Global-Scale Information-Theoretic Secure Communication using QKD and Distributed Symmetric Key Establishment

R. S. Tessinari[1,*], R. I. Woodward[1] J. Johannsson[2], S. N. Altimari[2], M. Taylor[2] and A. J. Shields[1]

[1] *Toshiba Europe Ltd, Cambridge, UK*
[2] *Quantum Bridge Technologies Inc., Toronto, Canada*

[*] *rodrigo.tessinari@toshiba.eu*

Abstract: We propose and demonstrate a new network architecture for global-scale information-theoretic secure communication, combining QKD and Distributed Symmetric Key Establishment (DSKE), including the extension of draft emerging standards for vendor-interoperable quantum key relay (ETSI 020).

1. Introduction

With advances in quantum computing threatening conventionally secured communication methods, there is an urgent need to migrate towards quantum-safe communication technologies. The term 'quantum-safe' typically describes security mechanisms which are "hard" to break using even a quantum computer. While an improvement over conventional methods, for ultimate protection, it is desirable to achieve information-theoretic security (ITS), i.e. provable security, where the probability of compromise is bounded to an infinitesimally small value. This ensures long-term protection, invulnerable to future advances in quantum computing or advanced cryptanalysis.

ITS key distribution can be achieved using Quantum Key Distribution (QKD) [1], which is being increasingly deployed into operational networks worldwide. The range of QKD, however, is constrained by channel loss, which limits practical distances using optical fibre to 100s km [2]. Satellite QKD offers a potential future solution, although there is demand for nearer-term solutions without the cost and complexity of satellite communications. To meet this need, a new ITS key distribution protocol known as Distributed Symmetric Key Establishment (DSKE) has recently emerged. This uses pre-shared random data (PSRD) with multiple independent "Security Hubs" and combines hub-specific shares via a (k,n)-threshold secret-sharing scheme over public communications to generate keys (without public key cryptography) [3].

Here, we propose a new network architecture that combines QKD and DSKE. This combination overcomes challenges inherent to each primitive: DSKE enables operation over global-distances and QKD avoids the need for regular delivery of PSRD by trusted courier at the metro scale. Our network architecture enables practical global-scale ITS-secure communications using present-day technology, interfaced with emerging standards, which we demonstrate by connecting metro networks between Toronto (Canada) and Cambridge (UK).

2. Network Architecture

Our network architecture (Fig. 1), comprises QKD metro networks in Toronto and Cambridge connected via a DSKE link, where each site is a trusted node. It is instructive to visualize the network in a layered manner—as in classical networks, the top *Application Layer* serves users (e.g. encryptors) requesting secure keys for communication with other locations and a bottom *Physical Layer* includes point-to-point fibre links between sites. A *Key Management Layer* sits between these, responsible for routing & relaying ITS-secure keys between nodes.

Trusted-node QKD networks are already widely deployed, where a 'global key' is relayed across links hop-by-hop, encrypted with a 'local QKD key' for each link. One-time pad (OTP, i.e. XOR) encryption is used, achieving ITS security (Fig. 2a). The DSKE primitive also enables ITS key relay across a public channel, using PSRD and a secret sharing scheme to even mitigate against the compromise of some of the trusted nodes (Fig. 2b) [3].

To combine these primitives, we extend the emerging ETSI standard GS QKD 020 "Interoperable Key Management System (KMS) API" ("ETSI 020") [4], intended to enable key relay between different vendors that employ proprietary closed key management systems. A trusted node containing Key Management Entities (KMEs) from different vendors can use ETSI 020 to pass keys from one vendor domain to another. Similar to the well-established ETSI 014 standard [5] used by encryptors (a.k.a. Secure Application Entities, SAEs) to request keys, ETSI 020 is a REST API. We are actively contributing to the standardization of 020 within ETSI and use draft v0.5.1 in

