Demonstration of Quantum-Secure Communications in a Nuclear Reactor

Konstantinos Gkouliaras *[1], Vasileios Theos[1], True Miller[1], Brian Jowers[1], George Kennedy[2], Andy Grant[2], Terry Cronin[3], Philip G. Evans[4], and Stylianos Chatzidakis[1]

[1]School of Nuclear Engineering, Purdue University, USA
[2]Toshiba Europe Ltd, UK
[3]Toshiba International Corporation, USA
[4]Computational Sciences and Engineering Division, Oak Ridge National Laboratory, USA

May 2025

Abstract

Quantum key distribution (QKD), one of the latest cryptographic techniques, founded on the laws of quantum mechanics rather than mathematical complexity, promises for the first time unconditional secure remote communications. Integrating this technology into the next generation nuclear systems - designed for universal data collection and real-time sharing as well as cutting-edge instrumentation and increased dependency on digital technologies - could provide significant benefits enabling secure, unattended, and autonomous operation in remote areas, e.g., microreactors and fission batteries. However, any practical implementation on a critical reactor system must meet strict requirements on latency, control system compatibility, stability, and performance under operational transients. Here, we report the complete end-to-end demonstration of a phase-encoding decoy-state BB84 protocol QKD system under prototypic conditions on Purdue's fully digital nuclear reactor, PUR-1. The system was installed in PUR-1 successfully executing real-time encryption and decryption of 2,000 signals over optic fiber distances up to 82 km using OTP-based encryption and up to 140 km with AES-based encryption. For a core of 68 signals, OTP-secure communication was achieved for up to 135 km. The QKD system maintained a stable secret key rate of 320 kbps and a quantum bit error of 3.8% at 54 km. Our results demonstrate that OTP-based encryption introduces minimal latency while the more key-efficient AES and ASCON encryption schemes can significantly increase the number of signals encrypted without latency penalties. Additionally, implementation of a dynamic key pool ensures several hours of secure key availability during potential system downtimes. This work shows the potential of quantum-based secure remote communications for future digitally driven nuclear reactor technologies.

*kgkoulia@purdue.edu

1 Introduction

Advanced reactor designs (e.g., Microreactors, fission batteries) are proposed with unique new capabilities, such as remote monitoring and semi-autonomous operation. Their development is characterized by the goals of minimizing economic cost, leveraging passive safety systems, and enabling support of different energy outlet types [1]. Notably, advanced reactor designs would allow for a wide range of applications complementary to electricity generation, such as district heating and water desalination, while being compatible with grid-connected and off-grid applications. As of today, seventy Small Modular Reactor (SMR) designs have been reported, while three of them are currently operational. Of those, forty designs are advanced Gen-IV reactors [2].

While this architecture offers numerous advantages, it is nevertheless vulnerable to cyber attacks. The "cyber-attack surface" (i.e., the potentially vulnerable systems and components) is greater compared to conventional reactor designs, as a result of increased automation, I&C complexity, remote operation and operational personnel reduction [1]. The nuclear industry has been a target of such cyber attacks for the past 30 years, with many attacks aimed at gaining intelligence on Supervisory Control And Data Acquisition (SCADA) networks. This was ably demonstrated in attacks launched in 2014 against the Korea Hydro and Nuclear Power Co. that specifically targeted the blueprints and electrical flow charts of nuclear reactors [3]. Independent of the objectives or aims of an attack, attackers almost always first gather information about the target system to identify network topology, software versions, authorization or authentication mechanisms, and critical targets. This highlights that the first critical layer of defense against attacks would be to guarantee the confidentiality and authentication of any communication.

While cryptographic implementation was first proposed by the US NRC in 2010 [4], practical implementation at an actual power plant has not yet taken place [5]. Information-theoretical security (i.e., unconditional) can be achieved when the well-known symmetric encryption One-Time Pad (OTP) algorithm is implemented. To do so, OTP requires that communication parties have access to continuously refreshed and truly random keys, equal in size to the encrypted data [6]. These requirements are not easily implemented, as never-used keys need to be distributed between two parties in real time. Instead, current cryptographic schemes are based on the computational complexity of public key cryptography, i.e., on the difficulty of reversing certain mathematical functions. Unfortunately, public key cryptography has been shown to be vulnerable to the advent of quantum computers and Shor's algorithm [7–9]. For instance, predictions on the evolution and scalability of quantum computers reveal that they could compromise public key encryption (RSA) within hours [10]. Large scale quantum computers in the next decade is a realistic expectation with several initiatives launched, including the National Quantum Initiative Act [11], Google's AI Quantum Laboratory with plans to commercialize quantum computers [12–14], IBM Q [15, 16], etc.

Two main approaches are currently being explored to address this challenge: Post-Quantum Cryptography (PQC) and Quantum Cryptography (QC). PQC, an active area of research led by NIST focusing on quantum-safe algorithms [17], aims to develop classical cryptographic schemes which do not offer quantum computers an advantage over classical ones. QKD relies on the inherent properties of quantum mechanics to deliver unconditional security, without making assumptions on adversarial resources or strategy.

QKD is the most mature quantum cryptography application, enabling secure generation and distribution of a truly random key at two distant locations [18]. Leveraging the laws of quantum physics, specifically the uncertainty principle and the no-cloning theorem, QKD has been extensively studied. Since its first introduction in 1984 with the BB84 protocol [19], there have been multiple protocols [20–22], security proofs [23–30], hardware advancements [31, 32], experimental network demonstrations [33–39], and commercial realizations [40].

This paper presents an experimental demonstration of quantum-secure remote monitoring of a real-world nuclear reactor. Coupling the TOSHIBA Long-Distance QKD system (QKD-LD) with Purdue University's nuclear Reactor number One (PUR-1), we assemble a testbed for real-time exchange of encrypted reactor data. A series of measurements are conducted to evaluate key generation rates and system latency under different transmission distances, operational use cases, and encryption algorithms. Domain knowledge and experimental measurements are used to investigate the configuration-specific conditions for maintaining secure communication, even in the scenario of a QKD failure.

The significance of our implementation stems from two main reasons: firstly, it narrows the gap between theoretical/numerical estimations and real-world applications. The presented setup generates hands-on performance metrics and replicates the full Nuclear Power Plant (NPP) communication cycle (data generation, encryption, transmission, decryption, and storage). Secondly, it permits one to study in detail the nature and requirements of nuclear reactor data generated from an actual power plant. The study does not evaluate system performance generically from a secure network perspective, but incorporates domain knowledge originating from physics constraints, operational constraints, official regulation, and more.

The structure of this paper is as follows. Section 2 features a brief overview of QKD fundamentals, and Section 3 provides a background of nuclear cybersecurity and QKD applications for critical infrastructure. Section 4 introduces a description and mathematical formulation of the secure communication model. In Section 5, the PUR-1 nuclear reactor facility is presented and high-level operational use cases are defined. Section 6 analyzes the experimental setup installed at PUR-1, while Section 7 and Section 8 demonstrate the evaluated use-case configurations and discuss the corresponding results, with respect to key availability and latency, respectively. Finally, Section 9 presents concluding remarks and directions regarding the expansion of the present work.

2 Quantum Key Distribution

QKD was first introduced in 1984 by Bennett and Brassard [19]. A physical-layer security scheme, it leverages the laws of quantum mechanics to deliver information-theoretic security. QKD eventually generates truly random keys and delivers them in real time to the communication parties. A generic QKD system consists of two channels: a quantum channel (optical fiber or free space) and a classical channel (data link). The quantum channel is used to exchange single photons which carry information encoded in one of their degrees of freedom, such as polarization or phase. Once the photon pulses are detected, a series of communication rounds occur via the classical channel to correct errors and remove any knowledge potentially leaked to an adversary. The two parties gain access to quantum-

random bit strings, which can be used with symmetric encryption to provide unconditional security [41, 42].

The security guarantee of QKD lies in the principles of quantum physics. Due to the no-cloning theorem and Heisenberg's uncertainty principle, a potential adversary attempting to intercept the photons would cause the collapse of the quantum state. An adversarial attempt to recreate it would inevitably lead to the introduction of errors, which would be detectable by the legitimate communication parties. As a result, QKD-enhanced encryption does not rely on adversarial computational power or strategy, providing future-proof security even against a quantum-computer-initiated attack. In-depth discussions of QKD security for practical settings can be found in [43] and [24].

The main metric to evaluate QKD performance is the Secret Key Rate (SKR), describing the frequency at which secure bit streams are generated and become available to the parties. Abstractly speaking, SKR can be traced back to the raw key rate R_{raw} and the Quantum Bit Error Rate (QBER). The raw key is equal in size to the number of pulses detected at the receiver, representing the bit streams before any classical processing has taken place (sifting, error correction, privacy amplification). It is primarily affected by channel attenuation, a quantity proportional to the transmission distance, as well as by hardware imperfections (detector efficiency, source repetition rate, etc.). The sifted key is formed by discarding measurements conducted using a different basis than the one used for encoding. The key reduction in this stage is based on the selected protocol and is modeled with η_{sift}.

$$\eta_{\text{sift}} \triangleq \frac{\text{size of sifted key}}{\text{size of raw key}} \tag{1}$$

While for the original QKD protocol the sifting ratio was 50%, asymmetric implementations allow to improve efficiency through biased basis selection. On the other hand, QBER describes the inconsistencies between the sifted bit streams held by the two parties, i.e.,

$$E = \text{QBER} \triangleq \frac{\text{number of errors}}{\text{size of sifted key}} \tag{2}$$

After mismatches in measurement bases are discarded during sifting, errors in the two bitstreams are attributed to noise introduced due to channel imperfections (e.g., depolarization) or eavesdropping. QBER determines the fraction of the raw/sifted key that can be distilled to form the secret key by estimating i) the number of bits which need to be discarded during error correction, and ii) the amount of information which has potentially leaked to an adversary. Evidently, SKR is dependent on both raw key rate and QBER, as

$$\text{SKR} = R_{\text{raw}} \cdot \eta_{\text{sift}} \cdot g(E) \tag{3}$$

The analytical forms of R_{raw} and g depend on the specific QKD protocol and post-processing algorithms implemented. In a qubit-based system, the two terms are theoretically given as [44]:

$$R_{\text{raw}} = f_{\text{source}} \cdot \eta_d \cdot t_{\text{chan}} \tag{4}$$

$$g(E, \bar{e_1}, \underline{p_1}) = \underline{p_1} \left[1 - h\left(\overline{e_1}\right)\right] - f_{\text{ec}} h(E) \tag{5}$$

Where f_{ec} is the error correction efficiency, $\underline{p_1}$ is the lower bound for the probability that a sifted bit was registered from the detection of a single photon state, $\bar{e_1}$ is the upper bound for error rate in single photon states, and E is the QBER from Equation 1. The detection efficiency is represented as η_d and the channel transmissivity is given as:

$$t_{\text{chan}} = 10^{-al/10} \tag{6}$$

Here, l is the transmission distance and a is the channel attenuation coefficient in dB per unit length. A milestone in practical QKD realization was the development of the decoy state technique [45–47]. In decoy state protocols, signal photon states are randomly blended with the so-called decoy states to achieve higher key rates and security against advanced eavesdropping strategies, such as the Photon-Number Splitting (PNS) attack [43]. Therefore, an important contribution of the decoy state technique is the ability to approach the security of ideal QKD protocols while using practical, imperfect hardware. A schematic of the QKD key distillation procedure is shown in Figure 1.

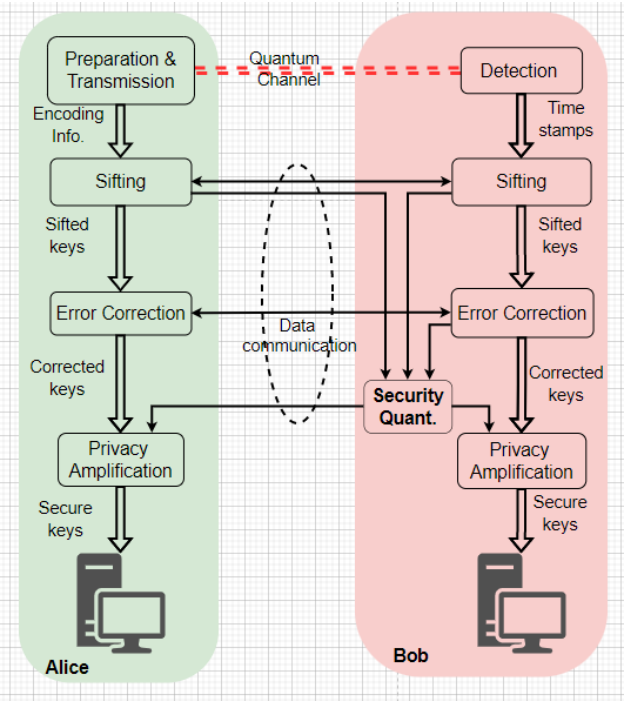


Figure 1: QKD key distillation procedure as presented in [44].

3 Related work

Cybersecurity for the nuclear power sector is a field gaining interest, especially since the release of U.S. Nuclear Regulatory Commission (U.S. NRC) Regulatory Guide 5.71 in 2010 [4]. The guidance introduced a compliance-based security approach, defining critical systems and corresponding Critical Digital Assets (CDAs). The systems are classified in security

levels, with restrictions applied to inter-level communication. A similar level-based security approach is proposed by the International Atomic Energy Agency (IAEA) [48].

Research has been conducted for vulnerability assessment [49,50] while intrusion detection systems have been proposed for software [51,52] as well as hardware implementations [53–55]. Several research works have explored classical encryption capabilities for nuclear power reactors. Emphasis has been given on hardware implementations, as with Field Programmable Gate Arrays (FPGAs) [56, 57] and Programmable Logic Controllers (PLCs) [5].

QKD has received significant attention for critical infrastructure and energy sector [58]. Proposed application areas include the smart grid [59–61], electrical utilities [62], and hydropower plants [63]. A detailed review of QKD energy applications is found in [58]. However, examining QKD potential for the nuclear power sector is a particularly underexplored topic, with related works limited in a preliminary concept study [64] and an investigation of wireless QKD application [65]. Our previous work included the development of a QKD simulator [66], leveraged to evaluate QKD performance for different nuclear environment use cases [67].

