Quantum Information Processing (2026) 25:65
https://doi.org/10.1007/s11128-026-05055-x

Design and simulation of secure data center intra-connectivity using entangled quantum key distribution

Miralem Mehic[1,4,5] · Peppino Fazio[2,4] · Stefan Rass[3,5] · Sergej Jakovlev[4,5] · Miroslav Voznak[4,5]

Received: 10 October 2025 / Accepted: 2 January 2026

Abstract

The integration of quantum key distribution (QKD) into data centers represents a promising advance in secure communications. As cyber threats evolve and the volume of sensitive information grows, strengthening intra-data center security has become a strategic necessity for ensuring confidentiality and operational resilience. This paper explores the application of an entanglement-based QKD method for securing intra-connectivity within data centers, focusing on deploying the BBM92 protocol in a controlled environment. We detail the system architecture, technical requirements, and operational considerations, and we report simulation results from a 100-block BBM92 run: an average sifted key of 1224 bits per block, with 25% used for QBER estimation, reconciliation disclosures of 352 bits, and privacy amplification removing an additional 13 bits, yielding a final secure key of 554 bits per block at an average rate of 52 bps. Across the run, 86 keys were delivered to applications, enabling 43 IKEv2/IPsec sessions, with an initial ramp-up before reaching steady, near-linear key service. These findings indicate that entanglement-based QKD can provide robust, quantum-safe key distribution for data center environments while highlighting practical integration challenges and performance trade-offs.

✉ Miroslav Voznak
miroslav.voznak@vsb.cz

Miralem Mehic
miralem.mehic@etf.unsa.ba

1 Department of Telecommunications, Faculty of Electrical Engineering, University of Sarajevo, Zmaja od Bosne bb, 71000 Sarajevo, Bosnia and Herzegovina

2 DSMN, Ca' Foscari University of Venice, Via Torino 155, Venice 30172, Italy

3 LIT Secure and Correct Systems Lab, Johannes Kepler University, Altenberger Straße 69, 4040 Linz, Austria

4 Department of Telecommunications, VSB – Technical University of Ostrava, 17. listopadu 2172/15, 70800 Ostrava, Czechia

5 Marine Research Institute, Klaipeda University, Universiteto al. 17, 92295 Klaipėda, Lithuania

Published online: 12 February 2026

Keywords Quantum key distribution · Simulations · Networking · Security

1 Introduction

The rise of quantum computing presents significant challenges to classical cryptographic techniques. Unlike existing cryptographic solutions that rely on the complexity of mathematical solutions, quantum key distribution (QKD) guarantees an information-theoretical secure (ITS) growth of symmetric secrets between two geographically distant users [1]. QKD secures the distribution of symmetric cryptographic keys between users by leveraging the principles of quantum mechanics. Such a level of security is of interest to those organizations and facilities that exchange highly sensitive communication content. Among them are data centers that strive for the highest security standards that cannot be provided by classical cryptographic methods.

The QKD connectivity differs from traditional telecommunication links in various ways. The logical QKD link comprises a quantum channel for transferring confidential values encoded in unique photon properties and a public channel for verifying and processing the data exchanged. The quantum channel is a point-to-point connection between two nodes. In contrast, public channels can be implemented as conventional IP connections with an arbitrary number of intermediate devices. The length of QKD links is limited by the attenuation in the quantum channel, which also affects the key generation rate. However, the controlled environment of a data center allows for high rates of key generation, sufficient for securing numerous high-frequency data transfers and communications. The short distance of the links, which is characteristic of intra-data center connectivity, ensures significantly less attenuation during the transmission of photons in the quantum channel and enhances the stability of the quantum channel, which is of particular importance for entanglement-based QKD protocols. While QKD has been demonstrated in various settings [2], including fiber optic networks and free-space communication, its application within data center environments presents unique opportunities and challenges.

Here, we investigate the feasibility and benefits of implementing the entanglement-based BBM92 protocol to secure intra-connectivity within data centers. Several simulation and emulation techniques were used to realize the entire system. These include QKD key generation, processing and storage at the key management layer, and key consumption using practical multiple IPsec VPN sessions using a software encryptor [3].

This paper is organized as follows: Sect. 2 provides fundamentals of BBM92 entanglement-based protocol. Section 3 discusses system architecture for applying entanglement-based QKD protocol in data centers. Description of simulation setup is provided in Sect. 4. The results of performed experiments are shown and discussed in Sect. 5. Section 7 concludes the study.

2 Background and related work

Charles Bennett and Gilles Brassard introduced an intriguing concept in 1984 to show how quantum phenomena might be used to create a communications quantum channel, from which data cannot be reliably read or reproduced [4, 5]. Heisenberg's uncertainty principle [6] and the *no-cloning* theorem [7] guarantee the properties of information transfer through elementary quantum systems, such as polarized photons. Thus, passive eavesdropping attempts on the quantum channel could be identified. Additionally, Bennett and Brassard described a scheme [4, 5], now known as the BB84 protocol, that allows two distant parties, Alice and Bob, to securely distribute symmetric keys as long as they have access to both the quantum channel and an authenticated public channel. In the first-ever free-space QKD experiment conducted at a distance of 32.5 centimeters in 1989 [8], Bennett and Brassard demonstrated their theory experimentally. This experiment sparked interest in the technology's integration and broader use, which persists to this day [9].

The BBM92 protocol, proposed by Bennett, Brassard, and Mermin in 1992, is a two-photon extension of the BB84 protocol that utilizes entangled photon pairs for secure key distribution [10]. The security of these protocols derives from the properties of quantum states as described in quantum theory, and BBM92 particularly leverages the resource of entangled particles of light to implement them. As a built-in feature in such systems, an eavesdropper attempting to intercept the quantum signals would introduce detectable anomalies in the quantum states, thereby providing immediate alerts to the presence of a malicious third party.