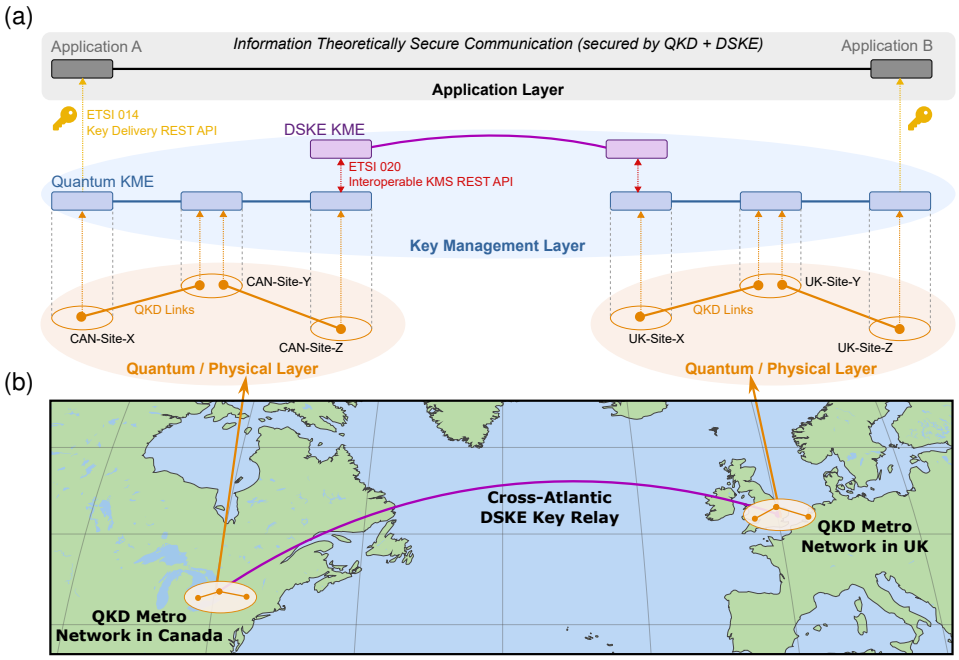

Fig. 1. Demonstrated network connecting QKD metro networks in Canada (CAN) and UK via DSKE: (a) schematic layout showing conceptual network layers; (b) geographical layout.

this work. Fig. 2c illustrates its operation, sharing keys from QKD KME to DSKE KME via a `HTTP POST` to the `ext_keys` API endpoint with a JSON payload containing the keys (& corresponding IDs) and related SAE IDs. ETSI 020 supports both blocking (synchronous) and non-blocking (asynchronous) operation; we adopt the newer non-blocking scheme here for better scalability. After receiving an `ext_keys` request, the DSKE KME returns HTTP Code 202 to indicate it has been accepted (or Code 400 error in case of an invalid request) and then proceeds performing onward relaying. To ensure keys are not delivered to initiating encryptors before the key is relayed to the target location (i.e. avoiding race conditions), the QKD KME waits for an acknowledgment that relaying succeeded. When completed, the DSKE KME issues a `POST` request to the `ext_keys/ack` endpoint of the QKD KME to acknowledge successful delivery of keys.

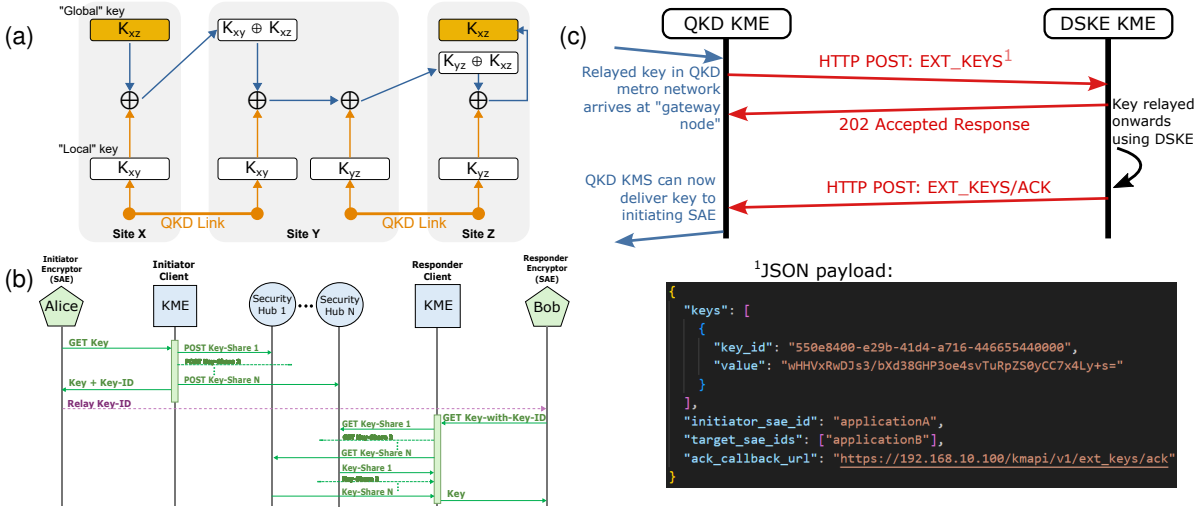

Fig. 2. Illustrations of various enabling primitives in the global ITS network: (a) Trusted-node relaying; (b) DSKE protocol; (c) ETSI 020 key relay between different vendor KMEs.