As of yet, there has been no experimental demonstration of quantum nuclear reactor communications, to the best of our knowledge. While the nuclear industry shares characteristics with other energy sectors, it also exhibits certain distinguishing differences. Such traits justify the need to specifically evaluate QKD system in nuclear settings. Firstly, nuclear operation prioritizes plant availability, a principle that any non-safety systems (e.g., communication modules) need to comply with. In addition, nuclear systems have zero tolerance for data discontinuities, thus emphasizing the importance of timely, real-time operation. Finally, it remains to be shown whether radiation environments would affect QKD performance and whether such interference would be depicted in system metrics. The above arguments further highlight the potential impact of the present experiment.

4 Secure communication model

The goal of this work is to investigate the compatibility of QKD with nuclear reactor control systems, for realizing secure data exchange. The distinctiveness of such systems lies in two main characteristics, potentially differentiating them from other sector counterparts. Firstly, there is a requirement for 100% system availability. Therefore, disrupting system operation is not a viable option except for scheduled and absolutely necessary tasks (e.g., refueling). Secondly, no data inconsistencies can be allowed, as the data historian needs to precisely archive past reactor states and be easily accessible for future reference.

To evaluate system performance under different use cases, we formulate a communication model tailored to nuclear reactor operations. The model defines a set of eight parameters with respect to data generation, encryption, and transmission. In addition, it describes the different stages of the data exchange loop, and mathematically derives the constraints for sustaining uninterrupted secure communication. As a result, it provides the tools to investigate the compatibility of a reactor-agnostic remote operation use case with an arbitrary QKD system.

Table 1: Summary of secure communication use-case parameters.

Symbol	Name	Units	Description
Data parameters			
N	Number of signals	Unitless	Number of signals to be transmitted
f_s	Sampling rate	Cycles/s	Rate of controller signal update
f_{rep}	Reporting rate	Cycles/s	Rate at which signals are sent to remote location
p	Precision	Bits/value	Number of bits allocated to each value
Security parameters			
f_{enc}	Key reusability factor	Unitless	Disposable key bits required per bit of encrypted data
t_{auto}	Communication autonomy	Minutes	Minimum secure operation time after key generation failure
Channel parameters			
l	Channel length	Kilometers	Distance between two secure locations
E	Quantum Bit Error Rate	%	Noise level in the quantum channel

4.1 Communication parameters

Model parameters are classified into three groups: data, security and channel. Data parameters are associated with the signal resolution and quantity, and they are determined based on domain knowledge and use case analysis. Security parameters are determined based on the use-case confidentiality and availability requirements. Finally, channel parameters are related to the properties of the QKD transmission link. The parameters are summarized in Table 1.

The *number of signals* (N) is determined by the amount of information a particular use case requires. While data historian requires the entirety of generated signals to be transmitted, a remote monitoring application might limit such number to include only a subset of signals necessary to verify normal operation.

The *data sampling rate* (f_s) describes the frequency with which the reactor controller records field sensor data. Meanwhile, *data reporting rate* (f_{rep}) is a quantity referring to the rate at which data are reported to the remote terminal unit. The two parameters do not need to be identical by default. For example, data could be sampled every 1 millisecond but reported once every 100 milliseconds. In this scenario, the remaining values are discarded. However, this might not always be the case; for instance, it could be possible that even though data are updated 10 times per second ($f_s = 10$ Hz), they are reported once every second as a batch.

The *precision* is the number of bits required to encode each data point in digital format. Precision is dependent on the data representation scheme, making assumptions on the float-

ing point accuracy. Using the IEEE-754 standard for floating point arithmetic [68], the main options are either single precision (32 bits per value) or double precision (64 bits per value).

Finally, *key reusability factor* f_{enc} describes the number of disposable key bits required to encrypt one bit of data, that is,

$$f_{\text{enc}} = \frac{\text{key size}}{\text{encrypted data size}} \in (0, 1]. \tag{7}$$

The reusability factor depends on the cryptographic algorithm implemented. Lower values of the ratio represent higher key economy, potentially at the cost of theoretic security. Information-theoretic security requires one disposable key bit per encrypted data bit, thus $f_{\text{enc}} = 1$. This is the case with OTP. All remaining symmetric cryptographic algorithms practically exhibit $f_{\text{enc}} < 1$, as key material is somehow reused. In those cases, coupling with QKD offers only computational security. However, security bounds can be improved by increasing the key refresh rate, a task which is challenging when using conventional key distribution methods (e.g., public cryptography) [8]. Therefore, a QKD implementation has the potential to actually upgrade communication confidentiality, not only in the ideal scenario of coupling with OTP, but even when combined with applied encryption algorithms.

The *channel length* l describes the distance between the reactor site and the remote location. Along with the *error rate* (channel noise), it determines the secret key generation rate, as larger distances introduce increased photon attenuation in the optical fiber. Finally, *communication autonomy* t_{auto} describes the target system uptime following a potential failure of the key generation system (e.g., channel interception). During this interval, the system is expected to maintain secure communication using a reserve of secret keys.

Based on the above parameters, a use case can be evaluated to determine the key consumption rate, the secret key generation rate, and the latency per operation. The model input and output parameters are shown in Figure 2. As explained in the following sections, the outputs are evaluated based on several constraint conditions, to determine the feasibility of the use case.

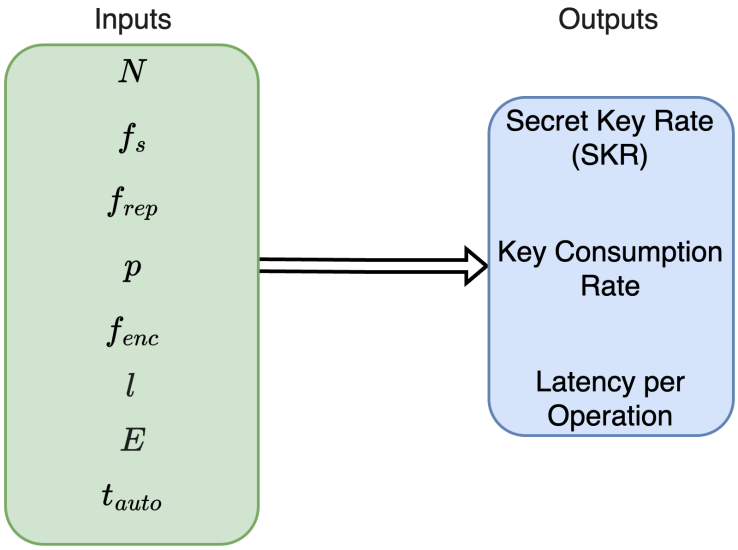


Figure 2: Communication model input and output parameters.

4.2 Procedure

The communication procedure stages are demonstrated in Figure 3. Terminal A fetches data from the reactor digital controller and encodes them in a digital representation scheme (e.g., IEEE-754). Following, it communicates with Key Server Alice requesting an encryption key, the size of which is dictated by the encryption algorithm and/or data size. Key Server Alice replies by sending the key and the associated key ID. The data are encrypted, and the ciphertext is transmitted to Terminal B over the authenticated channel along with the key ID. Upon receipt, Terminal B requests the decryption key from Key Server Bob, providing the ID. The ciphertext is decrypted and reactor data are extracted. Finally, an automated model (ML/AI, rule-based) analyzes the received data and provides some form of feedback to the operator regarding action to be taken. For example, the model might provide guidance for rod movement to match the target reactor power or neutron flux.

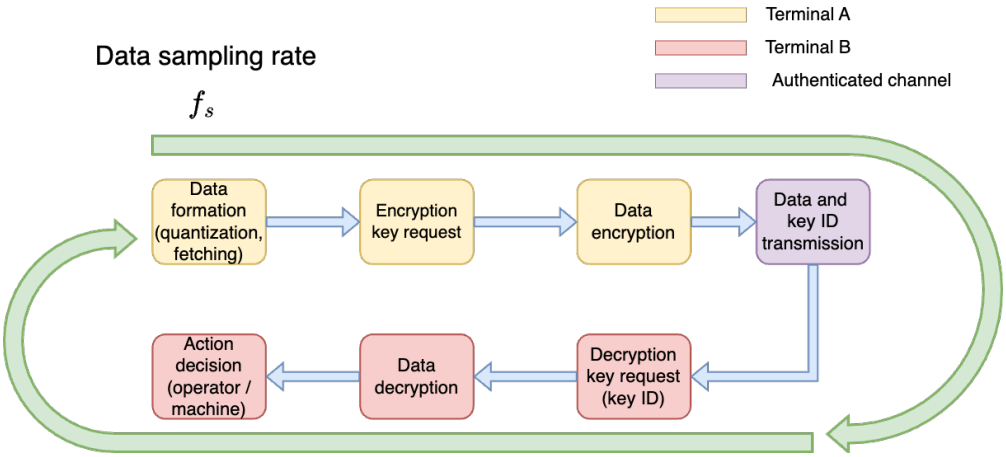


Figure 3: Data communication loop schematic. Terminal A is connected to the reactor PLC while Terminal B is the remote station. Total latency is the sum of latencies from each individual data processing stage. The target latency is determined by the data sampling rate f_s.

Two main metrics are used to evaluate system performance, latency and key availability. The parameters associated with each use case determine the target latency and target key availability. For a particular configuration to be realizable, *both* latency and key availability conditions need to be satisfied. A third condition is related to meeting the target communication autonomy, in case of key distribution failure. Such conditions are mathematically derived in the following sections.

4.3 Latency condition

Latency is the first performance metric for evaluating the feasibility of a use case. The data sampling period ($\Delta t = 1/f_s$) determines the time limit during which all stages need to have been completed, as reactor data are updated. In the scenario where data are transmitted to the remote terminal in fixed time intervals as batches, the threshold value is defined by the

reporting period $1/f_{\text{rep}} = \kappa \cdot \Delta t$, where $\kappa \in \mathbb{N}^*$. Any excess time contributes to latency. As a result, the target latency condition can be expressed as:

$$t_{\text{fetch, A}} + t_{\text{key, A}} + t_{\text{enc, A}} + t_{\text{transm}} + t_{\text{key, B}} + t_{\text{dec, B}} + t_{\text{action, B}} \leq \max(\frac{1}{f_s}, \frac{1}{f_{\text{rep}}}) \tag{8}$$

Where each variable represents the elapsed time associated with each communication stage. Indexes A, B represent the terminal where the particular process occurs. Neglecting the time required for data analysis, Equation 8 can be written as:

$$t_{\text{total}} = t_{\text{qkd}} + t_{\text{crypto}} + t_{\text{com}} \leq \Delta\tau_{\text{ef}} \tag{9}$$

Where $t_{\text{qkd}} = t_{\text{key, A}} + t_{\text{key, B}}$ is the total time involving key request and delivery via QKD server communication, $t_{\text{crypto}} = t_{\text{enc}} + t_{\text{dec}}$ is the encryption/decryption interval, and $t_{\text{com}} = t_{\text{fetch,A}} + t_{\text{transm}}$ is the overall time required for data exchange (fetching from PLC and transmitting between Terminals A and B). The effective period $\Delta\tau_{\text{ef}}$ is defined as:

$$\Delta\tau_{\text{ef}} = \max\left(\frac{1}{f_s}, \frac{1}{f_{\text{rep}}}\right) \tag{10}$$

The overall latency is dependent on the communication parameters (Table 1).

4.4 Key availability condition

The target key availability condition dictates that the secret key formed during the data generation interval should be at least equal in size to the key n required to encrypt the data. Therefore, we can write:

$$n(N, p, f_{\text{enc}}) \leq \text{SKR}(l, E, t) \cdot \Delta\tau_{\text{ef}} \tag{11}$$

Where l and E are the distance and error rate of the quantum channel, respectively. SKR is the corresponding secret key rate reported in the effective period $\Delta\tau_{\text{ef}}$, and is dependent on the channel parameters (length, error rate). The required key size n is a function of the data and security parameters. For each reporting period, the amount of generated data in bits is:

$$n_{\Delta\tau_{\text{ef}}} = N \cdot p \cdot \frac{f_s}{f_{\text{rep}}} = N \cdot p \cdot f_s \cdot \Delta\tau_{\text{ef}} = N_{\text{ef}} \cdot p \tag{12}$$

Where the effective number of signals is defined as:

$$N_{\text{ef}} = \kappa \cdot N \tag{13}$$

The number of key bits needed per effective period is therefore:

$$n = n_{\Delta\tau_{ef}} \cdot f_{\text{enc}} \tag{14}$$

Where the key reusability factor f_{enc} was given in Equation 7. The condition of Equation 11 constitutes the tightest bound, assuming that any part of the key not consumed

during the data reporting period is discarded. In practice, excess keys will be stored in the key management system contributing to a key reserve pool. Therefore, a more realistic condition is to ensure that the dynamic key pool size remains positive during all times.

The size of the dynamic key pool d can be thought of as the difference between key material contributed (from QKD) and key material consumed (from the secure application). Generated keys are added to the key pool in irregular times t_g (once the key distillation iteration is completed and the secret key is formed), where $g \in \{0, 1, 2, ...\}$ is the QKD cycle index. The key generation intervals are thus defined as:

$$\Delta t_g = t_{g+1} - t_g \tag{15}$$

Furthermore, key requests also occur periodically according to the data sampling/reporting rate. The duration of key generation intervals typically exceeds the nuclear data reporting period ($\Delta t_g >> \Delta \tau_{\text{ef}}$). As a result, the dynamic key pool size is given as:

$$d[k] = d[0] + \sum_{g \in G(k)} (\Delta t_g \cdot \text{SKR}_g) - \sum_{i=0}^{k} n[i], \quad \forall k \in \{0, 1, 2, ...\} \tag{16}$$

Where $k = t/\Delta \tau_{\text{ef}}$ is the communication loop index with respect to Figure 3 and:

$$G(k) = \{g : t_{g+1} \leq k \cdot \Delta \tau_{\text{ef}}\} \tag{17}$$

Equation 16 assumes that key consumption n could vary over time, due to a potential change in communication parameters. Here, the time step $k = 0$ marks the initiation of reactor operation and data exchange. The initial pool size $d[0]$ is related to the QKD operational time before the beginning of data encryption (lead time) or the size of pre-shared symmetric keys. Therefore, the updated target key availability condition is written as:

$$d[k] > 0, \quad \forall k \in \{0, 1, 2, ...\} \tag{18}$$

The dependence of the key availability condition on previous time terms guarantees that the encryption module treats newly generated data in chronological order. Thus, evaluating Equation 18 for a given time step k satisfies that all data generated since the beginning of operations have been successfully processed.

