Information Rates with Non Ideal Photon Detectors in Time-Entanglement Based QKD

Christopher Cheng, *Member, IEEE,* Christopher Cheng, *Fellow, OSA,*

and Emina Soljanin, *Fellow, IEEE*

Abstract

In modern implementations of QKD, we establish a cryptographically secure encryption key between two communicating parties by distributing entangled photons between them. In theory, security is guaranteed by the fact that any eavesdroppers attempting to measure the photons will disturb their entanglement, leading to channel errors which can be discarded in post-processing steps. These entangled photons are most commonly produced using an SPDC crystal, wherein each photon passing through has a chance of spontaneously splitting into an entangled photon pair. The simplest way to extract key bits from these photons is measuring their polarization, a method which yields us one key bit per photon at best. Unfortunately, the SPDC effect occurs fairly rarely, leading to ”photon-scarce” conditions that call for alternative methods. One promising method involves using the time of arrival (ToA) of the photons at each detector to extract data. This is because it turns out that polarization isn’t the only thing that’s entangled; both photons in the pair are created at the same time, resulting in time-entanglement. This leads to a strong correlation between the ToAs observed at each detector, where we can use specially-designed binning schemes to extract more than one key bit per photon. However, there is a limit to how much improvement we can squeeze out by changing our method of bit extraction – it seems to be the case that with current hardware, QKD is not yet able to deal with the immense amounts of internet traffic supported by modern cryptographic ”infrastructure”. Therefore we must take the initiative to design our methods with the hardware of the future – in which our detectors and photon sources are

The authors are with the Department of Electrical and Computer Engineering, Rutgers University, New Jersey.

greatly improved – in mind. In doing this, we realize that there are more pitfalls than one might expect. In this paper, we will explore the key rates we can achieve with this bit extraction method and introduce the pitfalls we observed and how to get around them.

Index Terms

IEEEtran, journal, LaTeX, paper, template.

I. INTRODUCTION

In this article, we will consider a setup in which two parties, which we may call Alice and Bob, share a quantum channel and a public classical channel. The goal is to establish an encryption key between them only by using those channels. To address photon-scarce conditions, we turn to time-entanglement and use the ToA at each detector to extract key bits. To see how this allows us to extract more than one key bit (and thus show that using only time-entanglement is superior to using only polarization-entanglement in these conditions), consider a binning scheme known as Pulse Position Modulation, or PPM. In PPM, we break time apart into equally-sized pieces called bins, and group a certain number of bins n together into a ”frame”. Each bin can be represented by a single bit; 1 if it contains at least one photon, and 0 otherwise. We then perform a one-hot decoding on each frame – all frames that contain a single 1 are decoded, and all other frames are discarded. The bits extracted per valid frame is $\log_2(n)$, so if n is larger, more bits can be extracted from a valid frame – but make n too large, and the probability that a frame is valid will start to drop, thus reducing the overall number of bits extracted. This directly leads to a maximization problem; if the probability of a bin being occupied is p, then the average bits per frame R is:

$$R = \log_2(n) np(1-p)^{n-1} \tag{1}$$

We can address this by reducing the bin width k. However, reducing k too much will expose us to jitter errors.

To increase key rates, we can generally address two points:

1) Increase detector resolution & accuracy
2) Increase the rate of entangled photon-pair production

In other words, we can improve things at the source or the destination. By increasing detector resolution, you directly increase the number of bits which can be practically extracted per photon using timing. On the other hand, by increasing the pair production rate, you can achieve greater key rates without any change at the detector. Then, what if we improve both at the same time? Unfortunately, it isn't that simple. Turn the pair production too high and the key rate obtained through time-entanglement actually starts to fall due to an effect known as detector recovery-time. At this point, it may be better to simply return to the polarization-based method of extracting photon data. So at what point should the switch happen? Is recovery-time always bad? And could there be another way to improve key rate?

II. Preliminaries and Definitions

In support of the following sections, we define some variables and establish some background with regards to the properties of entangled photon pair sources and single photon detectors involved in QKD.

