Qubit-Based Clock Synchronization for QKD Systems Using a Bayesian Approach

Roderick D. Cochran * and **Daniel J. Gauthier**

Department of Physics, The Ohio State University, 191 West Woodruff Ave., Columbus, OH 43210, USA; gauthier.51@osu.edu
* Correspondence: cochran.467@osu.edu

Abstract: Quantum key distribution (QKD) systems provide a method for two users to exchange a provably secure key. Synchronizing the users' clocks is an essential step before a secure key can be distilled. Qubit-based synchronization protocols directly use the transmitted quantum states to achieve synchronization and thus avoid the need for additional classical synchronization hardware. Previous qubit-based synchronization protocols sacrifice secure key either directly or indirectly, and all known qubit-based synchronization protocols do not efficiently use all publicly available information published by the users. Here, we introduce a Bayesian probabilistic algorithm that incorporates all published information to efficiently find the clock offset without sacrificing any secure key. Additionally, the output of the algorithm is a probability, which allows us to quantify our confidence in the synchronization. For demonstration purposes, we present a model system with accompanying simulations of an efficient three-state BB84 prepare-and-measure protocol with decoy states. We use our algorithm to exploit the correlations between Alice's published basis and mean photon number choices and Bob's measurement outcomes to probabilistically determine the most likely clock offset. We find that we can achieve a 95 percent synchronization confidence in only 4140 communication bin widths, meaning we can tolerate clock drift approaching 1 part in 4140 in this example when simulating this system with a dark count probability per communication bin width of 8×10^{-4} and a received mean photon number of 0.01.

Keywords: quantum key distribution (QKD); clock synchronization; Bayesian statistics

1. Introduction

Introduced in 1984 [1], quantum key distribution (QKD) is a symmetric encryption protocol that promises unconditional information security founded on the fundamental laws of physics, rather than on the difficulty of computational problems. Bennett and Brassard established the first QKD protocol (BB84), which used the polarization degree of freedom of single photons to transmit information. Subsequently developed protocols have extended QKD to different types of systems [2] and relaxed the requirement for a true single-photon source [3], paving the way for practical implementations of quantum cryptography.

For the sake of concreteness, we consider a polarization-based prepare-and-measure protocol. Here, one user (Alice) prepares and transmits a periodic sequence of quantum states with period τ_A encoded in at least two mutually unbiased orthonormal bases. In our example system, we use two bases: horizontal/vertical (H/V) polarization and left circular/right circular (L/R) circular polarization. We also use the decoy-state protocol where Alice occasionally sends the vacuum quantum state. A second user (Bob), measures each quantum state randomly in one of the two bases and records the result. After the measurement phase is complete, Alice and Bob publish their basis choices for each measurement and keep only the measurements where Bob registers a click with his single-photon counting detectors and they use the same basis. This process, called sifting, allows distilling a raw key, which, after error correction and privacy amplification [4], becomes the secret classical

key securely shared between Alice and Bob. Because qubits are lost to the environment via transmission loss and environmental radiation is detected due to stray light and thermal effects, our system is formally considered open. However, the security of the system is still guaranteed using privacy amplification based on the quantum bit error rate (QBER). Our example system uses a pulsed stochastic photonic source with decoy states [3], where the decoys are photonic wavepackets with a lower mean photon number. To simplify the example system and make it more efficient, we only transmit one state in the monitoring basis, which gives an equivalent secure key rate in comparison to transmitting both states in this basis [5,6].

A practical issue in quantum communication protocols is synchronizing Alice and Bob's two data streams. If Bob does not know precisely when Alice begins data transmission, he must begin recording measurements early or else risk missing some of Alice's transmission. In either case, because some signals do not arrive at Bob due to channel loss, and extraneous events are caused by stray light and detector dark counts, the first event Bob records is unlikely to be the first event Alice sends, resulting in some timing offset that must be determined. Correcting this offset is an essential precursor to sifting: If Alice and Bob do not agree on the timing of the events, they will compare basis choices from different events, resulting in a high QBER and likely share no information. In addition, determining which time bins correspond to Alice's wavepacket arrival and which do not allows timing-based noise filtering.

Further complicating the communication protocol is that the relative clock offset may not be a constant due to drift in the relative phase and frequency between the transmitter and receiver clocks. Alice has a communication protocol temporal bin width τ_A that may be different from Bob's bin width τ_B. The timing offset between their clocks Δ at the nth communication time bin since the most recent clock synchronization is given by

$$\Delta = t_0 + (\tau_A - \tau_B)n + \varepsilon \tag{1}$$

for an initial timing offset t_0 and higher-order timing error ε. In this way, small differences in clock frequencies can gradually change the clock offset so that a previously calculated synchronization is no longer valid. Other timing errors, such as clock jitter and frequency drift, also contribute to the need for a more robust synchronization solution. We denote the time over which synchronization is maintained as T_b, i.e., the time over which the error in $\Delta \ll \tau_A$.