4.5 Lead time and post-failure uptime

As availability remains one of the main priorities in critical infrastructure, particularly in the nuclear power sector, any remote operation needs to be designed in a manner minimizing the probability of reactor shut down. Due to the fact that fission products are strong neutron absorbers (e.g., Xenon-135), the reactor cannot be instantly restarted (reactor poisoning). Therefore, an emergency shutdown could potentially have broad implications by failing to meet the energy demand for a prolonged time period. From a cybersecurity perspective, it becomes clear that shutting the plant is not an acceptable cyber event response strategy, and

should only take place if absolutely necessary. To maintain uninterrupted secure communication, two related parameters are defined, the QKD lead time and post-failure operational time.

Lead time describes the interval before the initiation of secure communication, during which key distribution is operating. During the lead time interval, QKD contributes secret keys to form the reserve key pool, i.e.,:

$$d_0 = d[k_{\text{lead}}] = \sum_{g \in G(k_{lead})} (\Delta t_g \cdot \text{SKR}_g) \tag{19}$$

Where $k_{\text{lead}} = t_{\text{lead}}/\Delta\tau_{\text{ef}}$. To explicitly account for the QKD lead time, the dynamic pool size of Equation 16 can be expressed as:

$$d[k] = \sum_{g \in G(k)} (\Delta t_g \cdot \text{SKR}_g) - \sum_{i=k_{\text{lead}}+1}^{k} n[i], \quad \forall i \in \{0, 1, ..., k\} \tag{20}$$

The initial key reserve can be approximated based on the time-averaged SKR and lead time as:

$$d_0 \approx \overline{\text{SKR}}(l, E) \cdot t_{\text{lead}} \tag{21}$$

The goal of the initial reserve is to provide a safety margin for balancing key consumption requirements, during the initial stages of secure communication. As contributions to the key pool take place at discrete times, meeting the key availability condition might be challenging even if the average SKR is higher than the key consumption rate. The assignment of a QKD lead time helps maintain the positive size of the key pool throughout the reactor operation. Based on this criterion, subsection 7.3 determines the minimum lead time for a variety of parameter combinations.

A second benefit of the initial reserve is prolonging secure communication in case of an emergency failure of the key distribution system. We refer to the elapsed time between QKD failure and the exhaustion of key material as post-failure uptime, defined as:

$$\Delta t_{\text{up}} = t_{\text{d=0}} - t_{\text{fail}} \tag{22}$$

Here, $t_{\text{d=0}}$ is the time when the key reserve reaches zero and t_{fail} is the QKD failure instance. Δt_{up} is a function of the secure communication parameters, including the lead time. In subsection 7.4, post-failure uptimes are evaluated for various parameter configurations.

A third condition can be formulated by defining a minimum acceptable communication autonomy (threshold uptime) t_{auto}, such that:

$$\Delta t_{\text{up}} \geq t_{\text{auto}} \tag{23}$$

Equation 23 constitutes the secure uptime condition. With respect to the key pool size at failure, it can be equivalently written as:

$$d[k_{\text{fail}}] \geq \frac{n_{\text{pf}} \cdot t_{\text{auto}}}{\Delta\tau_{\text{ef}}} \tag{24}$$

Where $k_{\text{fail}} = t_{\text{fail}}/\Delta\tau_{\text{ef}}$ is the discrete time index of the key distribution failure instance. n_{pf} is the post-failure key consumption rate per effective period. Although n_{pf} could be equal to the pre-failure key consumption rate, this might not always be the case; to maximize the uptime, it is possible that during the outage only a subset of critical signals are transmitted. Similarly, the encryption algorithm could be switched to a practical cipher to achieve higher key economy. For convenience, we define the generalized key consumption rate as:

$$\tilde{n}[k] \begin{cases} 0, & \text{for } 0 < k < k_{\text{lead}} \\ n, & \text{for } k_{\text{lead}} \leq k \leq k_{\text{fail}} \\ n_{\text{pf}}, & \text{for } k > k_{\text{fail}} \end{cases} \tag{25}$$

Substituting Equation 20 and Equation 25 into Equation 24, the final inequality becomes:

$$\sum_{g \in G(k_{\text{fail}})} (\Delta t_g \cdot \text{SKR}_g) - \sum_{i=0}^{k_{\text{fail}}} \tilde{n}[i] \geq \sum_{i=k_{\text{fail}}+1}^{k_{\text{auto}}} \tilde{n}[i] \tag{26}$$

Where $k_{\text{auto}} = t_{\text{auto}}/\Delta\tau_{\text{ef}}$. The above inequality thus evaluates both the key availability and secure uptime conditions. Grouping the $\tilde{n}$ terms, we obtain:

$$\sum_{g \in G(k_{\text{fail}})} (\Delta t_g \cdot \text{SKR}_g) - \sum_{i=0}^{k_{\text{auto}}} \tilde{n}[i] \geq 0 \tag{27}$$

To obtain a practical estimate when a time-dependent dataset is not available, the sum terms can be replaced by the average values to obtain the simplified expression of Equation 28:

$$t_{\text{fail}} \left[\overline{\text{SKR}}(l, E) - \frac{\bar{n}}{\Delta\tau_{\text{ef}}} \left(1 - \frac{t_{\text{lead}}}{t_{\text{fail}}} \right) \right] \geq \frac{\bar{n}_{\text{pf}} \cdot t_{\text{auto}}}{\Delta\tau_{\text{ef}}} \tag{28}$$

Equations 26- 28 can be handful to determine the minimum QKD lead time required to achieve a specific post-failure uptime, and vice versa.

In summary, for a use case to be feasible, the model outputs need to satisfy the latency condition (Equation 9) and the key availability condition (Equation 11 or Equation 18). Given the fulfillment of the two constraints, a minimum operational lead time can be determined from Equation 28 to satisfy the specified communication autonomy requirement and prolong system operation following a potential key distribution failure.

5 Use cases

PUR-1 is a pool-type research reactor located at Purdue University. To date, it is the only fully digital reactor licensed by the US NRC. As the future of the nuclear power sector is associated with digitalization, PUR-1 acts as a prototype of I&C architectures to be incorporated in anticipated realizations of advanced reactor designs (microreactors, SMRs). Consequently, an implementation based on PUR-1 is ideal to gain maximum insight on future reactor challenges, from a control and monitoring perspective. The PUR-1 reactor room is shown in Figure 4.

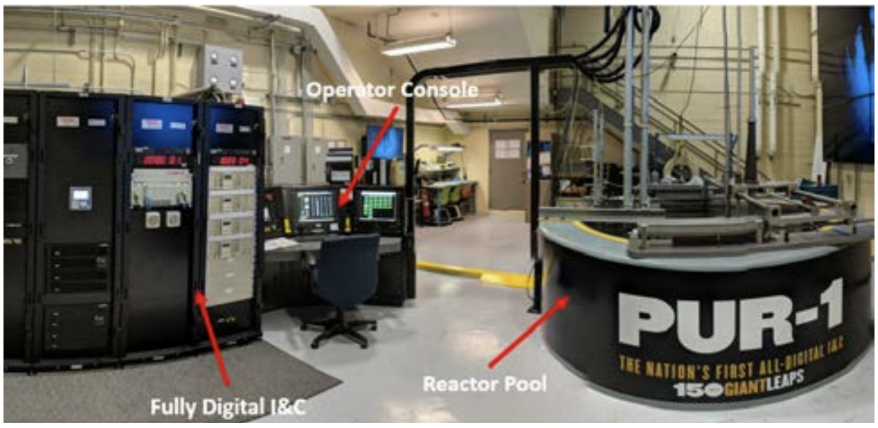


Figure 4: PUR-1 reactor room.

The Programmable Logic Controller (PLC) allows remote monitoring and collection of more than 2,000 parameters, including digital values (e.g., manual SCRAM control) and digitized analog quantities (e.g., neutron flux). Of these, 67 signals have been found to be most relevant for representing important system behavior. This selection has been conducted based on domain knowledge, excluding parameters not directly related to the power generation process (e.g., room temperature) [69]. A timestamp is also included to form a set of 68 signals in total.

Based on this classification, two general categories of communication use cases can be defined, remote monitoring and data historian. In the first category, a remote operator needs to obtain real-time information on the reactor state to allow potential action to be taken. The main priority is to have minimum latency and zero delay, while only relevant signals are required. As a general approach, this use case benefits from a higher sampling rate to obtain adequate resolution in the time domain. In the second category, the complete set of signals needs to be transmitted to the remote server. On top of documentation purposes, the entirety of data would be used for providing long-term analytics (e.g., for load following) and for training Digital Twin models. Therefore, all signals generated per time step need to be remotely transmitted. Based on the specifics of the system, the sampling rate can be selected optimally to satisfy time resolution requirements, without consuming excess storage space in the long term. The two use cases are summarized in Table 2.

Table 2: PUR-1 remote operation use cases.

Use case	Name	Number of signals	Latency priority	Sampling rate	Description
#1	Remote monitoring	68	High	High	Core signals transmitted to remote operator.
#2	Data historian	2,000	Medium	Medium	All signals transmitted for remote storage.

The control system supports arbitrary sampling frequencies, limited by the sensor capa-

bilities. Typical sampling frequencies are found in the range of less than ten samples per second. Regarding data resolution, it has been shown in [67] that single precision (32 bits) is sufficient to quantize and digitally encode reactor-generated data.

6 Experimental setup

The experimental setup leverages PUR-1 and the commercial Toshiba Long Distance QKD system (QKD-LD). QKD-LD consists of four devices in total: QKD-Alice, QKD-Bob, Key Server Alice and Key Server Bob. QKD-Alice and QKD-Bob connect using a quantum and a classical channel, both of which are single-mode optical fibers. For the quantum communication stage, QKD-LD implements the T12 QKD protocol [44,70]. T12 is a modified version of phase-encoding decoy state BB84, using asymmetric basis selection. One decoy and a vacuum state are blended with signal states with probabilities of 1.661% and 1.466%.

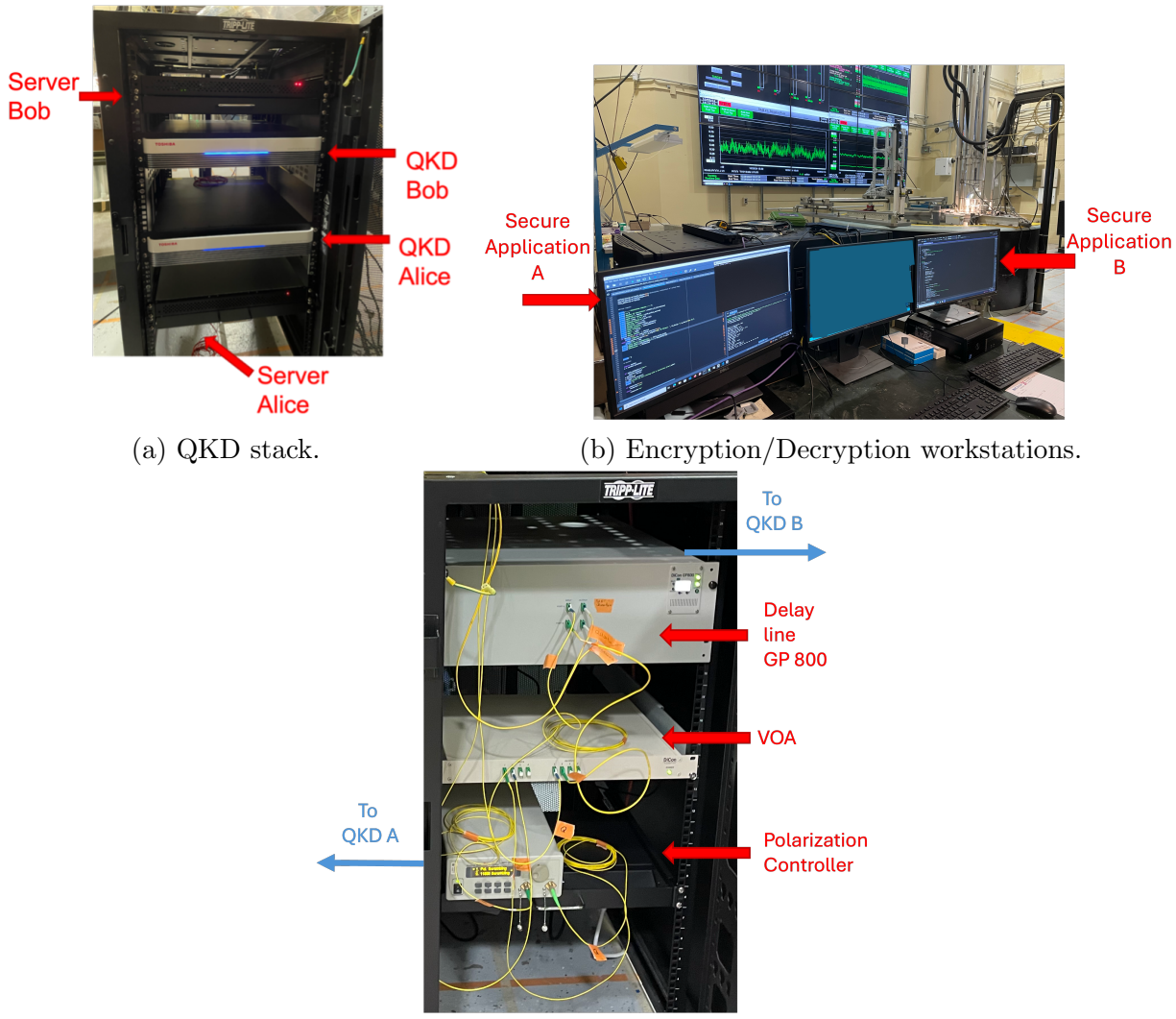
Figure 5 displays the prototypic QKD setup installed in PUR-1 reactor, while Figure 6 provides a schematic of the system. The system is structured around two workstations for the sender (Alice) and receiver (Bob), referred to as WA and WB. WA and WB represent the two remote locations, with WA physically connected to PUR-1, thus having access to reactor data. The two workstations run Windows 11 OS and communicate over a regular TCP/IP, non-dedicated LAN connection, shared with other network devices. Their purpose is to perform encryption and decryption operations, respectively, on real-time reactor data.

