Extending QKD Information-Theoretic Security to the Last Mile with Q-Stream

A QRNG-Embedding Framework for End-to-End Unconditional Key Delivery

Adrian Neal
Oxford Scientifica

adrian.neal@oxfordscientifica.com

September 2025

Abstract

Quantum key distribution (QKD) provides provable information-theoretic security by generating shared random keys over quantum channels. Yet its adoption is constrained by the persistent "last-mile problem": distributing QKD-generated keys from backbone or metro quantum links to end-user devices requires classical transport, where conventional cryptography reintroduces computational assumptions and future quantum risks.

We address this challenge with *Q-Stream*, a framework that embeds QKD keys directly into large blocks of quantum-random bits (QRNG outputs) distributed over classical networks. Each block, or Q-Block, is personalised to a recipient using a short secret Defragmentation Key (DFK), which determines the hidden locations of both the QKD key and the next DFK. To any adversary, a transmitted Q-Block is indistinguishable from pure QRNG noise, ensuring that embedding does not reduce the ε-security of the underlying QKD key.

This construction applies *Operational Perfect Secrecy* (OPS), a generalisation of Shannon's secrecy model, to bridge quantum backbones with classical information-theoretic channels. The result is a practical mechanism for last-mile delivery of QKD keys that preserves unconditional security end-to-end. We present deployment architectures combining QKD master nodes with Q-Stream edge proxies, and discuss applications in financial trading, military field communications, and critical infrastructure. Our approach resolves a central barrier to the real-world deployment of QKD by securing the last hop without reliance on computational hardness assumptions.

Keywords: Quantum key distribution (QKD); last-mile problem; information-theoretic security (ITS); operational perfect secrecy (OPS); Q-Stream; QRNG embedding; quantum-random blocks; key distribution; hybrid quantum–classical networks.

1 Introduction

Quantum key distribution (QKD) provides a unique cryptographic primitive: the ability for two remote parties to generate shared random keys with information-theoretic security (ITS), guaranteed even against adversaries with unbounded computational or quantum power. Protocols such as BB84 [2] and their modern refinements achieve composable ε-security [10], ensuring that the distributed key is statistically indistinguishable from uniform to any eavesdropper. This makes QKD a compelling candidate for securing communications in a post-quantum world.

Despite this theoretical strength, practical deployment of QKD remains limited by the so-called *last-mile problem*. QKD links can successfully deliver quantum-generated keys between backbone nodes, metropolitan hubs, or trusted data centres, but extending those keys to end-user devices requires classical transport over ordinary networks. At this stage, existing solutions typically rely on computational cryptography (RSA, ECC, or PQC) to bridge the final hop. This reintroduces precisely the risks QKD was designed to remove: reliance on conjectured hardness assumptions and vulnerability to "store-now, decrypt-later" attacks by future quantum computers.

In this paper we address the last-mile challenge by embedding QKD-generated keys into *Q-Stream* Q-Blocks: large blocks of quantum-random bits (QRNG outputs) transmitted over classical networks. Each Q-Block is personalised to a recipient through a short secret Defragmentation Key (DFK) [7], which specifies the hidden positions of both the embedded QKD key and the next DFK for future use. To an adversary without the DFK, a Q-Block is indistinguishable from pure QRNG noise. This embedding mechanism ensures that the original ε-security of the QKD key is preserved, while enabling its transport across entirely classical networks.

Our construction builds on *Operational Perfect Secrecy* (OPS) [6], a generalisation of Shannon's secrecy model that quantifies adversarial success probability rather than enforcing an all-or-nothing secrecy condition. By applying OPS to the embedding process, we demonstrate that QKD keys retain their information-theoretic security classification when carried inside QRNG-derived Q-Blocks. The result is a practical framework for extending QKD into the last mile, enabling end-to-end ITS key delivery from quantum backbones to commodity devices. We outline system architectures combining QKD master nodes with Q-Stream edge proxies, and we highlight applications in financial trading networks, military field communications, and critical infrastructure.

2 Background

2.1 QKD and Information-Theoretic Security

Quantum key distribution (QKD) protocols such as BB84 [2] enable two parties to establish a shared secret key with information-theoretic security (ITS). Unlike classical key exchange mechanisms, QKD does not rely on computational hardness assumptions: its security follows from the laws of quantum mechanics, specifically the no-cloning theorem and the disturbance introduced by measurement. Composable security analyses [10] show that the final QKD key

K is ε-close to uniform, even against adversaries holding arbitrary quantum side information, a property sometimes referred to as *quantum information-theoretic security* (Q-ITS).

