

Obfuscated Quantum and Post-Quantum Cryptography

Anju Rani*, Xiaoyu Ai*, Aman Gupta*, Ravi Singh Adhikari* and Robert Malaney*

Abstract—In this work, we present an experimental deployment of a new design for combined quantum key distribution (QKD) and post-quantum cryptography (PQC). Novel to our system is the dynamic obfuscation of the QKD-PQC sequence of operations, the number of operations, and parameters related to the operations; coupled to the integration of a GPS-free quantum synchronization protocol within the QKD process. We compare the performance and overhead of our QKD-PQC system relative to a standard QKD system with one-time pad encryption, demonstrating that our design can operate in real time with little additional overhead caused by the new security features. Since our system can offer additional defensive strategies against a wide spectrum of practical attacks that undermine deployed QKD, PQC, and certain combinations of these two primitives, we suggest that our design represents one of the most secure communication systems currently available. Given the dynamic nature of its obfuscation attributes, our new system can also be adapted in the field to defeat yet-to-be-discovered practical attacks.

Index Terms—Quantum key distribution, quantum communication, post-quantum cryptography, entanglement

I. INTRODUCTION

The advancement of quantum computing poses a significant threat to the classical cryptographic algorithms widely used today. Algorithms based on the integer factorization problem, the discrete logarithm problem, and the elliptic-curve discrete logarithm problem are all vulnerable to a quantum adversary (someone equipped with a sufficiently powerful quantum computer) and can be broken in polynomial time [1]. Consequently, cryptographic solutions resistant to quantum algorithms are essential, not only to safeguard future communication infrastructures but also to ensure secure key distribution and data protection across emerging quantum networks [2]. The two primary strategies that have been proposed to address these challenges are quantum key distribution (QKD) and post-quantum cryptography (PQC).

QKD, in principle, enables information-theoretic secure communication between two legitimate parties even in the presence of an adversarial eavesdropper. Unlike classical cryptography methods that rely on computational hardness of the relevant mathematical problems, QKD leverages inherent quantum features, such as the no-cloning theorem, indistinguishability of non-orthogonal quantum states, and quantum entanglement, to achieve information-theoretic security, offering provable guarantees that remain valid regardless

of an adversary's computational power. QKD has achieved significant milestones in global deployment, including high secret key generation rates [3, 4], long-distance quantum communication [5, 6], photonic integration [7, 8], and the development of terrestrial and satellite-based quantum networks [9]. Since the implementation of the original prepare-and-measure QKD protocol [10] and the entanglement-based protocol [11], many new QKD protocols have been proposed (for a review, see [12]). However, the *practical* implementation of any QKD protocol continues to face ongoing debates in terms of the real-world security it currently provides [13, 14]. These debates generally focus on the fact that any implementation of QKD can generate imperfections and loopholes, due to deviations from the mathematical assumptions underpinning the chosen protocol [15–17]. It is important to recall that a prerequisite for all QKD protocols is the presence of a pre-shared key (PSK) known only to the sender-receiver pair (the reason why QKD is termed a *key-growing* protocol).

The alternative to QKD, namely PQC, encompasses various cryptographic families, including lattice-based, hash-based, code-based, multivariate, and isogeny schemes. PQC does not provide information-theoretic security, but remains, as far as we currently know, computationally secure against a quantum adversary; a form of security we henceforth refer to as quantum resistant security. Assuming that a shared symmetric secret key is available of at least 256 bits length, the Advanced Encryption Standard (AES) is also known to be quantum resistant [18]. However, there are still vulnerabilities. For example, the most modern encryption schemes used in transport layer security (TLS) v1.3, AES-Galois Counter Mode and AES-Counter have been shown to be vulnerable in implementation [19–25]. Concerning scenarios where no such symmetric key is *a priori* available, multiple protocols are being investigated. The National Institute of Standards and Technology has announced the candidate lists for the key exchange and digital signature schemes for standardization [26]. Among the five selected schemes, CRYSTALS-Kyber [27] and HQC [28] are selected as key encapsulation schemes, and CRYSTALS Dilithium [29], FALCON [30], and SPHINCS+ [31] are the three selected digital signature schemes. Similarly to QKD and AES, the implementation of any PQC protocol will always give rise to the possibility of attack avenues. For more details on the status of PQC, the challenges faced, and the threats in implementation, the reader is referred to [32–34].

Considering the practical limitations perceived in both

*Anju Rani, Xiaoyu Ai, Aman Gupta, Ravi Singh Adhikari, and Robert Malaney are with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia.

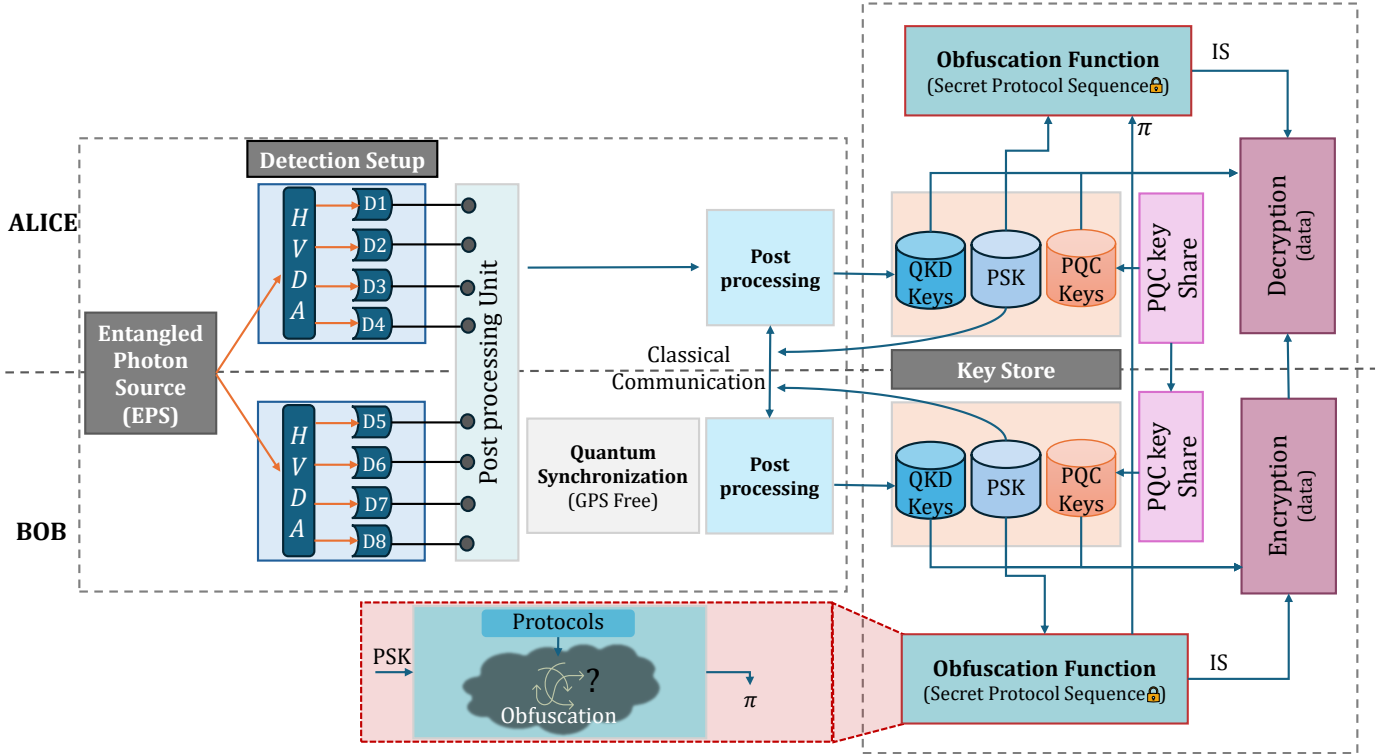


Fig. 1: The experimental setup and the combined QKD-PQC encryption-decryption module. This includes the optical setup with single photon detectors D1 through D4 at Alice detecting the horizontal (H), vertical (V), diagonal (D), or anti-diagonal (A) basis states, respectively (D5 through D8 similarly for Bob); and the post-processing unit, followed by quantum synchronization embedded within the QKD process. A software-implemented obfuscation function is used to determine a secret mode of system operations and settings, provided as an instruction sequence (IS), which is encrypted to form π (an encrypted message (or identifier) sent from Bob to Alice so that the IS is known only to them). An example IS could be the type and order of the encryption-decryption protocols. Critical to the experiment is the pre-shared key (PSK), assumed to be known only to the data sender (Bob) and data receiver (Alice) and *a priori* shared between them. Part of the PSK is required for QKD, part for our obfuscation function, and part for AES. The EPS is external to both Alice and Bob. The bottom centred box (pink) illustrates the internal operations carried out within the obfuscation function module (bottom-blue box).