A. *QKD Preliminaries*

Broadly, in Quantum Key Distribution, two communicating parties (Alice and Bob) generate identical secret keys by distributing and measuring entangled elements of reality. Properties of quantum mechanics predict that they will receive the same result given they perform the same measurements. Entanglement based QKD also leverages quantum mechanics as a source of randomness theoretically providing perfect randomness. Polarization entanglement based QKD relies on measuring photons entangled in polarization such that a secret bit is received from each photon pair. Time Entanglement QKD is a specific variant which aims to increase secret key generation rates by retrieving multiple random key bits from each distributed entangled photon pair. This is done by measuring the entangled time of arrival (ToA) of a Spontaneous Parametric Down Conversion (SPDC) generated photon pair. Thus, an arbitrary amount of bits can be extracted given sufficient ToA measurement precision. The experiment we model here has a single SPDC photon source which sends one photon of each entangled pair to two measurement stations comprised of an interferometer and a Single Photon Detector (SPD) with a ToA readout. The interferometers are used to approximate the level of entanglement shared in a sample of photon pairs and can be used to bound the level of passive eavesdropping on the quantum channel. We will not focus on this quantum eavesdropping and assume there is none for this work.

B. Key Extraction

Alice and Bob rely on the correlated random photon arrivals to generate their secret keys. There are many possible methods to extract keys from this correlated information. One popular method is to use Pulse Position Modulation (PPM). In PPM Alice and Bob synchronize their clocks and discretize their timelines into time frames of size T_f each consisting of N time bins. Each time bin has a width of $\tau_b = T_f/N$. In PPM Alice and Bob agree to only consider time frames in which they both detect only a single photon arrival. This single photon is said to occupy a time bin depending on where within the frame it arrives. The bin count within the time frames is usually a factor of 2 such that we can extract $\log_2(N)$ bits from each frame based on the position of the occupied time bin within the given frame. As we only consider frames with a single arrival, PPM can be considered sub optimal.

PPM is illustrated in Figure 1 where we see an example scenario in which Alice and Bob agreed to discretize their timelines into time frames consisting of 4 time bins. We see that they both throw out the second frame because Alice detected an extra dark count in her frame. We can see that the first time frame works as expected and both parties extract the same key bits

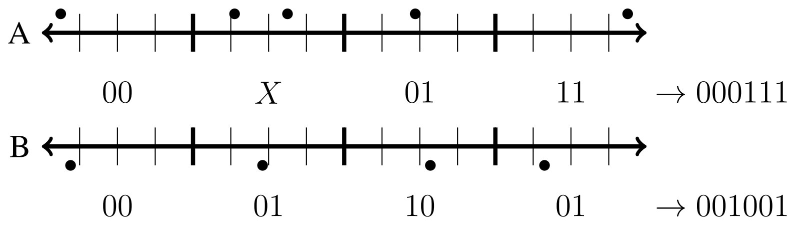

Fig. 1: Two potential arrival sequences at Alice's and Bob's stations

despite some small timing jitter that fits within the time bin. The third time frame, shows the way the timing jitter can cause errors in the system. Here the jitter caused the photons to be detected in separate bins and thus caused two bit errors. The final frame shows an example where Alice and Bob both detect a dark count in the same time frame. To them, this seems like a valid PPM frame despite the resultant bits being entirely uncorrelated. The specific design parameter choice can greatly affect the rate of each kind of error. Smaller bins leads to more potential bits per time frame but increases the likelihood of having jitter errors. Furthermore, larger time frames can lead to more unusable time frames due to multiphoton arrival events as in frame two of the example.

C. *SPDC Source Model*

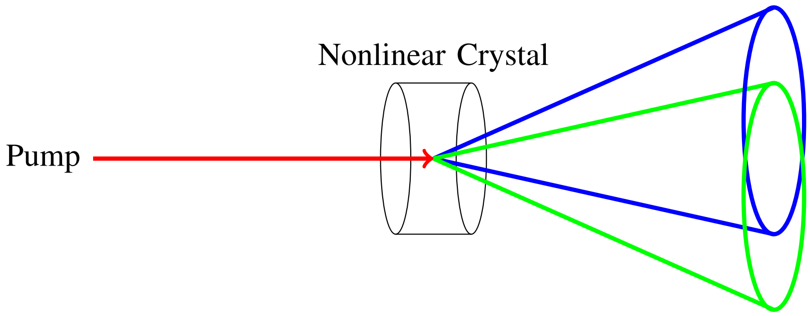

Fig. 2: SPDC Source generating photon pair in the state $|\phi\rangle = \frac{1}{\sqrt{N}} \int_{t_0}^{t_0+t_c} |t_A\rangle \, |t_B\rangle \, dt$