Clock synchronization is sometimes achieved by directly sending Alice's clock signal to Bob over a separate channel via an optical link or using a radio-frequency signal [7–16]. However, this introduces additional hardware requirements and increases the cost and complexity of the setup. One way to avoid these additional resource requirements is to use the quantum channel itself to transmit the information necessary to perform the synchronization [17–20]. One such qubit-based synchronization protocol was introduced and demonstrated by Calderaro et al. [17]. Their protocol uses a dedicated clock-synchronization phase followed by a key distribution phase. In the synchronization phase, a pre-agreed synchronization string is transmitted to Bob and the clocks are aligned during post-processing.

The pre-agreed synchronization string is used to find the initial offset between Alice and Bob's clocks. Because it must be public knowledge, it cannot be used to generate a secure key. If the clock frequencies are not consistent, simple clock offset recovery only temporarily aligns until the clock drift becomes of-the-order-of the communication protocol temporal bin width τ_A. Correcting for this clock frequency drift using only clock offset recovery requires repeated synchronization/key distribution phases with a regularity that depends on the stability of the clocks used in the experiment. This reduces the overall secure key rate because no QKD states can be sent while the synchronization states are being sent, which may result in zero key rate due to finite-key effects [21,22]. However, to account for this drift without needing to send regular synchronization strings, Calderaro et al. performs clock frequency recovery using the periodic arrival times of Alice's qubits. Unlike

the clock offset recovery, this does not require a pre-agreed synchronization string and thus does not decrease the amount of key that can be sent.

While our method only uses clock offset recovery at this time, it avoids these potential impacts on secure key rate by synchronizing the clocks using only information that is already publicly sent over the insecure classical channel by Alice and Bob for sifting and security analysis: The basis choices and the mean photon number of the transmitted signal. Because we are transmitting only one state in the monitoring basis, the basis choices provide information about which of Bob's measurement outcomes are more likely. The decoy state choices, which determine Alice's mean photon number for each wavepacket, also contain information about Bob's measurement outcomes. For example, Bob is unlikely to record any detections if Alice sends the vacuum decoy state.

By comparing this information to his measurement outcomes, Bob can probabilistically determine the timing offset. To account for potential clock drift, Bob can perform this synchronization in subsets of length T_b. Thus, Bob can find the up-to-date timing offset and ensure that the basis choices he publishes are properly lined up with the ones sent to him by Alice, but this requires an efficient analysis method to reduce the data requirements. Of course, our approach as well as Calderaro's requires low enough channel loss so that there are enough events received by Bob over a drift interval as discussed below.

Another example of a qubit-based synchronization protocol for continuously-pumped entanglement-based QKD systems was introduced by Ho et al. [20]. Here, they correlate Alice and Bob's detection events without considering basis information. Their synchronization method relies on Alice's knowledge that some communication time bins are empty (assuming essentially unit detection efficiency for Alice's setup) and hence Bob's corresponding time bin should also be empty. There is a single dominant peak in the correlation function that identifies Δ assuming a large enough number of Bob's detection events. Because the detection timing information must already be shared publicly, this strategy does not sacrifice any secure key. This method fails when the probability of Alice generating a photon per communication time bin approaches unity because every time bin is likely to be filled and hence the correlation function will have multiple high-value peaks that create timing ambiguity.

In the next section, we outline our synchronization algorithm and its advantages, and derive a formula for the synchronization probability using Bayesian analysis. In Section 3 we introduce a model system, and in Section 4 we simulate data in this model system to demonstrate the effectiveness of our method. In Section 5 we present our conclusions and the potential applicability of this work to other QKD systems.

2. Qubit-Based Synchronization Algorithm

Similar to previous approaches, our algorithm uses a cross-correlation of Alice's periodically transmitted data and Bob's received data to find the number of each type of event pairing, where the cross-correlation is computed efficiently using a Fast Fourier Transform (FFT). One complication of a prepare-and-measure scheme is that Alice attempts to send a quantum state every communication time bin, corresponding to the high-photon-probability limit of the Ho et al. [20] method discussed above. This problem is addressed here using the decoy-state protocol [3], which must be used anyway to prevent a photon-number-splitting attack.

Decoy states are sent by Alice randomly and correspond to wavepackets with a mean photon number smaller than the signal state and often includes sending the vacuum state. The vacuum state is particularly effective in the synchronization process because Alice has high certainty that she sent no photons, limited by her ability to completely block the source. Bob should then also see no photons, limited by the source of detection clicks from non-ideal effects such as detector dark counts, detector afterpulsing, stray light, and the bleed through of light from Alice's source.

Beyond the decoy states, there are additional sources of correlation that can be exploited to help improve the synchronization process. For example, Alice's use of the

efficient three-state protocol, where she only sends one state in the monitoring basis, gives useful information if Alice and Bob also share basis-state information, which is already required for sifting. We use a Bayesian statistical method, described below, that uses all prior knowledge of the system characteristics, such as the state fidelities, the mean photon numbers, the channel loss, the fractional sorting of Bob's device for the two bases, and the detector efficiency, to generate a lookup table of Bob's detection probabilities for Alice's different inputs. With these, we can easily compute the synchronization probabilities of different possible offsets using Bayesian statistics. Alice and Bob's data is most correlated when they are synchronized.

