# Post-Quantum Cryptographically-Secured Trusted Node for Quantum Key Distribution in a Deployed Network

Heming Huang, Yves Jaouën, Nicolas Fabre, Romain Alléaume, Jean-Sébastien Pegon, Thomas Camus, Martin Zuber, Jean-Charles Faugère, Pierre-Enguerrand Verdier, Baptiste Lacour, et al.

# Post-Quantum Cryptographically-Secured Trusted Node for Quantum Key Distribution in a Deployed Network


Heming Huang, Yves Jaouën — Telecom Paris, Institut Polytechnique de Paris

Nicolas Fabre, Romain Alléaume — Telecom Paris, Institut Polytechnique de Paris

Jean-Sébastien Pegon, Thomas Camus — ID Quantique SA

Martin Zuber, Jean-Charles Faugère — CryptoNext Security

Pierre-Enguerrand Verdier, Baptiste Lacour, Maxime Gautier, Thomas Rivera — Orange Innovation

Yoann Piétri, Matteo Schiavon, Amine Rhouni, Eleni Diamanti — Sorbonne Université, CNRS, LIP6


## Objective

Reduce the security risks associated with the usage of trusted nodes in a QKD network.

## Conclusion

The transported QKD key is secure agains honest-curious nodes at a lower key-rate cost than state-of-the-art.

## 1. The need for trusted nodes in a QKD network

QKD requires point-to-point quantum communication, which is highly unpractical for large networks. In theory, this could be overcome by using intermediate nodes equipped with optical switches. But these switches would add optical losses detrimental to the secret key rate ⟶ not in fact a range extension.

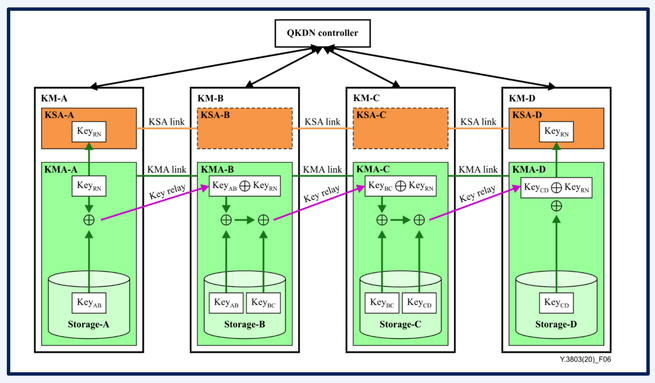
A practical solution to these issues is the use of **trusted nodes**: the whole link is composed of several sub-links between secure locations, and the intermediate nodes serve as key relays.

## 2. Initial key relay scheme

One option for key relay is to transfer the key linearly from node to node under the cover of a One-Time Pad (OTP) encryption (symbol ⊕).

This has a significant drawback: the key is deciphered and re-ciphered on each node. Nodes need to be trustued not only to stick to the key relay protocol but also to do so "blindfolded" and not retrieve the key.

Ideally, one could want to modify the key relay scheme so as to reduce the amount of trust given to the nodes: if the nodes are only honest-but-curious, they are only expected to follow protocol instructions but can try to glean information.

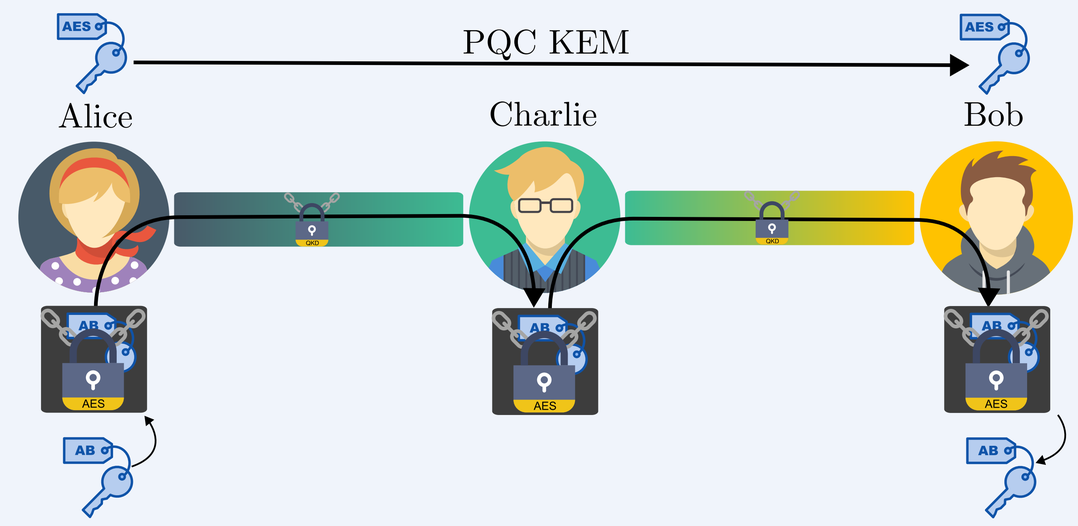



**An illustration of such a key relay from [1]**

## 3. Modified key relay scheme

1. Alice and Bob have access to a PQC KEM (Post-Quantum Cryptographic Key Encapsulation Mechanism). This KEM allows Alice and Bob to agree on a secret key K over an untrusted channel

2. Then both Alice and Charlie and Charlie and Bob perform QKD. Alice ends up with the key $k_{AC}$ Bob with $k_{BC}$ and Charlie with the keys $k_{AC}$ and $k_{BC}$ .