In Quantum Information experiments, entangled photons are most commonly generated by Spontaneous Parametric Down-Conversion (SPDC). This process takes place when a single photon passes through a non-linear crystal and splits into two photons which conserve energy and momentum. This process occurs randomly and extremely rarely at a rate on the order of $10^6 s^{-1} mW^{-1}$ [**?**]. Photons emitted from this type of source are coherent within a time window referred to as the pump coherence time (t_c). This parameter is used in the key extraction step as a limit to the time frame length. Photon pairs generated in this way arrive according to a Poisson Process. We parametrize this process using a rate variable λ_p to refer to the rate of entangled photon arrivals per unit time. In Figure 2 a simplified SPDC source is shown. Each degenerate photon pair will conserve momentum and thus one photon will travel along each of the two light cones illustrated. The photons selected at the intersection points of the cones are indistinguishable and exist in superposition. These entangled pairs are selected out and one photon is sent to Alice and one to Bob. The superposition in time can be described by the state in the figure where each photon pair is generated at any time within the coherence time and all generation times are equally likely. This is both our source of randomness and the method by which we ensure Alice and Bob base their keys off shared information.

D. Single Photon Detector Model

For QKD based on ToA measurements the most common single photon detectors are Superconducting Nanowire Single Photon Detectors (SNSPDs). These detectors currently exhibit properties closest to those of the ideal detectors. They have high efficiency, meaning they detect the majority of incident photon arrivals accurately. They also have low dark count rates, meaning they rarely report photon detections in the absence of photon arrivals. Furthermore, and perhaps most importantly, they have low detector downtime (d), small detector noise variance (σ_d^2). These two parameters are what we are most concerned with in this work. These imperfections lead to loss of entropy and higher bit error rates respectively. The detector jitter manifests as

Gaussian noise additive with the time of arrival. The SPDC source will generate a photon pair uniformly within the coherence time. We model this process as a uniform random variable U. The detected time on Alice's (Bob's) station will thus be described by the random variable t_A $(t_B) \sim U + N(0, \sigma_d^2)$. The detector downtime has a more complicated relation to the entropy of the system. When one photon is detected by the SPD, the detector goes into a down state wherein no other photon arrivals can be detected. This down time can have severe effects on the entropy if the photon arrival rate is very high compared to the counting rate allowed by this down time. Dark counts can cause significant errors if they make up a large portion of the detected photons. Primarily dark counts are a result of light leakage into the optical lines. We analyze the effect of considering dark counts in our model in the Appendix. Detector jitter is characterized as a Gaussian uncertainty around the actual detection time. However, the observed jitter errors occur due to both Alice and Bob's detector jitter. Thus, the observed jitter errors resulting from detector imperfection are distributed according to the convolution of the individual detector jitter probability density functions. Many commercial single photon detectors offer detector jitter specifications in terms of the full width half maximum of this uncertainty. We can calculate the variance of certain detectors from this specification and then determine the variance of the observed jitter errors by convolving the two distributions. This results in a Gaussian distribution with twice the variance as the detector jitter.

E. Eavesdropping Model

The system as described so far allows for the generation of identical raw encryption keys at two locations with guaranteed security against passive eavesdropping. Unfortunately, with the imperfections in the experimental system we cannot expect these raw keys to necessarily agree or be entirely random. To correct the errors between the keys, Alice and Bob must perform a process called information reconciliation, and to regain the lost randomness, they must perform privacy amplification. Both of these procedures reduce the key length. In this work, we assume

Parameter Variable	Definition
t_c	Laser Pump Coherence Time
λ_p	Entangled Photon Generation Rate
d	Detector Down Time
σ_d^2	Detector Jitter Variance
T_f	Time Frame Width
N	Time Bins per Time Frame
τ_b	Time Bin Width

Fig. 3: Parameters of Interest

there has been no eavesdropping on the quantum channel, but we assume that a malicious eavesdropper has total access to all public discussion necessary for information reconciliation. Thus, this extra loss of entropy must be accounted for in the privacy amplification step as well. Choice of information reconciliation code here can greatly affect the amount of entropy loss needed to regain key agreement and thus can have a great effect on the secret key rate post privacy amplification.