WA and WB are connected to the QKD servers of Alice and Bob, respectively, over dedicated Ethernet CAT-5e data links. The servers, running Linux OS, are responsible for implementing the Key Management System (KMS) by storing the QKD-generated keys and providing them upon request to the workstations, according to the ETSI GS QKD 014 standard [71]. Whenever one of the two workstations requests a key, the corresponding KMS server replies with a unique key ID associated with the key. The key ID, a 128-bit Universally Unique Identifier (UUID), is simultaneously forwarded to the second server. The remote workstation receives the key ID over the authenticated channel, and uses it to request the corresponding key from the KMS server. Through this process, the two communicating parties gain access to an identical key to subsequently use with a symmetric encryption scheme. Since a single key cannot be requested twice and the communication between workstation and server is authenticated, the keyID does not need to be encrypted.

The two QKD devices (QKD-Alice, QKD-Bob) are connected to Key Server Alice and Key Server Bob, respectively, through duplex multi-mode fiber. Following the QKD protocol specification, they are connected to each other through a quantum and a classical channel. Both channels are single mode fibers (Corning SMF-28) terminated with LC/UPC connectors. The two channels should be identical in terms of length.

To experimentally replicate different transmission distances and environmental conditions, additional equipment intercepts both SMF channels. Three devices are connected sequentially, a General Photonics Polarization Controller, a DiCon Variable Optical Attenuator (VOA), and a DiCon GP800 delay line. Figure 5c shows the stack of equipment intercepting the QKD channels.

The polarization controller enables manually controlling photon polarization by defining a voltage applied to a series of fiber squeezers. The VOA introduces channel attenuation



(a) QKD stack.

(b) Encryption/Decryption workstations.

(c) Equipment intercepting quantum and classical channel. Red arrows identify the devices, while blue arrows indicate integration with the QKD system.

Figure 5: QKD installation in PUR-1 control room.

up to 30 dB per channel, in order to replicate the effect of longer transmission distances. Additionally, two fixed 10 dB attenuators are introduced for the classical and quantum channel. Finally, the delay line uses MicroElectroMechanical (MEMS) optical switches to actually vary the fiber length connected, ranging from 0 to 32 km. The significance of the delay line stems from the fact that its effect is identical to adding different fiber segments, introducing not only photon attenuation but potential time/frequency dispersion effects.

The interfering modules are operated under different parameter combinations to generate several channel use cases. Given that typical loss in SMF operating at a wavelength of 1550 nm is approximately 0.2 dB/km [72], photon attenuation of a channel up to 200 km can be replicated. Combining the VOA and delay line allows for a more realistic fiber

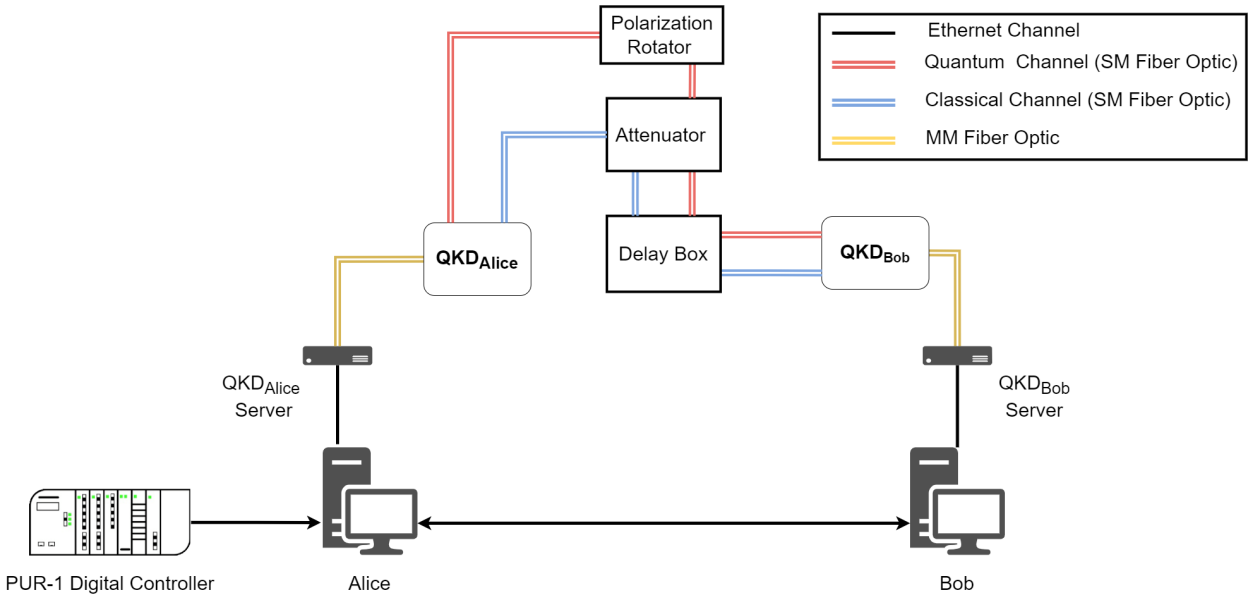


Figure 6: Schematic of PUR-1 QKD experiment setup. PUR-1 data are provided to sender (Alice) workstation (WA). WA requests keys from QKD server A to encrypt data. Encrypted data and key ID are transmitted over an authenticated channel. Receiver workstation (WB) requests the key from QKD server B by providing the key ID. The key is applied to received data for decryption according to the applied cryptographic scheme.

implementation while also further increasing the channel length capability.

The TOSHIBA system reports the Secret Key Rate (SKR) and Quantum Bit Error Rate (QBER), along with the corresponding timestamp. QKD data are reported after each key distillation cycle is completed. Processing the data, it is possible to identify the random key material contributed to the pool as a function of time.

7 Secret key generation

For the first stage of the experiment, QKD is operated at various channel lengths for prolonged periods of time. The distance was varied by modifying the VOA and delay line parameters. For each replicated fiber length, measurements were taken for a period of at least 10 hours of uninterrupted operation.

7.1 QKD performance evaluation

SKR and QBER values are averaged over time and are displayed in Figure 7. An average rate of approximately 315 kbps is obtained at 50 km, declining exponentially as the channel length increases. At 145 km, no secret key can be distilled, leading to zero secret key rate. Performance aligns with the 30 dB loss design of the Toshiba QKD LD system. QBER ranges from approximately 4% at 50 km to 7.5% at 145 km. The curve demonstrates that, despite channel length and QBER not being directly related, increasing the distance contributes to higher error rate in practice. The total absence of key generation at 145 km is thus attributed

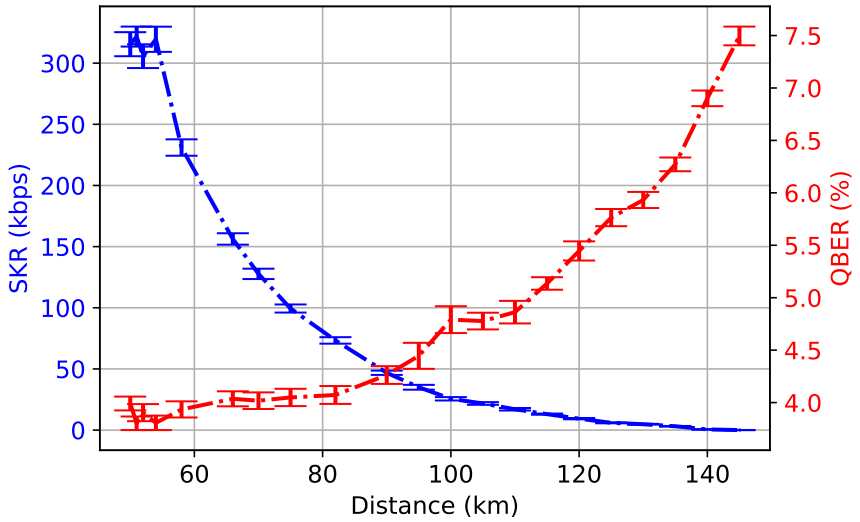


Figure 7: Average SKR and QBER as a function of distance. QKD data collected over 10 hours of operation at each length. Distances replicated using combinations of delay line and attenuators. Rate exceeds 315 kbps at 50 km (10 dB loss). System does not generate secure keys at a distance of 145 km, which aligns with the 30 dB loss design of the Toshiba QKD LD system. We observe that the error rate mostly increases with distance, reaching approximately 7.5% at 145 km.

not only to increased photon attenuation, but also to high error rate on the pulses actually detected, which prevents secure key distillation. Both SKR and QBER exhibit statistical fluctuations over time, as shown by the uncertainties in the plot. Indicatively, the two metrics at $l = 54$ km are plotted versus time for the 10-hour interval, and shown in Figure 8. The variance is approximately 10.3 kbps for SKR and only 0.07% for the error rate.

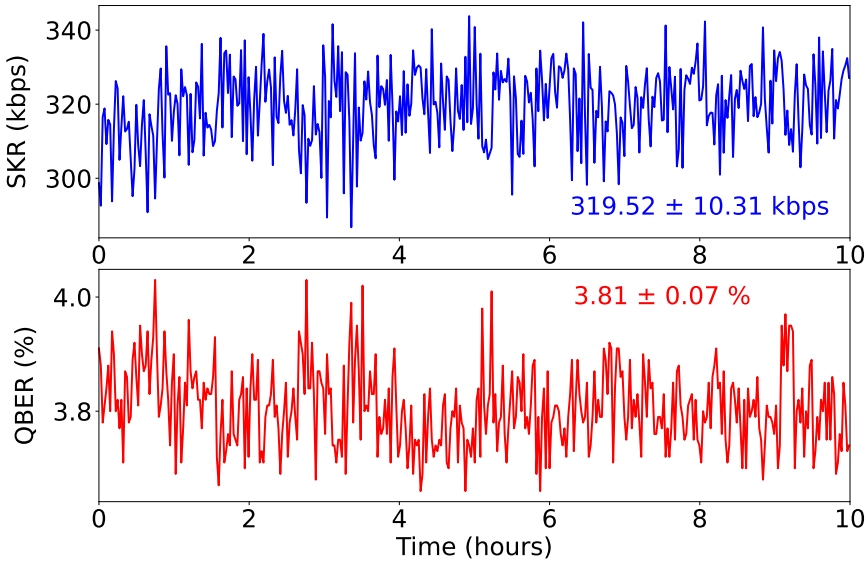


Figure 8: SKR and QBER versus time for 10 hours of operation ($l = 54$ km).

The goal is to determine the maximum distance satisfying the target key availability condition for different use cases. The tight bound of Equation 11 is used for a first estimate, assuming zero initial key reserves and that excess keys are discarded. Figure 9 demonstrates how the recorded average SKRs compare to representative key consumption rates. Rates are calculated through Equation 12, assuming OTP encryption ($f_{\text{enc}} = 1$) with equal reporting and sampling frequencies ($f_s = f_{\text{rep}}$). Following this conservative approach, it is shown that the target key availability can be achieved for up to approximately 85 km and 2000 signals. If only the 68 core signals are transmitted, the maximum achievable distance is approximately 135 km and 105 km, for $f_s = 1$ Hz and $f_s = 10$ Hz, respectively.

The plot also features two AES-256 configurations, at $f_s = 1$ Hz and $f_s = 10$ Hz. The key (256 bits) and the initialization vector (IV, 128 bits) are constantly updated, at the same rate as data sampling. Since the key/IV size is fixed per encrypted block, the target bandwidth remains constant for any number of signals, and is only dependent on the sampling/reporting rate. Even though AES is not information-theoretically secure, it is considered a -computationally speaking- robust encryption standard, officially adopted by NIST [73]. As demonstrated in the plot, the application of AES-256 allows to extend the distance up to 140 km for an arbitrary number of signals, without lowering the sampling frequency.

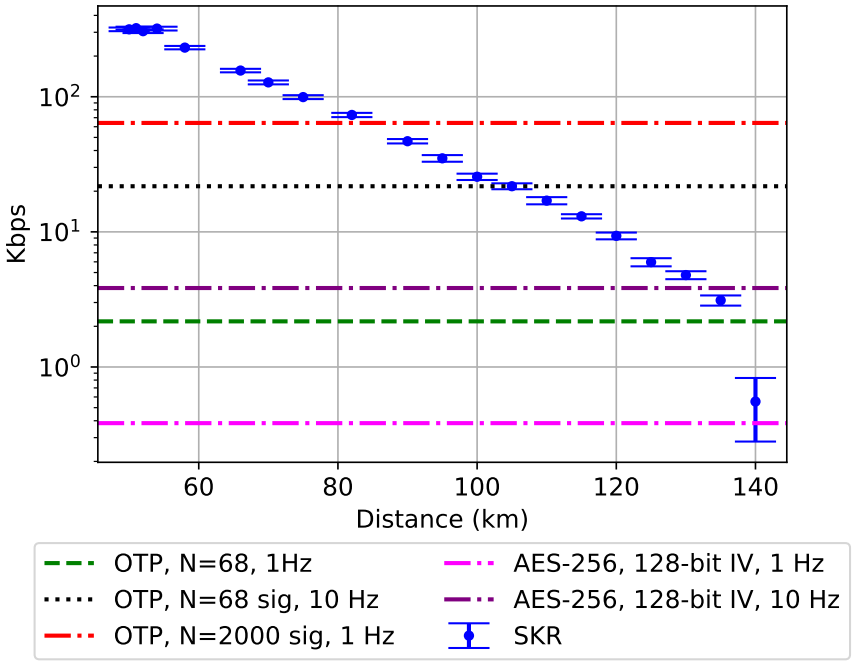


Figure 9: Maximum distance satisfying target key availability condition for indicative communication use cases. For $N = 2,000$ signals and $f_s = f_{\text{rep}} = 1$ Hz, the tight bandwidth condition of Equation 11 is fulfilled at up to 82 km. Excess keys and initial key pool size are ignored. Distances up to 140 km can be achieved either by selecting a lower sampling rate or by switching to AES from OTP.

7.2 Dynamic key pool size

The secure communication system of Figure 6 can be thought of as a combination of two interconnected but independent systems, the key generation system and the key distribution system. The key generation system, featuring the quantum layer, is responsible for creating a symmetric key reserve pool and continuously contributing the newly formed keys to it. The key pool is identical on the sides of Alice and Bob, stored in both servers. The key distribution system is responsible for removing keys from the pool upon request from the communication parties and encryption applications. The size and number of removed keys, as well as the frequency at which this process occurs, are dictated by the communication model parameters (Table 1). The system can be described by the balance Equation 20. We begin by studying the dynamics of the key pool size when isolated from the key distribution system (i.e., before secure communication/encryption is initiated). Processing the SKR data from the system, the curves of Figure 10 are obtained.