3. Network Operation, Results & Discussion

We demonstrated our network design with 2 QKD links in Toronto and 2 QKD links in Cambridge, connected via DSKE (Fig. 1). One trusted node in each metro network is designated a “gateway node”, containing both a QKD

KME and DSKE KME (with the DSKE KME instances at different sites communicating over the Internet). All QKD systems implemented the T12 (optimized efficient BB84) QKD protocol, although our network is compatible with any QKD hardware through the use of standardized interfaces. The QKD links in Toronto ran in back-to-back configuration (0 dB channel loss), achieving average secure bit rates (SBRs) of 3.95 Mbps and 2.89 Mbps, and quantum bit error rates (QBERs) of 2.6% and 3.2%, stable for many months (Fig. 3a). The 2 QKD links in UK ran over 10 dB fixed attenuation, with 352 kbps and 741 kbps SBR (QBERs of 3.0% and 2.4%). DSKE was configured with two security hubs and a (2,2) threshold.

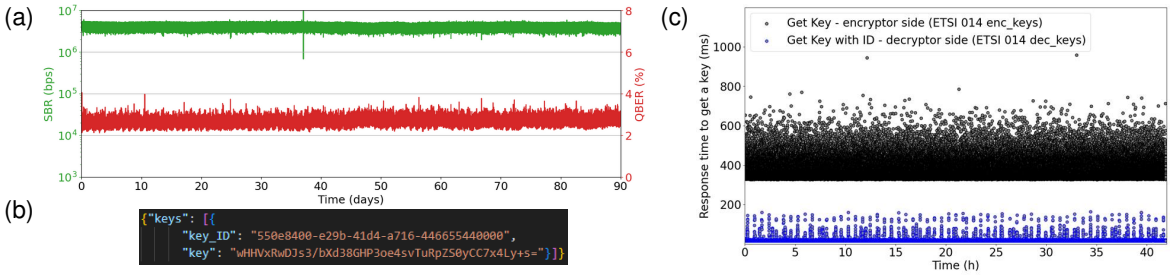

Fig. 3. Deployed QKD+DSKE network results: (a) QKD performance in back-to-back configuration; (b) example ETSI 014 response to encryptor request; (c) response times to encryptor requests.

An emulated application at CAN-Site-X regularly requested key material (via ETSI 014 API) to be shared with a corresponding application in UK-Site-Z. The QKD KMS relayed the key from CAN-Site-X to CAN-Site-Z, followed by ETSI 020 to hand the key to the DSKE KME co-located at CAN-Site-Z. DSKE securely relayed the key to UK-Site-X, where an ETSI 020 transfer was used again to hand the key to the QKD KMS in UK, which finally relayed it to UK-Site-Z (with an acknowledgment being sent back through the network to ensure synchronization). Application A received the key from CAN-Site-X KME (in JSON format via ETSI 014, Fig. 3b) and then advised Application B of the key ID (over a public, insecure channel), as well as using the key to encrypt its data. Application B then used the key ID to request the corresponding decryption key from UK-Site-Z KME, enabling it to decrypt the data from Application A. Thus, Application A and B are able to perform ITS-secure communication. Crucially, by following a layered model, the complex key handling and physical layer arrangements are abstracted away from the application layer, so encryptors do not require knowledge of the underlying network topology.

Keys were relayed between sites on-demand, enabling users to request any arbitrary key size and target SAE. To evaluate performance, we issued repeated requests for 256-bit keys between Applications A and B. The delay of the CAN-Site-X KME in responding to Application A's encryption key request was 365 ms average, $\pm$ 81 ms std. dev. (Fig. 3c), comprising both processing time to execute the relay and latency in UK-to-Canada communication (hence minor variation in response times over a mutli-day period). The delay of the KME at UK-Site-Z responding to Application B's corresponding decryption key request was 18 ms $\pm$ 5 ms—much smaller since the key with corresponding key ID was already present in the KME at Site Z. For applications requiring lower latency responses for encryption key requests, support for "pre-shared key" could be implemented where buffers of pre-shared fixed-size end-to-end relayed keys are accumulated between sites, ready for instantly delivering to encryptors upon request.

4. Conclusion

We introduced a novel network architecture for ITS communications exceeding the current capabilities of fibre-based QKD by leveraging the DSKE protocol. Importantly, this approach uses currently available technology and advances emerging standards, enabling global-scale secure communications today.

References

1. C. Portmann and R. Renner, "Security in quantum cryptography," Rev. Mod. Phys. 94, 025008 (2022).
2. M. Pittaluga et al., "Long-distance coherent quantum communications in deployed telecom networks", Nature 640, 911 (2025)
3. H.-K. Lo, M. Montagna, and M. von Willich, "Distributed Symmetric Key Establishment: A scalable, quantum-proof key distribution system," arXiv:2205.00615 (2024).
4. ETSI, "ETSI GS QKD 020 V0.5.1 Draft, Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API" (2025).
5. ETSI, "ETSI GS QKD 014 V1.1.1, Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API" (2019).