Increasing the Raw Key Rate in Energy-Time Entanglement Based Quantum Key Distribution

Esmaeil Karimi, Emina Soljanin, and Philip Whiting

Abstract

A Quantum Key Distribution (QKD) protocol describes how two remote parties can establish a secret key by communicating over a quantum and a public classical channel that both can be accessed by an eavesdropper. QKD protocols using energy-time entangled photon pairs are of growing practical interest because of their potential to provide a higher secure key rate over long distances by carrying multiple bits per entangled photon pair. We consider a system where information can be extracted by measuring random times of a sequence of entangled photon arrivals. Our goal is to maximize the utility of each such pair. We propose a discrete time model for the photon arrival process, and establish a theoretical bound on the number of raw bits that can be generated under this model. We first analyse a well known simple binning encoding scheme, and show that it generates significantly lower information rate than what is theoretically possible. We then propose three adaptive schemes that increase the number of raw bits generated per photon, and compute and compare the information rates they offer. Moreover, the effect of public channel communication on the secret key rates of the proposed schemes is investigated.

I. INTRODUCTION

A Quantum Key Distribution (QKD) protocol describes how two parties, commonly referred to as Alice and Bob, can establish a secret key by communicating over a quantum and a public classical channel that both can be accessed by an eavesdropper Eve. For the widespread adoption of QKD, it is mandatory to provide high key rates over long distances (see a related survey [1]). What has appeared as a bottleneck in practice is the inability to maximize the utility of information-bearing quantum states

E. Karimi is with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA (E-mail: esmaeil.karimi@tamu.edu).

E. Soljanin is with the Department of Electrical and Computer Engineering, Rutgers University, Piscataway, NJ 08854 USA (E-mail: emina.soljanin@rutgers.edu).

P. Whiting is with the Department of Engineering, Macquarie University, North Ryde, NSW 2109 Australia (E-mail: philip.whiting@mq.edu.au).

that are communicated over the quantum channel [2]–[4]. QKD based on energy-time entangled photons has emerged as a promising technique primarily because each entangled photon pair can carry multiple raw key bits, and thus potentially provide a higher secure key rate over long distances [5], [6]. Moreover, it has been shown that higher dimensional quantum states are more sensitive to eavesdropping and are also more robust to certain types of noise [7]–[10].

Timing information extraction in energy-time entanglement based QKD schemes is commonly achieved through a method known as time-bin encoding [11], [12]. The time-bin encoding method is essentially a Pulse-Position Modulation (PPM) scheme, which is a common technique that converts the binary time-pulse sequences into large-alphabet sequences of fixed alphabet size. Alice and Bob timestamp their photon arrivals, and then map the timestamps to bit strings. Under ideal conditions, Alice and Bob are supposed to receive identical sequences. The bit strings obtained in this case constitute the raw key. The objective of this paper is to maximize the length of the raw key.

Due to errors such as timing jitter, transmission loss and low detection efficiency, there are disparities between the received sequences in practical implementations [13]–[15]. In order to systematically increase the correlation between their key strings, while reducing Eves acquired information, Alice and Bob perform information reconciliation followed by privacy amplification, which reduces the key length [13]–[16]. Note that achieving long raw keys does not necessarily imply long secret keys. A modulation scheme with a higher raw key might be more susceptible to noise and eavesdropping, and thus result in a relatively short secret key. Such considerations are beyond the scope of the current paper as we here are concerned only with the raw key rate.

A simple PPM scheme was proposed in [17]. Although the simple PPM scheme eliminates the effect of photon transmission losses, it is not efficient for preserving useful information. In [18], a generalized version of the simple PPM scheme, called adaptive PPM, was proposed which utilizes a good portion of the information discarded by the simple PPM scheme.

In this work, our goal is to show that carefully modeled modulations can offer substantial raw key rate improvements, and also to pave the way for further exploration of high rate, low latency quantum-secure networks. We propose a new photon arrival model, a discrete time model for the photon arrival process with geometric distribution replacing the Poisson, and establish a theoretical bound on the number of secret bits that can be generated under this model (see Sec. II). Inspired by [17], [18], we first propose a simple binning scheme and show that this scheme generates significantly lower information rate than what is theoretically possible. We then propose three adaptive schemes that increase the number of raw bits generated per photon, and compute and compare the information rates they offer. Unlike the schemes in [17], [18], we not only use the single occupied bins but also utilize the single empty bins to generate

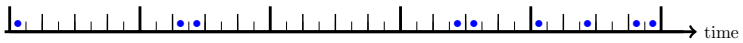

Fig. 1: Five frames consisting of 8 time units with bins consisting of 2 time units.

secret bits (see Sec. III). Furthermore, we investigate the effect of public channel communication on the secret key rates of the proposed schemes (see Sec. IV).

