Quantum Key Distribution with Efficient Post-Quantum Cryptography-Secured Trusted Node on a Quantum Network

Yoann Piétri, Pierre-Enguerrand Verdier, Baptiste Lacour, Maxime Gautier, Heming Huang, Thomas Camus, Jean-Sébastien Pegon, Martin Zuber, Jean-Charles Faugère, Matteo Schiavon, et al.

Quantum Key Distribution with Efficient Post-Quantum Cryptography-Secured Trusted Node on a Quantum Network

Yoann Piétri,[1] Pierre-Enguerrand Verdier,[2] Baptiste Lacour,[2] Maxime Gautier,[2] Heming Huang,[3] Thomas Camus,[4] Jean-Sébastien Pegon,[4] Martin Zuber,[5] Jean-Charles Faugère,[5] Matteo Schiavon,[1] Amine Rhouni,[1] Yves Jaouën,[3] Nicolas Fabre,[3] Romain Alléaume,[3] Thomas Rivera,[2] and Eleni Diamanti[1]

[1] *Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*
[2] *Orange Innovation, F-92326 Châtillon, France*
[3] *Telecom Paris, Institut Polytechnique de Paris, F-91120 Palaiseau, France*
[4] *ID Quantique SA, CH-1227 Genève, Switzerland*
[5] *CryptoNext Security, F-75005 Paris, France*

(Dated: April 3, 2025)

Quantum Key Distribution (QKD) enables two distant users to exchange a secret key with information-theoretic security, based on the fundamental laws of quantum physics. While it is arguably the most mature application of quantum cryptography, it has inherent limitations in the achievable distance and the scalability to large-scale infrastructures. While the applicability of QKD can be readily increased with the use of intermediary trusted nodes, this adds additional privacy requirements on third parties. In this work, we present an efficient scheme leveraging a trusted node with lower privacy requirements thanks to the use of post-quantum cryptographic techniques, and implement it on a deployed fiber optic quantum communication network in the Paris area.

I. INTRODUCTION

The significant expected progress in algorithmic techniques and computing power in the next years, including using powerful quantum processors, has brought to the forefront the need for developing quantum-safe cryptographic solutions. Such solutions may advantageously combine techniques leveraging mathematical algorithms believed to be robust against quantum attacks, namely Post-Quantum Cryptography (PQC), and techniques exploiting quantum resources, in particular Quantum Key Distribution (QKD). The latter is an ensemble of methods and protocols that allows two distant users, usually called Alice and Bob, equipped with an untrusted public quantum channel and a public authenticated classical channel, to exchange a random string of bits with information-theoretic security. This security, based on the fundamental laws of quantum physics, ensures that this bitstring can later be used as a symmetric cryptographic key.

The field of QKD has seen remarkable progress in the last year [1]. However, the limited achievable distance and the difficulty in scaling to large networks remain important practical challenges in QKD implementations. The limit in range is due to the fundamental law allowing QKD in the first place: an unknown quantum state cannot be cloned and since photon transmission decays exponentially in fibers, the achievable distance is limited in theory by well-established bounds [2]. Furthermore, QKD requires point-to-point communication for the exchange of the quantum states, which is rather unpractical in large networks. To overcome this issue, it is possible to use intermediary nodes with optical switches, a technique known as physical bypass, but doing so is detrimental to the key rate and does not extend the range of communication.

A practical solution to these limitations is to break the communication link into several sublinks and perform QKD on each sublink. The final key is then relayed by the intermediary nodes using the QKD keys. This solution has already been implemented in several quantum communication networks, but lowers the security of the key exchange: first because the trusted node is an additional location for the malicious adversary, Eve, to physically attack, and second because of the full trust that has to be accorded to the intermediary node, which will directly be in possession of the final key.

Hybrid solutions, combining PQC and QKD techniques, can be used to mitigate the practical security challenges encountered in QKD implementations. Several proposals targeting, for instance, the authentication step or the aforementioned trusted node security issue, have been made [3–8]. In this work, we also address the trusted node security issue; in particular, by combining the standard trusted node relay protocol with a post-quantum key encapsulation mechanism and AES encryption, we show that we are able to lower the trust requirement on the intermediary node. Our approach is similar to the one presented in [7], however our protocol features a better efficiency in terms of key bit usage, saturating the final secret key rate. We also demonstrate its practical relevance by implementing it in a deployed optical fiber quantum communication network.

The paper is structured as follows: in section II we present the standard trusted node protocol and the modified version we will implement. Then, in section III we present the Paris Quantum Network, along with the QKD setup, before describing the results of the experiment in section IV and drawing some conclusions in section V.