QKD and PQC, several hybrid QKD-PQC¹ schemes have emerged in recent years. Some works combine QKD and PQC keys into a single new key [35–44], some use PQC to authenticate or establish trust within QKD [45–49], and some use PQC encryption for security coupled with QKD encryption for route anonymity [50]. Other works use PQC-encrypted reconciliation information to improve the secret key rates of QKD [51], use QKD as a seed generator to improve the security of PQC [52], discuss how quantum random number generators can improve the combination of QKD and PQC [53], or consider the advantages of distributed architectures to the QKD-PQC paradigm [54]. These hybrid schemes offer the potential advantage of QKD’s information-theoretic security alongside the quantum resistant security of the PQC schemes - and point to a paradigm for real-world communication security in the quantum computing era. If a successful attack on one primitive is available (for example, due to a flawed implementation), the other primitive still provides its inherent security. *In this work, we take this paradigm one step further and introduce an information-theoretic secure obfuscation of the system-level configuration*

setting that instructs how to combine the QKD and PQC primitives. One key outcome of this is that only the data sender and data receiver are aware of the sequence and number of the QKD and PQC implementations, as well as the important parameters of each primitive. Although this new obfuscation is redundant to any user when QKD is perfectly implemented and redundant to a classical-only user when PQC is perfectly implemented, the additional layer of security allows for the foiling of known practical attacks jointly on each primitive in addition to enhanced protection against yet-to-be-discovered practical attacks on each primitive.

The work presented here builds on our previous experiments [55] which demonstrated a QKD-PQC implementation that sequentially combines a QKD primitive based on BBM92 with quantum resistant AES (with a 256-bit key). Here, we extend that work by not only introducing the aforementioned obfuscation of the QKD-PQC configuration setup, but also the integration of a self-synchronizing mechanism in our QKD key generation system that eliminates the dependence on the global positioning system (GPS) or other classical synchronization methods. Our synchronization protocol utilizes the tight temporal correlation (at birth) of pairs of polarization-entangled photons. This provides for an additional level of time-based security against an intercept-resend attack, albeit one that is not information-theoretic secure (see the later

¹A note on terminology: The term ‘QKD-PQC’ will henceforth be used in this work to cover combinations of QKD, coupled to one or more quantum resistant algorithms. Quantum resistant AES is not formally classified as a member of the PQC family. However, we will ignore such definitional formalities in our use of the term ‘QKD-PQC’.

discussion). Also, by integrating time synchronization and QKD, we can significantly reduce hardware overhead. The new integrated QKD-PQC and quantum synchronized system that we implement is shown in Fig. 1. We suggest that this system represents the most secure practical communication system currently available.

The remainder of this paper is structured as follows. Sec. II-A provides the experimental implementation of the QKD protocol, including the details of our synchronization algorithm. Sec. II-C explains the design of our combined quantum and post-quantum system, and Sec. III presents the results, with a focus on the penalty in time incurred by the inclusion of QKD-PQC obfuscation. Finally, Sec. IV concludes with some remarks on our findings.

II. SYSTEM MODEL

As described above, our system is useful *relative to existing QKD-PQC architectures*, only on the premise that the normal information-theoretic security of the QKD keys is not applicable and that the quantum-resistant security of a single-use PQC primitive is not applicable. As such, our additional security is not formally defined, and is best described as an additional resource challenge to the adversary. For example, in the presence of two side-channel attacks that render our premise valid, the adversary is challenged on two new fronts: (i) She must consider all possible combinations of parameters and sequence primitives allowed by the system; and then (ii) find a series of side-channel attacks that would be successful against a significant fraction of those combinations (on average 1/2). The only portion of our system under our attack premise that can be information-theoretic secure is the security of the instruction sequence (the combinations) itself.

A. QKD Implementation

We implement an entangled version of QKD, namely BBM92 [56]. In entanglement-based QKD, the source can be an intermediary device that distributes highly correlated photons to two separate parties, Alice and Bob, via two independent quantum channels, which in our setup are largely free-space channels. Our prototype QKD system is eventually aimed at low Earth orbit deployment, in which case the entangled photon source (EPS) will be on board a satellite communicating to two widely separated ground stations. As a consequence of the tight temporal correlation at pair production, the EPS offers additional advantages to our QKD system through a GPS-free synchronization protocol, something of importance for satellite systems. Therefore, unless otherwise stated, in the following we assume that the EPS is embedded on a satellite (or other detached third-party system communicating through free space). For fiber-based QKD implementations, the reader is referred to one of the many papers in this area [57]. For fiber-based time synchronization, see [58].

Our EPS (fiber-coupled prior to launch into free space) is used to generate polarization-entangled photon pairs, known as the signal and idler. The state produced by our source is given by $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_{sig}|V\rangle_{id} + |V\rangle_{sig}|H\rangle_{id})$, where $|H\rangle_{sig}$ and $|V\rangle_{sig}$ represent horizontally and vertically polarized photons, respectively; and the subscripts *sig* and *id* indicate the signal and idler, respectively. The photon pairs co-propagate in free space and are separated and distributed to Alice and Bob.

The received photons at Alice and Bob are measured by projecting their polarization states onto four basis states, $\{H, V, D, A\}$, using four single-photon detectors. Here, *H*, *V*, *D*, and *A* represent the horizontal, vertical, diagonal, and anti-diagonal polarization basis states, respectively. The detected photons and their arrival times are recorded for post-processing and subsequent generation of the QKD keys. The post-processing hardware unit consists of a time tagging device with an inbuilt field programmable gate array (FPGA) unit, as shown in Fig. 1. Alice and Bob (two personal computers) also perform post-processing steps, including interactive time domain filtering, sifting, QBER estimation, error correction, and privacy amplification. More details on the post-processing follow, in which a QKD ‘session’ is defined as over by the completion of the privacy amplification described below.

Bit Mapping and Sifting: Once signal acquisition is completed, the arrival times of photons registered from each detector are placed in time tag arrays t_a and t_b at Alice and Bob, respectively. This information must first be corrected for any synchronization errors (see II-B). Once the time tag arrays are synchronized, Alice determines two bits for each time tag in t_a that indicate which of her four detectors registers the pulse (similar for Bob). The first mapped bit (corresponding to *H*, *V*, *D*, *A*) is then stored in a bit array, k_a (k_b for Bob), and the second bit (corresponding to the basis used) is stored in an array, b_a (b_b for Bob). Let the length of k_a and k_b be N_{raw} at this point. To perform the basis sifting, Alice and Bob exchange their b_a and b_b via classical communications - only bits measured in the same basis are retained. Each step performed through classical communication undergoes encryption as described by an instruction sequence (discussed later). The length of the remaining k_a and k_b will be on average, $N_{raw}/2$.

QBER Estimation: In this step, Alice randomly selects a subset (with the size of $N_{raw}/4$) of bits from k_a and sends them to Bob, who then compares these received bits with his corresponding bits in k_b and estimates the QBER (denoted by Q). Next, Bob discards the bits used in the comparison and informs Alice of the estimated QBER. Alice then also removes the selected bits from k_a . We denote the length of k_a and k_b by the end of this step as N .

Reconciliation with Message Authentication Codes (MAC): The bit vectors k_a and k_b are generally not identical due to quantum channel noise, time-tag errors, and synchronization errors. To reconcile the keys, a syndrome decoding technique based on an appropriate error correction code is adopted. Authentication in reconciliation is achieved through a Wegman-Carter MAC (WC-MAC) [59], which is an

information-theoretic many-time-MAC scheme. We note that the advantage of using this MAC in QKD is that it consumes only $\log_2(l^{sb})$ bit keys from the previous QKD session, where l^{sb} is the length of the syndrome, s_b .

Privacy Amplification: Assuming a successful reconciliation, Alice and Bob will have two identical bit vectors. In the privacy amplification step, they extract QKD keys from these bit vectors. Specifically, Alice first computes the QKD key rate, r , in bits per pulse, using the asymptotic analysis of the BBM92 protocol [60, 61]: $r = 1 - h(Q) - L$, where h is the binary entropy function, $L = 1 - R_c$, is the ratio of the information disclosed to Eve during the error correction step to the length N . Note, $R_c = (N - l^{sb})/N = 1 - f_E h(Q)$, where $f_E = l^{sb}/(Nh(Q))$ is the reconciliation efficiency of the code. Then, Bob will follow the instructions described in [62] to construct a 2-universal hashing matrix, \mathbf{T} , with the dimension of $\lceil rN \rceil$ -by- N and send \mathbf{T} to Alice. Finally, both parties generate their respective secret keys by multiplying their reconciled bit vectors with the matrix \mathbf{T} .

B. QKD Synchronization

In QKD protocols, precise time synchronization improves secure key generation by improving the signal-to-noise ratio, thus lowering the QBER [63–69]. As such, we introduce such a protocol into our system here. Our synchronization protocol, which comprises combining algorithms 1 and 2 in the appendix, estimates a relative time offset (τ) and time drift (τ_{drift}) between Alice and Bob. This must be done prior to the commencement of QKD, otherwise the QKD will likely fail. Bob performs a two-step synchronization procedure between Alice’s time tag array t_a and Bob’s time tag array t_b . To achieve this, these time tag arrays are manipulated sequentially into a series of significantly shorter time tag arrays \hat{t}_a and \hat{t}_b for Alice and Bob, respectively. Each shorter time tag array is associated with a ‘round,’ a number which specifies the creation order (first tag, round 1; second tag, round 2, etc.); and spans an acquisition period T_{acq} , meaning that a time difference between its first and last time tag is approximately T_{acq} . Note that to protect against a time tag attack [70], Alice encrypts her time tag information using some specific instruction sequence to form t_a^* , and sends this encrypted information to Bob, who decrypts.