II. System Model

Throughout the paper the base of $\log$ is 2, unless explicitly noted otherwise. Consider a scenario wherein two parties, referred to as Alice and Bob, desire to generate a secret key using a quantum and a public channel. There is a third party, Eve, who has access to both channels. A source (possibly co-located with Alice) emits entangled photon pairs to Alice and Bob, with one photon being sent to Alice, and the other to Bob. We consider a system where information can be extracted by measuring random times of a sequence of photon arrivals. We assume that time is measured in units such that at most one photon can arrive in a single time unit (See Fig. 1). The length of a time unit equals the minimum time that a photon detector needs to successfully detect a single photon. We assume that a photon arrives in each time unit with probability p independently of other arrivals. The value of p depends on the number of photons generated per second by the source. A similar model was adopted in [4], [18]. Photons are not fully utilized unless the arrival time of each received photon can be used to contribute information.

Theorem 1. *The maximum number of bits per time unit that can be extracted from the timestamps of photon arrival times equals the binary entropy with parameter p.*

$$h(p) = -p \log p - (1-p) \log(1-p) \tag{1}$$

All the proofs can be found in the Appendix. Observe that this result implies that (under the assumed model) the photon timing information gives us as much information as would the binary sequence indicating the photon arrival times.

III. Proposed Schemes

Considering the ideal case wherein all the incoming photons are transmitted and detected successfully, Alice and Bob receive their shares of the entangled pairs at random but identical time units. Alice and Bob timestamp their photon arrivals, and map these timestamps to bit strings, which they subsequently process to generate their common key. In this section, we ignore the effect of communication over the public channel on the raw key rate of a scheme.

A. Simple Binning

In simple binning , time is partitioned in frames consisting of n time units. We take n to be a power of two. Fig. 1 shows an example where $n = 8$. Each frame is divided into n/k bins, each consisting of $k \leq n$ time units, and we are free to choose k. Note that k also needs to be a power of two in order for n to be divisible by k. Bins are labeled by $\log(n/k)$ bit strings. A bin is called occupied if there is at least one photon present in the bin. Alice and Bob are able to generate a common random sequence based on the position of a single occupied bin or a single empty bin in the frames.

Information is extracted from a sequence of frames as follows: All frames are discarded except those containing either a single occupied bin or a single empty bin. Each frame with a single occupied bin contributes $\log(n/k)$ key bits identifying the single occupied bin since all positions of the occupied bin are equally likely. Similarly, each frame with a single empty bin contributes $\log(n/k)$ key bits. When there is one occupied bin and one empty bin, Alice and Bob consider the bit string label of the occupied bin as their common random sequence. Note that communication over the public channel is not needed here.

In the example of Fig. 1, if the bin size is chosen to be 2, then the first 2 frames would contribute 2 bits each since there is only one occupied bin among the four bins in each frame. The third and the fourth frames would be discarded since one is empty and the other one consists of two occupied and two empty bins. The fifth frame also contributes 2 bits of information since it contains only one empty bin among its four bins. If, on the other hand, the bin size is chosen to be 1, then all but the first frame would be discarded, and we would be left with 3 bits of information.

The probability that a bin consisting of k time units is occupied is given by $\pi_k \triangleq 1 - (1-p)^k$. Let the probability that a bin consisting of k time units is empty be given by $\bar{\pi}_k \triangleq (1-p)^k$. We define the *raw key rate of a scheme* as the expected number of raw key bits per time unit.

Theorem 2. *Let n be the number of time units in a frame, and let each frame be divided into n/k bins, each consisting of $k \leq n$ time units. The raw key rate of the simple binning scheme is given by*

$$r_{SB} = \begin{cases} 0, & k = n, \\ \frac{1}{k}\pi_k \bar{\pi}_k, & k = \frac{n}{2}, \\ \frac{1}{k}\left[\pi_k \bar{\pi}_k^{\frac{n}{k}-1} + \pi_k^{\frac{n}{k}-1}\bar{\pi}_k\right] \log \frac{n}{k}, & \textit{otherwise}. \end{cases} \tag{2}$$

We define *the photon utilization of a scheme* as the ratio between its raw key rate and the rate of the ideal scheme given by (1). Fig. 2 depicts the performance of the simple binning scheme. Two crucial parameters in simple binning encoding are the bin width and the frame size, which have to be carefully

selected in order to maximize the photon utilization. The choice of these parameters also affects certain type of errors. It is therefore essential to understand the limitations that the system and physics impose on these parameters. Under no constraints, smaller bins and larger frames would maximize the photon utilization. However, physical constraints on energy-time entangled photons prevent the bin widths from becoming infinitely small. The minimum bin width is limited to the length of a time unit and the maximum frame size is limited by the coherence time of the entangled photon pair, which is determined by the spontaneous parametric down-conversion bandwidth [4], [12]. Observe that, under restrictive conditions, the highest photon utilization achievable by the simple binning scheme will be limited, e.g., it is about 0.5 for the frames of $n = 64$ time units. This low efficiency is due to discarding a large fraction of frames. We next propose three more efficient schemes which use all or at least a large fraction of the frames.