A significant advantage of our approach is that it does not sacrifice any secure key: We only use the information that is already sent publicly over the insecure classical channel. This is an improvement over synchronization protocols that share some fraction of the raw data for synchronization purposes, as well as protocols that have a dedicated clock-synchronization phase [17] during which no QKD states can be sent.

Bayesian analysis is a logical choice for synthesizing all available information and using it to make accurate predictions about Δ. It also has the advantage that it predicts the probability that $\hat{\Delta}$ is the best estimate of synchronization offset. This allows us to quantitatively express our level of confidence in the synchronization estimate. Furthermore, the additional information we incorporate in the protocol allows us to make a decision with fewer received qubits, which makes the system more robust to clock drift.

Our algorithm uses FFTs to compute cross-correlations between Alice's inputs and Bob's outputs, allowing us to count the number of each type of input-output pairing for the different time offsets. The computational complexity of our algorithm is dominated by these FFTs, which go as $\mathcal{O}(N \log N)$ where N is the number of sampling bins. Each cross-correlation requires three FFT computations, so the number of FFTs that must be performed is $3 \times n_{in} \times n_{out}$ for a number of distinct inputs n_{in} and distinct outputs n_{out}. In this example, $n_{in} = 5$ (H/V signal, H/V decoy, L/R signal, L/R decoy, and vacuum) and $n_{out} = 4$ (H,V,L, and R), thus maintaining the computational complexity of $\mathcal{O}(N \log_2 N)$.

Synchronization Probability

Here we will use the strings of Alice and Bob's data. A string of Bob's data consists of the results of each of his detectors at each sampling bin. Typically, Bob's strings are very sparse because there are many sampling bins in which he registers no detections. A string of Alice's data consists of her published information at each sampling bin. If the communication time bin width is greater than the sampling time bin width, Alice will have multiple string entries for each state she sends, each corresponding to what she is sending at that part of her duty cycle. Determining the synchronization probability consists of comparing different strings of Bob's data (starting at different temporal offsets) to strings of Alice's data and calculating which of Bob's strings D is most likely to be the one generated by Alice's corresponding string. We determine, for a particular string of Bob's, the probability that it could have been generated by Alice's published string.

Mathematically, we phrase this as the likelihood $p(D|S)$ of generating Bob's string D given the assumption that its generating string is the one Alice has published, denoted by S. The uninformed assumption, which we will denote as $\bar{S}$, is that Bob's string D has been generated by a random string other than Alice's published string (from some other portion of Alice's sent data), with the stipulation that the other string is also periodic. This mathematical framework will consider a subset of Alice's data of N sampling bin widths compared against a subset of Bob's data of $N + M$ sampling bin widths, meaning there will be M possible offsets to consider.

To begin in our protocol formalism, we note that D is a string of length $M + N$ of Bob's measurements at each sampling bin (including sampling bins where no detections

were received). Each measurement B_i in Bob's string consists of the click or no-click results at all of Bob's detectors. Bob's string D can be written as

$$D = \{B_1, ..., B_{M+N}\}, \tag{2}$$

which we can rewrite as

$$D = \{B_1, D'\}, \tag{3}$$

where

$$D' = \{B_2, ..., B_{M+N}\}. \tag{4}$$

We prefer to write the likelihood $p(D|S)$ in terms of known quantities such as the $p(B_1|S)$, the conditional probability of a time bin measurement B_1 given S. Using this notation, $p(D|S)$ is given by

$$p(D|S) = p(B_1, D'|S) = p(B_1|D', S)p(D'|S), \tag{5}$$

where the final equality is a result of the product rule. Because we have assumed that B_1 is generated from Alice's string, knowing D' gives us no additional information about B_1. At best, it informs us whether S is true, which is already assumed; the bits are otherwise independent because Alice's sequence is random. Using these observations, we obtain

$$p(B_1|D', S) = p(B_1|S), \tag{6}$$

and, by extension,

$$p(D|S) = \prod_{i=1}^{N+M} p(B_i|S), \tag{7}$$

allowing us to write the likelihood as the product of the measurement probabilities at each sampling bin. We note that even in the example where Alice only sends one state in the monitoring basis, Bob must still measure both states in each basis to detect potential eavesdropper attacks [5,6]. For computational ease, we also determine each sampling bin measurement probability as the product of the probabilities of the outcomes at the four different detectors b_ℓ, which are given by

$$p(B_i|S) = \prod_{\ell=1}^{4} p(b_\ell|S) \tag{8}$$

Again, because the detectors' events are assumed to be generated by independent random processes, these probabilities can be considered independent when the generating string is known.