2.2 The Last-Mile Challenge in QKD Networks

Practical QKD deployments, such as the SECOQC Vienna network [8] and the Tokyo QKD testbed [9], typically terminate in secure hubs or data centres. Keys must then be transported to end-user devices over classical networks. At this point, existing solutions rely on either trusted relays or post-quantum cryptography (PQC), both of which undermine the unconditional guarantees of QKD. Trusted relays concentrate risk, while PQC bridges reintroduce reliance on conjectured mathematical hardness assumptions [3, 1].

2.3 Operational Perfect Secrecy (OPS)

Shannon's definition of perfect secrecy requires that ciphertext distributions be independent of the underlying message, a binary condition that is difficult to scale. Operational Perfect Secrecy (OPS) [6] generalises this model by quantifying adversarial success probability rather than requiring all messages to be equally likely. OPS enables secrecy guarantees to be maintained under composition and embedding, making it suitable for extending QKD security into classical network segments.

2.4 Quantum Random Number Generators

Quantum random number generators (QRNGs) produce classical randomness by sampling quantum processes such as photon arrival times or phase noise [5]. Although their outputs are classical, they are provably close to uniform and independent of adversaries, making them suitable as cover randomness for embedding operations. In the Q-Stream framework, QRNG-derived blocks (*Q-Blocks*) serve as carriers into which QKD keys can be hidden, producing distributions indistinguishable from pure quantum noise to any external observer.

2.5 Q-Stream

Q-Stream is a framework introduced in prior work [7] for distributing arbitrary-length symmetric keys with information-theoretic security guarantees. Its design is based on the concept of *Q-Blocks*, large blocks of quantum-random bits generated by a QRNG, and *Defragmentation Keys* (DFKs), short secrets that allow authorised recipients to extract hidden positions within each Q-Block. Each transmitted block yields both a message-encryption key (MEK) and a fresh DFK, enabling indefinite cycling without reusing key material.

In earlier formulations, Q-Stream was proposed as a general-purpose key distribution mechanism applicable to one-time pad encryption and post-quantum secure communication. In this paper, we adapt the framework to a new role: embedding QKD-generated keys into Q-Blocks to provide last-mile distribution. This integration ensures that the ε-security of the original QKD key is preserved, while the Q-Block mechanism enables transport over classical networks without reliance on computational assumptions.

3 Problem Statement: The Last-Mile Challenge

Quantum key distribution (QKD) protocols such as BB84 and their variants provide ε-secure keys between backbone or metro nodes connected by quantum channels. These keys are guaranteed to be indistinguishable from uniform even against adversaries holding arbitrary quantum side-information. In practice, however, QKD links typically terminate at secure data centres or network aggregation points, not at end-user devices [8].

The *last-mile problem* arises when QKD-generated keys must be delivered from these backbone nodes to endpoints such as laptops, mobile devices, field terminals, or application servers. This segment of the network is almost always classical: it runs over IP, WiFi, or mobile infrastructure. To bridge this gap, current deployments rely on conventional cryptography—RSA, ECC, or more recently post-quantum cryptography (PQC)—to transport the keys. This reintroduces computational assumptions [3] and leaves the system vulnerable to "store-now, decrypt-later" attacks if the chosen algorithm is later broken.

Formally, the last-mile problem can be described as follows: given a QKD-generated key K that is ε-secure at a backbone node, find a mechanism to transport K to a remote end-device across a classical network such that (i) the ε-security guarantee is preserved, and (ii) no additional computational hardness assumptions are introduced.

Despite decades of research into QKD protocols and network integration, no widely deployed solution exists that satisfies these requirements. Trusted relays can forward keys, but they concentrate risk and break the end-to-end ITS model. PQC bridges remove quantum channels from the critical path but degrade unconditional security to conjectured hardness. This motivates the need for a method that can extend QKD keys into the last mile while retaining their information-theoretic classification.

4 OPS-Based Last-Mile Extension

We propose to address the last-mile problem by applying *Operational Perfect Secrecy* (OPS) to the distribution of QKD-generated keys across classical networks. OPS generalises Shannon's secrecy definition [6] by quantifying adversarial success probability rather than requiring an all-or-nothing indistinguishability condition. This allows secrecy guarantees to be extended operationally across different channels while preserving information-theoretic security.