B. Adaptive Binning

The idea here is to not fix the size of the bins in advance, but instead adapt it to the photons observations for each frame. The size of the bins in a given frame is chosen by Alice and Bob deterministically based on the number and the locations of the photons observed in the frame as follows. Each bin is constructed using a collection of k consecutive time units. The bin construction starts from the first time unit and ends at the last time unit in the frame. Alice and Bob choose the minimum k that satisfies the following conditions: 1) the bins in a frame form a partition for the set of time units in the frame, and 2) either only one bin is occupied by photons among all the bins, or only one bin is empty among all the bins. We refer to these two conditions as the binning conditions. The rest follows the same steps as in the simple binning scheme.

In this scheme, communication over the public channel is not required because the bin construction is done deterministically. In the example of Fig. 1, for the first frame, the minimum bin size that satisfies the binning conditions is 1. Hence, the first frame contributes 3 bits of information. The proper bin size for the second frame is 2, and it contributes 2 bits of information. The third frame is discarded. Let the time units in the fourth frame be labeled $1, \ldots, 8$. If we consider $k = 2$, the bins will be $\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$, and $\{7, 8\}$. It is easy to see that the second and the third bins are occupied and the first and the fourth bins are empty. Thus, $k = 2$ does not satisfy the binning conditions. If we let the bin size be $k = 4$, we will be left with two occupied bins, and thus $k = 4$ also does not satisfy the binning conditions. Hence, the minimum bin size for the fourth frame that satisfies the binning conditions is $k = 8$. That is, the fourth frame consists of only one occupied bin. Thus, using this scheme, no information can be extracted from the fourth frame. The minimum bin size for the fifth frame that satisfies the binning conditions is 2.

There would be only one empty bin (third bin) among all four bins. Thus, the fifth frame also contributes 2 bits of information.

Theorem 3. *Let n be the number of time units and ℓ the number of photons in a frame. The raw key rate of the adaptive binning scheme is given by*

$$r_{AB} = \sum_{\ell=1}^{n/2} \sum_{i=\lceil \log \ell \rceil}^{\log(n/2)} \frac{1}{2^i} \binom{2^i}{\ell} p^\ell (1-p)^{n-\ell} + \sum_{i=0}^{\log(n/4)} \frac{1}{2^i} \pi_{\frac{n}{2^i}-1} \bar{\pi}_{2^i} (\log n - i). \tag{3}$$

C. Adaptive Aggregated Binning

In this scheme, the size of the bins in individual frames depends only on the number of photons observed in the frame. When a frame is occupied with $\ell \leq n/2$ photons, Alice partitions the set of time units in the frame into $m = n/2^{\lceil \log \ell \rceil}$ bins of size $k = 2^{\lceil \log \ell \rceil}$, denoted by $B_1, B_2, \ldots, B_m$. Then, Alice chooses a bin randomly, say B_i, and assigns all the ℓ time units carrying a photon to this bin. Also, from the remaining time units, $k - \ell$ randomly chosen time units will be assigned to B_i. After this step, from the remaining time units, k randomly picked time units will be assigned to each bin B_j for $j \in \{1, 2, \cdots, m\} \setminus i$. Note that there exists only one occupied bin and the position of this bin is uniformly distributed.

Otherwise, when $\ell > n/2$ photons have been observed in a frame, Alice partitions the set of the time units in the frame into $m = n/2^{\lfloor \log(n-\ell) \rfloor}$ bins of size $k = 2^{\lfloor \log(n-\ell) \rfloor}$, denoted by $B_1, B_2, \ldots, B_m$. Then, Alice chooses a bin randomly, say B_i, and assigns k randomly picked empty time units to this bin. From the remaining time units, Alice assigns k randomly chosen to each bin B_j for $j \in \{1, 2, \cdots, m\} \setminus i$. Note that there exists only one empty bin and the position of this bin is uniformly distributed. After forming the bins, Alice sends the binning information to Bob over the public channel.

In the example of Fig. 1, the first frame contributes 3 bits of information. The second and the fourth frames contribute 2 bits of information each since Alice is able to form 4 bins of size 2 where only one of the bins is occupied. The third frame would be discarded. The fifth frame contributes 1 bit of information since the time units in the frame can be partitioned into 2 bins of size 4 while only one of the bins is occupied.