When the generating string is not known (under the uninformed assumption $\bar{S}$), the detection probabilities can be approximated as independent when the received mean photon number is low. Because the synchronization task is most difficult in low-signal regimes, we use this approximation going forward. Thus,

$$p(D|\bar{S}) = \prod_{i=1}^{N+M} p(B_i|\bar{S}) \tag{9}$$

and

$$p(B_i|\bar{S}) = \prod_{\ell=1}^{4} p(b_\ell|\bar{S}). \tag{10}$$

For a given input from Alice, each of Bob's four detectors has an opportunity to detect a photon above the detection clicks arising from non-ideal behaviors. Naturally, we will use our knowledge of the system (the state fidelities, the quality of the polarization sorting, the dark count rates, the detector efficiencies, and the signal and decoy received mean

photon number) to estimate the detection probabilities as accurately and efficiently as possible. Using a lookup table of the detection probabilities for the different inputs from Alice, these likelihoods can be calculated using standard statistical methods.

However, the likelihood of generating D from Alice's published string is not the same as the probability that Alice's published string is the one that generated D, which is given by $p(S|D)$ and is the most relevant quantity to determine synchronization. Bayes' theorem allows us to rewrite this quantity, called the posterior, as

$$p(S|D) = \frac{p(D|S)p(S)}{p(D)}. \tag{11}$$

In addition, we must also include the information that we expect exactly one correct synchronization offset (not just one on average).

To formulate the problem as an exclusive synchronization, we must find the probability that some discreet timing offset, given by the time-bin index j, is the correct synchronization offset, and that all the other offsets are incorrect. In other words, the probability that, for a given string of length N published by Alice, all the measurements before the jth bin are generated randomly, the measurements from j to $j + N$ are generated from Alice's published string, and the measurements after $j + N$ are generated randomly. Under these assumptions, we can write $p(B_1, ..., B_{M+N}|S_j)$ as a product of the likelihoods of these three sections as

$$p(B_1, ..., B_{M+N}|S_j) = p(B_1, ..., B_{j-1}|\bar{S}_j)p(B_j, ..., B_{j+N}|S_j)p(B_{j+N+1}, ..., B_{M+N}|\bar{S}_j). \tag{12}$$

Here we introduce $\bar{S}_j$, the assumption that the data is produced by a random string other than the synchronization string in question, but one with the same phase (i.e., the signal arrives at the same time bin in each period as it does for S_j).

We can find the conditional probability for matching Alice's string to Bob's string at a potential synchronization index j in this framework using Equation (11), which gives

$$p(S_j|B_1, ..., B_{M+N}) = \frac{p(B_1, ..., B_{M+N}|S_j)p(S_j)}{p(B_1, ..., B_{M+N})}. \tag{13}$$

Equation (13) is our main result and is the quantity of interest to identify clock synchronization between Alice and Bob. We determine the optimum synchronization index based on the value of j that maximizes this quantity, and the quantity itself gives us our confidence in that choice.

The denominator in Equation (13) can be written in terms of known quantities using marginalization. Marginalization consists of rewriting a probability as a sum of the comprehensive conditional probabilities; in this case, the different possible synchronization indices written as

$$p(S_j|B_1, ..., B_{M+N}) = \frac{p(B_1, ..., B_{M+N}|S_j)p(S_j)}{\sum_{i=1}^{M} p(B_1, ..., B_{M+N}|S_i)p(S_i)}, \tag{14}$$

where the i denotes the other potential synchronization indices.

To evaluate Equation (13), the likelihoods $p(B_1, ..., B_{M+N}|S_j)$ and $p(B_1, ..., B_{M+N}|S_i)$ can be determined using Equations (7), (9) and (12). The quantity $p(S_j)$, called the prior, is the ad hoc probability that D corresponds to Alice's published string. That is, $p(S_j)$ is the probability that we are at the correct synchronization index. We use a uniform prior, which assumes each candidate has a naïve $1/M$ probability of being the correct one given that we have M candidate indices, which means that

$$p(S_i) = p(S_j) = \frac{1}{M} \tag{15}$$

so that the prior terms cancel, giving us

$$p(S_j|B_1, ..., B_{M+N}) = \frac{p(B_1, ..., B_{M+N}|S_j)}{\sum_{i=1}^{M} p(B_1, ..., B_{M+N}|S_i)}. \tag{16}$$

Next, we apply Equation (12) to obtain

$$p(S_j|B_1, ..., B_{M+N}) = \tag{17}$$
$$\frac{p(B_1, ..., B_{j-1}|\bar{S}_j)p(B_j, ..., B_{j+N}|S_j)p(B_{j+N+1}, ..., B_{M+N}|\bar{S}_j)}{\sum_{i=1}^{M} p(B_1, ..., B_{i-1}|\bar{S}_i)p(B_i, ..., B_{i+N}|S_i)p(B_{i+N+1}, ..., B_{M+N}|\bar{S}_i)}$$

and use Equations (7) and (9) (of which the latter uses a low received mean photon number approximation) to write everything in terms of known quantities as

$$p(S_j|B_1, ..., B_{M+N}) \approx \frac{\prod_{k=1}^{j-1} p(B_k|\bar{S}_j) \prod_{k=j}^{j+N} p(B_k|S_j) \prod_{k=j+N+1}^{M+N} p(B_k|\bar{S}_j)}{\sum_{i=1}^{M} \left(\prod_{k=1}^{i-1} p(B_k|\bar{S}_i) \prod_{k=i}^{i+N} p(B_k|S_i) \prod_{k=i+N+1}^{M+N} p(B_k|\bar{S}_i) \right)} \tag{18}$$