The first step of the synchronization protocol performs a coarse alignment (see algorithm 1 in the appendix), where Bob performs a cross-correlation scan between \hat{t}_a and \hat{t}_b over a range $R < T_{acq}$, using a fixed step size $\delta < R$. This leads to the first estimate of τ , which we refer to as τ_{coarse} . Note that this coarse alignment is performed only once during initialization (the first round). Bob then performs a second step commencing in the first round, the fine alignment (see algorithm 2 in the appendix). Here, the cumulative offset τ_{accum} is defined as the total relative offset accumulated during previous rounds (set to zero during the first round). The fine alignment estimates the relative time offset τ more precisely, updates Bob’s shorter time tag array to \hat{t}_b , and updates the cumulative

offset τ_{accum} . Algorithm 2 also automatically detects the time drift τ_{drift} and eliminates it.

Our synchronization protocol is similar to that reported in [67]. However, here we incorporate a step-size scan during the first round, making it less vulnerable to large time offsets, such as those possible in Earth-to-satellite channels (target channels for our prototype). The synchronization procedure is highly parallelizable (and is implemented as such), making it faster for scanning a wide range of possible time offsets. Our protocol enables real-time implementation, is easy to implement in QKD systems, offers flexibility and robustness in real-world conditions, and is sufficient for entanglement-based key distribution. However, it is the encapsulation of our synchronization protocol within a general QKD-PQC framework that is of main interest here. QKD encryption of the time tag information, although information-theoretic secure, would be expensive due to the large amount of time tag information, likely absorbing more QKD key than produced by the QKD protocol. In [71], 128-bit AES encryption is used, with QKD keys only used as a seed as a means to bypass this issue, a process that is not information-theoretic secure. However, our obfuscated encryption of the time tag information allows up to $2^{N_{obs}}$ obfuscated encryption configurations to be used, adding an additional layer of pragmatic security to synchronization.

In addition to the benefits offered to the communications through our enhanced synchronization (e.g., freedom from GPS spoofing and enhanced throughput), the tighter correlation in time of the arriving photons at Alice and Bob provides a layer of enhanced timing-based security. Due to the conservation of energy and momentum, the creation of the photon pairs via the spontaneous parametric down-conversion (SPDC) of a pump photon into a signal and idler pair often results in more temporal correlation than could be expected from separate sources. For example, for conditions similar to our hardware, the work of [72] has demonstrated a time correlation of order 100 fs (femtoseconds) between photons produced via SPDC. It is also shown that this corresponds to a violation of more than 100 standard deviations from the uncertainty relation that two classical light pulses must satisfy [72]. This extraordinary coupling of times of arrival of the photons at Alice and Bob leads to an enhanced level of security for our QKD system as an attacker must be able to complete their measurements and resending of the photons in shorter timescales. This enhanced security is in addition to the security already offered in our system through the encryption of Alice’s time tagging information referred to earlier. In the circumstance where the photon pairs remain jointly entangled in polarization and in frequency, additional timing-based security becomes available in our system since, conditioned on both photons being detected by Alice and Bob, the increased spread in energy of the entangled-pair state leads to improved received timing correlations [73]. However, we do point out that although intrinsically embedded in our system, taking advantage of the above enhanced correlations in time would require detector time resolutions beyond those used in our current experimental setup.

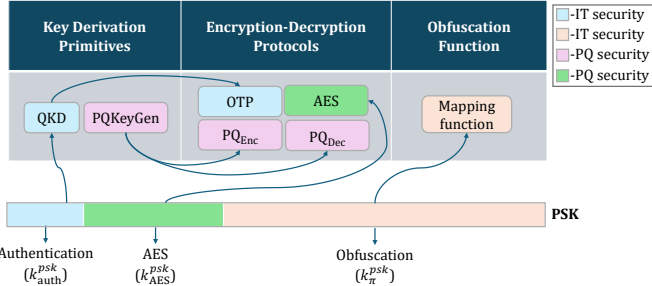


Fig. 2: A schematic of the logical flow between the PSK and the different elements of our architecture. The first portion of the PSK is used for QKD authentication. As per normal usage within QKD, when this is exhausted, the new grown QKD key is utilised for ongoing authentication. For AES, the PSK is only used to form a symmetric key. IT refers to information-theoretic security, and PQ refers to quantum-resistant security. π denotes the encrypted identifier for an instruction sequence.

C. Hybrid Quantum and Post Quantum Design

Our architecture comprises QKD and PQC key derivation primitives (KDPs) that generate symmetric QKD keys and asymmetric PQC keys. We also use a subset of a PSK to generate an encrypted sequence of instructions that inform Alice and Bob of the type and order of the encryption-decryption protocols. Additionally, the keys from different KDPs do not combine to generate a hybrid key; instead, a series of encryptions (and their corresponding decryptions) using different keys derived from the KDPs are performed. The proposed architecture ensures information-theoretical security in an ideal operational scenario and quantum-resistant security as long as at least one primitive is not compromised. An overview of our security architecture is presented in Fig. 2, where the interface between the PSK and the different elements of the architecture is shown. Note that henceforth, when we refer to AES we will mean 256-bit AES, unless otherwise specified.

The length of the PSK, of course, will dictate the complexity of the overall configuration settings. An important parameter is N_{obs} , the number of bits available for obfuscation. Regarding the instruction sequence (IS), this will allow for up to $2^{N_{obs}}$ independent IS possibilities. There are several methods for the system to decide on the different forms of the IS. They can be set *a priori* between Alice and Bob in a secured environment (the same environment in which the PSK is set). However, this does not offer dynamic behaviour (re-adjustment of the configuration settings in the field), instead necessitating a permanent fix of the settings for a pair of devices. In contrast, Bob (the data sender in our system) could encrypt all aspects of the configuration settings in an encrypted message to Alice. This allows for the maximum flexibility and maximum dynamic behaviour, since no configuration settings are pre-set by Alice or Bob (but this will normally allow for less than $2^{N_{obs}}$ configurations to be used). A third possibility is that an *a priori* look-up table could be set and made publicly available where the configuration settings are preset and linked to a unique label (identifier), this label being then encrypted and sent from Bob to Alice. For clarity of exposition, in the following we assume the latter mode of operation to be the

case. This chosen operation offers the possibility of dynamic behaviour, albeit from a set of prearranged settings. So that not all the obfuscation key is consumed in one cycle, we set a new length, $\hat{N}_{obs} \ll N_{obs}$, and consume only \hat{N}_{obs} of key bits per cycle (per one use of the look-up table).

In general, the IS could contain any information related to the configuration, such as the parameters for any protocol, and instructions on how to encrypt/decrypt time tag information. However, for clarity, we discuss in detail a specific implementation of the generic framework provided in Fig. 2. In this specific implementation, we assume that the IS is constructed only from the three underlying primitives (with set parameters) and that the time tag information (and other classical communications associated with QKD reconciliation) are encrypted only using AES. Our specific implementation, shown in Fig. 3, possesses two sets of keys. The first set of keys, namely, k_{auth}^{psk} , k_{AES}^{psk} , k_{π}^{psk} , are used for the authentication in QKD reconciliation, AES encryption of classical data communicated and the derivation of the encrypted identifier of IS, respectively. Note that the encrypted identifier is denoted by π , and OTP encryption is used to encrypt the identifier. The IS can be written as $(\xi_1, \xi_2, \dots, \xi_n)$, where $\xi_i \in \{\text{OTP, AES, PQ}_{Enc}\}$ and $i = (1, 2, \dots, n)$, where n is the number of encryption-decryption protocols to be applied to the data (the data is the actual message M communicated from Bob to Alice that the entire system is set up to protect). The second set of keys, denoted by k_{ξ_i} , is used by the encryption protocols (ξ_i), and if the decryption protocol is used then the corresponding decryption keys are represented by \bar{k}_{ξ_i} , where $\bar{\xi}_i \in \{\text{OTP, AES, PQ}_{Dec}\}$ are the corresponding decryption protocols.

Fig. 3 describes the flow chart of the specific protocol, assuming Bob is the sender of the data M while Alice is the receiver of M . The steps are summarized below, where one ‘cycle’ of the QKD-PQC setup is the completion of steps (1)-(5) below.

1) *Handshake*: Alice and Bob perform an initialization handshake; they share the required system configurations (e.g., security parameters, FPGA parameters, and post-processing parameters). They also choose N_{AES} bits from k_{AES}^{psk} , since in this specific protocol time tags and some other classical communications (e.g., reconciliation information) are always encrypted with AES.