3. Alice then generates the final key $k_{AB}$ using a Quantum Random Number Generator, and encrypts it with the shared key as: $k^{enc} = \mathrm{Enc}_{\mathrm{AES}}(K, k_{AB})$ using the AES encryption standard.

4. Alice sends $k^{enc}$ using One-Time Pad (OTP) with the key $k_{AC}$ . Charlie then relays $k^{enc}$ by deciphering the OTP with $k_{AC}$ and performing again OTP with $k_{BC}$ . Bob can finally decipher the OTP and perform

$$k_{AB} = \mathrm{Dec}_{\mathrm{AES}}(K, k^{enc})$$

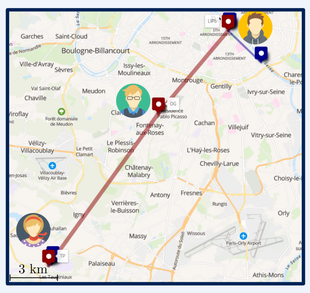
to recover the final key.

**With this approach, Charlie never has direct access to the final key and the resources that he would need to learn some information about the key are increased.**

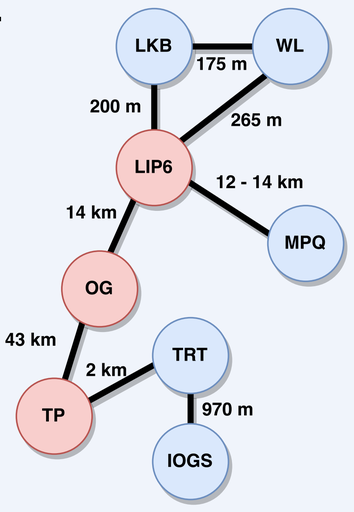
## 4. Implementation of the scheme

We have implemented this scheme with one trusted node on the Parisian Quantum Network. The overall network, with optical (dark) fibers dedicated to quantum communication applications, is composed of 8 nodes corresponding to locations of academic and industrial partners.

The PQC KEM used is Crystals-Kyber (precursor to the future FIPS standard ML-KEM).
Although several quantum-safe KEMs have been submitted since NIST launched its PQC competition, Kyber is the only KEM that has been selected for standardisation as of today.



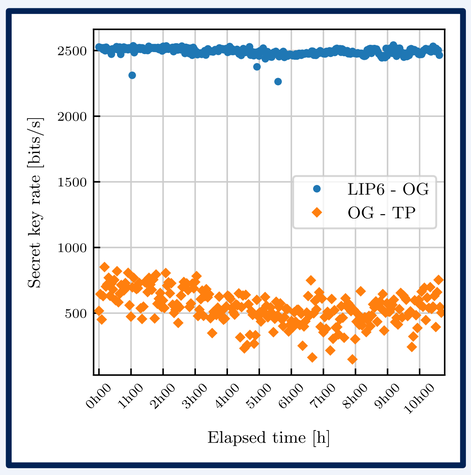

**On-scale map of the network**




**Graph-like representation of the overall network**

Average Quantum Bit Error Rates (QBERs) of 1.93% +/- 0.57% (OG-LIP6) and 1.72% +/- 0.68% (OG-TP) and average visibilities of 0.998 +/- 0.012 and 0.959 +/- 0.024 respectively were obtained.

This corresponds to an average key rate of respectively 2493 bit/s (standard deviation 28 bit/s) and 612 bit/s (standard deviation 139 bit/s), yielding an **overall LIP6 - TP key rate of 612 bit/s on average.**




## 5. Comparison with previous work

The work that most closely matches ours is a similar attempt at mitigating the risk posed by trusted nodes using PQC in [2].

The main difference between the protocol presented by the authors and ours is in the encryption method used as an additional layer of protection for the key $k_{AB}$ where we use an AES encryption with keys exchanged through PQC, they use a PQC encryption scheme directly (Kyber).

Because a Kyber ciphertext is much bigger in size than an AES ciphertext, our method drastically reduces the amount of key needed for the transfer during the OTP operation and saturates the achievable secret key rate over the overall link.

Transferring a 256-bit key using PQC encryption directly would consume around 2 kB of OTP keys while using AES with a PQC-based key consumes 2 x 256 bits of OTP keys.

## Bibliography


[1] ITU. 'ITU-T - Y.3803 : Quantum Key Distribution Networks - Key Management', December 2020.

[2] Geitz, Marc, Ronny Döring, and Ralf-Peter Braun. 'Hybrid QKD & PQC Protocols Implemented in the Berlin OpenQKD Testbed'. In 2023 8th International Conference on Frontiers of Signal Processing (ICFSP), 69–74. Corfu, Greece.



**Acknowledgements** This work has been funded through the ParisRegionQCI project.