4.1 Embedding Construction

Let $K \in \{0,1\}^n$ be a QKD-generated key that is ε-secure at a backbone node. Let $R \in \{0,1\}^N$ be a block of quantum-random bits generated by a QRNG at a Q-Stream Master-Node, independent of K. Each client device holds a secret, one-time Defragmentation Key (DFK) S, established during secure bootstrap. The embedding process constructs a Q-Block $B \in \{0,1\}^N$ by overwriting positions in R determined by S with the bits of K, along with a fresh next-round DFK S'. The Q-Block is then transmitted in cleartext across the classical network.

On receipt, the intended device applies the public extraction function $F(S, B)$ to recover both the embedded key K and the next DFK S'. After extraction, the old DFK S is securely erased. This mechanism ensures forward evolution of DFKs while embedding the QKD key into what is, to any adversary, indistinguishable from uniform QRNG noise.

4.2 Preservation of QKD Security

The central question is whether embedding a QKD key into a QRNG-derived Q-Block alters its security classification. We show that it does not: the ε-security of the original QKD key is preserved under embedding [7], and the adversary gains no additional advantage.

Lemma 1 (Preservation of QKD Security under Q-Stream Embedding)**.** *Let $K \in \{0,1\}^n$ be a QKD key that is ε-secure in the composable sense:*

$$\left\| \rho_{KE} - \tau_K \otimes \rho_E \right\|_1 \leq \varepsilon,$$

where τ_K is uniform on $\{0,1\}^n$. Let $R \in \{0,1\}^N$ be an independent QRNG block, and let S be a secret one-time DFK determining embedding positions. Define $B = \mathsf{Embed}(R, K, S)$.

Then:

1. *(**Indistinguishability**) The adversary's view of (B, E) is ε-close to uniform:*

$$\left\| \rho_{BE} - \tau_B \otimes \rho_E \right\|_1 \leq \varepsilon.$$

2. *(**Key secrecy**) The embedded key remains ε-secure against an unbounded adversary:*

$$\left\| \rho_{KBE} - \tau_K \otimes \rho_{BE} \right\|_1 \leq \varepsilon.$$

3. *(**OPS bound**) The adversary's maximum success probability in guessing K satisfies*

$$\max_A \Pr[A(B) = K] \leq 2^{-n} + \tfrac{\varepsilon}{2}.$$

Proof sketch. The result follows from the monotonicity of trace distance under CPTP maps. Applying the embedding map Embed to both sides of the QKD secrecy definition preserves the ε bound. If K were perfectly uniform, overwriting positions in an independent uniform block R yields a block B that is itself uniform. With ε-close K, indistinguishability holds within ε. Preserving K in the output register shows joint secrecy is maintained. Finally, the relation between trace distance and optimal guessing probability yields the OPS adversary bound. □

4.3 Discussion

This embedding construction achieves two goals simultaneously: it delivers QKD keys across classical networks while ensuring the adversary's view remains indistinguishable from QRNG noise, and it evolves the DFK forward to enable indefinite secure operation. The result is that last-mile delivery preserves the original QKD ε-security without introducing computational assumptions, thereby extending end-to-end information-theoretic security from the quantum backbone into end-user devices.

5 System Design for Last-Mile QKD

Having established that embedding QKD keys into QRNG-derived Q-Blocks preserves their ε-security, we now describe the system design that enables this construction in practice. The architecture combines QKD backbones with Q-Stream edge services, forming a hybrid quantum–classical network capable of end-to-end information-theoretic key delivery.

5.1 Architecture

The system consists of three layers:

- **QKD Backbone Nodes:** Trusted facilities connected by quantum channels that generate ε-secure keys using standard QKD protocols. These nodes serve as sources of high-assurance keys but are typically located in metro hubs or data centres, not directly accessible to end devices.
- **Q-Stream Master-Nodes:** Services co-located at the backbone edge that receive QKD keys and embed them into QRNG-derived Q-Blocks. Each Master-Node has access to a local QRNG and constructs per-device Q-Blocks according to the OPS embedding procedure.
- **Q-Stream Proxy-Nodes:** Organisation-specific relays deployed closer to end devices (e.g., in corporate networks, military bases, or telecom facilities). Proxy-Nodes forward Q-Blocks from Master-Nodes to devices but hold no device state or secret material, ensuring that compromise of a Proxy-Node does not affect confidentiality.