II. TRUSTED NODE PROTOCOL

Let us start by presenting the considered setup and the underlying assumptions. For this, we first introduce the following *notations*: if k is a key binary register of n bits, we denote by $|k| = n$ the size of the register, and for $0 \leq i \leq n$, by $\lfloor k \rfloor_i$ the truncated key up to the ith term, which is a key register of i bits. Additionally, we use the symbol $\oplus$ that refers to the bitwise modulo-2 addition between two registers.

A. Setup

Alice and Bob are two trusted users who want to exchange a key, while Charlie is an intermediary node. Eve is a malicious adversary wanting to learn the content of the key.

Alice and Bob are both linked to Charlie with a public quantum channel and a public authenticated classical channel. Alice and Bob are also linked with a public authenticated classical channel. We will denote by $QC(\text{Node 1}, \text{Node 2})$ (resp. $CC(\text{Node 1}, \text{Node 2})$) the public quantum channel (resp. authenticated classical channel) linking Node 1 and Node 2.

Alice, Bob and Charlie have the required hardware to run the QKD protocols, and in particular we suppose that Alice and Charlie can perform QKD with $QC(A, C)$ and $CC(A, C)$ and that Charlie and Bob can perform QKD with $QC(B, C)$ and $CC(B, C)$ (possibly with different QKD protocols and/or implementations). This also means that we make the standard assumptions in QKD implementations: Alice, Bob and Charlie have access to secure locations, trusted quantum and classical hardware, and true random number generators. Additionally, we make the assumption that the parties are bounded by the laws of quantum physics.

Another standard assumption in QKD is that Alice and Bob are behaving honestly, and follow the protocol instructions. As for Charlie, we want to introduce here more nuances by considering three possible honesty levels: Charlie could be *honest*, by blindly following the protocol instructions without leaking information or remembering what he sees, he could be *honest-but-curious* (or *semi-honest*), where he follows the protocol instructions but attempts to learn as much information as possible from the received messages and he could be *malicious*, where he can deviate from the protocol with no constraints. In the last case, we can say that Charlie is controlled by the adversary Eve.

B. Standard trusted node protocol

The standard trusted node protocol goes as follows:

Protocol 1: QKD with a trusted node

Alice, Bob and Charlie have access to a `QKD` subroutine.

1. Alice and Charlie perform `QKD` using $QC(A, C)$ and $CC(A, C)$. They both end up with a key k_{AC} of length l_{AC}.
2. Bob and Charlie perform `QKD` using $QC(B, C)$ and $CC(B, C)$. They both end up with a key k_{BC} of length l_{BC}.
3. Bob communicates the value of l_{BC} to Alice over the classical channel $CC(A, B)$.
4. If $l_{AC} = 0$ or $l_{BC} = 0$, Alice makes the protocol abort, otherwise she computes $l = \min(l_{AC}, l_{BC})$. Alice communicates l to Bob and Charlie over the classical channels $CC(A, B)$ and $CC(A, C)$.
5. Alice generates the random key k_{AB} of length l and computes $m_1 = k_{AB} \oplus \lfloor k_{AC} \rfloor_l$. Alice sends m_1 to Charlie over the classical channel $CC(A, C)$.
6. Charlie recovers the key k_{AB} by $k_{AB} = m_1 \oplus \lfloor k_{AC} \rfloor_l$ and computes $m_2 = k_{AB} \oplus \lfloor k_{BC} \rfloor_l$. Charlie sends m_2 to Bob over the classical channel $CC(B, C)$.
7. Bob recovers the key k_{AB} by $k_{AB} = m_2 \oplus \lfloor k_{BC} \rfloor_l$.

Alice and Bob end up with the key k_{AB} of length $l = \min(l_{AC}, l_{BC})$.

Since the combination of QKD with One-Time Pad (OTP), corresponding to steps 5, 6 and 7 in the protocol, achieves perfect secrecy, the messages m_1 and m_2 cannot be deciphered to recover k_{AB} by the adversary Eve, in the cases where Charlie is honest or semi-honest.

However, in this protocol, Charlie directly holds the key k_{AB} meaning that he could decipher all messages exchanged between Alice and Bob that were encrypted using this key, by simply monitoring the classical channels. This means that the standard trusted node protocol allows no protection against an honest-but-curious Charlie.

As mentioned earlier, another downside of trusted node QKD is that it introduces an additional location that can be attacked by the adversary. While this is not an issue when considering the standard assumptions of QKD, since we are considering that no information comes out of the secure locations except for the quantum and classical channels, it could be an issue in some practical QKD scenarios. Indeed, Alice and Bob may be reticent to trust the security of Charlie's location over which they might have no control.