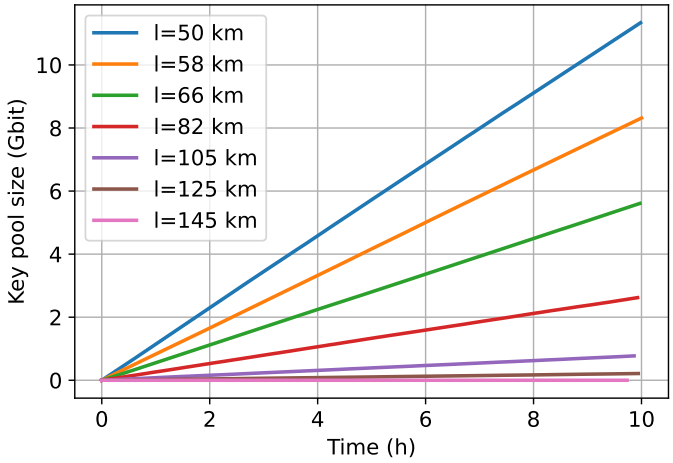
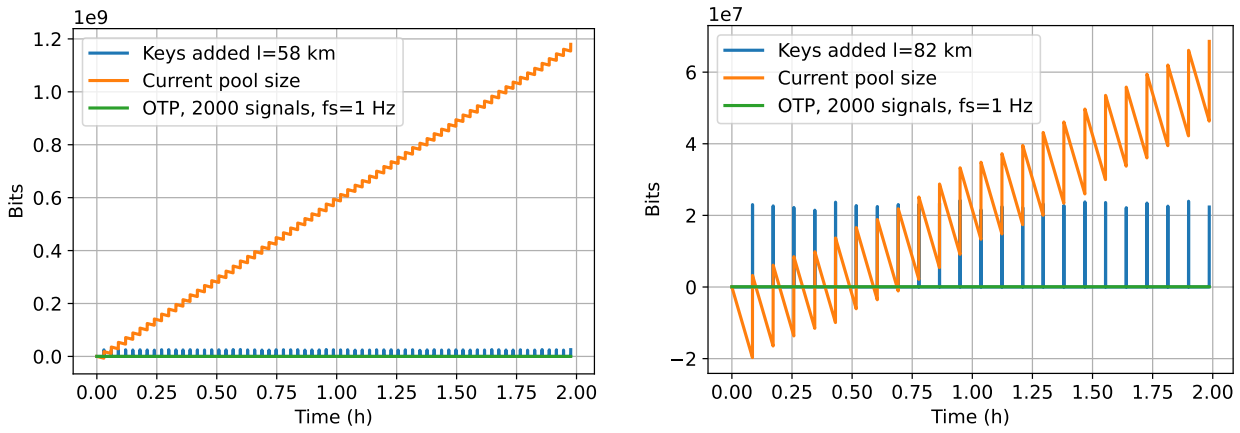


Figure 10: Accumulation of generated keys as a function of time for various distances.

After 10 hours of operation, a key reserve of more than 11 Gbits is formed at 50 km, falling to approximately 1 Gbit at 105 km. The dynamic size of the key pool as a function of time can be calculated for different configurations, using Equation 16 for $d_0 = 0$. Following an intense key consumption scenario, Figure 11 demonstrates the time evolution of the key pool as a function of time for indicative communication distances. The plots also display key generation and key consumption terms. This calculation is faithful to the actual scheme, as excess keys are stored in the key pool in real time. As a result, the corresponding key availability condition is given by Equation 18, dictating that uninterrupted secure communication requires the current pool size to remain positive at all times.

The plots demonstrate that shorter distances exhibit more frequent key contributions, sustaining a positive dynamic pool and forming a considerable key reserve. However, with increasing distances, a dead time appears after starting the operation, during which the key reserve is not sufficient to sustain secure communication. As an example, $l = 82$ km requires more than 45 minutes of operation before the dynamic pool size becomes consistently positive. During this interval, real-time encryption cannot occur. To mitigate this effect,

countermeasure strategies need to be applied, such as introducing QKD lead time.



(a) $l = 58$ km (b) $l = 82$ km

Figure 11: Dynamic key pool size for different communication distances. The practical-dynamic key availability condition of Equation 18 is evaluated, as the key pool size needs to be positive at all times.

7.3 QKD lead time

To fulfill the key availability condition, QKD operation might need to be initialized before starting secure data exchange. This allows to form an initial key reserve for balancing the key consumption rate. As previous operation contributes additional complexity to the system, it is important to ensure that the QKD lead time is minimized. A systematic way of directly determining the minimum lead time required in each scenario is needed, given the transmission distance and use case parameters.

For this reason, an automated script was developed which processes the QKD dataset and determines the lead time required for each use case configuration and distance. The algorithm evaluates Equation 20 for $k \cdot \Delta\tau_{\text{ef}} = 10$ hours of operation. The process is repeated for increasing lead time values until Equation 18 is satisfied. In each case, the dynamic pool is evaluated using Equation 20. A configuration is considered nonviable if the obtained lead time exceeds 5 hours, suggesting that it should first be modified for bandwidth optimization. The script is executed for two signal sets ($N = 68, N = 2,000$), three sampling frequencies ($f_s = 1$ Hz, $f_s = 10$ Hz, $f_s = 20$ Hz), two encryption algorithms (OTP, AES-256), and 21 distances, with results presented in Table 4 and Table 5. The trends corresponding to the remote monitoring use cases ($N = 68$) and data historian use cases ($N = 2,000$) are displayed in Figure 12 and Figure 13, for OTP and AES, respectively.

In the remote monitoring scenario, a maximum distance of 135 km can be achieved when $f_s = 1$ Hz. However, this comes at the cost of approximately 40 minutes of QKD lead time. If the frequency is increased to 20 cycles per second, the maximum distance is limited to 90 km, with a required lead time of 8 minutes. The results are indicative for the data historian use case. For $f_s = 1$ Hz, the maximum achievable distance is 82 km for a lead time of 6

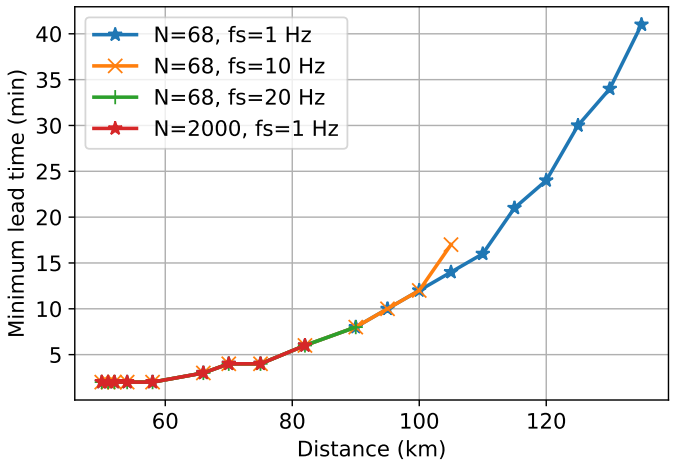


Figure 12: Minimum QKD lead times required for uninterrupted OTP encryption.

minutes. As the sampling rate increases, it is shown that OTP cannot be self-sustained. Although introducing prolonged lead times could be an option for supporting OTP with higher sampling rates for limited periods of time, it seems preferable to investigate data optimization methods instead. Such approach could lead to higher overall system reliability.

AES-256 is evaluated as a backup or alternative for use cases which combine intense data generation and long transmission distances. Lead time is not affected by the number of signals generated per time step as, unlike OPT, the block cipher defines a fixed key length not directly related to the size of plaintext. Due to the reduced key consumption rate, higher distances and sampling frequencies can be supported. The most demanding use case with 20 cycles/sec at 120 km requires only 24 minutes of QKD early operation, while distances up to 95 km require less than 10 minutes regardless of the data configuration. Notably, using AES practically expands the maximum achievable distance for data-heavy communication beyond 100 km. The AES-256 metrics confirm the potential to use the standard for those use cases where OTP cannot satisfy the key availability condition, by significantly reducing key consumption. This approach can be also found useful in case of an emergency or QKD system failure (e.g., fiber link interruption) for sustaining secure communication with increased key economy, explored in the next section.

7.4 Key distribution failure

The QKD experimental dataset is processed to determine the post-failure secure communication uptime Δt_{up}, for various parameter combinations. For each scenario evaluated, the optimal lead time t_{lead} determined in subsection 7.3 is assigned as the starting point of secure communication. In the first stage, QKD failure is assumed to occur at $t_{\text{failure}} = t_{\text{lead}} + 1$ hour. The uptimes are determined by evaluating Equation 27.

The OTP results are shown in Table 6. The results demonstrate the dependence on distance and key consumption parameters. The maximum achievable distance for each configuration is still determined by the ability to obtain uninterrupted secure communication for a given lead time. For $l = 50$ km the secure uptime is at least 4.1 hours for $N = 2,000$

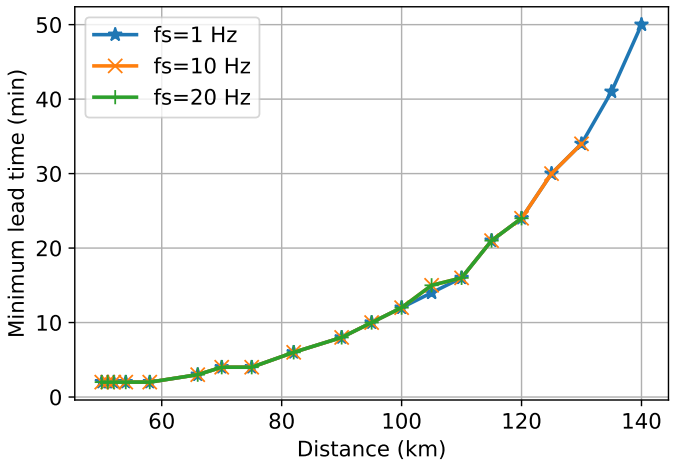
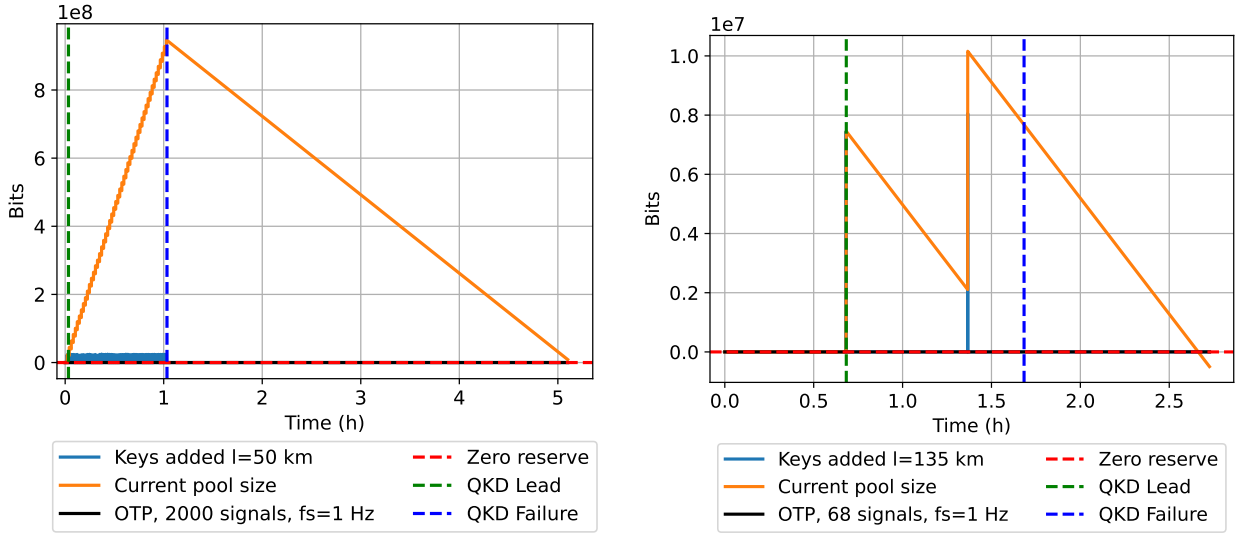


Figure 13: Minimum QKD lead time for AES-256 encryption with 128-bit IV under different parameter configurations. Key and IV are truly random bit sequences, updated in every encryption operation.

(Figure 14a), reaching 149.1 hours when $N = 68$. However, for 68 signals and $l = 135$ km, secure operation is sustained for approximately 59 minutes before the key reserve is exhausted (Figure 14b).



(a) $l = 50$ km, $N = 2000$, $f_s = 1$ Hz

(b) $l = 135$ km, $N = 68$, $f_s = 1$ Hz

Figure 14: Two representative use cases of key distribution failure. System lead time is assumed equal to the optimization value for each use case. Failure occurs 1 hour after secure communication is initiated. OTP is applied.

QKD failure time t_{fail} can be arbitrarily set for investigating different events. In Figure 15, the dynamic key pool at $l = 82$ km is plotted for various t_{fail} values. As a result, reversing the problem allows one to set a minimum acceptable time-to-failure as a target communication

autonomy for an arbitrary I&C system, and determine the required operational lead time.

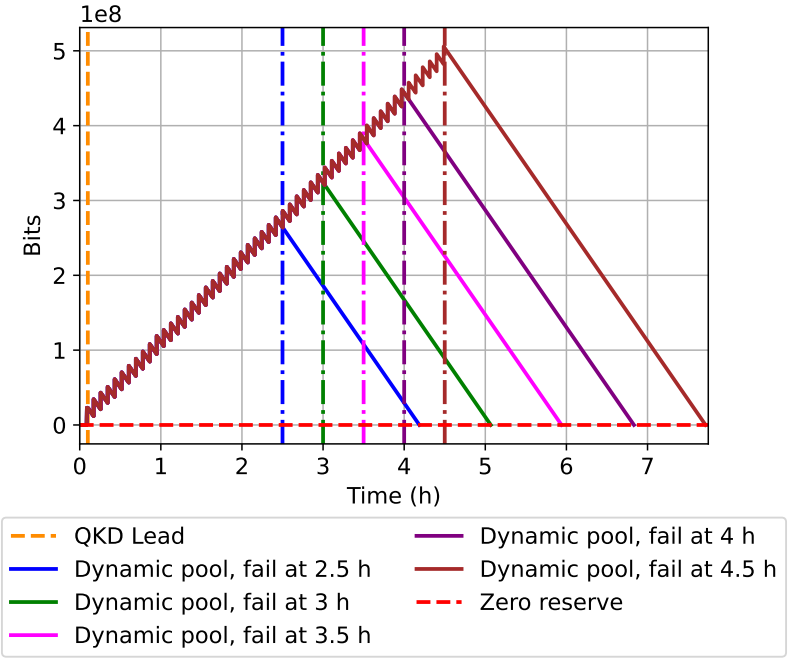


Figure 15: Dynamic key pool for QKD failure at different instances t_{fail} ($l = 82$ km, $N = 68$, $f_s = 20$ Hz, $p = 32$ bits, $f_{\text{enc}} = 1$, $t_{\text{lead}} = 6$ min).