Alice and Bob each share a photon of an entangled photon pair, for which they measure the polarization state in a randomly chosen bases out of two non-orthogonal bases. The result is a correlated, but not symmetric, sequence of secret bits, often denoted as the "raw key". The protocol follows the same post-processing procedure as other QKD protocols: extraction of the raw key (sifting), error estimation, error reconciliation, privacy amplification, and authentication.[1]

It is important to note that newer approaches seek to optimize the choice of bases. Approaches on using machine-learning-enhanced qubit-based synchronization are reported [11]. Synchronization of bases can improve protocol security [12, 13]. In our previous work [14], base selection is totally synchronized using a hashed-seed pseudo-random number generator, which significantly improves protocol performances. However, in this paper, we implemented the original approach in which bases are selected randomly.

When Alice and Bob make the same basis measurement choice and the channel is ideal, entanglement ensures that their outcomes are correlated (or anti-correlated). The correlation or anti-correlation of the measurement results is controlled by the

[1] Sifting is a method for identifying and discarding experimental outcomes that cannot generate shared random bits of the raw key. Error reconciliation is used to detect and correct bit-flip errors induced by channel and equipment imperfections, or by actions taken by eavesdropper Eve. In privacy amplification, Alice and Bob assess the amount of information Eve could have extracted from their key based on measured error rates in their system during both the quantum communication and information reconciliation steps, and then perform a distributed algorithm that results in a shorter, more secret shared key. Finally, they exchange hash values to make sure that the processed key is indeed symmetrical on both sides.

entangled state Alice generates. A logical NOT operation on one user's key transforms anti-correlated bits to correlated bits, so Alice and Bob can always generate a shared key as long as they know which entangled state is generated. In practice, when the channel is not ideal due to attenuation, noise, or Eve's interference, the secret key rate is reduced. The loss can be categorized into: localized insertion loss, such as reflections at optical components (inputs, outputs, fiber splices, etc.), propagation loss defined by the length of the quantum channel and the loss per unit length in dB/km, and the efficiency of the source and detector. In practice, those parameters define how many photons will be detected and used to generate the key.

However, even those polarization-encoded qubits sent through the channel can be affected by misalignment of the measurement bases. It is a consequence of polarization rotation due to the birefringence of the fiber. The measurement bases are no longer aligned with the basis in which the qubit was prepared, which leads to uncorrelated qubits that are measured by Alice and Bob. Such bit-flip events need to be measured and monitored to be below the acceptable threshold. Eve can perform a man-in-the-middle attack by measuring and resending the photons, thereby increasing the measured quantum bit error rate (QBER) above the defined threshold and triggering security alarms.

Current-generation QKD systems have the potential to produce keys at a rate of several hundred kbps over mid-range optical links [2, 15]. Measurement-device independent QKD (MDI-QKD) offers a way to address many security flaws [16], at least on the quantum parts, and to increase the achievable distances [17]. In MDI-QKD, neither Bob nor Alice detects photons; instead, both generate them. Charlie, an intermediary relay node situated between Alice and Bob, implements measurements. Side-channel detector attacks do not compromise protocol security because neither Bob nor Alice has detectors installed. If Alice and Bob are given the measurement results, they can still create a secret key, even if an attacker controls the Charlie node. The public channel is used to announce these results, but the key itself is not disclosed. Therefore, there is no trust assumption on Charlie between Alice and Bob required.

The state-of-the-art twin-field QKD (TF-QKD) protocol enables transmission over 830 km in the fiber channel. The TF-QKD uses single-photon interference to produce secret key rates scaling as the square root of channel length by having Alice and Bob send phase-encoded weak coherent pulses (WCP) to an untrusted central node, Charlie. This allows for quantum-secured communication over previously unreachable distances [18, 19].

Conference quantum key agreement (QCKA) is a promising application of quantum networks that allows a group of users to efficiently distribute ITS quantum keys [20–22]. Establishing multi-partite entanglement between remote participants is the basis of QCKA [23]. Still, due to simulation limitations, we follow the straightforward approach of the BBM92 entanglement-based QKD protocol in this paper.

It is worth noting the idea of establishing direct, confidential communication between users by sending messages over a quantum channel. This approach is known as "Quantum Secure Direct Communication" [24–26]. Coupling QSDC with quantum memory is essential for completing the communication task because the complete implementation of a quantum protocol always necessitates the capacity to effectively manage the transfer of a message in the time domain [25]. Therefore, quantum net-

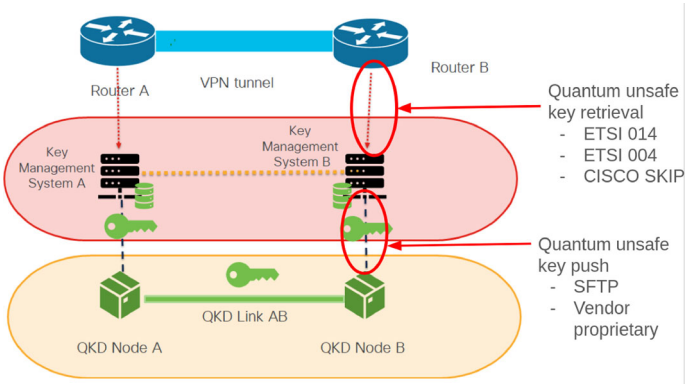


Fig. 1 Logical layered structure of the QKD network. Keys are generated by QKD devices and pushed to assigned key management systems (KMS) where they are processed and stored. The communication from QKD devices to KMSs is not standardized, thus, multiple solutions exist in practice. The application devices (routers) are seeking for keys to establish secure VPN tunnels. There are several APIs for key delivery but they are not quantum-safe since they do not use ITS keys for secure key delivery [33]

works without a quantum repeater are restricted either to a limited area of directly connected nodes or to nodes connected to a common node. Approaches combining QSDC and classical repeaters have been reported as an interim solution toward a quantum Internet (QInternet) [27]. QSDC schemes have been developed over optical fiber and free-space channels, based on discrete-variable (DV) [28, 29] and continuous-variable (CV) systems [30]. Recent results report QSDC implementations over several hundred kilometers [31, 32], which can be attractive for securing data center long-range connectivity. However, in this paper, we focus on data center intranet.