2) *Obfuscation Function*: Bob derives an IS from $2^{\hat{N}_{obs}}$ possible instructions. Next, Bob uses a mapping table f_{Map} (publicly available) to obtain an identifier for the IS. He encrypts this identifier by XORing with \hat{N}_{obs} bits of k_{π}^{psk} to generate π , which Alice decrypts upon receiving to obtain the same IS.

3) *QKD Key Derivation*: Here, the QKD protocol, as described in Sec. II-A, is used to establish the QKD keys between Alice and Bob. In Fig. 3, the process of obtaining the time tag from detecting a quantum signal is denoted by the SignalDetection() function and the post-processing step is denoted by QKD_KDP. The symbols in the figure corresponding to this step are denoted in Sec. II-A. Note that

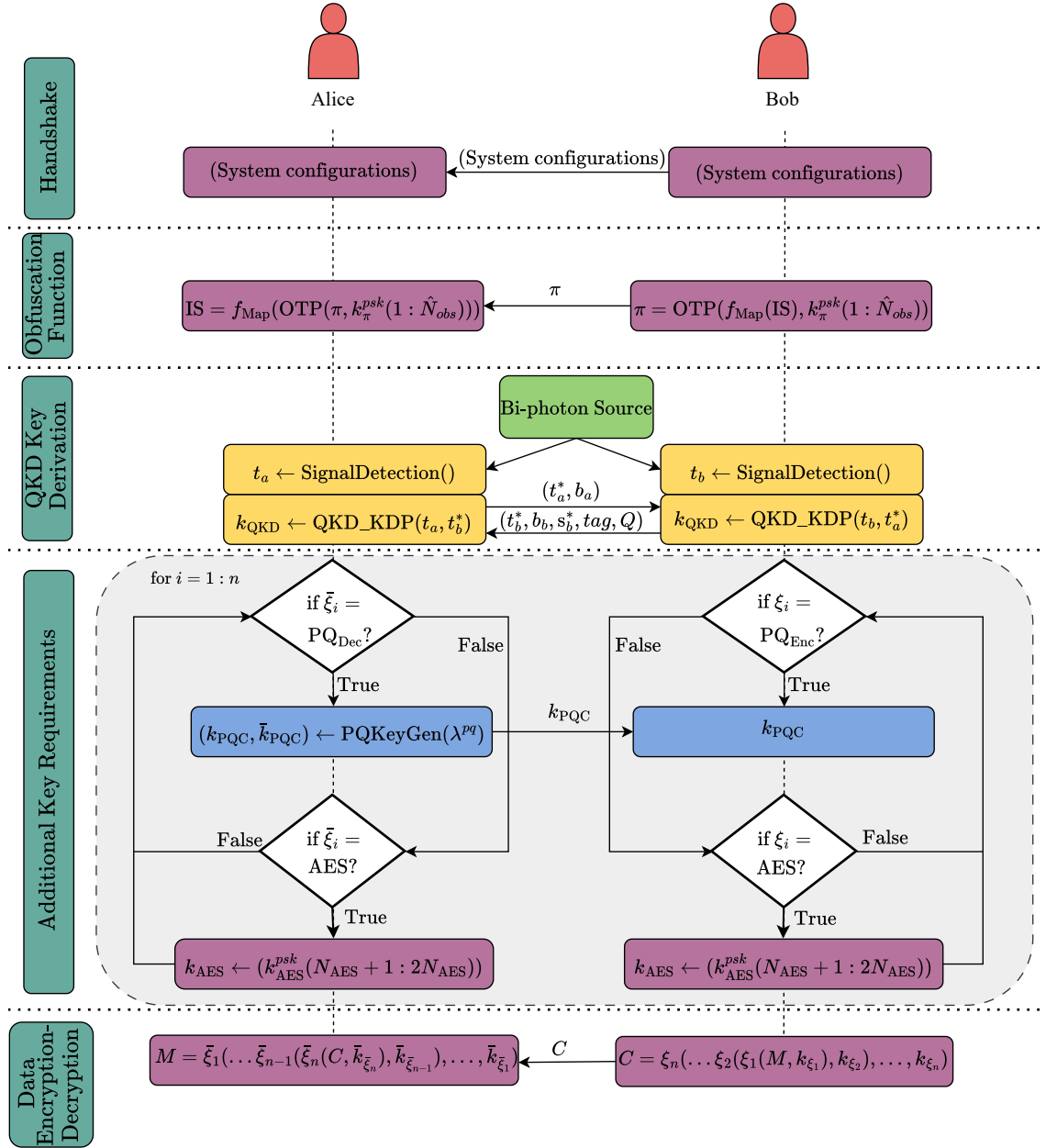


Fig. 3: The flowchart describes one cycle of a proposed QKD-PQC system. In the figure, it is assumed that Bob intends to communicate a data message (M) to Alice. The term $k_{\pi}^{\text{psk}}(1 : \hat{N}_{\text{obs}})$ is used to represent that the next \hat{N}_{obs} number of unused bits are taken from PSK. Similarly, the term $k_{\text{AES}}^{\text{psk}}(N_{\text{AES}} + 1 : 2N_{\text{AES}})$ is used to represent that the next N_{AES} bits are used for all data encryption-decryption, where the IS contains AES (the first N_{AES} are used for encryption-decryption in QKD reconciliation). The output of $f_{\text{Map}}(\text{IS})$ is an identifier associated with the instruction sequence that is obtained from the mapping table. The output of Data Encryption obtained via algorithm 3 (the decryption is done with algorithm 4) is the ciphertext denoted by C .

encrypted time tag arrays are shown as t_a^*, t_b^* and encrypted syndrome as s_b^* .

4) *Additional Key Requirements:* This step depends on the IS contents. If the IS contains the element PQ_Dec , then Alice generates the asymmetric keys $(k_{\text{PQC}}, \bar{k}_{\text{PQC}})$ using the post-quantum key generation function PQKeyGen [74] with the security strength² λ^{pq} and sends the public key k_{PQC} to Bob. If the IS contains the AES element, then Alice and Bob obtain the next N_{AES} bits of $k_{\text{AES}}^{\text{psk}}$ to form the key k_{AES} .

²Security strength is a number associated with the amount of work (the number of operations) that is required to break a cryptographic algorithm or system [75]. It is generally a value of the set $\{80, 112, 128, 192, 256, \dots\}$.

5) *Data Encryption-Decryption:* At this stage, all the desired keys and instructions are generated. Bob encrypts a data message according to the IS using the algorithm 3 and sends the ciphertext to Alice, which she decrypts using the reverse of the IS via the algorithm 4. This completes a cycle of our cryptographic architecture (many QKD sessions could reside within one QKD-PQC cycle).

D. System Advantages

As mentioned earlier, the encrypted sequence of operations can provide additional burden (thereby providing

additional security) on a successful attacker who may have arrived at independent side-channel attacks on QKD and PQC, rendering other hybrid QKD-PQC systems vulnerable. An example scenario would be a successful attack on QKD through a power analysis [76], coupled to a successful power analysis attack on PQC [77, 78]. By providing $2^{N_{obs}}$ potential sequences of encryptions (some of which may include a series of multiple encryptions beyond two), currently successful power analysis attacks become ineffective with high probability. A similar argument could be formed based on time analysis attacks on QKD [79] and PQC [80]. In addition, even though both QKD and PQC are safe against ciphertext-only attacks, if other side-channel attacks, such as those mentioned above, are successful, a ciphertext-only attack has a chance of succeeding in other hybrid QKD-PQC systems, but it is ineffective in our system with high probability.

Beyond the system model adopted here, the use of an IS for obfuscation can also be applied to different hybrid QKD-PQC configurations, different QKD protocols, different photon sources, different physical channels, and different hardware. The photon source (sources) may be embedded in Alice or (and) Bob. The use of an IS can also be applied outside the post-processing stage. For example, a host of side channel attacks can be specific to the QKD hardware (or channel) and possibly be relevant in different phases of the QKD protocol (for the BBM92 protocol, these are listed in [81]). Extended systems can address such side-channel attacks through various means, such as setting intermittent use of the quantum channels for purposes beyond QKD or setting detector parameters, with the information necessary to coordinate these settings being secretly communicated as part of the IS. We do not claim that our approach is the only method to counter hardware-based side-channel attacks: rather, we offer a more flexible and easy-to-implement solution.