Equation (18) is our master equation for the synchronization probability of an index j. The numerator consists of the probability of an N-length string of Bob's data starting at j being produced by Alice's published string, along with the probability that the remaining data was produced by an unknown string of Alice's data. The denominator sums this same quantity over all possible synchronization indices, ensuring normalization. We take the value of j that maximizes this quantity to be the optimum synchronization index, and the value of $p(S_j|B_1, ..., B_{M+N})$ gives us the probability that we are correct. We can compute this conditional probability using FFTs to count the number of each unique bin measurement along with a lookup table of the probabilities of the events.

3. Model System

To illustrate our protocol, we simulate a model QKD system using a polarization-based prepare-and-measure protocol with decoy states and only sending one state in the monitoring basis. We set Alice's repetition rate to be $f_A = 1/\tau_A$ and a wavepacket duration of $\Delta t = \tau_A/m$ with $m = 8$ for a duty cycle of 12.5 percent. We set Bob's sampling rate to $n f_A$ with $n = 8$ so that his sample period is matched to the wavepacket duration. These conditions are illustrated in Figure 1. Alice generates a pseudorandom sequence such that four quantum states L/R/H and a vacuum decoy state (a decoy state with mean photon number equal to zero) are sent in equal parts on average.

For our numerical experiments, we simulate a QKD session by generating data that emulates the state preparation and measurement, including aspects such as the *received* mean photon number μ, probability of a detector dark count d over one communication bin width τ_A, and variation in Δ due to clock drift, assumed to be constant over T_b. This allows us to test how these factors impact the synchronization performance. We assume a transmitted mean photon number $\mu_A = 1$ where the received mean photon number $\mu = \eta\mu_A$ for a channel transmission η. While this μ_A is on the upper end of values used in typical experiments, it allows us to explore the performance and limitations of our algorithm at or beyond the greatest received mean photon number one would realistically use: $\mu_A = 1$ with zero loss.
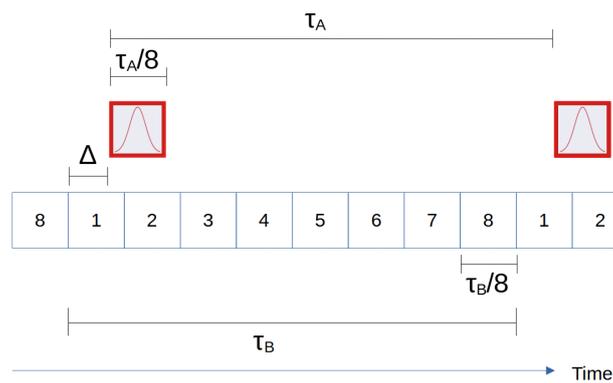
Figure 1. Illustration of the relative times used in the QKD protocol. Here, the signal (red) straddles bins 1–2 due to an offset of Δ, and we do not consider bins 3–8. We take $\tau_A = \tau_B$, which is approximately correct for a short enough data subset.

Assuming a Poisson distribution for Alice's source, the probability of Bob registering a click $p(click, \ell)$ over a period τ_A at a particular detector ℓ is given by

$$p(click, \ell) = 1 - (1 - d)e^{-\mu_\ell} \tag{19}$$

where μ_ℓ is the mean photon number received by detector ℓ. The portion of the total mean photon number μ that goes to the different detectors depends on which polarization state is sent. We use ideal BB84 sorting in our model system so that all states have an equal chance of being measured in either basis. States measured in the same basis as they are prepared are detected accurately, while states measured in the opposite basis have an equal chance of being measured in either opposite-basis state. For example, if Alice prepared an H-state that Bob receives $\mu = 0.8$, Bob's measures $\mu_H = 0.4$, $\mu_v = 0$, and $\mu_L = \mu_R = 0.2$.

We assume that the observation window is long enough so that the p's and μ's can be estimated accurately from the finite number of observations. This means the average click probability can be extracted from the Bob's raw data and we rewrite Equation (19) as a function of $p(click, \ell)$ so that

$$\mu_\ell = ln\left(\frac{1 - d}{1 - p(click, \ell)}\right) \tag{20}$$

The mean photon numbers of the constituent pulses incident at the four detectors sum to the average mean photon number of the main pulse just before it enters Bob's detection apparatus, so we can estimate the received mean photon number of a signal state as

$$\mu = \frac{4}{3} \sum_{\ell=1}^{4} ln\left(\frac{1 - d}{1 - p(click, \ell)}\right), \tag{21}$$

where the factor of 4/3 accounts for the fact that we are sending vacuum states 25% of the time.