3 System architecture

System organization is the primary topic when integrating QKD in the data center network. Figure 1 shows the layered organization of the QKD network. At the bottom, QKD devices generate keys and push them to assigned KMS devices. It is essential to point out that currently, there are no standardized approaches for QKD device-KMS communication, which leaves room for various vendor-proprietary solutions or reliance on manual tools such as SFTP. By default, this communication is secured using standard Elliptic-curve Diffie–Hellman (ECDH) cryptography, which is not quantum-safe.

When KMS receives the keys, it will analyze them and, if necessary, merge them into larger keys or separate them into more minor keys. The goal is to prepare keys in advance and reduce waiting time when the application requests them [33, 34]. Finally, at the top are the end-user applications (software programs or hardware devices) that will contact the KMS to obtain the necessary keys. There are several specifications for this communication, such as ETSI 014, ETSI 004, and vendor-priority protocols such as Cisco Secure Key Integration Protocol (SKIP) [35]. ETSI 014 and ETSI 004 are

based on The Transport Layer Security (TLS) protocol version 1.2 or 1.3, while Cisco SKIP only works with TLS 1.2 authentication based on pre-shared keys. However, this communication cannot be considered quantum-safe because ECDH cryptography is mostly used.

3.1 Compact application, key management and QKD devices

All of the above sets significant limitations when defining the system architecture. In practice, QKD devices, KMSs, and end-user applications should be located within a secure perimeter (domain). Our aim is to provide quantum-safe communication between different sectors/rooms within data center. Thus, it is necessary to reduce the distance between end-user applications and KMS, as well as between QKD systems and KMS (see Fig. 1). This imposes an ideal design in which all three layers of the QKD system should be combined in a single rack-mounted device.[2]

From an application perspective, such a device should be able to establish quantum-safe VPN connections with remote peer devices and act as a proxy (accepting and forwarding data traffic to other end-user machines in its secure domain/rack). Thus, we will hypothetically assume the availability of such functionality and use in data centers.

However, due to economic reasons, it is difficult to assume that such a device can be implemented on every server located in data center racks. Therefore, it is more economical to assume that such a device would be installed on top-of-the-rack routers and used to provide quantum-safe communication between racks.

3.2 Centralized entangled photon source setup

Implementing BBM92 in a data center necessitates a centralized entangled photon source. This source, as shown in Fig. 2 is located in a secure and controlled environment, generating pairs of entangled photons that are distributed via fiber optic cables to different nodes within the data center.[3] Fiber optic cables are employed to transmit entangled photons from the centralized source to other network nodes. Given the short distances typical of data center environments, fiber optic cables minimize photon loss and decoherence, maintaining the integrity of the entangled states. Each node is equipped with single-photon detectors capable of performing measurements in randomly chosen bases. We assume that a secure classical communication channel is

[2] Some commercial devices combining multiple functionalities are available: https://heqa-sec.com/sceptre-duo/.

[3] Due of the detector's high sensitivity to temperature, vibration, and other external factors, which raises the price, one could propose a scenario where only one detector would be implemented with multiple sources. These sources would hypothetically be set at remote locations in the data center, so the question of establishing entangled-based photons between those device arises. Potentially, it is possible to use remote state preparation (RSP-BBM92) [36] or entanglement-swapping (ES-BBM92) [37] protocols. Although they allow the establishment of entangled photons between nodes at greater distances (which is not a major issue for intra-data center connectivity), they imply the use of an additional dedicated source to generate entangled-based photons that will be directed toward the nodes. This means that the nodes would again be in the role of detector, which is not a gain compared to the proposed architecture with a single source and multiple detectors.

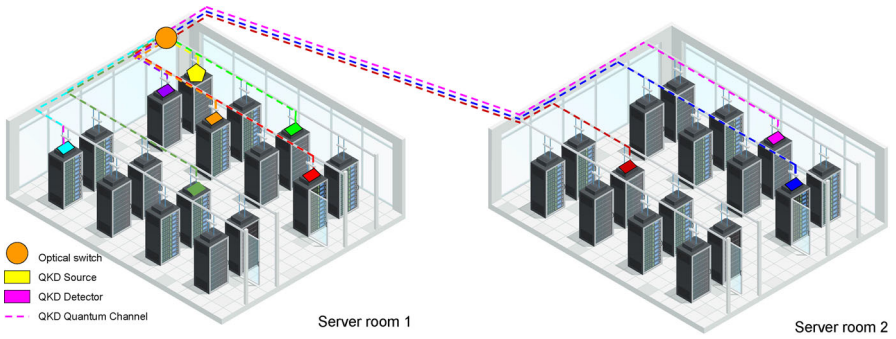


Fig. 2 Logical organization of QKD network between server rooms of a data center. It is based on BBM92 time-bin protocol enabling a network of the multiple participants connected via quantum channel to an optical switch (orange). Entangled photons are generated by the source (yellow) located closely to the switch to minimize losses

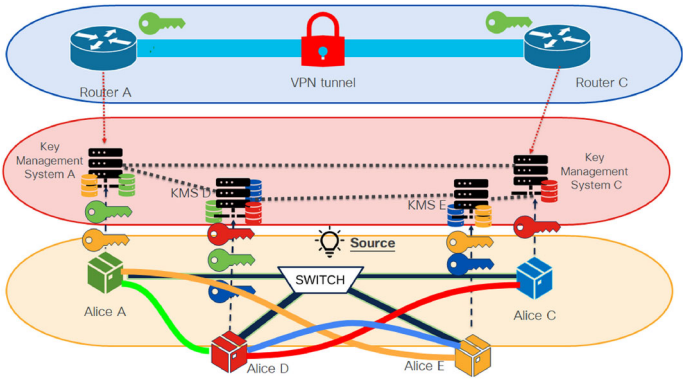


Fig. 3 Key management organization of the entanglement-based QKD network within data center. Entangled photons are generated by the source and delivered to QKD detector nodes via optical switch. After synchronization, nodes can measure entanglement-based photons and ultimately establish symmetric keys, i.e., QKD links (in the picture they are shown with solid lines: green, red, blue, and orange). These keys are further stored in the corresponding KMSs for further processing and serving

established using existing data center TCP/IP networking infrastructure. This channel allows nodes to publicly share their measurement bases after receiving the photons. They discard any results where the bases do not match, and the remaining correlated outcomes are used to generate key in post-processing phase.