Theorem 4. *Let n be the number of time units and ℓ the number of photons in a frame. The raw key rate of the adaptive aggregated binning scheme is given by*

$$r_{AAB} = \frac{1}{n} \left[\sum_{\ell=1}^{n/2} \binom{n}{\ell} p^\ell (1-p)^{n-\ell} \Big(\log n - \lceil \log \ell \rceil \Big) + \sum_{\ell=\frac{n}{2}+1}^{n-1} \binom{n}{\ell} p^\ell (1-p)^{n-\ell} \Big(\log n - \lfloor \log(n-\ell) \rfloor \Big) \right]. \tag{4}$$

D. Adaptive Framing

Unlike the other schemes, in this scheme, the bin size do not vary from frame to frame and for all the frames is $k = 1$. Having observed $\ell \leq n/2$ photons in a frame, the set of time units in the frame will be partitioned into ℓ subframes by Alice. It should be noted that a subframe does not consist of adjacent time units necessarily. Let $F_1, F_2, \ldots, F_\ell$ denote these subframes, and let $i_1, i_2, \ldots, i_\ell$ be the indices of the time units carrying a photon. At the beginning, Alice assigns the time unit i_j to the subframe F_j for $j \in \{1, 2, \cdots, \ell\}$. Then, starting from the first subframe, each subframe randomly picks an unassigned time unit. The previous step will be done repeatedly until all the time units have been assigned. In each subframe, there is exactly one bin occupied with a photon and its position is uniformly distributed. This procedure results in r subframes of size $m + 1$ and $\ell - r$ subframes of size m, where $n = m\ell + r$ and $0 \leq r < \ell$. Hence, each frame occupied with $\ell \leq n/2$ photons contributes $\rho = r \log(m + 1) + (\ell - r) \log m$ bits of information. The following lemma shows that this is the maximum information that can be extracted from a frame of size n containing $\ell \leq n/2$ photons using the adaptive framing scheme.

Lemma 1. *Let n be the size of a frame consisting of $\ell \leq n/2$ photons. Alice constructs ℓ sets and assigns one each of the occupied time units to the respective sets. The remaining time units are assigned at random to the sets. Let $d_i \geq 1$ denote the number of elements in set i. The total information that can be extracted from the frame is therefore $I = \sum_{i=1}^{\ell} \log d_i$. It holds that*

$$I = \sum_{i=1}^{\ell} \log d_i \leq r \log(m + 1) + (\ell - r) \log m,$$

where $n = m\ell + r$ and $0 \leq r < \ell$.

On the other hand, when the number of photons observed in a frame is $\ell > n/2$, Alice partitions the set of time units in the frame into $n - \ell$ subframes. Let $F_1, F_2, \ldots, F_{n-\ell}$ denote these subframes, and let $i_1, i_2, \ldots, i_{n-\ell}$ be the indices of the empty time units. First, the time unit i_j is assigned to the subframe F_j for $j \in \{1, 2, \cdots, n - \ell\}$ by Alice. Then, each subframe chooses an unassigned time unit at random starting from the first subframe. This step will be repeated until all time units have been assigned. In the end, there are $\bar{r}$ subframes of size $\bar{m} + 1$ and $n - \ell - \bar{r}$ subframes of size $\bar{m}$, where $n = \bar{m}(n - \ell) + \bar{r}$ and $0 \leq \bar{r} < n - \ell$. There is exactly one empty time unit in each subframe, and its position is uniformly distributed. Thus, each frame occupied with $\ell > n/2$ photons contributes $\bar{\rho} = \bar{r} \log(\bar{m} + 1) + (n - \ell - \bar{r}) \log \bar{m}$ bits of information. Using the following lemma, we show that this is the maximum information that can be extracted from a frame of size n containing $\ell > n/2$ photons using the adaptive framing scheme.

Lemma 2. *Let n be the size of a frame consisting of $\ell > n/2$ photons. Alice constructs $n-\ell$ sets and assigns one each of the empty time units to the respective sets. The remaining time units are assigned at random to the sets. Let $d_i \geq 1$ denote the number of elements in set i. The total information that can be extracted from the frame is therefore $I = \sum_{i=1}^{n-\ell} \log d_i$. It holds that*

$$I = \sum_{i=1}^{n-\ell} \log d_i \leq \bar{r} \log(\bar{m}+1) + (n-\ell-\bar{r}) \log \bar{m},$$

where $n = \bar{m}(n-\ell) + \bar{r}$ and $0 \leq \bar{r} < n-\ell$.

The subframes information will be sent to Bob over the public channel by Alice. In the example of Fig. 1, the first frame contributes 3 bits of information. The second and the fourth frames contribute 4 bits of information each. For instance, consider the second frame. Let index the time units in the second frame using the numbers 1 to 8. The time units 3 and 4 are occupied with photons. Alice forms two subframes denoted by F_1 and F_2, and assigns the time units 3 and 4 to these two subframes, respectively. Then, from the remaining time units, Alice assigns 3 time units to each subframe randomly as it was explained before, and sends the subframes information to Bob over the public channel. Thus, Alice and Bob have information about two subframes containing four time units while only one time units carries a photon in each subframe. These two subframes contribute 2 bits of information each. The third frame is discarded, and the fifth frame contributes 4 bits of information since it can be partitioned into 4 subframes of size 2 where there is one occupied time unit in each subframe.