C. Modified trusted node protocol

Let us now present the modified trusted node protocol. For this, we need to introduce the notion of a Key Encapsulation Mechanism (KEM). This is a protocol that allows to exchange a cryptographic key (usually to be used in symmetric encryption protocols) over a public channel, using asymmetric encryption. We say that it is a PQC-Key Encapsulation Mechanism (KEM) if the asymmetric mechanisms rely on post-quantum cryptographic methods.

The modified protocol goes as follows:

Protocol 2: QKD with PQC-secured trusted node

Alice and Bob have access to a `PQC-KEM` subroutine. Alice, Bob and Charlie have access to a `QKD` subroutine.

1. Alice and Bob use `PQC-KEM` to exchange the symmetric key k_{AES} over the public $CC(A, B)$.
2. Alice and Charlie perform `QKD` over their quantum and classical channels $QC(A, C)$ and $CC(A, C)$. They both end up with a key k_{AC} of length l_{AC}.
3. Bob and Charlie perform `QKD` over their quantum and classical channels $QC(B, C)$ and $CC(B, C)$. They both end up with a key k_{BC} of length l_{BC}.
4. Bob communicates the value of l_{BC} to Alice over the classical channel $CC(A, B)$.
5. If $l_{AC} = 0$ or $l_{BC} = 0$, Alice makes the protocol abort, otherwise she computes $l = \min(l_{AC}, l_{BC})$. Alice communicates l to Bob and Charlie over the classical channels $CC(A, B)$ and $CC(A, C)$.
6. Alice generates the random key k_{AB} of length l and encrypts it using the encryption function $k_{AB}^{enc} = \texttt{ENC}_{\text{AES}}(k_{AES}, k_{AB})$ and computes $m_1 = k_{AB}^{enc} \oplus \lfloor k_{AC} \rfloor_l$. Alice sends m_1 to Charlie over the classical channel $CC(A, C)$.
7. Charlie computes $k_{AB}^{enc} = m_1 \oplus \lfloor k_{AC} \rfloor_l$ and $m_2 = k_{AB}^{enc} \oplus \lfloor k_{BC} \rfloor_l$. Charlie sends m_2 to Bob over the classical $CC(B, C)$.
8. Bob computes $k_{AB}^{enc} = m_2 \oplus \lfloor k_{BC} \rfloor_l$ and decrypts the key $k_{AB} = \texttt{DEC}_{\text{AES}}(k_{AES}, k_{AB}^{enc})$.

Alice and Bob end up with the key k_{AB} of length $l = \min(l_{AC}, l_{BC})$.

The protocol is represented in a schematic way in Fig. 1.

This modified protocol increases the difficulty of an attack for an honest-but-curious Charlie. Indeed, he would have to recover the key k_{AES} to get the final key. This provides computational security against an honest-but-curious trusted node.

This method does not help against physical attacks against Charlie's location. Indeed, an unbounded adversary could recover the k_{AES} encryption by breaking the PQC-KEM and then by recovering k_{AB}^{enc} at the location of Charlie. Simply obtaining k_{AES} is however not sufficient to get the final key without attacking Charlie's location.

D. Efficiency analysis

Here we compare the efficiency of the presented protocol with respect to the one in [7], where the final key k_{AB} is directly encrypted and decrypted using the PQC-KEM algorithm Crystals-Kyber. In more details, the protocol goes as follows: 1. Alice (called WFD01 in [7]) generates a random key using an ID Quantique Quantum Random Number Generator (QRNG); 2. The random key is encrypted with Kyber using the public key of Bob (WFD03) [9]; 3. The PQC encrypted key is encrypted again using OTP and the QKD key shared with Charlie, and the ciphertext is send to Charlie (WFD02) over the public channel; 4. Using the key shared with Alice, Charlie decrypts the ciphertext (getting the PQC-encrypted version) and re-encrypts it using OTP (this time with the QKD key shared with Bob) before sending it to Bob; 5. Bob decrypts the ciphertext using the key shared with Charlie and the private PQC key to recover the final secret.

Let l be the target number of bits in the final key $|k_{AB}| = l$. The question is how many bits from the keys exchanged with QKD are necessary for the modified trusted node protocol.

The operation of Kyber is defined by a security parameter [10]. This parameter relates to the security performance and also impacts the size of the ciphertext in the KEM. Indeed, for an input key size of 256 bits, the ciphertext length, that we will denote l_{ct}, is 6144 bits for Kyber-512, 8704 bits for Kyber-768 and 12 544 bits for Kyber-1024 [10].