3.3 Key management organization

Once the key generation process is complete, keys are pushed to the KMS for processing and storage. Processing primarily refers to the consideration of the need to reduce the key or merge it with other keys to form a new key of longer length [34]. Then, KMS considers in which buffer to store the key so it can be timely available when requested by end-user applications [35].

Given that an entanglement-based protocol is used, it is important to note the difference on the key management layer compared to the discrete-variable protocols. The primary difference is that entanglement allows direct key establishment between remote nodes without a key-relay. As shown in Fig. 3, node D has established entanglement circuits with nodes A, C, and E. These circuits will be used for direct establishment of keys, so there is no need for additional key-relay operations. However, this does not prevent node D from requesting additional key-relay procedures at the key management layer. Such procedures may be needed to establish new keys when node notices that the directly generated keys are not sufficient for the application's needs. There are several ways to establish keys between remote nodes:

1. Direct establishment of keys using an entanglement-based protocol. This option provides the highest level of security because it does not involve intermediate nodes through key-relay operations.
2. Key-relayed keys are those based on key-relay operations through trusted-relay nodes. This approach provides keys with a lower security because it involves additional intermediate nodes that must be trusted. Also, the key-relay can be delayed or rejected because it requires synchronization and cooperation of all nodes in the key-relay chain [38].
3. Alternatively, instead of a key-relay, nodes can use local pseudo-random number generators (PRNG) to establish new keys. These PRNGs would be seeded with QKD keys allowing for quick establishment of new keys. This approach requires precise synchronization between nodes, but avoids key-relay procedures for establishing new key material [14]. In a different way, the embedding of pseudorandomly permuted bits also lends itself to authentication of key streams [39].

In the rest of the paper, we consider only those keys that were established by the direct method, that is, through an entanglement-based protocol.

4 Simulation setup

To analyze the full network system of integration of QKD into the data center networks, several simulation techniques were used as shown in Fig. 4. The QKD network components are divided into distinct docker containers for easier maintenance and organization, but deployed on a single Ubuntu 22.04 machine.

On the application layer, there is a docker container in which IPsec VPN tunnels are established. Mininet was used to simulate data center network connectivity. One of the main benefits of utilizing mininet is that any host on it may execute any Linux command supported by the hosts that are running mininet. Moreover, it is possible for every node in the mininet to run linux commands on the host to establish an independent IPsec tunnel using the strongSwan VPN client.

IPsec VPN tunnels are based on pre-shared cryptographic keys obtained from the key management layer. For the realization of this component, the QKDNetSim network simulation module was used [40, 41], placed in the emulation mode [42]. Several KMSs have been implemented, between which synchronization connections have been

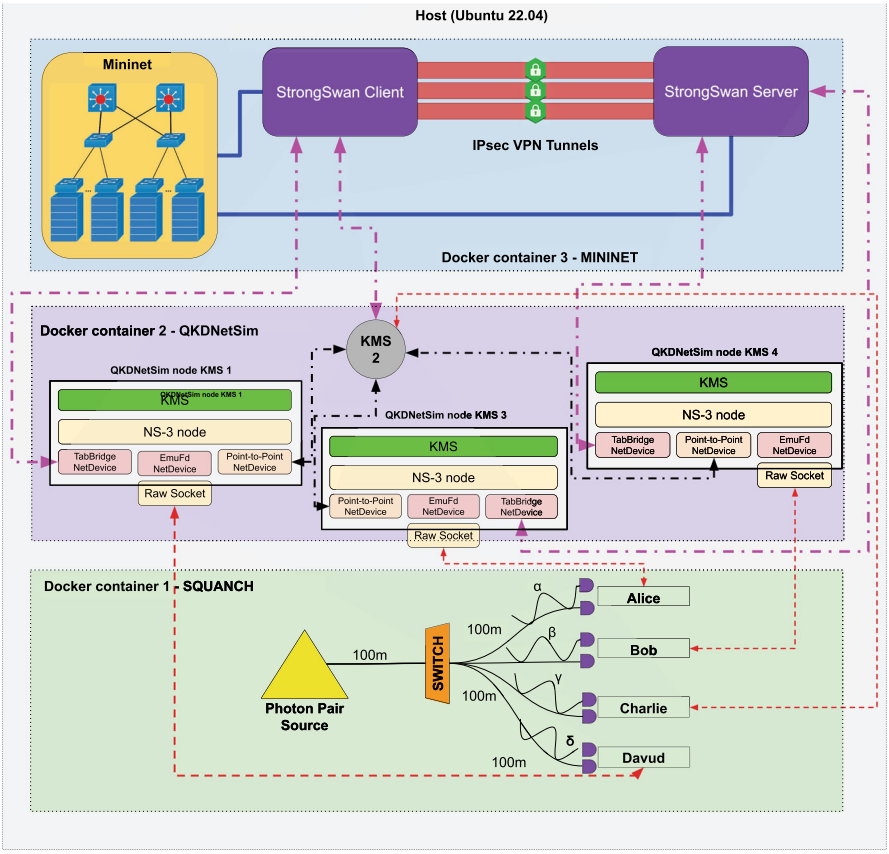
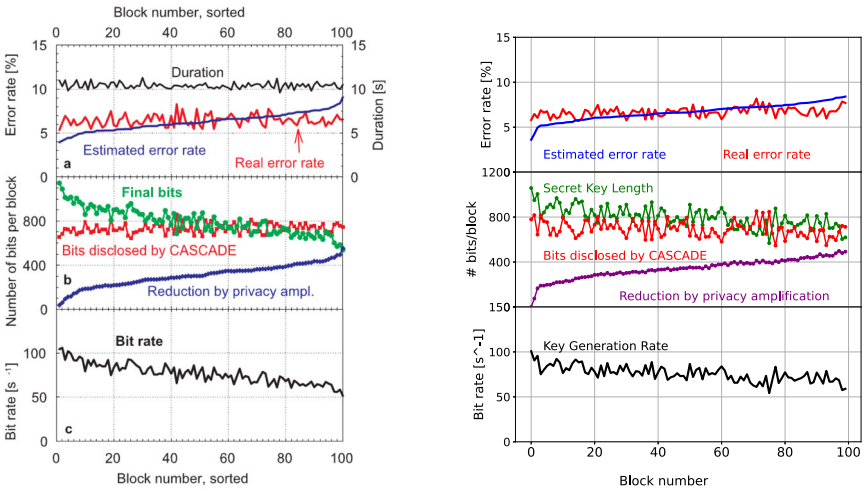