III. RESULTS AND DISCUSSION

We implemented a fully integrated real-time prototype QKD-PQC system in laboratory settings. The time synchronization for QKD is done by performing a cross-correlation analysis between the detection events at the different parties receiving entangled photons. The QKD experiment is conducted over a channel length of 1.5 m. An experimental loss of 10.3 dB is measured for the signal, accounting for transmission, optical, and detection losses. The EPS (QES2, Qubitekk) provides tunability over power and temperature, and can be configured for both degenerate and non-degenerate cases. In our setup, the source is configured for the degenerate case producing a degenerate signal and idler pair at 810 nm. The power of the source is varied and visibility is calculated for different power values to optimize the source for maximum visibility and count rate (see results in [55]). In our case, the source is set at a power value of milliwatts, achieving a coincidence rate of $10,000 \text{ s}^{-1}$ (just after the source, measured in fiber). The visibility of the source at the set power value is measured as 0.873 ± 0.019 . The detection efficiency of the detectors is 65% (Excelitas, SPCM-AQRH-14) with a

background count of 100 s^{-1} . The time tagging device is the OPX+ from Quantum Machines, which also serves as our post-processing unit and consists of an onboard FPGA with a timing resolution of 1 ns. For QKD reconciliation, a low density parity check matrix is adopted based on the progressive edge growth algorithm in [82] with a code rate $R_c = 0.5$, and degree distributions optimized for QKD as described in [83]. The length of N_{raw} is set to 40,000. Both the post-processing and the PQC module are handled in personal computers with 16 GB RAM and a 2.9 GHz clock speed GPU for both Alice and Bob. The PQC key generation and encryption-decryption modules are taken from the Post Quantum Safe Lib module [84], and the post-processing module was developed in MATLAB v2021.

We examined the impact of timing errors (introduced assuming Gaussian jitter noise in Bob's time tag array t_b) on the performance of the QKD system in terms of the secret key rate (SKR), which is calculated using our key rate equation. Fig. 4 illustrates the critical role played by precise time alignment in optimizing QKD performance. An increased timing error reduces the coincidence detection rate, which in turn increases the QBER and lowers the SKR.

In order to test our synchronization protocol (see appendix), we introduce a 10 ns (nanoseconds) relative time offset τ and a time drift τ_{drift} of 1 ns per 250 ms (milliseconds) in Bob's time tags. The parameter values used in the protocol are detailed in Table I. On average, the protocol takes approximately 5 ms per round, except during the first round, where the coarse alignment step takes approximately 0.5 sec due to heavier processing. In Fig. 5, which highlights the overall performance of the synchronization protocol, the abscissa axis represents a relative delay added to the input time-tag information in order to search for a peak in the correlation between Alice and Bob's input time tag arrays. If there were no synchronization errors in the input information, a peak should be found at zero. However, as we can see, without the application of our synchronization, no coincidence peak is evident in the counts at zero relative delay between Alice and Bob (as shown by the orange scatter points in Fig. 5). Instead, a broad distribution of low coincidence counts is observed in the relative delay range (the increase in counts between -10 ns to -38 ns can be attributed to a partial success in removing the drift component). If such a time tag array were used in QKD without correction, the QKD protocol would fail. Upon applying our synchronization, we remove the relative time offset and the time drift from the time tag array and retrieve a sharp coincidence peak at zero relative delay (as shown by the blue scatter points in Fig. 5) thereby illustrating the success of our protocol. From Fig. 5, we also observe that a coincidence window of 1 ns would be an excellent choice for QKD implementation.

In addition, we compared the performance and overhead of the combined QKD-PQC system. Table II compares the execution times, in seconds, of a standard (stand-alone) QKD system with OTP encryption with our new hybrid QKD-PQC system (with the same settings for the QKD part). To

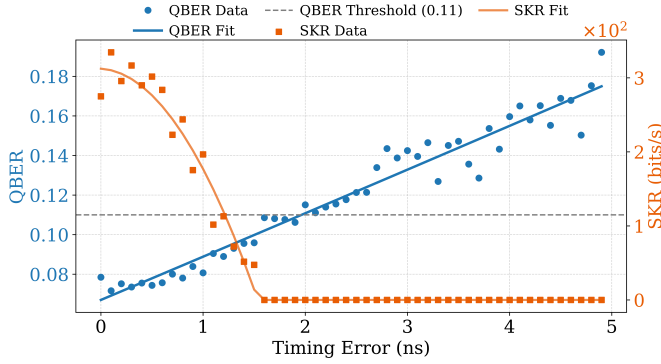


Fig. 4: QBER and SKR as functions of timing error. Due to imperfect reconciliation, SKR drops to zero as QBER exceeds 0.1 (not 0.11). Here, the timing error is the standard deviation of the timing jitter in the photon detectors (Gaussian noise assumed). The coincidence window used to determine the counts is 1 ns. Note, these key rates are upper limits due to the value of N adopted. Approximately a factor of ten more collection time is required for the rates shown to be achievable.

TABLE I: Synchronization Parameters

Parameter	Value
Acquisition period (T_{acq})	50 ms
Coarse scan step size (δ)	200 ns
Coincidence peak width (FWHM)	1 ns
Coarse scan range (R)	± 1 ms
Fine alignment bin width (w)	1 ns

demonstrate the hybrid design in an experimental setting, we used the mapping table f_{Map} , where the four possibilities of identifier \rightarrow IS are: 00 \rightarrow (OTP, AES), 01 \rightarrow (AES, OTP), 10 \rightarrow (OTP, PQ_{Enc}) and 11 \rightarrow (PQ_{Enc} , OTP). This determines $n = 2$ and $\hat{N}_{\text{obs}} = 2$, which sets the number of instruction sequences to be $2^{\hat{N}_{\text{obs}}} = 4$, resulting in the consumption of 2 bits of PSK per cycle to communicate one of the four configuration choices. For AES, we set the symmetric key, $N_{\text{AES}} = 256$ bits. The execution times for each codeblock were recorded over 10 runs and the mean and standard deviations were computed. A stable SKR of 298 ± 59 bits/s was observed and a QBER of 0.0745 ± 0.0047 . The increase in time in the codeblocks from ‘Synchronization’ to ‘Error Correction’ is due to the fact that we perform an additional AES encryption-decryption of classical information in the post-processing step. As can be seen, by the comparison of total times, there is approximately 5.8% overhead on Alice’s side and 5.4% overhead on Bob’s side in execution times in our combined QKD-PQC system compared to a standard QKD with OTP encryption. Assuming that a mapping table f_{Map} is constructed such that, on average asymptotically, an IS contains $n/2$ encryption-decryptations with OTP, $n/2$ with AES and $n/2$ with PQC, the execution time will increase by approximately a factor of $n/2$.

There are many variations and extensions on the actual implementation of the obfuscated hybrid QKD-PQC we have reported here. For example, the use of lossy compression codes (e.g., Universal and Huffman coding) could be invoked to optimize the per bit of PSK used in the obfuscation function. Other modules or parameters that undergo obfuscation could

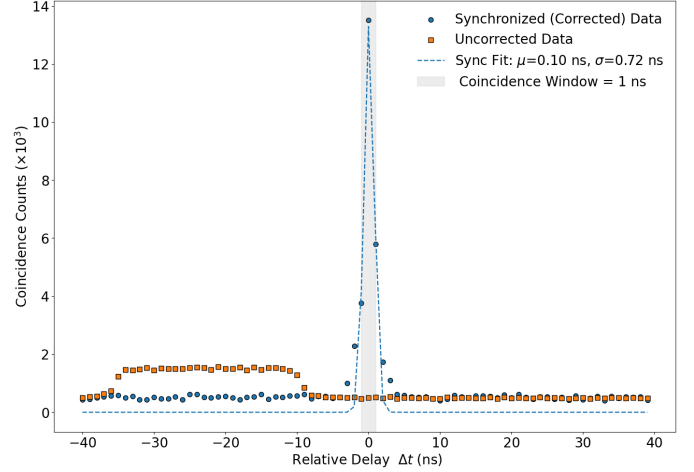


Fig. 5: Coincidence counts as a function of a relative delay, Δt , added to Bob’s time tag information. Counts are shown before (orange) and after (blue) application of the synchronization protocol. For each Δt , coincidences are counted only when Alice’s and Bob’s time tags match within a 0.5 ns window. The input information used here had a time offset of 10 ns and a timing drift of 1 ns per 250 ms applied. The points representing the information after applying our synchronization show a centered coincidence peak at $\Delta t = 0$, indicating the time offset and drift have been successfully removed. The data shown is accumulated over 7 s.

be introduced. Examples of these would be the channel or reconciliation codes used in classical communications and the block length of the codes. These could be invoked through more sophisticated handshake protocol modules. Other protocols could be merged into our system, such as quantum location verification, leading to position-dependent cryptography (e.g., see [85, 86]. The merging of security attributes such as those provided by other hybrid QKD-PQC systems (see Introduction) could be convolved within our system, the anonymous routing of [50] being an example. The full use of photon time correlations, in SPDC creation, for enhanced timing-based security [72] is another avenue for future work. Finally, we have not shown that all possible instruction sequences allowed by our system lead to data transfers that are formally quantum resistant to the same dual side-channel attacks that can make previous QKD-PQC architectures insecure. Formal analyses in this direction would be useful.