Theorem 5. *Let n and ℓ denote the number of time units and the number of photons in a frame, respectively. The raw key rate of the adaptive framing scheme is given by*

$$r_{AF} = \frac{1}{n}\left[\sum_{\ell=1}^{n/2} \binom{n}{\ell} p^{\ell}(1-p)^{n-\ell}\rho + \sum_{\ell=\frac{n}{2}+1}^{n-1} \binom{n}{\ell} p^{\ell}(1-p)^{n-\ell}\bar{\rho}\right]. \tag{5}$$

IV. Effect of Public Channel Communication

In this section, we investigate the effect of public channel communication on the raw key rate. For the simple binning and the adaptive binning, communication over the public channel is not required. However, in the adaptive aggregated binning and adaptive framing, after each time frame, Alice needs to form bins or subframes and send the information to Bob over the public channel. Thus, for these two schemes, we partition time into a number of windows, which we further split into two phases: sensing phase and communication phase. In the sensing phase, which consists of n time units, Alice and Bob observe photon arrival times ,and in the communication phase, they talk over the public channel. Let D

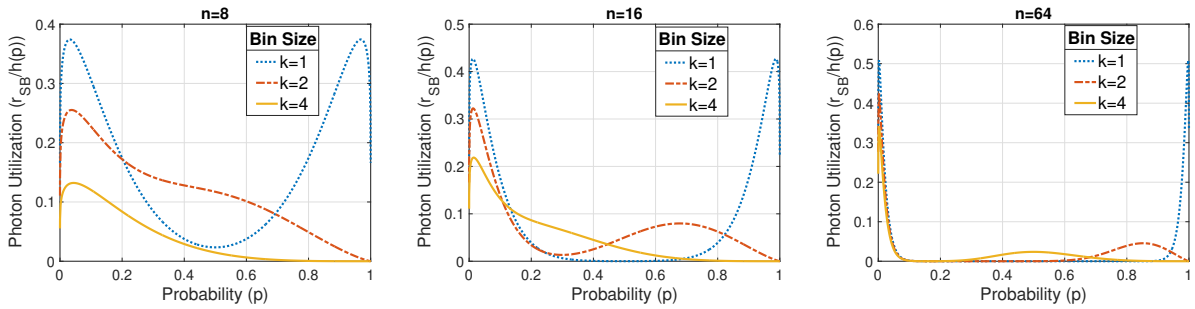

Fig. 2: Average photon utilization of the simple binning scheme vs. the time unit occupancy probabilities (cf. (1) and (2)), for: a) frames of $n = 8$ time units and three different bin sizes $k \in \{1, 2, 4\}$, b) frames of $n = 16$ time units and three different bin sizes $k \in \{1, 2, 4\}$, and c) frames of $n = 64$ time units and three different bin sizes $k \in \{1, 2, 4\}$.

and T denote the communication time over the public channel and the length of a time unit, respectively. Hence, the length of a window is $nT + D$ and the number of raw secret bits that a scheme generates in a window is given by $n\times$(raw key rate of the scheme). We define the *effective raw key rate of a scheme* as the expected number of raw key bits per time unit considering the effect of public channel communication. The raw key rates and the effective raw key rates of the simple binning and the adaptive binning schemes are the same. The effective raw key rate of the adaptive aggregated binning and adaptive framing schemes are given as follows

$$\tilde{r}_{AAB} = \frac{nT}{nT + D} r_{ABB},$$

$$\tilde{r}_{AF} = \frac{nT}{nT + D} r_{AF}.$$

Note that the typical length of a time unit is about tens of picoseconds (10^{-12} seconds) [5], [12].

V. Comparison Results

In this section, we evaluate and compare the performance of the proposed schemes. Fig. 2 illustrates the performance of the simple binning scheme. It can be observed that for all three different frame sizes, the maximum photon utilization is achieved when the bin size is set to 1. It can also be seen that increasing the frame size improves the highest achievable photon utilization for all three different bin sizes. Note that, for some range of the time unit occupancy probability, bin sizes $k = 2$ and $k = 4$ result in a higher photon utilization in comparison to bin size $k = 1$.