Fig. 4 An emulated QKD network that includes the entire QKD ecosystem with the processes of generation, storage/management, and consumption of keys. Multiple docker containers are installed on a single host machine. QKDNetSim with separate EmuFdNetDevice devices enable emulation connections. SQUANCH is installed in an independent container, generating keys that are sent to QKDNetSim KMS for further processing and storage. The strongSwan client and server applications are installed in top docker container, and IPSec/IKEv2 VPN tunnels are established between Mininet nodes. The key for the VPN connection is obtained from the QKDNetSim KMS

established. KMSs store keys and deliver them to mininet IPsec end-user applications via ETSI 014 API.

We used Simulator for Quantum Networks and Channels SQUANCH) [43] to model quantum systems. The reason we opted for SQUANCH instead of other quantum network simulator tools is because of its agent-based paradigm, which allows completely parallelized simulations with independent processes for each agent. To facilitate expansion to multi-agent simulations, we introduce privacy amplification, information reconciliation, and key sifting procedures not present in SQUANCH, along with modular and customizable agent behaviors. More precisely, we modeled a quantum noise-affected channel, methods for statistical modeling of quantum stream lengths necessary to reproduce the results of experiments were defined, and precise modeling



(a) Experiment reported in [44] (b) Our simulation results

Fig. 5 Comparison of our SQUANCH simulations with results obtained within practical BBM92 QKD experiment as reported in [44]. The diagrams show the results obtained for a total of 100 executions (blocks) sorted by estimated QBER in ascending order

of implicit and explicit losses in the system was performed, which optimizes simulation performance. Finally, as described in [44], we explicitly apply our approach to the simulation of a fiber-based QKD network. The SQUANCH model was extended by the use of the notes listed in [45]. The experiment reported in [44] is a straightforward BBM92 implementation published in 2004 and was used as a basis for simulation verification. More recent results show a larger number of entangled users in line with more modern approaches [46, 47].

4.1 Simulation of BBM92 QKD link

SQUANCH has been extended to faithfully model the BBM92 point-to-point QKD protocol. This includes modeling losses implicitly (loss at insertion into and output from the fiber) and explicitly (channel loss) and bit-flip errors, which are crucial for defining QBER. Our model includes, also, QBER estimation, error reconciliation using CASCADE, and reduction of key in privacy amplification. The average QBER was 6.4%. The total channel loss over a 1.45-km long fiber with 3.2 dB/km was 12.45 dB. The length of the sifted key was, on average, 2441 bits, whereas 609 bits (25%) were used for QBER sample estimation; Cascade disclosed an average of 399 bits while privacy amplification reduced key for an additional 340 bits. The average length of the final secure key was 796 bits. The experiment duration was 10.5 s, resulting in an average key rate of 75.87 bps.

To verify our SQUANCH model, we compared our data with the results of the BBM92 experiment performed in Vienna in 2004 [44]. In Fig. 5, we compare the 100 simulated executions (blocks) to the experimental results (Fig. 3 in [44]). Overall,

the concordance between simulated and reported findings is acceptable. Except for execution duration (value taken from the reported experiment), all quantities appear to fall within a similar range and shape. Since the outcomes are random, precise agreement cannot be anticipated.

4.2 Simulation of QKD network

To extend the simulated BBM92 point-to-point quantum key distribution (QKD) system to a full-scale intra-data center QKD network, several essential components must be integrated. Central to this architecture is a high-performance entangled photon source (EPS) that continuously generates entangled photon pairs[4] and distributes them to users via an optical switch. The switch, ideally a low-loss N-port Micro-Electro-Mechanical Systems optical switch (MEMS)-based device, dynamically routes entangled photons to selected user pairs based on a predefined or dynamic schedule. However, due to the nature of entanglement, each user can only participate in one entangled session at a time. Consequently, when a user is paired with another, it is unavailable for any other entanglement session until the current one is complete. This mutual exclusivity limits the number of simultaneously active links to $\lfloor N/2 \rfloor$ for N users. Additionally, the photon source itself introduces a fundamental bottleneck: a single EPS can only emit one entangled photon pair per pulse, meaning that regardless of switch capability only one user pair can be served per time. To support multiple users, the system must implement a time-division multiplexing (TDM) strategy where user pairs are sequentially granted access to the EPS in rotating time slots.

Loss modeling is equally important for accurately simulating the network's performance. Although intra-data center fiber lengths are typically short ($\leq$100 m), resulting in negligible fiber attenuation (0.02 dB at 0.2 dB/km), other losses dominate, estimated for our simulation setup. These include optical switch insertion loss (1.5 dB), connector/splice losses (0.5 dB each), internal optic losses (1 dB), coupling collection loss (1.8 dB) and detector inefficiencies (3 dB each). Combined, these yield a total effective loss of 7.83 dB that governs whether a photon successfully reaches its destination from the source via switch to one detector (one-arm path). This is implemented in SQUANCH using probabilistic models based on exponential attenuation. We used the same settings for other parameters from our previous point-to-point BBM92 simulation as defined in [45]. Those implies that local detected pair rate $R_{\text{loc}} = 8200$ pairs/sec which defines the number of photon pairs per second detected at the output of the source; window duration $\delta = 10$ ns which defines the temporal duration of a coincidence window; temporal duration for generation of a single key block $T = 10.5$ s and QBER sample interval $n_{\text{sample}} = 25\%$ of the sifted key.