5.2 Workflow

The delivery of a QKD key to an end device proceeds as follows:

1. *QKD generation:* Two backbone nodes run a QKD protocol to generate a shared key K, which is ε-secure by construction.
2. *Embedding:* At the Master-Node, a fresh QRNG block R is sampled. Using the device's current Defragmentation Key (DFK) S, the embedding function produces a Q-Block $B = \mathsf{Embed}(R, K, S \parallel S')$, where S' is the device's next DFK.
3. *Distribution:* The Q-Block B is transmitted over classical networks in the clear, passing through Proxy-Nodes if applicable. Proxy-Nodes merely relay the block; they neither store nor modify embedded content.
4. *Extraction:* The end device applies the public extraction function $F(S, B)$ to recover (K, S'). The device erases S and retains S' for the next round.
5. *Use:* The recovered QKD key K is now available for one-time-pad encryption or for seeding higher-level protocols at the application layer.

5.3 Trust Boundaries

The trust assumptions are minimal and clearly delineated:

- *Master-Nodes* are trusted to generate QRNG randomness and to embed QKD keys correctly. They maintain minimal per-device synchronisation state (the current round index) and destroy prior state once new Q-Blocks are acknowledged.
- *Proxy-Nodes* are not trusted with any secrets. They act as transparent relays and may enforce policy or logging but cannot recover keys or DFKs.
- *End devices* hold their own evolving DFKs, which are provisioned securely during onboarding and never transmitted in cleartext. The secrecy of these DFKs is the sole device-side assumption.

5.4 End-to-End Security

This architecture ensures that:

1. QKD provides Q-ITS secrecy in the backbone.
2. Q-Stream embedding preserves ε-security across the classical last mile.
3. No computational assumptions (RSA, ECC, PQC) [4] are introduced at any stage.

Thus, the combined system achieves end-to-end information-theoretic key delivery from quantum backbones to commodity end devices, resolving the last-mile barrier to QKD deployment.

6 Security Analysis

We now analyse the security of Q-Stream as applied to last-mile QKD. Our goal is to show that embedding QKD keys into QRNG-derived Q-Blocks preserves their ε-security under a strong adversary model.

6.1 Threat Model

We assume an adversary with the following capabilities:

- Full visibility and control of the classical communication network: the adversary may intercept, modify, replay, or drop any Q-Block in transit.
- Access to all Q-Stream Master-Nodes and Proxy-Nodes as network services, including logs and metadata.
- Unbounded computational power, including future quantum computers.

- Complete knowledge of the Q-Stream protocol, including the embedding algorithm and extraction function $F(S, B)$.

The adversary *does not* have access to:

- Device-specific DFKs, which are provisioned securely and never transmitted in cleartext.
- The QRNG internals of Master-Nodes, assumed to be entropy sources with outputs indistinguishable from uniform.
- The physical security of backbone QKD nodes, which are trusted facilities by design.

This model aligns with the classical "ciphertext-only" adversary extended with full network control and quantum computational capabilities.

6.2 OPS Bound for Embedded Keys

Let K be a QKD-generated key with ε-security at a backbone node. Let B be the Q-Block produced by embedding K into QRNG noise using a device's DFK. By Lemma 1, the joint state of the adversary (B, E) satisfies:

$$\left\| \rho_{KBE} - \tau_K \otimes \rho_{BE} \right\|_1 \leq \varepsilon.$$

From the relation between trace distance and guessing probability, it follows that:

$$\max_A \Pr[A(B) = K] \leq 2^{-n} + \tfrac{\varepsilon}{2}.$$

Thus, the adversary's advantage in distinguishing the embedded QKD key from uniform remains bounded by the same ε parameter as in the original QKD proof.

6.3 Composability with QKD

Because Q-Stream embedding is a classical post-processing map applied to an ε-secure QKD key, the composable security framework [10] ensures that the combined system remains ε-secure. That is, the process:

$$\text{QKD generation} \rightarrow \text{Q-Stream embedding} \rightarrow \text{Q-Block transmission}$$

is equivalent to a direct delivery of the QKD key to the end device, up to ε in statistical distance. The embedding introduces no additional leakage channels and no reliance on computational assumptions.