In [7], the output ciphertext of the KEM is directly encrypted using OTP. For simplicity, let's suppose that the final key length l is a multiple of 256 (in practice, the ID Quantique Cerberis system that we will use for our demonstration stores the key in 256 bit blocks), so $l = 256p$ for $p \in \mathbb{N}$. This means that the final key will be encrypted in p blocks of l_{ct} bits, each one of them using OTP and the keys distributed using QKD. Hence, we can compute the ratio of the final key length with the number of bits used for OTP:

$$\eta = \frac{l}{p \times l_{ct}} = \frac{256}{l_{ct}}. \tag{1}$$

Here we compute the ratio with respect to the key consumption on one QKD link. In this way, the value of η will be directly used to derive the final key rate as

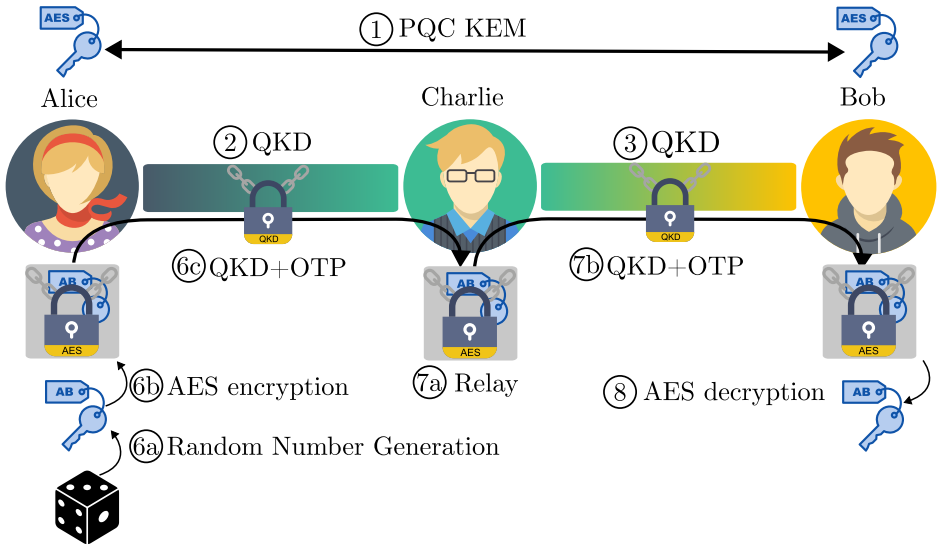


Figure 1. Schematic representation of the protocol. Numbers match the steps indicated in Protocol 2. Classical communications over classical channels are represented with black arrows, while QKD operation is represented on the gradient rectangle. For simplicity, some classical communications were omitted from the scheme, in particular the classical communication for QKD and steps 4 and 5 of the protocol.

$r_{\text{final}} = \eta \min(r_{AC}, r_{BC})$ where $r_{\text{final}}, r_{AC}, r_{BC}$ are respectively the secret key rate of the final key exchange, QKD exchange between Alice and Charlie, and QKD exchange between Bob and Charlie (this assumes that both QKD links are running simultaneously). Note that, when considering a key relay with perfect secrecy with respect to the outside world, as is the case here, the maximal final secret key rate is bounded by $\min(r_{AC}, r_{BC})$ since as many bits of QKD key as in the final key are required for perfect secrecy. In this sense, $r_{\text{final}} \leq \min(r_{AC}, r_{BC})$ and $\eta \leq 1$. The value of η for the different Kyber parameters are given in Table I.

In comparison, when we first exchange a random 256 bits key using the Kyber KEM on a public channel and use this key for AES-256, the following happens: AES-256 uses a block size of 128 bits, and each ciphertext of a 128 bit-block is also of length 128 bits. This means, that our final key of length $l = 256p$ is encrypted into $2p$ blocks of length 128 bits giving the efficiency

$$\eta = \frac{l}{2p \times 128} = 1. \tag{2}$$

Changing the parameter of the Kyber protocol will induce a longer key which will result in a higher number of bits exchanged on the public channels (in the first step), which is not a bottleneck.

If the key has a length that is not a multiple of 128 or 256, there is an added inefficiency due to the required padding, but this tends to 0 as the key length grows, since the number of padded bits is always less than 128 or 256.

We believe that the security of the protocol is not impacted in a significant way by our modifications compared with the protocol in [7]. In particular, in Tab. II we explicit the protocol(s) that need to be broken by Charlie (or Eve) to gain access to the final secret key.