The process is repeated with AES-256 instead of OTP (Table 7). Applying AES drastically increases the encryption uptime in case of QKD failure. At 1 Hz and distances less than 58 km, the system provides approximately 850 hours of encrypted data transmission. Although autonomy is reduced for higher rates and increasing distances, the system preserves computational security for at least 30 minutes, even in the worst-case scenario.

The identified trade-off between encryption robustness and key consumption allows to design a redundancy mechanism, where AES acts as a backup scheme until QKD communication is restored. This scenario can be particularly useful in larger distances with limited key generation, as it reduces key consumption and prolongs communication autonomy. In Figure 16, we recreate the key failure event at $l = 135$ km with $N = 68$ and $f_s = 1$ Hz. QKD failure takes place 2 hours after secure communication begins. The plot displays the two response scenarios, maintaining OTP or switching to AES. While OTP provides an uptime of 67 minutes after failure, switching to AES after failure yields 6.3 hours. Similarly, for $t_{\text{fail}} = t_{\text{lead}} + 1$ h, OTP offers 58 minutes of autonomy compared to 5.5 hours offered by switching to AES. The list of secure uptimes when switching from OTP to AES-256 at the time of failure is featured in Table 8.

8 Latency

Latency is the second metric of interest for evaluating the performance of a use case. In this stage, the results from real-time secure communication cycles are studied. Secure com-

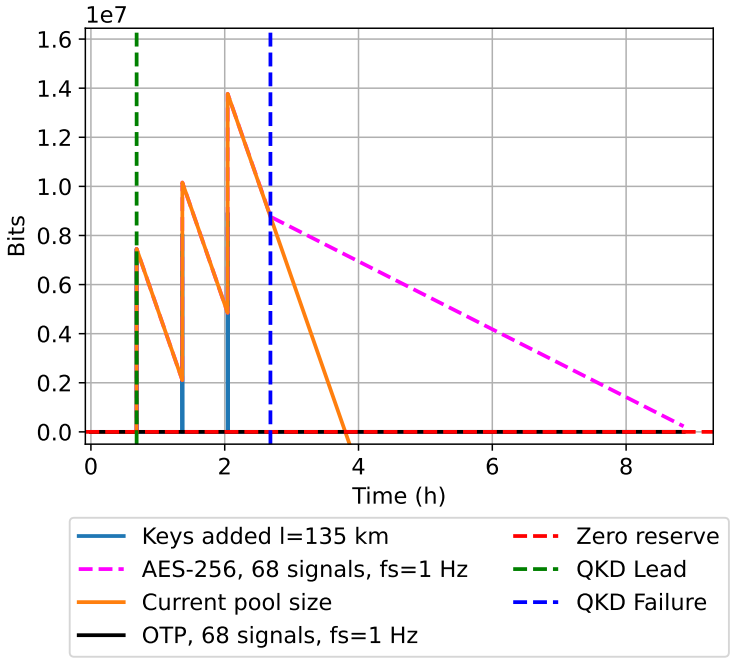
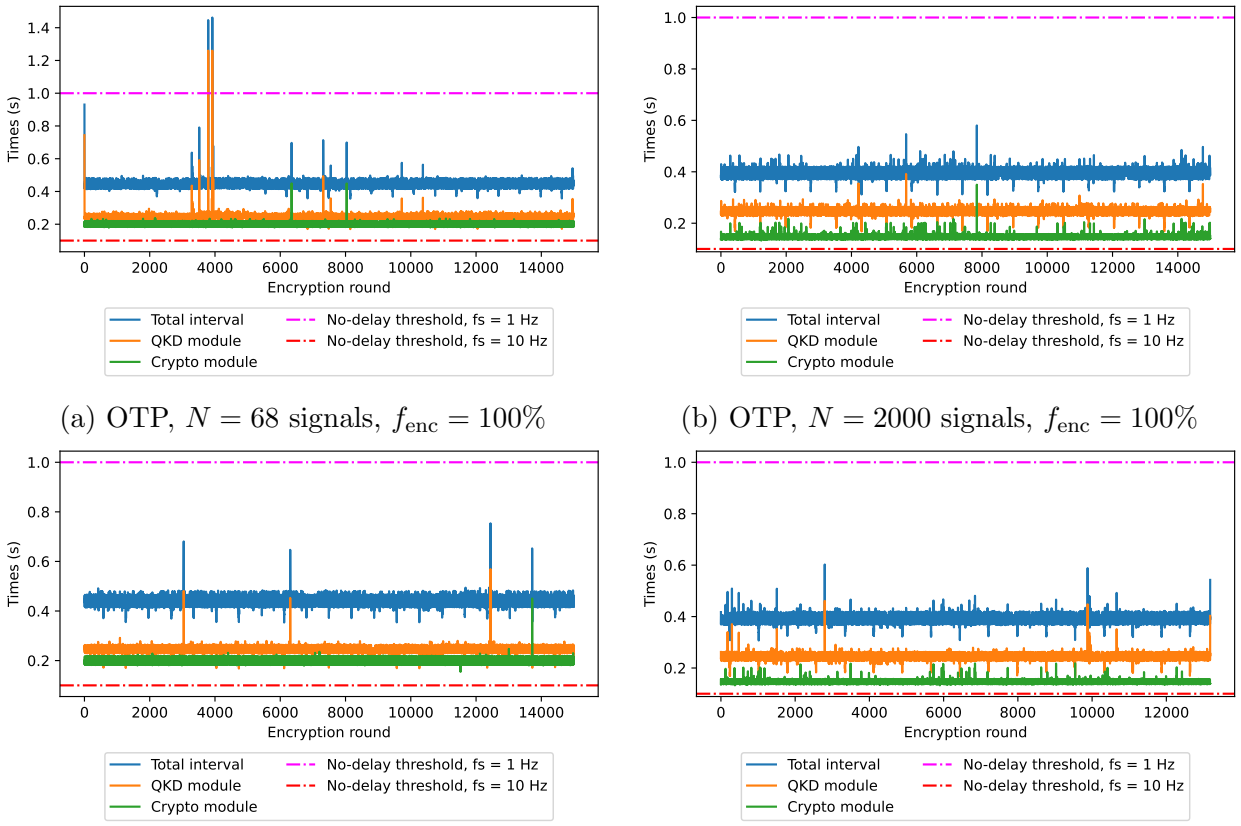


Figure 16: Dynamic key pool for at $l = 135$ km. Switching to AES encryption after QKD failure provides an additional 5.2 hours of operation compared to OTP ($t_{\text{fail}} = t_{\text{lead}} + 2$).

munication between the two terminals (Figure 6) occurs following the procedure stages of Figure 3. The experiments are conducted for three cryptographic algorithm families (OTP, AES, ASCON). Cryptographic operations have been implemented through software, using open-source Python libraries. Time measurements are obtained for each use case configuration, for each of which the latency condition of Equation 9 is evaluated. The following sections present the measurement results.

In the fundamental case, OTP encryption is considered. The reporting rate is identical to the sampling rate (i.e., each row of parameters corresponding to the current time step is encrypted and transmitted by itself). The 2,000 signals are fetched, encrypted and transmitted according to the communication procedure. The experiment is conducted for 15,000 data generation cycles, at a rate of 10 samples/sec. Figure 17b demonstrates the total latencies as well as those corresponding to the specific modules. The average time per data cycle is 395 ± 15 ms, out of which 248 ms and 145 ms are reported in the QKD and Crypto modules, respectively. The experiment is repeated only for the 68 core signals, with the results shown in Figure 17a. Although there is significant difference in terms of key availability, the number of signals does not considerably affect latency in OTP encryption. Key distribution takes on average the same time as in the 2,000 signals case (248 ms), and the Crypto module requires approximately 50 ms more. The slight increase could be attributed to the overall higher efficiency of the encryption/decryption processes when handling larger data chunks.

AES-256 is the most secure variant of the Advanced Encryption Standard, featuring a 256-bit key and 128-bit IV. Since both the key and the IV are updated per data cycle, a total of 384 bits are requested at every iteration. Using Equation 7, the key reusability factor is found equal to 17% and 0.6% for $N = 68$ and $N = 2,000$, respectively. Similarly to OTP, the



(a) OTP, $N = 68$ signals, $f_{\text{enc}} = 100\%$

(b) OTP, $N = 2000$ signals, $f_{\text{enc}} = 100\%$

(c) AES-256, $N = 68$ signals, $f_{\text{enc}} = 17\%$

(d) AES-256, $N = 2,000$ signals, $f_{\text{enc}} = 0.6\%$

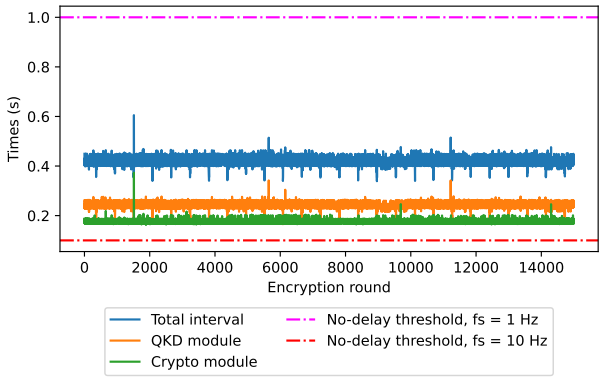
Figure 17: Latency for OTP and AES-256 encryption.

latency metrics are evaluated and shown in Figure 17c and Figure 17d. Although AES has higher complexity compared to the bitwise operations in OTP, the results do not indicate additional delay. Specifically, the average time of cryptographic operations is almost identical to the OTP cases (195 ms for $N = 68$ and 145 ms for $N = 2,000$). The QKD module time is slightly reduced (5 ms), though the reduction is not proportional to the key reusability factor decrease. Therefore, the performance of AES in terms of latency is similar to OTP, with its primary advantage remaining higher key economy.

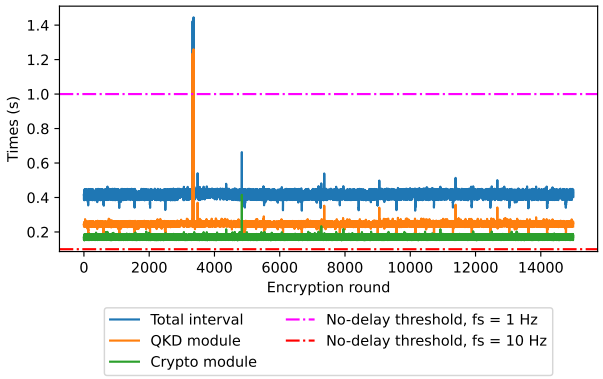
A similar approach is followed to evaluate the performance of ASCON variants. ASCON is the official selection of NIST for the novel field of Light-Weight Cryptography (LWC). LWC algorithms are designed around simpler operations, to enable cryptographic capabilities even in devices with limited computational resources [74, 75]. In this implementation, three prominent variants are examined (ASCON-128, ASCON-128a, ASCON-80pq). Notably, ASCON-80pq is a post-quantum cryptography cipher, claiming to be more robust against a quantum computer-initiated attack [76].

In addition to the low computational resource requirements, the ASCON family offers authenticated encryption with associated data (AEAD). The key size is 128 bits for the 128 and 128a variants, while 80pq handles an 160-bit key. All three variants further require an 128-bit nonce. As in the previous cases, the key and nonce are refreshed per data generation

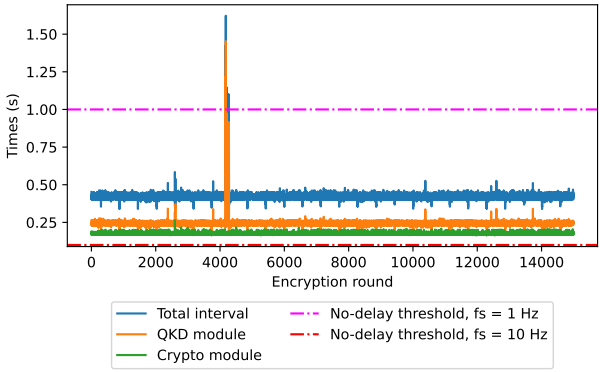
cycle. Therefore, the key reusability factor is 0.4 % for ASCON-128/128a and 0.45 % for ASCON-80pq, when $N = 2000$. The performance metrics are demonstrated in Figure 18.



(a) ASCON-128, $f_{\text{enc}} = 0.04\%$



(b) ASCON-128a, $f_{\text{enc}} = 0.04\%$



(c) ASCON-80pq, $f_{\text{enc}} = 0.045\%$

Figure 18: Latencies in ASCON variants ($N = 2000$ signals, $p = 32$ bits)

All three variants remain within the boundaries of 1 and 10 sampling iterations per second. While there is still delay for a use case of 10 Hz, the cryptographic module time is slightly reduced compared to OTP and AES by approximately 20-25 ms per cryptographic cycle. The QKD module intervals continue to average around 245 ms, confirming that the elapsed time for establishing communication between QKD servers and secure applications includes an unavoidable overhead.

The obtained metrics for all tested algorithms and configurations are summarized in Table 3 and displayed in Figure 19. Overall, the total latency is consistently within the acceptable bounds, for the use case where data is sampled every second. In fact, there is an average margin of more than 0.5 seconds to immediately compensate for any delay outliers (e.g., the two peaks of Figure 17a). The results confirm the potential of unconditionally secure remote operation, since $f_s = 1$ Hz provides sufficient time resolution for the majority of monitored parameters.