Additionally, channel noise—such as polarization misalignment or temporal drift—is modeled using a *RandomUnitaryError* driven by a tunable Gaussian parameter σ, which determines the QBER according to the theoretical model $\text{QBER}(\sigma) = \frac{1-e^{-\sigma^2}}{2}$. For $\sigma = \pi/6$, the calculated QBER (per connection to the switch) is 6.4% as reported

[4] Commercial solutions are already available such as https://outshift.cisco.com/blog/cisco-quantum-data-center-vision.

in [44]. However, for the total link (two arms), this value is duplicated and exceeds the limit of 11%, so smaller values are considered in the experiment.

For the purposes of the demonstration, a simulation was performed with four nodes (Alice, Bob, Charlie, Diana) connected to a switch to which an EPS is connected. In total, six entangled combinations are possible.

After generation, key blocks are sent to the KMS for storage and preparation for delivery to end applications. We implemented four KMSs, which are connected to corresponding QKD systems. Thus, we created a total of 24 Mininet hosts (12 StrongSwan IPsec client–server pairs) that request keys. Using a pre-shared key (PSK), the StrongSwan client and server applications on the mininet hosts built an IKEv2/IPSec VPN. StrongSwan does not allow IPSec key refreshes to be triggered by the volume of traffic exchanged; instead, refreshes are defined based on the amount of time that has elapsed. A bash script has been created to run periodically every 60 s, meeting these requirements. It tries to obtain a 512-bit long key using *wget* from KMS. If successful, the fetched key is saved in */etc/ipsec.secrets* and StrongSwan is instructed to start a new IPsec session with the fetched key. But, if the key is not fetched, the session cannot be started and will be attempted again in the following iteration. The duration of the IPsec session was set at 20 s. In the case that the key is not available, the previous session is not terminated. When the following key is obtained, and a new session is successfully created, the old session will end.

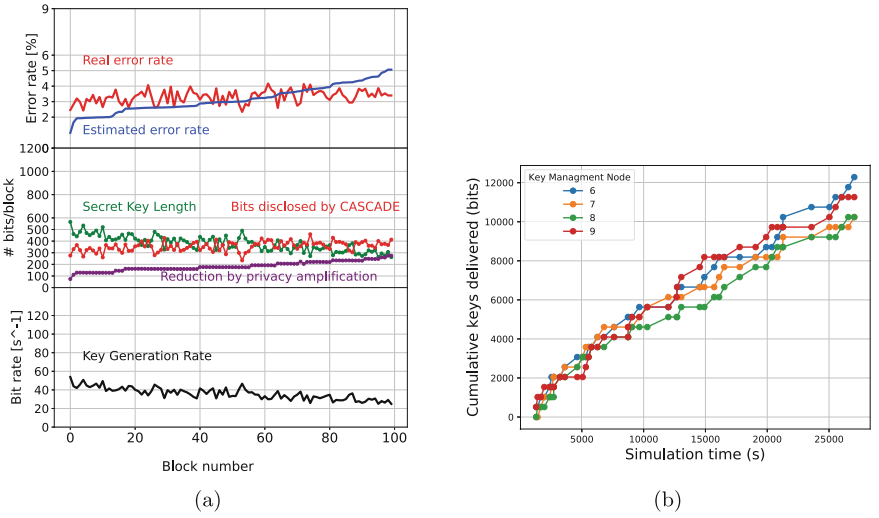


Fig. 6 Results of BBM92 data center simulation. Left: The diagrams show the results obtained for a total of 100 executions (blocks) over all entangled links, sorted by estimated QBER in ascending order. Right: The cumulative number of keys delivered from KMSs to mininet StrongSwan VPN applications

5 Simulation results

Figure 6a shows the results of the BBM92 network simulations obtained within 100 generated blocks, summarized across all entangled links. The length of the sifted key was, on average, 1224 bits, whereas 306 bits (25%) were used for QBER sample estimation; Cascade disclosed an average of 352 bits, while privacy amplification reduced the key for an additional 13 bits. The average length of the final secure key was 554 bits. The experiment duration was 10.5 s, resulting in an average key rate of 52.08 bps.

Although 100 keys (blocks) have been generated, the KMSs delivered 86 keys the mininet StrongSwan applications. Delivered keys of 512 bits are the result of key merge/split operations performed on QKDNetsim KMSs, and they were used to establish 43 IKEv2/IPsec sessions. As shown in Fig. 6, at the beginning of the simulation, there is a noticeable delay in key delivery, as it takes time for the keys to be stored, collected, and processed to satisfy application requests. After the 900th simulation second, requests are processed almost linearly since a stable intensity of key service is reached.

6 Applicability in data centers

Within controlled intra-data center environments, our results indicate practical suitability of BBM92 for periodic VPN refreshes, with key delivery stabilizing after initial startup latency as the KMS buffers fill and service rate becomes steady. The primary scaling constraints are architectural rather than physical: a single EPS, scheduled via TDM, limits simultaneous entangled sessions to $\lfloor N/2 \rfloor$ and one pair per pulse, and the dominant non-fiber losses in short links require careful optical design and KMS buffering to meet application refresh policies. Continuous QBER monitoring on the secure classical channel remains central to anomaly detection and operational assurance.

The simulations do not support claims of surplus keying capacity for inter–data center backbones. Longer spans are fundamentally constrained by attenuation; extending connectivity would rely on a combination of MDI-QKD with trusted key-relay (with reduced security and added coordination) or multipath transmission (to arbitrarily weaken trusted-relay assumptions), possibly leverating PRNG expansion via PQC-secure primitives (e.g., seeded by QKD), and requiring precise inter-node synchronization. We leave these beyond our scope in this work.

From an integration standpoint, data centers' short, stable links align well with BBM92's requirements, and existing delivery interfaces (e.g., ETSI 014/004 and vendor protocols like Cisco SKIP) facilitate automated key consumption into IKEv2/IPsec, even though these APIs themselves may not be quantum-safe in transport. Overall, QKD is a viable building block inside data centers when engineered with TDM scheduling, optical loss margins, and KMS buffering aligned to application policies.