We divide the data set into subsets duration T_b and perform synchronization and sifting on each subset. Bob can record up to eight events (each of which may or may not include a detection event or dark count) assuming that the detector deadtime is less than Bob's sampling time. However, because the clocks can only be synchronized to a resolution of Bob's sampling bin width, we expect Alice's wavepacket to straddle 2 bins as illustrated in Figure 1, with the end bins only having a partial wavepacket. The remaining six bins only contain dark counts, which can be discarded after we determine Δ to reduce noise. This amounts to detector time-gating in the post-analysis.

We assume that Bob begins recording before Alice begins transmitting, and continues to record after she stops sending, so our received data is bookended by low signal regions.

We find a best-fit step function to identify where the transmission begins and ends, which gives us a coarse approximation of the synchronization index. For a range of different string lengths N that determine the number of sampling bin widths in each synchronization subset, we examine a window of $M = 4000$ nearby potential synchronization indices. This value is chosen based on the typical precision of the coarse approximation of the synchronization given by the best-fit step function.

4. Synchronization Simulations

To verify that our algorithm returns an accurate probability of synchronization, we run 1000 simulated trials with a known synchronization index and compare the average calculated probability of synchronization $p(S_j|B_1, ..., B_{M+N})$ to the average rate of finding the correct index, which we denote by $f(S_j|B_1, ..., B_{M+N})$, in Figure 2. If our model is accurate, then $p(S_j|B_1, ..., B_{M+N}) \sim f(S_j|B_1, ..., B_{M+N})$, in which case we can take $p(S_j|B_1, ..., B_{M+N})$ to be a reliable metric for quantifying our confidence in obtaining the correct Δ.
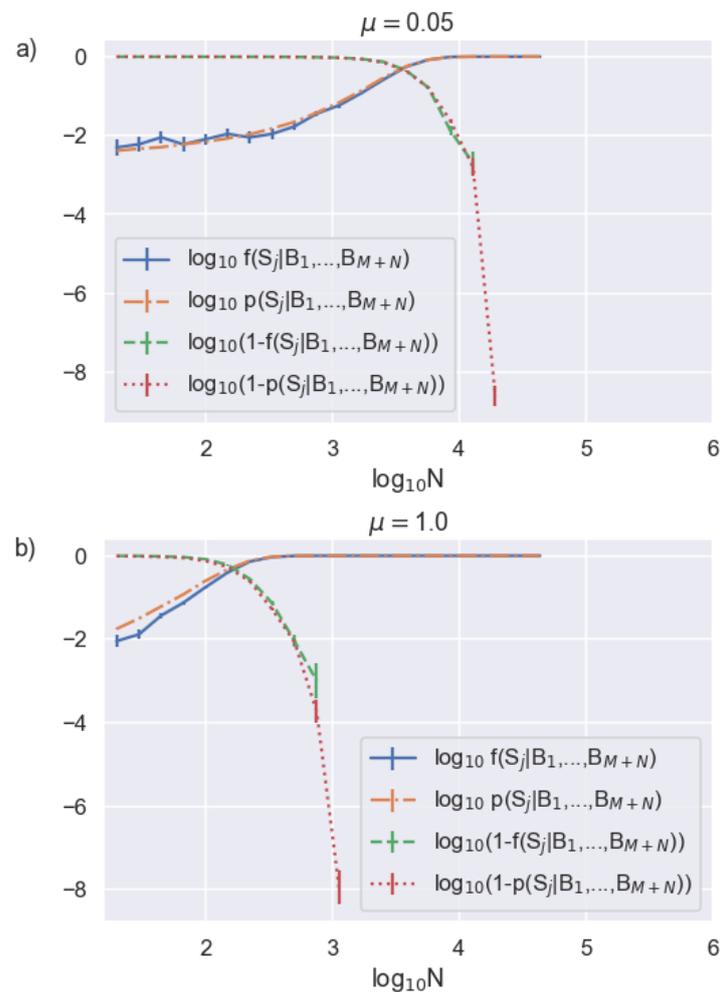
Figure 2. Bob's required data record length needed to determine synchronization for two different channel transmissions of (**a**) $\eta = 0.05$, corresponding to $\mu = 0.05$ and (**b**) $\eta = 1$, corresponding to $\mu = 1$. We also show the probability of not obtaining synchronization, which better highlights transition to high-certainty synchronization.

We see that $p(S_j|B_1, ..., B_{M+N}) \sim f(S_j|B_1, ..., B_{M+N})$ to within our errorbars for moderate channel loss (Figure 2a). However, $p(S_j|B_1, ..., B_{M+N})$ is consistently larger than $f(S_j|B_1, ..., B_{M+N})$ for the case of zero channel loss (Figure 2b), a condition that is unlikely to be encountered in an experiment but highlights the limitation of our algorithm. This

result is not surprising given that our derivation given in Section 2 assumes low μ to arrive at Equation (9). Assuming a transmitted mean photon number of 1, Figure 2b corresponds to a zero channel loss system. This represents an upper limit on μ encountered in a typical decoy state protocol where $\mu_A \lesssim 1$ and thus, also serves as a lower bound on the accuracy of our calculated synchronization probability.