IV. CONCLUSION

We proposed a new hybrid cryptographic system that generates QKD and PQC keys whilst obfuscating in an information-theoretic manner both the sequence on how these keys are used and relevant system parameters. We achieved this, in part, by using an encrypted instruction sequence that indicated a specific order of encryption-decryption of data messages. Our system also provided a GPS-free time-synchronization feature within the QKD key generation system. The described system reduces the vulnerability of hybrid QKD-PQC solutions to known (and yet-to-be discovered) simultaneous practical attacks on the underlying cryptographic primitives. We carried out a full experimental deployment, comparing the time overhead of our hybrid system with a standard QKD system, demonstrating the feasibility of the

TABLE II: The mean execution times (in seconds) of a standard QKD system with OTP encryption on both Alice’s side and Bob’s side, compared with the mean execution time of our combined QKD-PQC system for the same message and same system settings on both Alice’s side and Bob’s side. The Classical Communications is the total time taken in the classical communication of information in the QKD post-processing. The synchronization only occurs in Bob’s side; hence, no execution time for synchronization in Alice’s side. The codeblock ‘Message Enc-Dec’ in a standard QKD system corresponds to a simple XOR operation, while in our hybrid system it is the Data Encryption-Decryption defined in step (II-C5) of Sec. II-C.

Codeblock	Standard QKD system with OTP (Time in sec.)		Our QKD-PQC system (Time in sec.)	
	Alice	Bob	Alice	Bob
Signal Accumulation	224.70 ± 4.65	236.01 ± 7.64	188.05 ± 4.84	196.36 ± 6.16
Synchronization	–	0.80 ± 0.13	–	0.90 ± 0.15
Time Tag Filtering	0.0007 ± 0.0001	0.0055 ± 0.0003	17.56 ± 0.24	35.42 ± 2.91
Sifting	0.0009 ± 0.0005	0.0022 ± 0.0034	0.26 ± 0.01	0.42 ± 0.04
QBER Estimation	0.0005 ± 0.0002	0.0007 ± 0.0004	0.0003 ± 0.0001	0.0007 ± 0.0003
Error Correction	0.72 ± 0.11	0.95 ± 0.10	0.69 ± 0.03	1.09 ± 0.25
Privacy Amplification	0.20 ± 0.01	0.21 ± 0.02	0.20 ± 0.01	0.23 ± 0.06
Obfuscation	–	–	0.0003 ± 0.0003	0.0005 ± 0.0008
PQC Key Share	–	–	1.43 ± 0.61	2.13 ± 0.59
Message Enc-Dec	0.0020 ± 0.0003	0.0066 ± 0.0011	0.61 ± 0.51	3.07 ± 1.73
Classical Communications	22.73 ± 2.56	13.55 ± 4.75	54.02 ± 10.73	25.51 ± 4.67
Total time (in sec.)	248.35 ± 5.31	251.52 ± 8.99	262.82 ± 11.80	265.13 ± 8.79

former. Our new architecture illustrates the important role that hybrid systems can play in real-world deployments of the QKD and PQC primitives. Future users of our hybrid QKD-PQC system who remain skeptical about QKD security issues in a practical setting can be assured that the worst-case security outcome for them is enhanced PQC security relative to the level of PQC security they normally accept. Regarding QKD itself, we believe that ultimately all QKD deployments will be deployed in a hybrid fashion similar to that reported here.

ACKNOWLEDGMENTS

The authors thank Dr. Dushy Tissainayagam from Northrop Grumman Australia for constructive feedback and support received during the course of this experiment. This research has been carried out as a project co-funded by Northrop Grumman Australia, and the Defence Trailblazer Program, a collaborative partnership between the University of Adelaide and the University of New South Wales co-funded by the Australian Government, Department of Education.

REFERENCES

- [1] C. Wang, J. Yu, Z. Pei, Q. Wang, and C. Hong, “A first successful factorization of RSA-2048 integer by D-wave quantum computer,” *Tsinghua Science and Technology*, vol. 30, no. 3, pp. 1270–1282, 2024.
- [2] Y.-K. Liu and D. Moody, “Post-quantum cryptography and the quantum future of cybersecurity,” *Physical Review Applied*, vol. 21, no. 4, Art. No. 040501, 2024.
- [3] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, “Provably secure and high-rate quantum key distribution with time-bin qudits,” *Science Advances*, vol. 3, no. 11, Art. No. e1701491, 2017.
- [4] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami *et al.*, “10-Mb/s quantum key distribution,” *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, 2018.
- [5] 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, 2021.
- [6] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, “Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference,” *PRX Quantum*, vol. 3, no. 2, Art. No. 020315, 2022.
- [7] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan *et al.*, “Chip-based quantum key distribution,” *Nature Communications*, vol. 8, no. 1, Art. No. 13984, 2017.
- [8] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein *et al.*, “Metropolitan quantum key distribution with silicon photonics,” *Physical Review X*, vol. 8, no. 2, Art. No. 021009, 2018.
- [9] 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 *et al.*, “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.
- [10] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014.
- [11] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.
- [12] M. Kumar and B. Mondal, “A brief review on quantum key distribution protocols,” *Multimedia Tools and Appli-*

- cations, pp. 1–40, 2025.
- [13] US NSA (National Security Agency), “Quantum Key Distribution (QKD) and Quantum Cryptography (QC) - Retrieved on July 22, 2025,” <https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/>, 2023.
 - [14] R. Renner and R. Wolf, “Quantum advantage in cryptography,” *AIAA Journal*, vol. 61, no. 5, pp. 1895–1910, 2023.
 - [15] D. Tupkary, E. Y.-Z. Tan, S. Nahar, L. Kamin, and N. Lütkenhaus, “QKD security proofs for decoy-state BB84: protocol variations, proof techniques, gaps and limitations,” *arXiv preprint arXiv:2502.10340*, 2025.
 - [16] A. Huang, S. Barz, E. Andersson, and V. Makarov, “Implementation vulnerabilities in general quantum cryptography,” *New Journal of Physics*, vol. 20, no. 10, Art. No. 103016, 2018.
 - [17] A. Rani, J. Ramakrishnan, T. Sharma, P. Chandravanshi, A. Biswas, and R. P. Singh, “Experimental shot noise measurement using the imperfect detection—a special case for pulsed laser,” *IEEE Journal of Quantum Electronics*, vol. 59, no. 5, pp. 1–8, 2023.
 - [18] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, “Quantum security analysis of AES,” *IACR Transactions on Symmetric Cryptology*, pp. 55–93, 2019.
 - [19] H. Böck, A. Zauner, S. Devlin, J. Somorovsky, and P. Jovanovic, “Nonce-disrespecting adversaries: practical forgery attacks on GCM in TLS,” in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, 2016.
 - [20] J. P. Mattsson, “Collision-based attacks on block cipher modes - exploiting collisions and their absence,” Cryptology ePrint Archive, Paper 2024/1111, 2024.
 - [21] W. Chung, S. Hwang, S. Kim, B. Lee, and J. Lee, “Making GCM great again: Toward full security and longer nonces,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2025, pp. 33–61.
 - [22] A. Albertini, T. Duong, S. Gueron, S. Kölbl, A. Luykx, and S. Schmieg, “How to abuse and fix authenticated encryption without key commitment,” in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 3291–3308.
 - [23] P. Kampanakis, M. Campagna, E. Crockett, A. Petcher, and S. Gueron, “Practical challenges with AES-GCM and the need for a new cipher,” in *The Third NIST Workshop on Block Cipher Modes of Operation*, 2023.
 - [24] D. Jayasinghe, R. Ragel, J. A. Ambrose, A. Ignjatovic, and S. Parameswaran, “Advanced modes in AES: Are they safe from power analysis based side channel attacks?” in *IEEE 32nd International Conference on Computer Design (ICCD)*. IEEE, 2014, pp. 173–180.
 - [25] M. Tienteu, E. Smith, E. M. Santillan, K. Kornegay, P. Harvey, O. Toutsop, T. Yimer, V. Morris, and K. Wandji, “Template attack against AES in counter mode with unknown initial counter,” in *IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2023, pp. 0525–0533.
 - [26] D. Moody, “NIST PQC standardization update,” *National Institute of Standards and Technology*, pp. 2021–10, 2021.
 - [27] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, “CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM,” in *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018, pp. 353–367.
 - [28] C. A. Melchor, N. Aragon, S. Bettaiieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, and I. Bourges, “Hamming quasi-cyclic (HQC),” *NIST PQC Round*, vol. 2, no. 4, Art. No. 13, 2018.
 - [29] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, “Crystals-dilithium: A lattice-based digital signature scheme,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 238–268, 2018.
 - [30] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang *et al.*, “Falcon: Fast-fourier lattice-based compact signatures over NTRU,” *Submission to the NIST’s Post-Quantum Cryptography Standardization Process*, vol. 36, no. 5, pp. 1–75, 2018.
 - [31] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, “The SPHINCS+ signature framework,” in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2129–2146.
 - [32] B. S. Rawal and P. J. Curry, “Challenges and opportunities on the horizon of post-quantum cryptography,” *APL Quantum*, vol. 1, no. 2, Art. No. 026110, 2024.
 - [33] H. Nguyen, S. Huda, Y. Nogami, and T. T. Nguyen, “Security in post-quantum era: A comprehensive survey on lattice-based algorithms,” *IEEE Access*, vol. 13, pp. 89 003–89 024, 2025.
 - [34] N. Alnahawi, D. Haas, E. Mauß, and A. Wiesmaier, “SoK: PQC PAKEs - cryptographic primitives, design and security,” Cryptology ePrint Archive, Paper 2025/119, 2025.
 - [35] S. Ricci, P. Dobias, L. Malina, J. Hajny, and P. Jedlicka, “Hybrid keys in practice: combining classical, quantum and post-quantum cryptography,” *IEEE Access*, vol. 12, pp. 23 206–23 219, 2024.
 - [36] P. Zeng, D. Bandyopadhyay, J. A. M. Méndez, N. Bitner, A. Kolar, M. T. Solomon, Z. Ye, F. Rozpędek, T. Zhong, F. J. Heremans *et al.*, “Practical hybrid PQC-QKD protocols with enhanced security and performance,” *arXiv preprint arXiv:2411.01086*, 2024.
 - [37] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, and D. Stebila, “Hybrid key encapsulation mechanisms and authenticated key exchange,” in *International Conference on Post-Quantum Cryptography*. Springer, 2019, pp. 206–226.
 - [38] L. Garms, T. K. Paraíso, N. Hanley, A. Khalid, C. Rafferty, J. Grant, J. Newman, A. J. Shields, C. Cid, and M. O’Neill, “Experimental integration of quantum key distribution and post-quantum cryptography in a hybrid