Protocol	Protocol in [7]			Our protocol		
Kyber	512	768	1024	512	768	1024
η	4.17 %	2.94 %	2.04 %	100 %	100 %	100 %

Table I. Efficiency depending on the protocol and Kyber parameter.

Note that in all three cases, Eve has to break the OTP+QKD exchange (assuming all other locations secure). Additionally in [7] or our protocol, she also has to break either the PQC-KEM or AES (this second one only in our version). Note that in comparison with [7], in our protocol another option is given to both Charlie and Eve with respect to breaking the PQC-KEM, which is to break AES. However, it is believed that breaking a symmetric protocol such as AES will still remain harder than breaking an asymmetric one, even with a quantum computer.

III. THE PARIS QUANTUM NETWORK

Next, we describe the Paris Quantum Network, where we performed the experimental demonstration of our protocol, the characteristics of the links and the devices that were used for the QKD exchanges.

Protocol	Charlie (Honest-But-Curious)	Eve	η
Usual Trusted Node	Nothing	OTP+QKD	100%
Protocol in [7]	PQC-KEM	OTP+QKD and PQC-KEM	2-4%
Our protocol	PQC-KEM or AES	OTP+QKD and (PQC-KEM or AES)	100%

Table II. Protocol(s) to break in order to gain access to the final key.

A. Physical infrastructure

The physical infrastructure of the Parisian Quantum Network is currently composed of 8 nodes, located in the Paris Region, as shown in Fig. 2b.

The three nodes of interest here are LIP6 (LIP6, Sorbonne Université, in the 5th district of Paris), OG (Orange Innovation in Châtillon) and TP (Télécom Paris, Institut Polytechnique de Paris in Palaiseau). For completeness, the other connections are described in more detail in appendix A. The connections are done using dark fibers dedicated to quantum communication applications, which are standard SMF-28 fibers. The network was assembled by splicing existing segments that were once used for classical communications. Between LIP6 and OG, two fibers of length 14 km (average losses of 3.8 dB) are available and between OG and TP, two fibers of length 43 km (average losses of 10.4 dB) are available.

B. QKD systems

The QKD systems are the commercial devices Cerberis XGR from ID Quantique [11]. They are performing the Coherent One Way (COW) protocol [12] using time-bin qubits.

Each QKD system is composed of two nodes of standard size 1U, one containing the transmitter (Alice) and the other one containing the receiver (Bob). The two nodes need to be connected with an optical fiber serving as the quantum channel. Moreover, they also need to be connected by one or two optical fiber(s) allowing for full duplex communication between them, for synchronization. The fiber(s) should be about the same length as the quantum channel fiber. Finally the two nodes also need to be addressable with direct IPv4 links, and by the central management software, hosted in Châtillon.

We implement the full-duplex synchronization channel by using a single optical fiber and bi-directional modules (Skylane Optics SBHEDB22L32D and SBHEUB22L32D) that use the Coarse Wavelength Division Multiplexing (CWDM) technology to have one channel (CWDM high) in $[\lambda_T + 1.5\,\text{nm}, \lambda_T + 6.5\,\text{nm}]$ and the second channel (CWDM low) in $[\lambda_T - 6.5\,\text{nm}, \lambda_T - 1.5\,\text{nm}]$ where λ_T is the central operating wavelength. In our case, we choose a wavelength close to the one used in the quantum channel $\lambda_T = 1550\,\text{nm}$.

To perform the trusted node scheme, two QKD systems are needed (and hence 4 nodes) and we will refer to them as Pair 1 and Pair 2 with the nodes Alice 1, Bob 1, Alice 2 and Bob 2. The first pair operates with an attenuation up to 18 dB and the second pair with an attenuation up to 12 dB. Due to the asymmetry of our links, we choose to deploy Pair 1 on the TP-OG link (43 km, 10.4 dB) since with the additional connectors it would be close to or surpass the 12 dB limit. Pair 2 is deployed on the OG-LIP6 link (14 km, 3.8 dB).

C. Classical network

Since direct IPv4 addressing is required to operate the Cerberix XGR systems, the solution of using a Virtual Private Network (VPN) was chosen. Hence a VPN was established between the three remote locations over the internet, using the Wireguard software [13] . Each node was equipped with a router to operate the VPN and communicate with the local equipment. Here, we stress that the VPN was established for routing purposes only and that the security of the QKD exchanges and the overall key exchange does not rely on the inherent security provided by the VPN.