A lower received mean photon number means a lower density of detected events. Because detected events provide more information than no-detection events, a lower μ requires us to consider a larger set of sampling bin widths N to achieve the same synchronization confidence. Despite the fact that $p(S_j|B_1,...,B_{M+N})$ does not match $f(S_j|B_1,...,B_{M+N})$ as well at higher values of μ, we can still achieve equivalent average values of $f(S_j|B_1,...,B_{M+N})$ at lower values of N. This fact is also illustrated in Figure 3, where we see a direct correlation between μ and the N at which the synchronization probabilities converge to one. The higher values of μ converge at lower values of N.
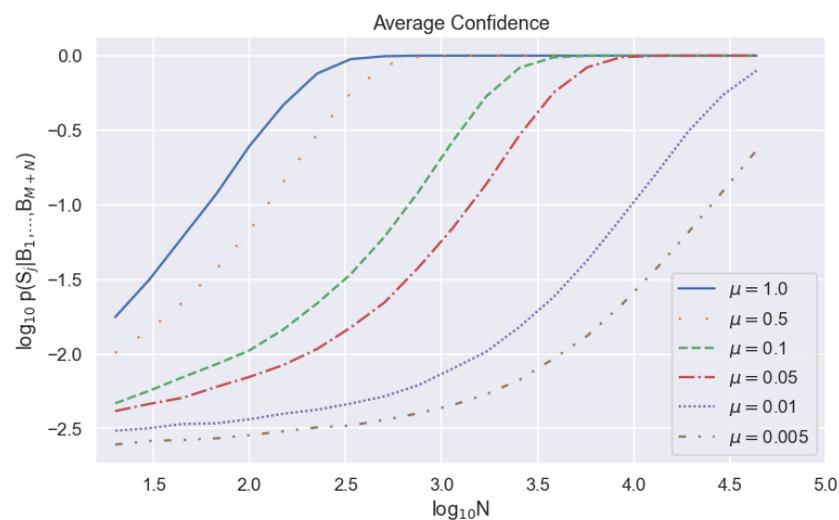
Figure 3. Average calculated synchronization probability as a function of string length on a logarithmic scale for different received mean photon numbers. The probability of registering a dark count during one communication bin width is $d = 8 \times 10^{-4}$.

Another way to view this relation between μ, N, and $p(S_j|B_1,...,B_{M+N})$ is to consider the string length N required to achieve a particular synchronization confidence as a function of μ as shown in Figure 4. For high μ and low N, we observe an approximately linear relation between $log_{10}\mu$ and $log_{10}N$ with a slope of ~ -1, which means that $N \sim 1/\mu$. For lower μ, where there are fewer events and dark counts play a larger role, the probability curves exhibit steeper slopes, demonstrating that synchronization becomes increasingly difficult. This data can be used to estimate whether it is possible to synchronize over an experimentally measured temporal block length T_b and, if it is possible, how low a value of μ can be tolerated while still synchronizing reliably. As a concrete example, Bob needs 33,110 sampling bin widths, or about 4140 communication bin widths, to achieve a 95% confidence for clock synchronization for $\mu = 0.01$ and $d = 8 \times 10^{-4}$. This means we can tolerate clock drifts approaching 1 part in 4140, or 242 µs of drift per second, because our method assumes that the clock drift is much less than one communication bin width. For context, we measure the rate of clock drift between two phase lock loops driven by crystal oscillator clocks on DE10 Standard field programmable gate arrays (FPGAs), and find the average clock drift rate to be 13.5 µs per second. Thus, our algorithm can tolerate realistic clock drift rates in this example.
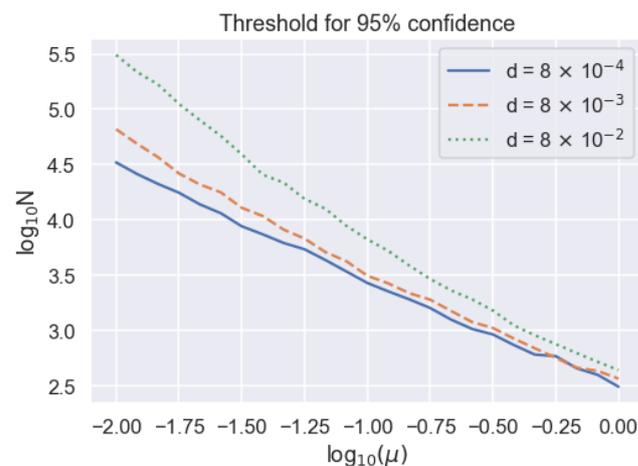
Figure 4. Dependence of string length threshold to achieve 95 percent synchronization confidence on received mean photon number on a logarithmic scale, parameterized by different dark count probabilities.