- quantum-safe cryptosystem,” *Advanced Quantum Technologies*, vol. 7, no. 4, Art. No. 2300304, 2024.
- [39] B. Dowling, T. B. Hansen, and K. G. Paterson, “Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange,” in *International Conference on Post-Quantum Cryptography*. Springer, 2020, pp. 483–502.
- [40] S. Bruckner, S. Ramacher *et al.*, “Muckle+: End-to-End hybrid authenticated key exchanges,” in *International Conference on Post-Quantum Cryptography*. Springer, 2023, pp. 601–633.
- [41] N. Aquina, S. Rommel, and I. T. Monroy, “Quantum secure communication using hybrid post-quantum cryptography and quantum key distribution,” in *24th International Conference on Transparent Optical Networks (ICTON)*, 2024, pp. 1–4.
- [42] J. S. Buruaga, R. B. Méndez, J. P. Brito, and V. Martin, “Hybrid quantum-safe integration of TLS in SDN networks,” *Computer Networks*, Art. No. 111355, 2025.
- [43] C. R. Garcia, A. C. Aguilera, J. J. V. Olmos, I. T. Monroy, and S. Rommel, “Quantum-resistant TLS 1.3: A hybrid solution combining classical, quantum and post-quantum cryptography,” in *IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2023, pp. 246–251.
- [44] J. Blanco-Romero, P. O. García, D. Sobral-Blanco, F. A. Mendoza, A. F. Vilas, and M. Fernández-Veiga, “Hybrid quantum security for IPsec,” *arXiv preprint arXiv:2507.09288*, 2025.
- [45] M. Geitz, R. Döring, and R.-P. Braun, “Hybrid QKD & PQC protocols implemented in the Berlin OpenQKD testbed,” in *8th International Conference on Frontiers of Signal Processing (ICFSP)*. IEEE, 2023, pp. 69–74.
- [46] F. R. Ghashghaei, Y. Ahmed, N. Elmabit, and M. Yousefi, “Enhancing the security of classical communication with post-quantum authenticated-encryption schemes for the quantum key distribution,” *Computers*, vol. 13, no. 7, 2024, Art. No. 163, 2024.
- [47] L.-J. Wang, K.-Y. Zhang, J.-Y. Wang, J. Cheng, Y.-H. Yang, S.-B. Tang, D. Yan, Y.-L. Tang, Z. Liu, Y. Yu *et al.*, “Experimental authentication of quantum key distribution with post-quantum cryptography,” *npj Quantum Information*, vol. 7, no. 1, Art. No. 67, 2021.
- [48] A. Prakasan, K. Jain, and P. Krishnan, “Authenticated-encryption in the quantum key distribution classical channel using post-quantum cryptography,” in *6th International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2022, pp. 804–811.
- [49] D. Marchsreiter and J. Sepúlveda, “A PQC and QKD hybridization for quantum-secure communications,” in *26th Euromicro Conference on Digital System Design (DSD)*. IEEE, 2023, pp. 545–552.
- [50] P. Otero-García, J. Blanco-Romero, A. Fernández-Vilas, D. Sobral-Blanco, M. Fernández-Veiga, and F. Almenares-Mendoza, “Onion routing key distribution for QKDN,” *arXiv preprint arXiv:2502.06657*, 2025.
- [51] I. B. Djordjevic, “Joint QKD-post-quantum cryptosystems,” *IEEE Access*, vol. 8, pp. 154 708–154 712, 2020.
- [52] —, “QKD-enhanced cybersecurity protocols,” *IEEE Photonics Journal*, vol. 13, no. 2, pp. 1–8, 2021.
- [53] R. Azarderakhsh and M. S. A. T. Zadeh, “Integrating post-quantum cryptography (PQC) with quantum key distribution (QKD): performance, security, and practical challenges,” in *Quantum Information Science, Sensing, and Computation XVII*, vol. 13451. SPIE, 2025, pp. 96–101.
- [54] C. Kim, S. Kim, K. Sohn, Y. Son, M. Kumar, and S. Kim, “Secure and scalable file encryption for cloud systems via distributed integration of quantum and classical cryptography,” *Applied Sciences*, vol. 15, no. 14, 2025.
- [55] A. Rani, X. Ai, A. Gupta, R. S. Adhikari, and R. Malaney, “Combined Quantum and Post-Quantum Security for Earth-Satellite Channels,” in *International Conference on Quantum Communications, Networking, and Computing (QCNC)*. IEEE, 2025, pp. 301–308.
- [56] S. Mishra, A. Biswas, S. Patil, P. Chandravanshi, V. Mongia, T. Sharma, A. Rani, S. Prabhakar, S. Ramachandran, and R. P. Singh, “BBM92 quantum key distribution over a free space dusty channel of 200 meters,” *Journal of Optics*, vol. 24, no. 7, Art. No. 074002, 2022.
- [57] A. Tanaka, M. Fujiwara, K.-i. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, “High-speed quantum key distribution system for 1-Mbps real-time key generation,” *IEEE Journal of Quantum Electronics*, vol. 48, no. 4, pp. 542–550, 2012.
- [58] K. Kapoor, S. Xie, J. Chung, R. Valivarthi, C. Peña, L. Narváez, N. Sinclair, J. P. Allmaras, A. D. Beyer, S. I. Davis, G. Fabre, G. Iskander, G. S. Kanter, R. Kettimuthu, B. Korzh, P. Kumar, N. Lauk, A. Mueller, M. Shaw, P. Spentzouris, M. Spiropulu, J. M. Thomas, and E. E. Wollman, “Picosecond synchronization system for the distribution of photon pairs through a fiber link between Fermilab and Argonne National Laboratories,” *IEEE Journal of Quantum Electronics*, vol. 59, no. 4, pp. 1–7, 2023.
- [59] M. N. Wegman and J. L. Carter, “New hash functions and their use in authentication and set equality,” *Journal of Computer and System Sciences*, vol. 22, no. 3, pp. 265–279, 1981.
- [60] X. Ma, C.-H. F. Fung, and H.-K. Lo, “Quantum key distribution with entangled photon sources,” *Physical Review A*, vol. 76, no. 1, Art. No. 012307, 2007.
- [61] R. Y. Cai and V. Scarani, “Finite-key analysis for practical implementations of quantum key distribution,” *New Journal of Physics*, vol. 11, no. 4, Art. No. 045024, 2009.
- [62] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, “Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations,” *Physical Review A*, vol. 92, no. 5, Art. No. 052339, 2015.
- [63] A. Pljonkin, K. Rumyantsev, and P. Kumar Singh, “Synchronization in quantum key distribution systems,” *Cryptography*, vol. 1, no. 3, Art. No. 18, 2017.