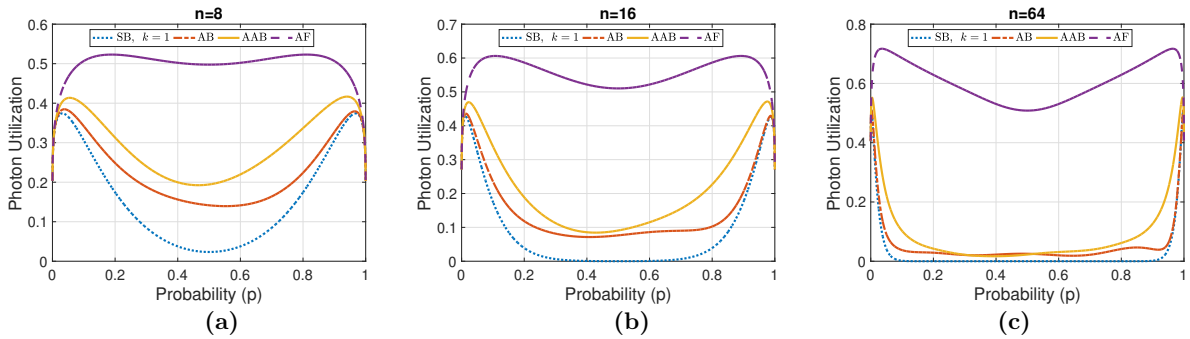

Fig. 3: Average photon utilization of the simple binning (SB) for bin size $k = 1$ (cf. (2)), the adaptive binning (AB) (cf. (3)), the adaptive aggregated binning (AAB) (cf. (4)), and the adaptive framing (AF) (cf. (5)) schemes vs. the time unit occupancy probability, for: a) frames of $n = 8$ time units, b) frames of $n = 16$ time units, and c) frames of $n = 64$ time units.

The photon utilization of the simple binning (SB) for bin size $k = 1$, the adaptive binning (AB), the adaptive aggregated binning (AAB), and the adaptive framing (AF) schemes as a function of the time unit occupancy probability is depicted in Fig. 3. Observe that the AF outperforms the other three schemes for all range of the time unit occupancy probability. For all four schemes, the highest photon utilization is obtained when the time unit occupancy probability is either close to 0 or close to 1. Moreover, the performances of all the schemes are identical when time unit occupancy probability is very small or very large, since almost all the occupied frames carry 1 photon or $n - 1$ photons, respectively. Note that, although the AF and the AAB have a superior performance in comparison to the SB and the AB, they require public channel communication.

REFERENCES

[1] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, no. 1, Nov 2016. [Online]. Available: http://dx.doi.org/10.1038/npjqi.2016.25

[2] N. Islam, C. Lim, C. Cahall, J. Kim, and D. Gauthier, "Provably-secure and high-rate quantum key distribution with time-bin qudits," *Science Advances*, vol. 3, 09 2017.

[3] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018. [Online]. Available: https://science.sciencemag.org/content/362/6412/eaam9288

[4] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," *Phys. Rev. Lett.*, vol. 98, p. 060503, Feb 2007.

[5] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, "High-rate field demonstration of large-alphabet quantum key distribution," 2016.

[6] M. C. Sarihan, K.-C. Chang, X. Cheng, Y. S. Lee, T. Zhong, H. Zhou, Z. Zhang, F. N. Wong, J. H. Shapiro, and C. W. Wong, "High dimensional quantum key distribution with biphoton frequency combs through energy-time entanglement,"

in *Conference on Lasers and Electro-Optics*. Optical Society of America, 2019, p. FTh1A.3. [Online]. Available: http://www.osapublishing.org/abstract.cfm?URI=CLEO˙QELS-2019-FTh1A.3

[7] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.*, vol. 88, p. 127902, Mar 2002. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.88.127902

[8] G. M. Nikolopoulos and G. Alber, "Security bound of two-basis quantum-key-distribution protocols using qudits," *Phys. Rev. A*, vol. 72, p. 032320, Sep 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.72.032320

[9] G. M. Nikolopoulos, K. S. Ranade, and G. Alber, "Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication," *Phys. Rev. A*, vol. 73, p. 032325, Mar 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.73.032325

[10] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," *Phys. Rev. A*, vol. 82, p. 030301, Sep 2010. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.82.030301

[11] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, "Security of high-dimensional quantum key distribution protocols using franson interferometers," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 46, no. 10, p. 104010, may 2013.

[12] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," *New Journal of Physics*, vol. 17, no. 2, p. 022002, feb 2015. [Online]. Available: https://doi.org/10.1088/1367-2630/17/2/022002

[13] H. Zhou, L. Wang, and G. Wornell, "Layered schemes for large-alphabet secret key distribution," in *2013 Information Theory and Applications Workshop (ITA)*, Feb 2013, pp. 1–10.

[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. USA: Cambridge University Press, 2011.

[15] S. Yang, M. C. Sarihan, K.-C. Chang, C. W. Wong, and L. Dolecek, "Efficient information reconciliation for energy-time entanglement quantum key distribution," 2020.

[16] H. Mao, Q. Li, Q. Han, and H. Guo, "High throughput and low cost ldpc reconciliation for quantum key distribution," 2019.

[17] Y. Kochman and G. W. Wornell, "On high-efficiency optical communication and key distribution," in *2012 Information Theory and Applications Workshop*, Feb 2012, pp. 172–179.