5. Conclusions

In conclusion, we develop a novel probabilistic approach to qubit-based clock synchronization using Bayesian analysis. By exploiting correlations between information Alice shares publicly, such as basis and decoy state choices, and Bob's detection events, we can find the correct synchronization clock offset without sacrificing any secret key. Additionally, our algorithm is more robust to noise, loss, and clock drift in comparison to other protocols by incorporating all publicly available information using the Bayesian framework. Finally, we demonstrate that our algorithm is successful and robust using a simulated BB84 communication scheme, which confirms that our synchronization metric corresponds to the probability of synchronization, especially in the low-μ limit. Our algorithm is applicable to other QKD systems that use other degrees-of-freedom of the photon for which it is possible to divulge some timing information.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Ekert, A. Quantum cryptography based on bell theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663.10.1103/PhysRevLett.67.661. [CrossRef] [PubMed]
3. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. 230504. [CrossRef] [PubMed]
4. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28. [CrossRef]
5. Islam, N.T.; Lim, C.C.W.; Cahall, C.; Kim, J.; Gauthier, D.J. Securing quantum key distribution systems using fewer states. *Phys. Rev. A* **2018**, *97*, 042347. [CrossRef]
6. Tamaki, K.; Curty, M.; Kato, G.; Lo, H.K.; Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **2014**, *90*, 052314. [CrossRef]
7. D'Auria, V.; Fedrici, B.; Ngah, L.A.; Kaiser, F.; Labonté, L.; Alibart, O.; Tanzilli, S. A Universal, Plug- Synchronisation Scheme Pract. Networks. *Npj Quantum. Inf.* **2020**, *6*, 21. [CrossRef]
8. Korzh, B.; Lim, C.C.W.; Houlmann, R.; Gisin, N.; Li, M.J.; Nolan, D.; Sanguinetti, B.; Thew, R.; Zbinden, H. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photonics* **2015**, *9*, 163–168. [CrossRef]
9. Liu, Y.; Chen, T.Y.; Wang, J.; Cai, W.Q.; Wan, X.; Chen, L.K.; Wang, J.H.; Liu, S.B.; Liang, H.; Yang, L.; et al. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express* **2010**, *18*, 8587–8594. [CrossRef]
10. Liu, P.; Yin, H.L. Secure and efficient synchronization scheme for quantum key distribution. *OSA Contin.* **2019**, *2*, 2883–2890. [CrossRef]
11. Walenta, N.; Burg, A.; Caselunghe, D.; Constantin, J.; Gisin, N.; Guinnard, O.; Houlmann, R.; Junod, P.; Korzh, B.; Kulesza, N.; et al. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New J. Phys.* **2014**, *16*, 013047. [CrossRef]
12. Dynes, J.; Tam, W.; Plews, A.; Fröhlich, B.; Sharpe, A.W.; Lucamarini, M.; Yuan, Z.; Radig, C.; Straw, A.; Edwards, T.; et al. Ultra-High Bandwidth Quantum Secur. Data Transm. *Sci. Rep.* **2016**, *6*, 35149. [CrossRef] [PubMed]
13. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409. [CrossRef]
14. Wang, S.; Chen, W.; Yin, Z.Q.; Li, H.W.; He, D.Y.; Li, Y.H.; Zhou, Z.; Song, X.T.; Li, F.Y.; Wang, D.; et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **2014**, *22*, 21739–21756. [CrossRef] [PubMed]
15. Vallone, G.; Marangon, D.G.; Canale, M.; Savorgnan, I.; Bacco, D.; Barbieri, M.; Calimani, S.; Barbieri, C.; Laurenti, N.; Villoresi, P. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. *Phys. Rev. A* **2015**, *91*, 042320. [CrossRef]
16. Bourgoin, J.P.; Gigov, N.; Higgins, B.L.; Yan, Z.; Meyer-Scott, E.; Khandani, A.K.; Lütkenhaus, N.; Jennewein, T. Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations. *Phys. Rev. A* **2015**, *92*, 052339. [CrossRef]
17. Calderaro, L.; Stanco, A.; Agnesi, C.; Avesani, M.; Dequal, D.; Villoresi, P.; Vallone, G. Fast and Simple Qubit-Based Synchronization for Quantum Key Distribution. *Phys. Rev. Appl.* **2020**, *13*, 054041. [CrossRef]
18. Agnesi, C.; Avesani, M.; Calderaro, L.; Stanco, A.; Foletto, G.; Zahidy, M.; Scriminich, A.; Vedovato, F.; Vallone, G.; Villoresi, P. Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder. *Optica* **2020**, *7*, 284–290. [CrossRef]
19. Avesani, M.; Calderaro, L.; Foletto, G.; Agnesi, C.; Picciariello, F.; Santagiustina, F.B.L.; Scriminich, A.; Stanco, A.; Vedovato, F.; Zahidy, M.; et al. Resource-effective quantum key distribution: A field trial in Padua city center. *Opt. Lett.* **2021**, *46*, 2848–2851. [CrossRef]
20. Ho, C.; Lamas-Linares, A.; Kurtsiefer, C. Clock synchronization by remote detection of correlated photon pairs. *New J. Phys.* **2009**, *11*, 045011. [CrossRef]
21. Hayashi, M. Upper bounds of eavesdropper's performances in finite-length code with the decoy method. *Phys. Rev. A* **2007**, *76*, 012329. [CrossRef]
22. Lim, C.C.W.; Curty, M.; Walenta, N.; Xu, F.; Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **2014**, *89*, 022307. [CrossRef]