7 Conclusion

The implementation of the BBM92 QKD protocol within a data center environment offers a promising approach to securing intra-connectivity against both classical and quantum threats. By leveraging the principles of quantum mechanics, BBM92 provides robust, quantum-safe key distribution, enhancing the security of data center operations. A controlled environment (low quantum channel distance and stable environmental conditions) provides almost ideal conditions for the implementation of QKD connections. However, limitations are visible in the number of users that the entanglement-based approach can support. They are limited by TDM multiplexing due to the possibility that a source sends entangled photons to only one pair in the considered time period. Thus, accurately determining the number of keys and their sizes for establishing secure VPN sessions is crucial, as limited resources (keys) can be utilized most effectively.

The main contribution of this article is an analysis of the feasibility and benefits of implementing an entanglement-based BBM92 protocol to secure intra-connectivity within the data centers.

Acknowledgements This project has received funding from the Research Council of Lithuania (LMTLT), agreement No. P-ITP-24-9. The work was partly supported by the Ministry of Science, Higher Education and Youth of Canton Sarajevo, Bosnia and Herzegovina - project Post-Quantum Crypto Agile Solution for Protection by Encryption Resilience - PQCASPER (27-02-35-55988-3/25). The authors thank Djeylan Aktas and Riccardo Piccoli for their constructive feedback and comments.

Author contributions M.M was contributed writing—review and editing, writing—original draft, visualization, validation, and methodology; P.F, S.R. and S.J. were involved in investigation, formal analysis, data processing, and conceptualization; Miroslav Voznak was performed funding acquisition, formal analysis, and supervision.

Funding Open access publishing supported by the institutions participating in the CzechELib Transformative Agreement.

Data availability No datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Mehic, M., Michalek, L., Dervisevic, E., Burdiak, P., Plakalovic, M., Rozhon, J., Mahovac, N., Richter, F., Kaljic, E., Lauterbach, F., et al.: Quantum cryptography in 5G networks: a comprehensive overview. IEEE Commun. Surv. Tutor. **26**(1), 302–346 (2023)
2. Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., et al.: Quantum key distribution: a networking perspective. ACM Comput. Surv. **53**(5), 1–41 (2020). https://doi.org/10.1145/3402192
3. Dervisevic, E., Mehic, M.: Overview of quantum key distribution technique within IPsec architecture (2021). arXiv preprint arXiv:2112.13105
4. Bennett, C.H., Brassard, G.: An update on quantum cryptography. In: Workshop on the Theory and Application of Cryptographic Techniques, pp. 475–480. Springer (1984)
5. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, p. 8 (1984)
6. Heisenberg, W.: Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. Z. Angew. Phys. **43**(3–4), 172–198 (1927)
7. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature **299**(5886), 802–803 (1982)
8. Bennett, C.H., Brassard, G.: Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. ACM SIGACT News **20**(4), 78–80 (1989)
9. Mehic, M., Rass, S., Fazio, P., Voznak, M.: Fundamentals of quantum key distribution. In: Quantum Key Distribution Networks, pp. 1–28. Springer, Cham (2022)
10. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121 (1992). https://doi.org/10.1103/PhysRevLett.68.3121
11. Tian, Z., Xie, Z., Chen, Y., Fan, X., Huang, J., Mu, T., Guo, J., Wei, K., Sun, S.: Reference-frame-independent quantum key distribution based on machine-learning-enhanced qubit-based synchronization. Sci. China Phys. Mech. Astron. **68**(7), 270312 (2025)
12. Li, H.-W., Hao, C.-P., Chen, Z.-J., Gong, L., Lu, Y.-F., Wang, Y., Li, J.-J., Zhang, C.-M., Wang, R., Yin, Z.-Q., et al.: Security of quantum key distribution with virtual mutually unbiased bases. Sci. China Phys. Mech. Astron. **67**(7), 270313 (2024)
13. Chen, Z.-J., Hao, C.-P., Gong, L., Guo, J.-S., Wang, Y., Zhang, C.-M., Li, H.-W.: Improving the performance of quantum key distribution with weak-randomness basis selection: Z. J. Chen et al. Quantum Inf. Process. **24**(6), 162 (2025)
14. Dervisevic, E., Voznak, M., Mehic, M.: Bases selection with pseudo-random functions in BB84 scheme. Heliyon **10**(1), e23578 (2024). https://doi.org/10.1016/j.heliyon.2023.e23578
15. Lucamarini, M., Yuan, Z.L., Dynes, J.F., Shields, A.J.: Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature **557**(7705), 400–403 (2018)
16. Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**(13), 130503 (2012). https://doi.org/10.1103/PhysRevLett.108.130503
17. Tamaki, K., Lo, H.K., Fung, C.H.F., Qi, B.: Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. Phys. Rev. A At. Mol. Opt. Phys. **85**(4), 1–17 (2012). https://doi.org/10.1103/PhysRevA.85.042307. arXiv:1111.3413
18. Xie, Y.-M., Lu, Y.-S., Weng, C.-X., Cao, X.-Y., Jia, Z.-Y., Bao, Y., Wang, Y., Fu, Y., Yin, H.-L., Chen, Z.-B.: Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. Prx Quantum **3**(2), 020315 (2022)
19. Wang, S., Yin, Z.-Q., He, D.-Y., Wang, R.-Q., Ye, P., Zhou, Y., Fan-Yuan, G.-J., Wang, F.-X., Chen, W., Chen, W., et al.: Twin-field quantum key distribution over 830-km fibre. Nat. Photon. **16**(2), 154–161 (2022)
20. Bose, S., Vedral, V., Knight, P.L.: Multiparticle generalization of entanglement swapping. Phys. Rev. A **57**(2), 822 (1998)
21. Proietti, M., Ho, J., Grasselli, F., Barrow, P., Malik, M., Fedrizzi, A.: Experimental quantum conference key agreement. Sci. Adv. **7**(23), 0395 (2021)
22. Pan, J.-W., Chen, Z.-B., Lu, C.-Y., Weinfurter, H., Zeilinger, A., Żukowski, M.: Multiphoton entanglement and interferometry. Rev. Mod. Phys. **84**(2), 777–838 (2012)
23. Lu, Y.-S., Yin, H.-L., Xie, Y.-M., Fu, Y., Chen, Z.-B.: Repeater-like asynchronous measurement-device-independent quantum conference key agreement. Rep. Prog. Phys. **88**(6), 067901 (2025)