F. Problem Formulation and Summary of Results

III. Information Loss due to Error Reconciliation

we lose key rate because we expose parity bits on the public channel

IV. Information Loss due to Down Time

Down-Time is a somewhat sneakier form of information loss. This is because in theory, ”errors” caused by down-time aren’t accounted for by typical error reconciliation techniques. In this way, down-time can be categorized as a ”synchronous” error, because it does damage to our

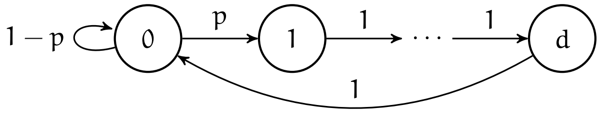

Fig. 4: Each bubble represents the state of the detector, and arrows show the probability of transitions between each state. State 0 represents the detector in its default state of being able to register photon arrivals. What this Markov Chain represents is that the detector sees a photon with probability p, and once it does it enters into a period of down-time lasting for d states.

key bits the same way for both parties. Recall that our input bit sequence, which we then run through a binning scheme (ppm or otherwise) to extract our raw key bits, could be modelled by a Bernoulli distribution. The key here is that bin occupancies were origin ally independent. But after introducing down-time, it could be that photon detections in one bin end up preventing the detection of photons in subsequent bins. That is, memory has been introduced into the system. As a result, we've taken to Markov Chains (a way to model the statefulness of the system) to tackle the problem of describing this new down-time afflicted system.

Taking this new detector down-time behavior into account, we can construct a Markov Chain that mirrors the bin-by-bin state of the detector. See Fig.4.

The Markov Chain entropy of the Markov Chain seen in Fig.4 gives us an upper bound on the information rate of our extracted key. This upper bound is as follows:

$$R_{ToA}(p,d) \leq \frac{h(p)}{1+pd} \text{ bits/bin}$$

By plotting this bound as a curve, one can observe that as d increases, the maximum key rate decreases, and is given by smaller values of p. Those in charge of designing QKD systems of the future must be aware of this, lest they set the value of p too high, thinking that more photons will necessarily give us more information rate. This is especially the case when it comes to binning schemes such as PPM. To see why, consider Fig.5, which depicts the key rate when we use PPM,

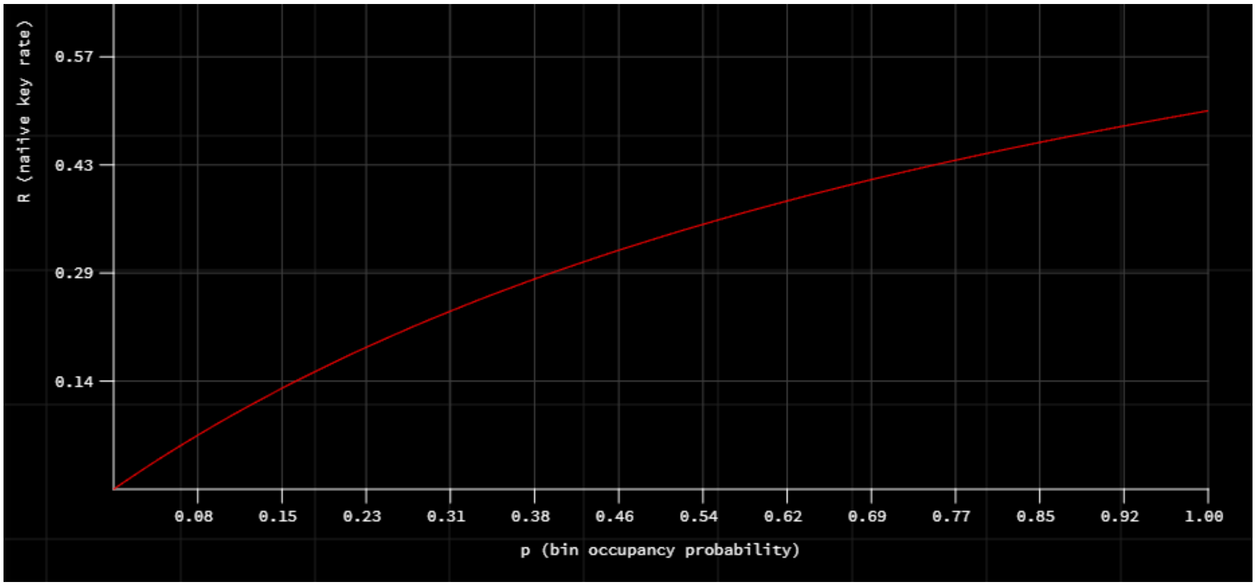

Fig. 5: The key rate when we use PPM, plot as a function of p. Here, we are *not* taking into account the loss of entropy by any mechanism, and only show the number of bits we get per bin as a result of using the PPM binning scheme on the input we get from the detector. This image was generated using an online tool that can be found at the following URL: https://cc1539.github.io/qkd-binning-demo-2/