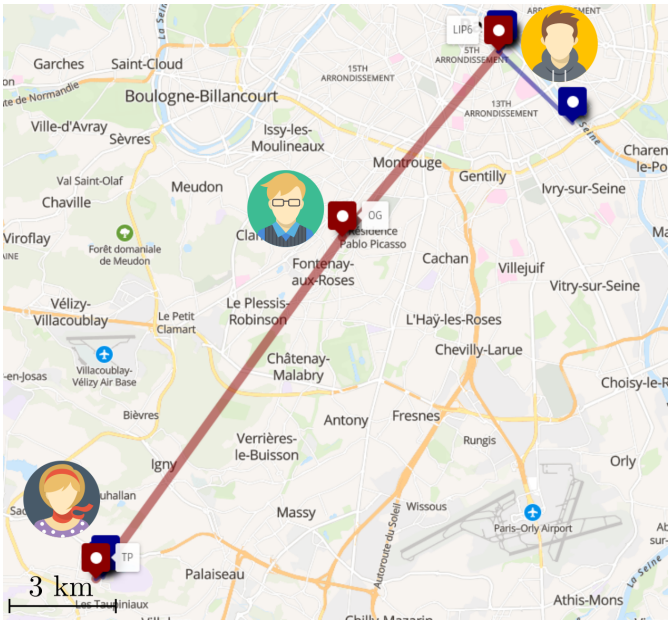
Additionally, the router in OG was also the central management node of the QKD nodes used to deploy the configuration and collect statistics. This was done using the Quantum Management System (QMS) solution of ID Quantique.

D. Encryptors

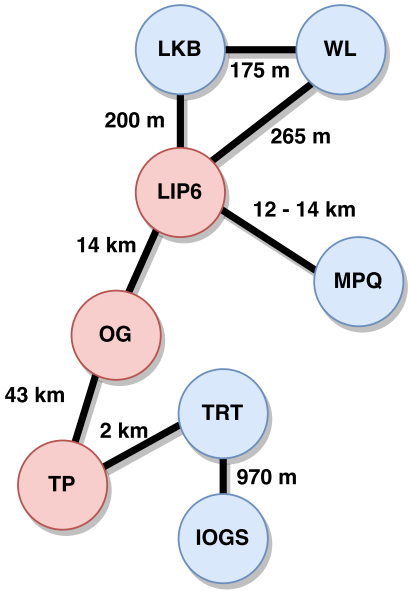
Keys were retrieved by interacting with the Key Management System (KMS) of each node using the standardised communication protocol ETSI-QKD-014 [14]. In practice, this was done using a specifically modified version of the IP9001 Mistral encryptors from Thales [15]. The encryptors were used to encrypt the data of a 4K video streaming service [16].

IV. RESULTS

For the implementation of the PQC-KEM, the Crystals-Kyber Key Encapsulation Mechanism was chosen [17], and implemented by CryptoNext Security [18]. Crystals-Kyber is based on the Learning-With-Errors (LWE) problem, and was submitted, along with many



(a) On-scale map of the quantum network. The actual fiber links do not correspond to the straight depicted line. The nodes and links of interest here are in red. Nodes and links in blue were not part of the implementation of this protocol. An interactive version of this map can be found at `https://u.osmfr.org/m/1051066`.



(b) Graph-like representation of the quantum network. The nodes of interest are in red. This figure is not to scale. The length of the fibers have been indicated.

Figure 2. The Paris Quantum Network.

others, to the NIST Post-Quantum Cryptography Standardization process. It is the only one selected to be standardized for key establishment [19] (as the ML-KEM algorithm in the FIPS 203 standard [20]).

The QKD systems were operating in the Paris quantum network during several weeks, and were used for the trusted node experiment during one week. In Fig. 3, we show the performance of the QKD exchanges for the last 11 h of the experiment, by plotting the secret key rate, Quantum Bit Error Rate (QBER) and visibility given by the QKD systems.

The average QBERs were respectively $1.93\,\% \pm 0.57\,\%$ (OG-LIP6) and $1.72\,\% \pm 0.68\,\%$ (OG-TP) with average visibilities of 0.998 ± 0.012 and 0.959 ± 0.024 respectively over the 11 hours. The relatively low visibility on the OG-TP link could be due to a misalignement in fiber on the Cerberis module interface but does not change the results on the performance of the trusted node protocol. The average key rates were respectively 2493 bit/s (standard deviation 28 bit/s) and 612 bit/s (standard deviation 139 bit/s). Since the heavy operations can be parallelised with the QKD key exchanges, there is no overhead and the final key rate is given by $r_{\text{final}} = \min(r_{LIP6-OG}, r_{OG-TP}) = r_{OG-TP}$. This yields an overall LIP6 - TP final key rate of 612 bit/s on average.