[18] H. Zhou and G. Wornell, "Adaptive pulse-position modulation for high-dimensional quantum key distribution," in *2013 IEEE International Symposium on Information Theory*, July 2013, pp. 359–363.

APPENDIX

PROOF OF LEMMAS AND THEOREMS

Proof of Theorem 1: The photon inter-arrival times are geometrically distributed. Thus, the maximum information that can be extracted from an observed photon is equal to the entropy of a geometric random variable with parameter p, which is given by $[-p\log p-(1-p)\log(1-p)]/p$. In the period of n time units, the average number of observed photons is equal to np, and thus the average number of bits that can be extracted in the period of n time units is $n[-p\log p-(1-p)\log(1-p)]$. Hence, the number of bits per time unit that can be obtained on average is given by $h(p)=-p\log p-(1-p)\log(1-p)$. $\square$

Proof of Theorem 2: Let A denote the event that there is only one occupied bin in a frame. The probability of event A is given by $P(A) = \binom{n/k}{1}\pi_k\bar{\pi}_k^{n/k-1}$. Also, let the event that only one empty bin exists in a frame be denoted by B. The probability of event B is given by $P(B) = \binom{n/k}{1}\pi_k^{n/k-1}\bar{\pi}_k$. The raw key rate of the simple binning scheme is given by $r_{SB} = \frac{1}{n}P(A \cup B)\log(n/k)$. For the case $k = n$, we have $\log(n/k) = 0$ and consequently $r_{SB} = 0$. The case $k = n/2$ indicates that there are two bins of size $n/2$ in a frame. One can readily confirm that the events A and B are equivalent for this case. Thus, we have $P(A) = P(B) = P(A \cap B)$. Note that $\log(n/k) = 1$ and $P(A \cup B) = P(A) = \frac{n}{k}\pi_k\bar{\pi}_k$ when $k = n/2$. Therefore, $r_{SB} = \frac{1}{k}\pi_k\bar{\pi}_k$ for the case $k = n/2$. For the cases where $k \leq n/4$, we have $P(A \cap B) = 0$ and consequently $P(A \cup B) = P(A) + P(B) = \frac{n}{k}\left[\pi_k\bar{\pi}_k^{\frac{n}{k}-1} + \pi_k^{\frac{n}{k}-1}\bar{\pi}_k\right]$. Thus, $r_{SB} = \frac{1}{k}\left[\pi_k\bar{\pi}_k^{\frac{n}{k}-1} + \pi_k^{\frac{n}{k}-1}\bar{\pi}_k\right]\log\frac{n}{k}$ when $k \leq n/4$. □

Proof of Theorem 3: Given that ℓ photons have been observed in a frame, the probability that bins of size k satisfy the binning conditions such that there is only one occupied bin in the frame is given by $p_k(\ell) = \binom{n/k}{1}\binom{k}{\ell}p^\ell(1-p)^{n-\ell}$. When $k < \ell$, it is assumed that $p_k(\ell) = 0$. Note that k is not necessarily the minimum bin size that satisfy the binning conditions, and thus $p_k(\ell)$ includes all the cases that $k/2^i$, $i \in \{0, 1, \cdots, \log k\}$, is the minimum bin size that satisfies the binning conditions. Hence, the probability that k is the minimum bin size that satisfies the binning conditions such that there is only one occupied bin in the frame is given by $p_k(\ell) - p_{k/2}(\ell)$. The number of bits obtained by the cases wherein there is only one occupied bin in the frame is given by $\sum_{\ell=1}^{n/2}\sum_{i=\lceil\log\ell\rceil}^{\log(n/2)}\left(p_{2^i}(\ell) - p_{2^{i-1}}(\ell)\right)(\log n - i)$. We can simplify $\sum_{i=\lceil\log\ell\rceil}^{\log(n/2)}\left(p_{2^i}(\ell) - p_{2^{i-1}}(\ell)\right)(\log n - i)$ by expanding it as follows. Let $x \triangleq \lceil\log\ell\rceil$ and $y \triangleq \log n$. Note that $p_{2^{x-1}}(\ell) = 0$ since $2^{x-1} < \ell$.

$$\sum_{i=x}^{y-1}\left(p_{2^i}(\ell) - p_{2^{i-1}}(\ell)\right)(y-i) = \cancel{p_{2^x}(\ell)(y-x)}$$

$$\cancel{+p_{2^{x+1}}(\ell)(y-x-1)} \cancel{-p_{2^x}(\ell)(y-x)} + p_{2^x}(\ell)$$

$$\cancel{+p_{2^{x+2}}(\ell)(y-x-2)} \cancel{-p_{2^{x+1}}(\ell)(y-x-1)} + p_{2^{x+1}}(\ell)$$

$$\vdots$$

$$+ p_{2^{y-1}}(\ell)(y-y+1) \cancel{-p_{2^{y-2}}(\ell)(y-y+2)} + p_{2^{y-2}}(\ell)$$

$$= p_{2^x}(\ell) + p_{2^{x+1}}(\ell) + \cdots + p_{2^{y-2}}(\ell) + p_{2^{y-1}}(\ell) = \sum_{i=x}^{y-1} p_{2^i}(\ell)$$