24. Beige, A., Englert, B.-G.G., Kurtsiefer, C., Weinfurter, H.: Secure communication with a publicly known key. Acta Phys. Pol. A 101(3), 357–368 (2002) https://doi.org/10.12693/APhysPolA.101.357. arXiv:0111106 [quant-ph]
25. Zhang, W., Ding, D.-S., Sheng, Y.-B., Zhou, L., Shi, B.-S., Guo, G.-C.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**(22), 220501 (2017)
26. Deng, F.-G., Long, G.L., Liu, X.-S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**(4), 042317 (2003)
27. Long, G.-L., Pan, D., Sheng, Y.-B., Xue, Q., Lu, J., Hanzo, L.: An evolutionary pathway for the quantum internet relying on secure classical repeaters. IEEE Netw. **36**(3), 82–88 (2022)
28. Deng, F.-G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A At. Mol. Opt. Phys. **69**(5), 052319 (2004)
29. Hu, J.-Y., Yu, B., Jing, M.-Y., Xiao, L.-T., Jia, S.-T., Qin, G.-Q., Long, G.-L.: Experimental quantum secure direct communication with single photons. Light Sci. Appl. **5**(9), 16144 (2016)
30. Paparelle, I., Mousavi, F., Scazza, F., Bassi, A., Paris, M., Zavatta, A.: Experimental direct quantum communication with squeezed states. Opt. Express **33**(14), 28917–28934 (2025)
31. Sheng, Y.-B., Zhou, L., Long, G.-L.: One-step quantum secure direct communication. Sci. Bull. **67**(4), 367–374 (2022)
32. Yang, Y., Li, Y., Li, H., Wu, C., Zheng, Y., Chen, X.: A 300-km fully-connected quantum secure direct communication network. Sci. Bull. **70**, 1445–1451 (2025)
33. Mehic, M., Rass, S., Dervisevic, E., Fazio, P., Jakovlev, S., Voznak, M.: Overview of quantum key distribution network key-delivery specifications. In: 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), pp. 83–90. IEEE (2025)
34. Dervisevic, E., Tankovic, A., Kaljic, E., Voznak, M., Mehic, M.: Design of a key management system for efficient key supply in quantum key distribution networks. J. Opt. Commun. Netw. (2025). https://doi.org/10.1364/JOCN.577670
35. Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., Mehic, M.: Quantum key distribution networks-key management: a survey. ACM Comput. Surv. **57**(10), 1–36 (2025). https://doi.org/10.1145/3730575
36. Lo, H.-K.: Classical-communication cost in distributed quantum-information processing: a generalization of quantum-communication complexity. Phys. Rev. A **62**(1), 012313 (2000). https://doi.org/10.1103/PhysRevA.62.012313
37. Scherer, A., Sanders, B.C., Tittel, W.: Long-distance practical quantum key distribution by entanglement swapping. Opt. Express **19**(4), 3004–3018 (2011). https://doi.org/10.1364/OE.19.003004
38. Mehic, M., Rass, S., Fazio, P., Voznak, M.: Quantum Key Distribution Networks: A Quality of Service Perspective. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-06608-5
39. Rass, S., König, S., Schauer, S., Maurhart, O.: Implementation and evaluation of intrinsic authentication in quantum key distribution protocols. Int. J. Adv. Secur. **9**(1 & 2), 2016 (2016)
40. Dervisevic, E., Mehic, M., Voznak, M.: Large-scale quantum key distribution network simulator. J. Opt. Commun. Netw. **16**(4), 449–462 (2024). https://doi.org/10.1364/JOCN.503356
41. Dervisevic, E., Lauterbach, F., Burdiak, P., Rozhon, J., Slívová, M., Plakalovic, M., Hamza, M., Fazio, P., Voznak, M., Mehic, M.: Simulations of denial of service attacks in quantum key distribution networks. In: 2022 XXVIII International Conference on Information, Communication and Automation Technologies (ICAT), pp. 1–5. IEEE (2022)
42. Mehic, M., Dervisevic, E., Burdiak, P., Lipovac, V., Fazio, P., Voznak, M.: Emulation of quantum key distribution networks. IEEE Netw. **39**(1), 116–123 (2025). https://doi.org/10.1109/MNET.2024.3398404
43. Bartlett, B.: A distributed simulation framework for quantum networks and channels (2018). arXiv preprint arXiv:1808.07047
44. Poppe, A., Fedrizzi, A., Ursin, R., Böhm, H., Lorünser, T., Maurhardt, O., Peev, M., Suda, M., Kurtsiefer, C., Weinfurter, H., et al.: Practical quantum key distribution with polarization entangled photons. Opt. Express **12**(16), 3865–3871 (2004). https://doi.org/10.1364/OPEX.12.003865
45. Vitullo, D.L., Cook, T., Jones, D.E., Scott, L.M., Toth, A., Kirby, B.T.: Simulating quantum key distribution in fiber-based quantum networks. J. Defense Model. Simul. (2023). https://doi.org/10.1177/15485129231154929
46. Huang, Y., Qi, Z., Yang, Y., Zhang, Y., Li, Y., Zheng, Y., Chen, X.: A sixteen-user time-bin entangled quantum communication network with fully connected topology. Laser Photon. Rev. **19**(1), 2301026 (2025)

47. Xiao, Y.-R., Yin, H.-L., Hua, W.-J., Cao, X.-Y., Chen, Z.-B.: Experimental efficient source-independent quantum secret sharing against coherent attacks. Phys. Rev. Lett. **135**(15), 150801 (2025)