6.4 End-to-End Guarantee

We conclude that the combined QKD + Q-Stream system achieves end-to-end information-theoretic security under the defined threat model:

1. During the quantum backbone phase, QKD ensures ε-secure key generation against adversaries with quantum side-information (Q-ITS).

2. During the classical last-mile phase, Q-Stream embedding ensures that the QKD key remains ε-secure when transported across untrusted networks (classical ITS).

Therefore, the system provides unconditional confidentiality guarantees from backbone to end device, resolving the last-mile problem without reliance on computational hardness assumptions.

7 Applications

By embedding QKD keys into QRNG-derived Q-Blocks, Q-Stream extends the reach of QKD into environments where quantum channels cannot be deployed directly. This enables practical end-to-end use of information-theoretically secure keys in several high-value domains.

7.1 Financial Trading Networks

In high-frequency trading and interbank settlement, confidentiality and integrity of data flows are paramount. Current deployments rely on TLS with classical or PQC key exchanges, both of which remain vulnerable to "store-now, decrypt-later" attacks. By combining QKD backbones between financial hubs with Q-Stream last-mile delivery into trading floors and datacentres, institutions can achieve unconditional confidentiality from exchange nodes directly into servers and terminals, without adding latency or relying on conjectured hardness.

The combination of QKD-supplied keys with Q-Stream delivery is particularly attractive when paired with one-time pad (OTP) encryption, since financial messages are typically small and latency-sensitive. This allows critical market data and order flows to be encrypted with true information-theoretic secrecy in real time. Further discussion of this model in the context of telecom-provided dedicated fibre services for financial institutions is given in Section 7.5, where the benefits for high-frequency trading (HFT) applications are analysed in more detail.

7.2 Military and Defence Communications

Deployed military systems face the dual challenge of operating in untrusted environments and being exposed to adversaries with potentially unbounded computational resources. QKD links can secure backbone or satellite-to-ground channels, but cannot reach handheld radios, vehicle systems, or mobile command terminals. Embedding QKD keys into Q-Stream Q-Blocks allows keys to be transported securely across conventional military networks, enabling one-time-pad or ITS-secure encryption in the field while preserving the original QKD security guarantees.

7.3 Critical Infrastructure and Energy Systems

Electric grids, transportation networks, and industrial control systems increasingly require secure telemetry and command channels. QKD can protect long-haul fibre routes between control centres, but extending protection to edge devices such as substations, sensors, and actuators requires last-mile distribution. Q-Stream provides a mechanism for delivering QKD

keys to such endpoints with ITS guarantees, removing reliance on computational cryptography for infrastructure that must remain secure for decades.

7.4 Integration into QKD Standards

The ETSI ISG-QKD standards framework currently recognises trusted relays and PQC bridging as solutions for extending QKD keys into classical networks. Q-Stream introduces a third option: classical transport of QKD keys without trust concentration or computational assumptions. This makes it suitable for integration into future ETSI QKD [4] network architectures as an end-device key delivery mechanism, complementing existing backbone standards.

7.5 Telecom Operators and Low-Latency Financial Services

Telecommunication providers increasingly operate dedicated fibre routes for financial institutions, offering guaranteed latency and service-level agreements for trading and settlement traffic. These specialised links are natural candidates for QKD deployment, as they already carry highly sensitive and time-critical information. QKD can secure the backbone between exchange data centres and major banking nodes, while Q-Stream provides the mechanism for securely extending those keys into colocated servers and client terminals.

A key advantage in this setting is the compatibility of Q-Stream with one-time pad (OTP) encryption. High-frequency trading (HFT) and low-latency financial messages are typically short—on the order of tens to hundreds of bytes—making OTP encryption practical without incurring excessive key consumption. With QKD supplying a continuous stream of quantum-secure keys and Q-Stream embedding them into QRNG-derived Q-Blocks for last-mile delivery, trading firms can encrypt market data and order flows with true information-theoretic secrecy while meeting stringent latency requirements.

This integration allows telecom providers to offer differentiated "quantum-secured low-latency services," combining dedicated fibre infrastructure with QKD and Q-Stream. For financial institutions, the result is not only protection against store-now, decrypt-later attacks but also an ultra-low-latency encryption mechanism aligned with the performance profile of HFT systems.

8 Related Work

Several approaches have been proposed to address the practical limitations of QKD deployment, particularly the last-mile challenge of distributing keys beyond secure backbone nodes.