- [64] Y. Pelet, G. Sauder, M. Cohen, L. Labonté, O. Alibart, A. Martin, and S. Tanzilli, “Operational entanglement-based quantum key distribution over 50 km of field-deployed optical fibers,” *Physical Review Applied*, vol. 20, no. 4, Art. No. 044006, 2023.
- [65] F. Basso Basset, M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino *et al.*, “Quantum key distribution with entangled photons generated on demand by a quantum dot,” *Science Advances*, vol. 7, no. 12, Art. No. eabe6379, 2021.
- [66] E. Villaseñor, K. Shimizu, R. Chandrasekara, W. Lau, and S. Gensemer, “Towards practical quantum secure time transfer,” in *Journal of Physics: Conference Series*, vol. 2889, no. 1. IOP Publishing, Art. No. 012028, 2024.
- [67] Y. Pelet, G. Sauder, S. Tanzilli, O. Alibart, and A. Martin, “Entanglement-based clock syntonization for quantum key distribution networks: Demonstration over a 50 km-long link,” *Applied Physics Letters*, vol. 126, no. 17, 2025.
- [68] R. Lafler and R. N. Lanning, “Quantum time transfer: A practical method for lossy and noisy channels,” *Physical Review Applied*, vol. 20, no. 2, Art. No. 024064, 2023.
- [69] C. Spiess, S. Töpfer, S. Sharma, A. Kržič, M. Cabrejo-Ponce, U. Chandrashekhara, N. L. Döll, D. Rieländer, and F. Steinlechner, “Clock synchronization with correlated photons,” *Physical Review Applied*, vol. 19, no. 5, Art. No. 054082, 2023.
- [70] M. Pahali, K. Durak, and U. Tefek, “Cryptographic security concerns on timestamp sharing via a public channel in quantum-key-distribution systems,” *Physical Review A*, vol. 106, no. 1, Art. No. 012611, 2022.
- [71] H. Dai, Q. Shen, C.-Z. Wang, S.-L. Li, W.-Y. Liu, W.-Q. Cai, S.-K. Liao, J.-G. Ren, J. Yin, Y.-A. Chen *et al.*, “Towards satellite-based quantum-secure time transfer,” *Nature Physics*, vol. 16, no. 8, pp. 848–852, 2020.
- [72] J.-P. W. MacLean, J. M. Donohue, and K. J. Resch, “Direct characterization of ultrafast energy-time entangled photon pairs,” *Physical Review Letters*, vol. 120, no. 5, Art. No. 053601, 2018.
- [73] V. Giovannetti, S. Lloyd, and L. Maccone, “Quantum-enhanced positioning and clock synchronization,” *Nature*, vol. 412, no. 6845, pp. 417–419, 2001.
- [74] O. Regev, “The learning with errors problem (invited survey),” in *IEEE 25th Annual Conference on Computational Complexity*, 2010, pp. 191–204.
- [75] E. Barker and Q. Dang, “NIST special publication 800-57 part 1, revision 5, recommendation for key management: Part 1—general,” *NIST, Tech. Rep.*, p. 171, 2020.
- [76] D. Park, G. Kim, D. Heo, S. Kim, H. Kim, and S. Hong, “Single trace side-channel attack on key reconciliation in quantum key distribution system and its efficient countermeasures,” *ICT Express*, vol. 7, no. 1, pp. 36–40, 2021.
- [77] H. Wang, Y. Gao, Y. Liu, Q. Zhang, and Y. Zhou, “In-depth Correlation Power Analysis Attacks on a Hardware Implementation of CRYSTALS-Dilithium,” *Cybersecurity*, vol. 7, no. 1, p. 21, 2024.
- [78] T. Kamucheka, M. Fahr, T. Teague, A. Nelson, D. Andrews, and M. Huang, “Power-based side channel attack analysis on pqc algorithms,” *Cryptology ePrint Archive*, 2021.
- [79] A. Lamas-Linares and C. Kurtsiefer, “Breaking a quantum key distribution system through a timing side channel,” *Opt. Express*, vol. 15, no. 15, pp. 9388–9393, 2007.
- [80] Q. Guo, T. Johansson, and A. Nilsson, “A key-recovery timing attack on post-quantum primitives using the fujisaki-okamoto transformation and its application on FrodoKEM,” *Cryptology ePrint Archive*, Paper 2020/743, 2020.
- [81] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, “Entanglement-based secure quantum cryptography over 1,120 kilometres,” *Nature*, vol. 582, no. 7813, pp. 501–505, Jun 2020.
- [82] H. Xiao and A. H. Banihashemi, “Improved progressive-edge-growth (PEG) construction of irregular LDPC codes,” in *IEEE Global Telecommunications Conference*, vol. 1. IEEE, 2004, pp. 489–492.
- [83] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, “Efficient reconciliation protocol for discrete-variable quantum key distribution,” in *International Symposium on Information Theory*. IEEE, 2009, pp. 1879–1883.
- [84] Kudelski Security, “Go post quantum safe lib,” <https://github.com/kudelskisecurity/crystals-go>, 2024.
- [85] R. Malaney, “The quantum car,” *IEEE Wireless Communications Letters*, vol. 5, no. 6, pp. 624–627, 2016.
- [86] —, “Quantum geo-encryption,” in *IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–6.

APPENDIX

For completeness, here we list the algorithms used in the specific implementation presented in this work.

The GPS-free synchronization protocol described in Section II-B uses algorithms 1 and 2 below. Note that most of the synchronization processing uses the latter algorithm, as the former is used only in the first round.

Algorithm 1: Coarse alignment Step (only for 1st round)

Input: The time tag array of Alice \hat{t}_a : the time tag array of Bob \hat{t}_b : the step size δ : the coincidence peak width of the EPS source FWHM: the coarse scan range R .

Output: Initial time offset τ_{coarse}

```

 $W \leftarrow \delta + 2\text{FWHM}$  /* Coincidence window width */
 $S \leftarrow \{-R, -R + \delta, \dots, R\}$  /* Time shifts to scan over */
for  $\nu \in S$  do
    /* Using MATLAB's Parallel Computing Toolbox here */
     $\hat{t}'_b \leftarrow \hat{t}_b + \nu$ 
     $C[\nu] \leftarrow |\{(a, b') : a \in \hat{t}_a, b' \in \hat{t}'_b, |a - b'| \leq W\}|$ 
    /* Coincidence count at  $\nu$  */
end
 $\tau_{coarse} \leftarrow \arg \max_{\nu} C[\nu]$ 

```

Note: The window W ensures that true coincidence events (entangled photon pair coincidence events) near the edges of adjacent steps are not missed.

Algorithm 2: Fine alignment Step

Input: The time tag array of Alice \hat{t}_a : the time tag array of Bob \hat{t}_b : the initial time offset τ_{coarse} : the bin width w : the cumulative offset τ_{accum} .

Output: The estimated time offset τ : the updated time tag array \hat{t}_b : τ_{accum}

```

 $\hat{t}_b \leftarrow \hat{t}_b + \tau_{coarse} + \tau_{accum}$ 
 $(\hat{t}_a^\dagger, \hat{t}_b^\dagger) \leftarrow \{(a, b) : a \in \hat{t}_a, b \in \hat{t}_b^\dagger, |a - b| \leq W\}$ 
for  $j = 1 : |\hat{t}_a^\dagger|$  do
     $\Delta \hat{t}_j \leftarrow \hat{t}_a^\dagger[j] - \hat{t}_b^\dagger[j]$ 
     $b_j \leftarrow \text{bin}(\Delta \hat{t}_j)$ 
end
 $b^\dagger \leftarrow \arg \max_b |\{j : b_j = b\}|$ 
 $\tau_{fine} \leftarrow b^\dagger \cdot w$ 
/* Compute total time offset, update cumulative offset, update Bob's time tags */
 $\tau \leftarrow \tau_{coarse} + \tau_{fine}$ 
 $\hat{t}_b \leftarrow \hat{t}_b + \tau$ 
 $\tau_{accum} \leftarrow \tau_{accum} + \tau$ 
 $\tau_{coarse} \leftarrow 0$ 

```

Note: Other than the first round, τ_{drift} is estimated by the τ (output of algorithm).

The specific implementation of the hybrid QKD-PQC protocol described in Section II-C uses algorithms 3 and 4 below. These algorithms are implemented in the last step of the control flow shown in Fig. 3, and largely relate to the encryption and decryption of the data M using the keys created by the hybrid system.

Algorithm 3: Data Encryption

Input: (Map, M, ξ, k_ξ, k_{psk})

Output: C

```

/*Step 1: Bob generates an instruction sequence using a mapping table based on a pre-shared key.*/
 $\pi \leftarrow f_{\text{Map}}^\xi(k_{psk})$  /*  $\pi = (\xi_{(1)}, \xi_{(2)}, \dots, \xi_{(n)})$  */
/* Step 2: Bob generates the key list based on the sequence  $\pi$ . */
 $k_\pi \leftarrow \text{SeqEncKeys}(\pi, k_\xi)$ ;  $C_{temp} \leftarrow M$ 
for  $i \leftarrow 1$  to  $\text{len}(\pi)$  do
     $C_{temp} \leftarrow \xi_{\pi(i)}(C_{temp}, k_{\pi(i)})$ 
end
 $C \leftarrow C_{temp}$ 
/* Step 3: Bob sends ciphertext  $C$  to Alice. */

```

Algorithm 4: Data Decryption

Input: (Map, $M, \bar{\xi}, \bar{k}_\xi, k_{psk}$)

Output: M

```

/*Step 1: Alice, upon receiving ciphertext  $C$  initiates the decryption process.*/
 $\pi^{-1} \leftarrow \pi \leftarrow f_{\text{Map}}^{\bar{\xi}}(k_{psk})$ 
/*Step 2: Alice generates the key list based on the sequence  $\pi^{-1}$ .*/
 $\bar{k}_\pi \leftarrow \text{SeqDecKeys}(\pi^{-1}, \bar{k}_\xi)$ ;  $M_{temp} \leftarrow C$ 
for  $i \leftarrow 1$  to  $\text{len}(\pi)$  do
     $M_{temp} \leftarrow \bar{\xi}_{\pi(n-i-1)}(M_{temp}, \bar{k}_{\pi^{-1}(i)})$ 
end
 $M \leftarrow M_{temp}$ 

```
