases.**

NO-CLONING THEOREM

The principle that an unknown quantum state **cannot be copied perfectly**, underlying QKD's ability to detect interception.

QUANTUM BIT ERROR RATE (QBER)

The measured error rate in the sifted key; a rate **above expected noise signals possible eavesdropping** and the session is discarded.

PRIVACY AMPLIFICATION

A post-processing step that **compresses the sifted key** to remove any partial information an eavesdropper may have gained.

TRUSTED NODE

An intermediate relay extending QKD past fiber-loss range; it **decrypts key material in the clear** and must be physically secured.

QUANTUM REPEATER

An experimental device meant to extend range **without exposing key material in the clear** at a relay; not yet widely deployed.