8.1 Trusted Relays and QKD Networks

Large-scale field trials such as the SECOQC network in Vienna [8] and the Tokyo QKD network [9] have demonstrated the feasibility of metropolitan-scale quantum key distribution. These systems typically employ *trusted relay nodes*, which terminate QKD links and forward

keys to subsequent hops. While effective in extending distance, this approach breaks the end-to-end information-theoretic security model, since compromise of a single trusted relay exposes all traffic that passes through it.

8.2 Post-Quantum Cryptography Bridges

Another proposed solution is to use post-quantum cryptography (PQC) to protect the last-mile segment. NIST has led a major standardisation effort in this area [3, 1], identifying lattice-based and code-based schemes as candidates for deployment. However, PQC introduces a fundamentally different security model: its strength is conjectured on the intractability of certain mathematical problems. Although PQC may resist near-term quantum adversaries, it does not provide unconditional security and remains vulnerable to store-now, decrypt-later attacks if breakthroughs occur in underlying assumptions.

8.3 Hybrid Key Management Frameworks

Standards initiatives such as ETSI ISG-QKD [4] have proposed hybrid architectures where QKD supplies keys to a key management system (KMS), which then distributes session keys to applications using conventional or PQC-secured transport. This offers interoperability but again reduces unconditional security to computational guarantees at the device edge. Similarly, research on entropic security and privacy amplification [10, 5] has explored combining classical and quantum techniques, but does not directly address the distribution of QKD keys into commodity endpoints.

8.4 Q-Stream in Context

In contrast to the above, Q-Stream preserves the ε-security of QKD keys during classical last-mile delivery without introducing trusted relays or computational assumptions. By embedding QKD keys into QRNG-derived Q-Blocks, Q-Stream provides a channel indistinguishable from quantum noise while remaining entirely classical in implementation. This places it as a complementary approach to existing QKD standards: QKD secures the quantum backbone (Q-ITS), while Q-Stream extends information-theoretic guarantees into the last mile (ITS), achieving end-to-end unconditional security.

9 Conclusion

Quantum key distribution (QKD) provides a unique promise: keys that remain secure even against adversaries with unbounded computational or quantum resources. Yet, despite successful field deployments, its adoption has been constrained by the persistent last-mile problem: transporting QKD-generated keys from backbone or metro hubs to end-user devices over classical networks. Existing solutions based on trusted relays or post-quantum cryptography reintroduce weaknesses that undermine the unconditional security guarantees of QKD.

In this work we proposed a new approach based on *Operational Perfect Secrecy* (OPS) and the *Q-Stream* framework. By embedding QKD keys into QRNG-derived Q-Blocks using short secret defragmentation keys, we demonstrated that the ε-security of the original QKD key is preserved under classical transmission. To any adversary without the DFK, Q-Blocks are indistinguishable from uniform QRNG noise, ensuring that embedding introduces no additional leakage or computational assumptions.

The result is an end-to-end architecture in which QKD secures the quantum backbone (Q-ITS) and Q-Stream extends information-theoretic guarantees into the classical last mile (ITS). This resolves the final barrier to unconditional security for real-world systems, enabling applications in finance, defence, critical infrastructure, and standards-driven QKD networks. Future work will explore integration of Q-Stream into ETSI-compliant key management systems and the performance trade-offs of deploying OTP encryption at scale in low-latency environments.

References

[1] Gorjan Alagic and et al. Status report on the third round of the nist post-quantum cryptography standardization process. Technical report, NIST, 2022.

[2] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[3] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. Report on post-quantum cryptography. Technical report, NIST, 2016.

[4] ETSI Industry Specification Group QKD. Quantum key distribution (qkd); overview on security framework. ETSI White Paper, 2018–2022. Accessed 2025.

[5] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators: a review. *Reviews of Modern Physics*, 89:015004, 2017.

[6] Adrian Neal. Beyond shannon: Operational perfect secrecy as a generalised model for information-theoretic security. Cryptology ePrint Archive, Paper 2025/1716, 2025.

[7] Adrian Neal. Q-stream: A practical system for operational perfect secrecy. Cryptology ePrint Archive, Paper 2025/1721, 2025.

[8] Momtchil Peev and et al. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009.

[9] Masahide Sasaki and et al. Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, 19(11):10387–10409, 2011.

[10] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, 2009.