The keys exchanged between Alice and Bob were then retrieved using the specifically modified Thales Mistral encryptors to encrypt a streaming service with 4K videos.

While we implemented the protocol on key exchange with one intermediary node, the protocol can be extended to more trusted nodes, maintaining a single KEM round and AES encryption and decryption, with all the intermediary nodes forwarding the AES ciphertext.

V. CONCLUSION

In this work we presented the implementation of an efficient PQC-secured trusted node protocol. While providing computational security against an honest-but-curious intermediary node, we maximise the efficiency of the protocol by saturating the bound for information-theoretic security to exterior adversaries.

The performance of the overall protocol could be improved, for instance by switching to the ID Quantique Clavis XGR using decoy-state BB84, other DV-QKD systems or Continuous-Variable (CV) QKD, which could yield higher key rates on the QKD links. This work however already readily demonstrates an important use case where bringing together quantum and post-quantum cryptographic techniques provides increased practical security in real-world configurations.

ACKNOWLEDGMENTS

The authors acknowledge financial support from the Île-de-France Region under the ParisRegionQCI project, the European Union's Horizon Europe research and

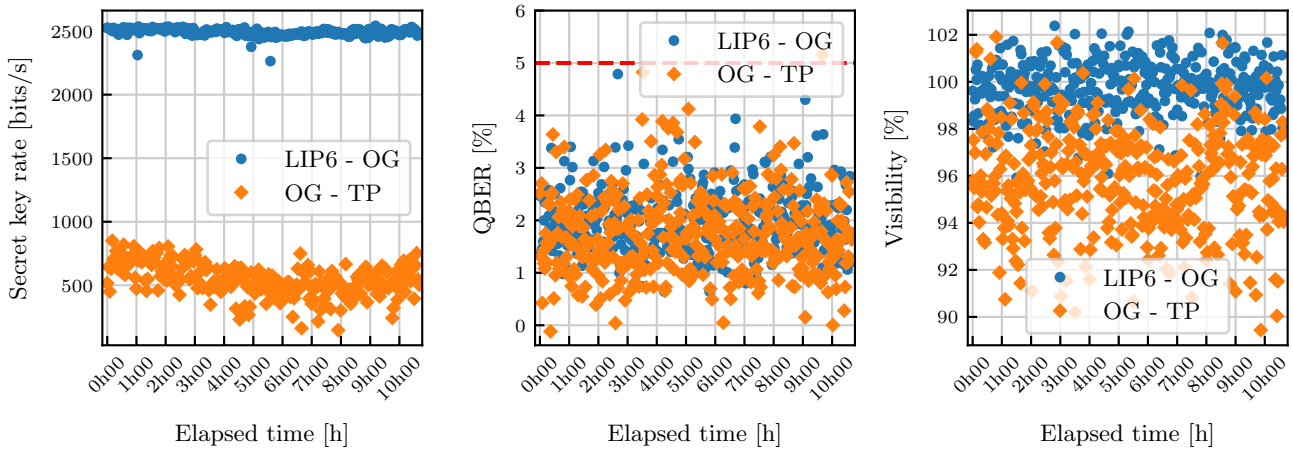


Figure 3. Secret key rate, QBER and visibility as a function of time for the two QKD links.

innovation program under the Grant Agreement No 101114043 (QSNP), and the PEPR integrated project QCommTestbed, ANR-22-PETQ-0011, which is part of Plan France 2030

Figures were created using illustrations from the Flat Profile Avatar collection (CC BY Ceria Studio), from the Travel Duotone Icons collection (PD Anita Csillag), the Sports And Games Icooon Mono Vectors collection (PD Icooon Mono) and from the Security 11 collection (CC0). Map was created using the umap tool with tiles from jawgmaps and map data from OpenStreetMap.

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advanced Quantum Technologies **12**, 1012 (2020).

[2] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nature Communications **8**, 15043 (2017).

[3] N. Walenta, D. Caselunghe, S. Chuard, M. Domergue, M. Hagerman, R. Hart, D. Hayford, R. Houlmann, M. Legré, T. McCandlish, L. Monat, A. Morrow, G. Ribordy, D. Stucki, M. Tourville, P. Trinkler, and R. Wolterman, "Towards a north american qkd backbone with certifiable security," QCRYPT 2015 (2015).

[4] B. Dowling, T. B. Hansen, and K. G. Paterson, in *Post-Quantum Cryptography*, edited by J. Ding and J.-P. Tillich (Springer International Publishing, Cham, 2020) pp. 483–502.