Table 3: Latency metrics for different encryption algorithm variants and number of signals. Reporting frequency is equal to the sampling rate, therefore each operation corresponds to a single data row.

Algorithm	Signals	Total time (ms)		QKD time (ms)		Crypto time (ms)	
		Mean	STD	Mean	STD	Mean	STD
OTP	68	444.95	20.91	248.76	17.28	195.79	11.47
OTP	2,000	395.23	14.61	248.18	11.32	144.72	8.33
AES-256	68	440.47	16.66	244.79	11.70	195.32	10.83
AES-256	2,000	390.45	14.71	244.32	11.48	144.27	7.86
ASCON-128	2,000	419.91	14.49	243.05	11.16	175.28	8.00
ASCON-128a	2,000	417.23	20.43	245.70	16.42	169.93	10.42
ASCON-80pq	2,000	421.53	27.83	244.02	26.11	175.89	8.30

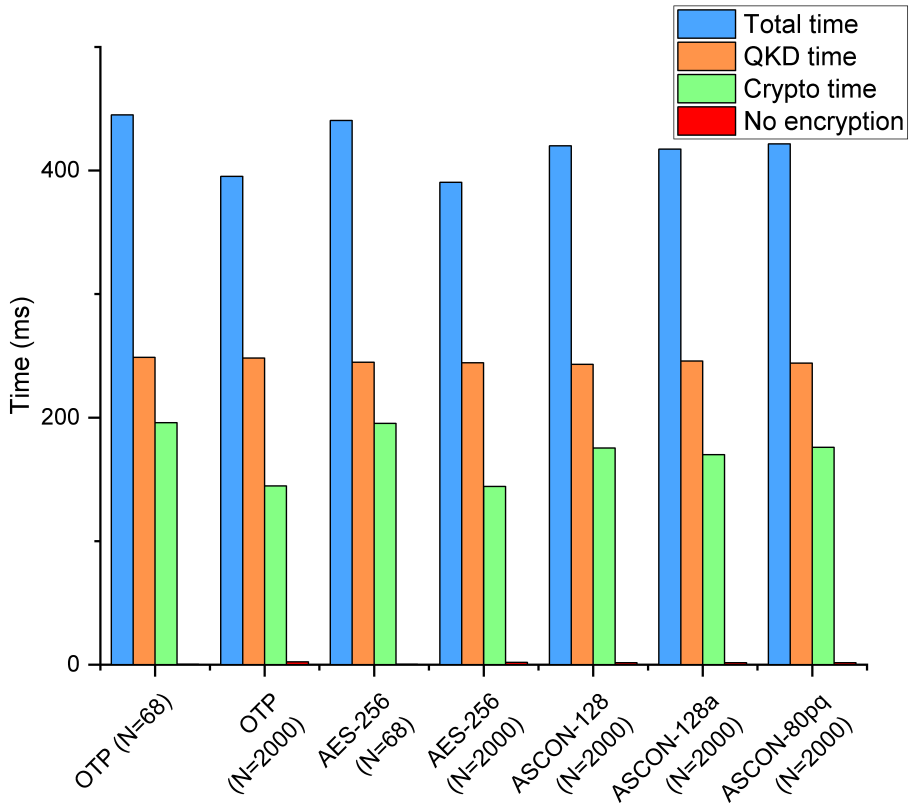


Figure 19: Average latency for evaluated cryptographic variants.

9 Conclusion

This paper presented an experimental demonstration of Quantum Key Distribution in a nuclear power reactor. An experimental setup was formed, leveraging PUR-1 research reactor and the commercial Toshiba QKD LD system. A secure communication model was formulated, defining detailed constraint conditions for evaluating the feasibility of a specific

system configuration.

The compatibility of QKD with nuclear reactor remote monitoring was confirmed through the design and replication of various use cases, characterized by different transmission lengths, reactor signals, sampling rates, and encryption algorithms. Secure, delay-free monitoring was achieved for up to 135 km for typical I&C sampling rates. The experimental data were further processed to generate key distribution failure scenarios, and subsequently determine the minimum QKD lead time required to prolong encrypted data exchange in case of an emergency. Results demonstrated that OTP-encrypted exchange can be achieved for 2,000 signals at up to 82 km when $f_s = 1$ Hz. If a core of 68 signals is transmitted instead, the distance can reach 135 km, 105 km, and 90 km, for $f_s = 1$ Hz, $f_s = 10$ Hz, and $f_s = 20$ Hz, respectively. Switching to AES-256, the maximum distance is expanded to 140 km for all 2,000 signals when $f_s = 1$ Hz.

Regarding future work, it is intended to investigate options for further minimizing latency, to enable secure transmission of higher data rates. Hardware implementation of the discussed encryption algorithms will be explored, in an attempt to further minimize latencies from the cryptographic module. In addition, procedure parallelization will be considered, to examine the potential of reducing the variance of latency attributed to QKD key requests.

Acknowledgment

This research is being performed using funding received from the DOE Office of Nuclear Energy's Nuclear Energy University Program under contract DE-NE00009174. The authors would like to thank Dr. Ben Cipiti at Sandia National Laboratories, and Katya LeBlanc at Idaho National Laboratories for fruitful discussions and expert input. Konstantinos Gkouliaras would like to acknowledge the Greek Atomic Energy Commission for supporting his doctoral studies through a graduate fellowship.

References

[1] R. Fasano, A. Hahn, A. Haddad, and C. Lamb, "Advance Reactor Operational Technology Architecture Categorization," Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), Tech. Rep. SAND2021-12084, Sep. 2021. [Online]. Available: https://www.osti.gov/biblio/1854723

[2] J. K. Nøland, M. N. Hjelmeland, C. Hartmann, L. B. Tjernberg, and M. Korpås, "Overview of Small Modular and Advanced Nuclear Reactors and Their Role in the Energy Transition," *IEEE Transactions on Energy Conversion*, pp. 1–12, 2025, conference Name: IEEE Transactions on Energy Conversion. [Online]. Available: https://ieeexplore.ieee.org/document/10841944

[3] C. Baylon, R. Brunt, and D. Livingstone, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks: Chatham House Report.* Chatham House for the Royal Institute of International Affairs, 2015.

[4] U. NRC, "Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities," *US NRC, Washington, DC*, 2010.

[5] J. Son, T. Tak, and H. Inhye, "Modeling cryptographic algorithms validation and developing block ciphers with electronic code book for a control system at nuclear power plants," *Nuclear Engineering and Technology*, vol. 55, no. 1, pp. 25–36, Jan. 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1738573322003527

[6] J. Katz and Y. Lindell, *Introduction to modern cryptography*, third edition ed., ser. Chapman & Hall/CRC Cryptography and Network Security Series. Boca Raton London New York: CRC Press Taylor & Francis Group, 2021.

[7] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018, arXiv:1804.00200 [cs]. [Online]. Available: http://arxiv.org/abs/1804.00200

[8] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, Apr. 2021, publisher: Verein zur Förderung des Open Access Publizierens in den Quantenwissenschaften. [Online]. Available: https://quantum-journal.org/papers/q-2021-04-15-433/

[9] P. Szikora and K. Lazányi, "The End of Encryption? – The Era of Quantum Computers," in *Security-Related Advanced Technologies in Critical Infrastructure Protection*, T. A. Kovács, Z. Nyikes, and I. Fürstner, Eds. Dordrecht: Springer Netherlands, 2022, pp. 61–72.

[10] R. Azhari and A. N. Salsabila, "Analyzing the Impact of Quantum Computing on Current Encryption Techniques," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 148–157, Feb. 2024, number: 2. [Online]. Available: https://aptikom-journal.id/itsdi/article/view/662

[11] "National Quantum Initiative." [Online]. Available: https://www.quantum.gov/

[12] H. Neven, "Meet Willow, our state-of-the-art quantum chip," Dec. 2024. [Online]. Available: https://blog.google/technology/research/google-willow-quantum-chip/

[13] J. Porter, "Google wants to build a useful quantum computer by 2029," May 2021. [Online]. Available: https://www.theverge.com/2021/5/19/22443453/google-quantum-computer-2029-decade-commercial-useful-qubits-quantum-transistor

[14] E. Roth, "Google reveals quantum computing chip with 'breakthrough' achievements," Dec. 2024. [Online]. Available: https://www.theverge.com/2024/12/9/24317382/google-willow-quantum-computing-chip-breakthrough

[15] M. Murphy, "AI and quantum computing: How IBM showed up at SXSW 2025," Mar. 2025. [Online]. Available: https://research.ibm.com/blog/ibm-research-sxsw-quantum-ai

[16] M. AbuGhanem, "IBM quantum computers: evolution, performance, and future directions," *The Journal of Supercomputing*, vol. 81, no. 5, p. 687, Apr. 2025. [Online]. Available: https://doi.org/10.1007/s11227-025-07047-7

[17] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, May 2022, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41586-022-04623-2

[18] A. Brazaola-Vicario, A. Ruiz, O. Lage, E. Jacob, and J. Astorga, "Quantum key distribution: a survey on current vulnerability trends and potential implementation risks," *Optics Continuum*, vol. 3, no. 8, pp. 1438–1460, Aug. 2024, publisher: Optica Publishing Group. [Online]. Available: https://opg.optica.org/optcon/abstract.cfm?uri=optcon-3-8-1438

[19] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514004241

[20] A. I. Nurhadi and N. R. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey," in *2018 4th International Conference on Wireless and Telematics (ICWT)*. Nusa Dua: IEEE, Jul. 2018, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8527822/

[21] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, "Decoy-state quantum key distribution with biased basis choice," *Scientific Reports*, vol. 3, no. 1, p. 2453, Aug. 2013, number: 1 Publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/srep02453

[22] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, May 2018, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41586-018-0066-6

[23] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, p. 1012, Dec. 2020. [Online]. Available: https://opg.optica.org/abstract.cfm?URI=aop-12-4-1012

[24] C. Portmann and R. Renner, "Security in quantum cryptography," *Reviews of Modern Physics*, vol. 94, no. 2, p. 025008, Jun. 2022, publisher: American Physical Society. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.94.025008

[25] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Communications*, vol. 3, no. 1,

p. 634, Jan. 2012, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/ncomms1631

[26] H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, "Security of quantum key distribution with multiphoton components," *Scientific Reports*, vol. 6, no. 1, p. 29482, Jul. 2016, number: 1 Publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/srep29482

[27] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, no. 1, p. 15043, Apr. 2017, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/ncomms15043

[28] M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nature Communications*, vol. 5, no. 1, p. 5235, Oct. 2014, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/ncomms6235

[29] Z. Li and K. Wei, "Improving Parameter Optimization in Decoy-State Quantum Key Distribution," *Quantum Engineering*, vol. 2022, pp. 1–9, Feb. 2022. [Online]. Available: https://www.hindawi.com/journals/que/2022/9717591/

[30] Z. Chen, X. Wang, S. Yu, Z. Li, and H. Guo, "Continuous-mode quantum key distribution with digital signal processing," *npj Quantum Information*, vol. 9, no. 1, pp. 1–8, Mar. 2023, number: 1 Publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41534-023-00695-8

[31] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in InGaAs/InP single-photon detector systems for quantum communication," *Light: Science & Applications*, vol. 4, no. 5, pp. e286–e286, May 2015, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/lsa201559

[32] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussières, and H. Zbinden, "Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems," *Nature Photonics*, vol. 17, no. 5, pp. 422–426, May 2023, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41566-023-01168-2

[33] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022, conference Name: IEEE Communications Surveys & Tutorials.

[34] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "A step towards global key distribution," *Nature*, vol. 419, no. 6906, pp. 450–450, Oct. 2002, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/419450a

[35] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, Jul. 2007, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/nphys629

[36] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nature Communications*, vol. 2, no. 1, p. 349, Jun. 2011. [Online]. Available: https://www.nature.com/articles/ncomms1348

[37] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photonics*, vol. 15, no. 8, pp. 570–575, Aug. 2021, publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41566-021-00828-5

[38] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, Jan. 2021, number: 7841 Publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41586-020-03093-8

[39] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, "600-km repeater-like quantum communications with dual-band stabilization," *Nature Photonics*, vol. 15, no. 7, pp. 530–535, Jul. 2021, number: 7 Publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41566-021-00811-0

[40] M. Balcı, "STRATEGIC REPORT Quantum Key Distribution (QKD) Systems," Tech. Rep., Jan. 2020.

[41] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*. Cham: Springer International Publishing, 2019. [Online]. Available: http://link.springer.com/10.1007/978-3-030-27565-5

[42] R. Wolf, *Quantum Key Distribution: An Introduction with Exercises*, ser. Lecture Notes in Physics. Cham: Springer International Publishing, 2021, vol. 988. [Online]. Available: https://link.springer.com/10.1007/978-3-030-73991-1

[43] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, Jul. 2009, aDS Bibcode: 2009RvMP...81.1301S. [Online]. Available: https://ui.adsabs.harvard.edu/abs/2009RvMP...81.1301S

[44] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, "10-Mb/s Quantum Key Distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, Aug. 2018, conference Name: Journal of Lightwave Technology.