The probability that k is the minimum bin size that satisfies the binning conditions such that there is only one empty bin in the frame is given by $\binom{n/k}{1}\pi_k^{\frac{n}{k}-1}\bar{\pi}_k$, where $k < n/2$. Note that $k = n/2$ has already been addressed as it is the same for the case that there is only one occupied bin in the frame. The number of bits obtained by the cases wherein there is only one empty bin in the frame is given by $\sum_{i=0}^{\log(n/4)}\binom{n/2^i}{1}\pi_{2^i}^{\frac{n}{2^i}-1}\bar{\pi}_{2^i}\log(\frac{n}{2^i})$. Thus, the raw key rate of the adaptive binning scheme is given by

$$r_{AB} = \frac{1}{n}\left[\sum_{\ell=1}^{n/2}\sum_{i=\lceil\log\ell\rceil}^{\log(n/2)} p_{2^i}(\ell) + \sum_{i=0}^{\log(n/4)}\binom{n/2^i}{1}\pi_{2^i}^{\frac{n}{2^i}-1}\bar{\pi}_{2^i}\log(\frac{n}{2^i})\right].$$

□

Proof of Theorem 4: In the adaptive aggregated binning scheme, when a frame contains $\ell \leq n/2$ photons, the time units in the frame are partitioned into $m = n/2^{\lceil\log\ell\rceil}$ bins of size $2^{\lceil\log\ell\rceil}$ such that only one of the bins is occupied. Thus, each frame containing $\ell \leq n/2$ photons contributes $\log m = \log n - \lceil\log\ell\rceil$ bits of information. The probability that ℓ photons are observed in a frame is given by $\binom{n}{\ell}p^\ell(1-p)^{n-\ell}$. Using a similar argument, one can show that each frame consisting of $\ell > n/2$ photons contributes $\log n - \lfloor\log(n-\ell)\rfloor$ bits of information. Thus, it is easy to see that (4) gives the raw key rate of the adaptive aggregated binning scheme. □

Proof of Lemma 1: If $r = 0$, this inequality is an immediate consequence of Jensens inequality and the concavity of the log function. Hence, suppose $r > 0$. There must be at least one i such that $d_i \leq m$ as otherwise $n < \ell(m+1) \leq \sum_{i=1}^{\ell}\log d_i$ which contradicts that the d_i's sum to n. Similarly, there is an i such that $d_i \geq m+1$. We will now show that if there is an i such that $d_i < m$ or $d_i > m+1$, then I can be strictly increased. First, suppose that there is an i_j such that $d_{i_j} < m$, and an i_h such that $d_{i_h} > m+1$. We may suppose these correspond to the largest and the smallest sets. Then, take an empty time unit from a set of size d_{i_h} and place it in one of the sets of size d_{i_j}. Since the log function is strictly increasing and strictly concave, we gain $(\log(d_{i_j}+1) - \log d_{i_j}) - (\log d_{i_h} - \log(d_{i_h}-1)) > 0$. Clearly, such exchanges can continue until either all sets have at least m members or no set has more than $m+1$ members. If all sets are of size m or $m+1$, then the argument is complete. Now, suppose that there is a set with more than $m+1$ time units with the remaining sets having m. Then, the number of sets of size m must be equal to $\ell - r + f$ with $f > 0$ as the total number of time units is equal to n. Now, take an empty time unit from the set with largest size and place it in a set of size m, which gives an increase in information as before. Repeat this until f becomes 0 so that I becomes $r\log(m+1) + (\ell - r)\log m$. A similar argument applies if there is a set $d_i < m$, and the remaining sets all have $m+1$ time units. □

Proof of Lemma 2: The proof is similar to the proof of Lemma 1, and thus omitted for the purpose of brevity. □

Proof of Theorem 5: It has been already shown that, in the adaptive framing scheme, each frame occupied with $\ell \leq n/2$ photons contributes $\rho = r\log(m+1) + (\ell - r)\log m$ bits of information, where $n = m\ell + r$ and $0 \leq r < \ell$. Also, it has been shown that each frame occupied with $\ell > n/2$ photons contributes $\bar{\rho} = \bar{r}\log(\bar{m}+1) + (n-\ell-\bar{r})\log\bar{m}$ bits of information, where $n = \bar{m}(n-\ell) + \bar{r}$ and $0 \leq \bar{r} < n - \ell$. The probability that ℓ photons are observed in a frame is given by $\binom{n}{\ell}p^{\ell}(1-p)^{n-\ell}$. Thus, it is easy to see that (5) gives the raw key rate of the adaptive framing scheme. □