[5] S. Bruckner, S. Ramacher, and C. Striecks, in *Post-Quantum Cryptography*, edited by T. Johansson and D. Smith-Tone (Springer Nature Switzerland, Cham, 2023) pp. 601–633.

[6] C. Battarbee, C. Striecks, L. Perret, S. Ramacher, and K. Verhaeghe, "Quantum-safe hybrid key exchanges with kem-based authentication," (2024), arXiv:2411.04030 [cs.CR].

[7] M. Geitz, R. Döring, and R.-P. Braun, in *2023 8th International Conference on Frontiers of Signal Processing (ICFSP)* (IEEE, 2023).

[8] P. Zeng, D. Bandyopadhyay, J. A. M. Méndez, N. Bitner, A. Kolar, M. T. Solomon, Z. Ye, F. Rozpędek, T. Zhong, F. J. Heremans, D. D. Awschalom, L. Jiang, and J. Liu, "Practical hybrid pqc-qkd protocols with enhanced security and performance," (2024), arXiv:2411.01086 [quant-ph].

[9] There is an additional step of authentication using the Falcon signature scheme that we do not consider here.

[10] "Kyber website," https://pq-crystals.org/kyber/, accessed: 2024-04-23.

[11] I. Quantique, "Cerberis xgr series," (2022).

[12] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, Optics Express **17**, 13326 (2009).

[13] J. A. Donenfeld, in *Proceedings of the Network and Distributed System Security Symposium (NDSS)* (2017).

[14] *Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API*, Group Specification ETSI GS QKD 014 v1.1.1 (ETSI, 2019).

[15] Thales, "Mistral ip9001," .

[16] The encryptors were using the final key to perform AES256 encryption of the streaming data.

[17] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (2018) pp. 353–367.

[18] C. Security, "Cryptonext quantum-safe library (c-qsl)," (2023).

[19] NIST, "Selected algorithms 2022 - post-quantum cryptography," .

[20] *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, Tech. Rep. (National Institute of Standards and Technology, 2023).

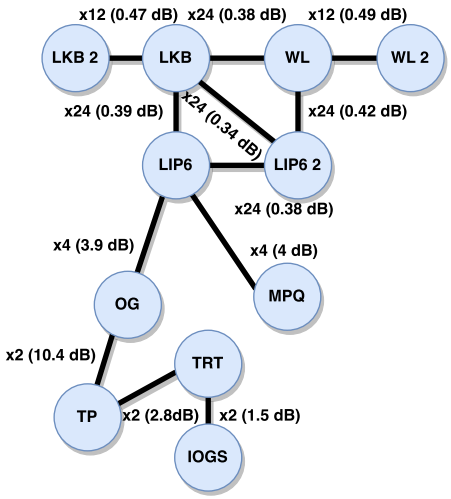


Figure 4. Complete description of the Quantum Communication backbone in the Parisian area. The labels on the edges indicate the number of the available fibers and their average losses.

Appendix A: Full description of the Paris Quantum Network

The Paris Quantum Network is currently composed of 11 nodes, where connections endpoints are available, corresponding to locations of academic and industrial partners. Since some nodes are administrated by the same partner, we considered in the main text the 8 main nodes correspoding to individual partners. The 8 partners are: Laboratoire Matériaux et Phénomènes Quantiques in Université Paris Cité, in the 13th district of Paris (Node MPQ), Laboratoire LIP6 in Sorbonne Université, in the 5th district of Paris (Node LIP6) with 2 endpoints (LIP6 and LIP6 2), Laboratoire Kastler-Brossel in Sorbonne Université in the 5th district of Paris (Node LKB) with two endpoints (LKB and LKB 2), Welinq company in the 5th district of Paris (Node WL) with two endpoints (WL and WL2), Orange Innovation group of the French network operator Orange in Châtillon (Node OG), Laboratoire Traitement et Communication de l'Information in Télécom Paris, in Palaiseau (Node TP), Thales Research and Technology division of the company Thales in Palaiseau (Node TRT) and Laboratoire Charles Fabry in Institut d'Optique Graduate School in Palaiseau (Node IOGS).

For completeness, we include a full map of the current network in Fig. 4, including the number of available fibers and the average losses on those fibers.

This network is used to benchmark quantum technologies, in particular Quantum Key Distribution, including Discrete-Variable and Continuous-Variable, interoperability between systems, coexistence with classical communication and protocols built on top of QKD. Moreover the network will be used for entanglement distribution and deployment of links integrating quantum memories.