[45] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, Aug. 2003, arXiv:quant-ph/0211153. [Online]. Available: http://arxiv.org/abs/quant-ph/0211153

[46] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," *Physical Review Letters*, vol. 94, no. 23, p. 230503, Jun. 2005, publisher: American Physical Society. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.94.230503

[47] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters*, vol. 94, no. 23, p. 230504, Jun. 2005, publisher: American Physical Society. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.94.230504

[48] I. A. E. Agency, "Computer Security Techniques for Nuclear Facilities," International Atomic Energy Agency, Text, 2021, iSBN: 9789201235206 Publication Title: Computer Security Techniques for Nuclear Facilities. [Online]. Available: https://www.iaea.org/publications/14729/computer-security-techniques-for-nuclear-facilities

[49] J. Peterson, M. Haney, and R. A. Borrelli, "An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants," *Nuclear Engineering and Design*, vol. 346, pp. 75–84, May 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0029549319300330

[50] J.-G. Song, J.-W. Lee, G.-Y. Park, K.-C. Kwon, D.-Y. Lee, and C.-K. Lee, "AN ANALYSIS OF TECHNICAL SECURITY CONTROL REQUIREMENTS FOR DIGITAL I&C SYSTEMS IN NUCLEAR POWER PLANTS," *Nuclear Engineering and Technology*, vol. 45, no. 5, pp. 637–652, Oct. 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1738573315300498

[51] F. Zhang, J. W. Hines, and J. B. Coble, "A Robust Cybersecurity Solution Platform Architecture for Digital Instrumentation and Control Systems in Nuclear Power Facilities," *Nuclear Technology*, vol. 206, no. 7, pp. 939–950, Jul. 2020, publisher: Taylor & Francis _eprint: https://doi.org/10.1080/00295450.2019.1666599. [Online]. Available: https://doi.org/10.1080/00295450.2019.1666599

[52] K. Gkouliaras, V. Theos, Z. Dahm, W. Richards, K. Vasili, and S. Chatzidakis, "False Data Injection Detection in Nuclear Systems Using Dynamic Noise Analysis," *IEEE Access*, vol. 12, pp. 94 936–94 949, 2024, conference Name: IEEE Access. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10589395

[53] J.-h. Roh, S.-k. Lee, C.-W. Son, C. Hwang, J. Kang, and J. Park, "Cyber Security System with FPGA-based Network Intrusion Detector for Nuclear Power

Plant," in *IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society*, Oct. 2020, pp. 2121–2125, iSSN: 2577-1647. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9255158

[54] D. Allison, K. McLaughlin, and P. Smith, "Goosewolf: An Embedded Intrusion Detection System for Advanced Programmable Logic Controllers," *Digital Threats: Research and Practice*, vol. 4, no. 4, pp. 59:1–59:19, Oct. 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3617692

[55] B. Karch, T. A. Gray, and M. T. Rowland, "Field Programmable Gate Array-Based Reactor Protection Systems and Potential for Inclusion of Secure Elements to Improve Cybersecurity," Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), Tech. Rep. SAND-2024-12082, Sep. 2024. [Online]. Available: https://www.osti.gov/biblio/2462968

[56] M. A. Elakrat and J. C. Jung, "Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network," *Nuclear Engineering and Technology*, vol. 50, no. 5, pp. 780–787, Jun. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S173857331730565X

[57] N. Kumar, V. M. Mishra, and A. Kumar, "Smart grid and nuclear power plant security by integrating cryptographic hardware chip," *Nuclear Engineering and Technology*, vol. 53, no. 10, pp. 3327–3334, Oct. 2021. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1738573321002576

[58] H. P. Paudel, S. E. Crawford, Y.-L. Lee, R. A. Shugayev, M. N. Leuenberger, M. Syamlal, P. R. Ohodnicki, P. Lu, D. Mollot, and Y. Duan, "Quantum Communication Networks for Energy Applications: Review and Perspective," *Advanced Quantum Technologies*, vol. 6, no. 10, p. 2300096, 2023, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/qute.202300096. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/qute.202300096

[59] F.-Y. Li, D. Wang, S. Wang, M. Li, Z.-Q. Yin, H.-W. Li, W. Chen, and Z.-F. Han, "Effect of electromagnetic disturbance on the practical QKD system in the smart grid," *Chinese Physics B*, vol. 23, no. 12, p. 124201, Dec. 2014. [Online]. Available: https://iopscience.iop.org/article/10.1088/1674-1056/23/12/124201

[60] M. Alshowkan, P. G. Evans, M. Starke, D. Earl, and N. A. Peters, "Authentication of smart grid communications using quantum key distribution," *Scientific Reports*, vol. 12, no. 1, p. 12731, Jul. 2022, number: 1 Publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41598-022-16090-w

[61] W. Grice, M. Olama, A. Lee, and P. Evans, "Quantum Key Distribution Applicability to Smart Grid Cybersecurity Systems," *IEEE Access*, pp. 1–1, 2025, conference Name: IEEE Access. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10852309

[62] P. G. Evans, M. Alshowkan, D. Earl, D. D. Mulkey, R. Newell, G. Peterson, C. Safi, J. L. Tripp, and N. A. Peters, "Trusted Node QKD at an Electrical Utility," *IEEE Access*, vol. 9, pp. 105 220–105 229, 2021, conference Name: IEEE Access. [Online]. Available: https://ieeexplore.ieee.org/document/9405393

[63] A. Green, J. Lawrence, G. Siopsis, N. A. Peters, and A. Passian, "Quantum Key Distribution for Critical Infrastructures: Towards Cyber-Physical Security for Hydropower and Dams," *Sensors*, vol. 23, no. 24, p. 9818, Jan. 2023, number: 24 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/23/24/9818

[64] M. Pantopoulou, S. Pantopoulou, M. Roberts, D. Kultgen, L. Tsoukalas, and A. Heifetz, "Monitoring and Secure Communications for Small Modular Reactors," in *Dynamic Data Driven Applications Systems*, E. Blasch, F. Darema, and A. Aved, Eds. Cham: Springer Nature Switzerland, 2024, pp. 144–151.

[65] M. Roberts and A. Heifetz, "Investigating Wireless Quantum Key Distribution for Advanced Reactor Communications," Argonne National Lab. (ANL), Argonne, IL (United States), Tech. Rep. ANL/NSE-21/49, Aug. 2021. [Online]. Available: https://www.osti.gov/biblio/1837006

[66] K. Gkouliaras, V. Theos, P. G. Evans, and S. Chatzidakis, "NuQKD: A Modular Quantum Key Distribution Simulation Framework for Engineering Applications," *Advanced Physics Research*, vol. 3, no. 7, p. 2400016, 2024, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/apxr.202400016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/apxr.202400016

[67] K. Gkouliaras, V. Theos, and S. Chatzidakis, "Exploring the Feasibility of Quantum-Based Secure Communications for Nuclear Applications," *Nuclear Technology*, vol. 0, no. 0, pp. 1–20, 2024, publisher: Taylor & Francis _eprint: https://doi.org/10.1080/00295450.2024.2368977. [Online]. Available: https://doi.org/10.1080/00295450.2024.2368977

[68] "IEEE Standard for Floating-Point Arithmetic," *IEEE Std 754-2019 (Revision of IEEE 754-2008)*, pp. 1–84, Jul. 2019, conference Name: IEEE Std 754-2019 (Revision of IEEE 754-2008). [Online]. Available: https://ieeexplore.ieee.org/document/8766229

[69] S. Chatzidakis, V. Theos, K. Gkouliaras, Z. Dahm, K. Vasili, T. Miller, B. Jowers, J. Lawrence, J. Hollern, D. Eskins, K. Cottrell, and A. Kim, "Characterizing Nuclear Cybersecurity States Using Artificial Intelligence/Machine Learning - Final Report," U.S. Nuclear Regulatory Commission, Tech. Rep. TLR RES/DE-2024-003, Jun. 2024. [Online]. Available: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML24193A008

[70] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Optics Express*, vol. 21, no. 21, pp.

24 550–24 565, Oct. 2013, publisher: Optica Publishing Group. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?uri=oe-21-21-24550

[71] "ETSI GS QKD 014: Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API," Feb. 2019. [Online]. Available: https://www.etsi.org/standards#page=1&search=QKD&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=2025-01-08&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1

[72] G. P. Agrawal, *Fiber-optic communication systems*, 4th ed., ser. Wiley series in microwave and optical engineering. New York: Wiley, 2010, no. 222.

[73] National Institute of Standards and Technology (US), "Advanced Encryption Standard (AES)," National Institute of Standards and Technology (U.S.), Washington, D.C., Tech. Rep. NIST FIPS 197-upd1, May 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf

[74] M. S. Turan, K. McKay, D. Chang, L. E. Bassham, J. Kang, N. D. Waller, J. M. Kelsey, and D. Hong, "Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process," Tech. Rep., 2023, publisher: Meltem Sonmez Turan, Kerry McKay, Donghoon Chang, Jinkeon Kang, Noah Waller .... [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8454.pdf

[75] K. Gkouliaras, V. Theos, S. Yilmaz, S. Revankar, and S. Chatzidakis, "Evaluating Lightweight Cryptography Algorithms for Nuclear Environment Applications," in *Transactions of the American Nuclear Society*, vol. 131, Orlando, FL, Nov. 2024, pp. 388–391.

[76] H. P. Nguyen and Y. Chen, "Lightweight, Post-Quantum Secure Cryptography Based on Ascon: Hardware Implementation in Automotive Applications," *Electronics*, vol. 13, no. 22, p. 4550, Jan. 2024, number: 22 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2079-9292/13/22/4550

Appendix A: Result tables

Table 4: Minimum QKD operational lead time to secure key availability condition with OTP encryption for varying distance, number of signals and sampling frequency. Single precision ($p = 32$ bits/value). Times determined from running the optimization algorithm on QKD data.

Distance (km)	Minimum Time (min)					
	$N = 68$			$N = 2000$		
	$f_s = 1$ Hz	$f_s = 10$ Hz	$f_s = 20$ Hz	$f_s = 1$ Hz	$f_s = 10$ Hz	$f_s = 20$ Hz
50	2	2	2	2	-	-
51	2	2	2	2	-	-
52	2	2	2	2	-	-
54	2	2	2	2	-	-
58	2	2	2	2	-	-
66	3	3	3	3	-	-
70	4	4	4	4	-	-
75	4	4	4	4	-	-
82	6	6	6	6	-	-
90	8	8	8	-	-	-
95	10	10	-	-	-	-
100	12	12	-	-	-	-
105	14	17	-	-	-	-
110	16	-	-	-	-	-
115	21	-	-	-	-	-
120	24	-	-	-	-	-
125	30	-	-	-	-	-
130	34	-	-	-	-	-
135	41	-	-	-	-	-
140	-	-	-	-	-	-
145	-	-	-	-	-	-

Table 5: Minimum QKD operational lead time to secure key availability condition (AES-256 with 128-bit IV, $p = 32$ bits)

Distance (km)	Minimum lead time (minutes)		
	$f_s = 1$ Hz	$f_s = 10$ Hz	$f_s = 20$ Hz
50	2	2	2
51	2	2	2
52	2	2	2
54	2	2	2
58	2	2	2
66	3	3	3
70	4	4	4
75	4	4	4
82	6	6	6
90	8	8	8
95	10	10	10
100	12	12	12
105	14	15	15
110	16	16	16
115	21	21	21
120	24	24	24
125	30	30	-
130	34	34	-
135	41	-	-
140	50	-	-
145	-	-	-

Table 6: System uptimes post QKD failure for various configurations. QKD lead time assigned in each configuration is the optimal value according to Table 4. QKD failure occurs with one-hour difference from the beginning of secure communication $t_{\text{fail}} = t_{\text{lead}} + 1h$. (OTP, $p = 32$ bits).

Distance (km)	Time to failure (hours)					
	$N = 68$			$N = 2000$		
	$f_s = 1$ Hz	$f_s = 10$ Hz	$f_s = 20$ Hz	$f_s = 1$ Hz	$f_s = 10$ Hz	$f_s = 20$ Hz
50	149.1311	14.0131	6.5066	4.1044	-	-
51	149.5491	14.0549	6.5275	4.1186	-	-
52	141.9219	13.2922	6.1461	3.8592	-	-
54	145.8739	13.6874	6.3437	3.9936	-	-
58	107.0347	9.8035	4.4017	2.6731	-	-
66	70.7764	6.1776	2.5888	1.4403	-	-
70	62.0944	5.3094	2.1547	1.1450	-	-
75	47.3700	3.8370	1.4185	0.6444	-	-
82	33.9222	2.4922	0.7461	0.1872	-	-
90	21.0992	1.2099	0.1050	-	-	-
95	15.8936	0.6893	-	-	-	-
100	13.0036	0.4004	-	-	-	-
105	10.9525	0.1953	-	-	-	-
110	7.1519	-	-	-	-	-
115	7.0978	-	-	-	-	-
120	4.2144	-	-	-	-	-
125	3.0753	-	-	-	-	-
130	1.5119	-	-	-	-	-
135	0.9794	-	-	-	-	-
140	-	-	-	-	-	-
145	-	-	-	-	-	-

Table 7: System uptimes post QKD failure for various configurations. QKD lead time assigned in each configuration is the optimal value according to Table 5. QKD failure occurs with one-hour difference from the beginning of secure communication (AES-256, $p = 32$ bits).

Distance (km)	Time to failure (hours)		
	$f_s = 1$ Hz	$f_s = 10$ Hz	$f_s = 20$ Hz
50	849.7436	84.0744	41.5372
51	852.1128	84.3113	41.6556
52	808.8911	79.9891	39.4946
54	831.2864	82.2286	40.6143
58	611.1981	60.2198	29.6099
66	405.7328	39.6733	19.3366
70	356.5353	34.7535	16.8768
75	273.0969	26.4097	12.7048
82	196.8928	18.7893	8.8946
90	124.2297	11.5230	5.2615
95	94.7317	8.5731	3.7866
100	78.3547	6.9355	2.9677
105	66.7317	5.7732	2.3866
110	45.1953	3.6196	1.3098
115	44.8875	3.5887	1.2944
120	28.5483	1.9549	0.4774
125	22.0944	1.3094	-
130	13.2350	0.4235	-
135	10.2181	-	-
140	0.9214	-	-
145	-	-	-

Table 8: System uptimes post QKD failure for various configurations. QKD lead time assigned in each configuration is the optimal value according to Table 4. QKD failure occurs with one-hour difference from the beginning of secure communication. Encryption algorithm switches from OTP to AES-256 at the time of QKD failure.

Distance (km)	Time to failure (hours)			
	$f_s = 1$ Hz ($N = 68$)	$f_s = 10$ Hz ($N = 68$)	$f_s = 20$ Hz ($N = 68$)	f_s=1 Hz ($N = 2,000$)
50	845.0769	79.4077	36.8705	684.0769
51	847.4461	79.6446	36.9890	686.4461
52	804.2244	75.3224	34.8279	643.2244
54	826.6197	77.5620	35.9477	665.6197
58	606.5314	55.5531	24.9432	445.5314
66	401.0661	35.0066	14.6700	240.0661
70	351.8686	30.0869	12.2101	190.8686
75	268.4303	21.7430	8.0382	107.4303
82	192.2261	14.1226	4.2280	31.2261
90	119.5631	6.8563	0.5948	-
95	90.0650	3.9063	-	-
100	73.6881	2.2688	-	-
105	62.0650	1.1067	-	-
110	40.5286	-	-	-
115	40.2208	-	-	-
120	23.8817	-	-	-
125	17.4278	-	-	-
130	8.5683	-	-	-
135	5.5514	-	-	-
140	-	-	-	-
145	-	-	-	-