plot as a function of p. As p approaches 1, it seems that the raw key rate approaches a maximum. But we just saw before that the information rate approaches 0 at the extremes of p. Indeed, when p is high, the entropy of the raw key gets lower and lower until at $p = 1$, we theoretically have a deterministic sequence which may yield a lot of literal bits, but no information, and definitely no security against attackers who are aware of the system configuration. Consider Fig.6, in which we do take into account the loss of entropy through down-time. Note how if down-time is low enough compared to the frame-size, this effect does not manifest, and raw key rate decreases just as information rate does. But realistic values for down-time and frame-size as seen in [source] and [source] suggest that down-time is typically much larger than a single frame-width. When this happens, we will see the phenomenon we observed earlier, with the raw key rate increasing

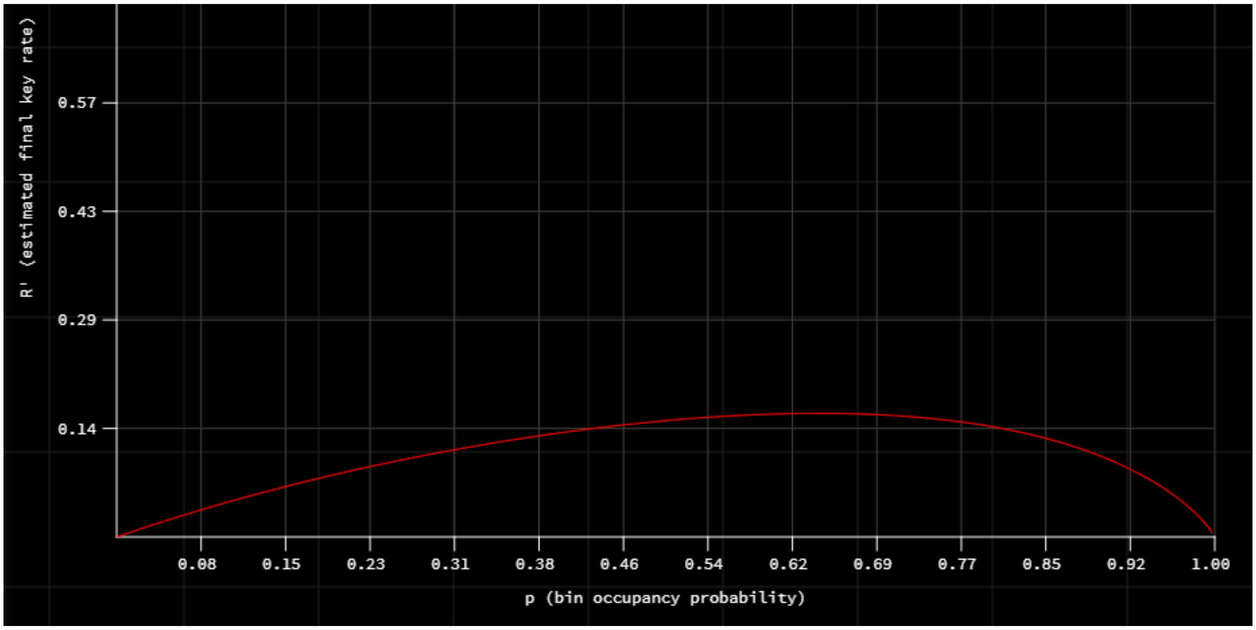

Fig. 6: The key rate when we use PPM, plot as a function of p. Here, we *are* taking into account the loss of entropy (as a result of down-time only). This image was generated using an online tool that can be found at the following URL:
https://cc1539.github.io/qkd-binning-demo-2/

while the information of the key decreases. So the behavior we observe in Fig.6 is actually the behavior we may observe in practical systems. Therefore once again, one must be careful not to increase λ_p (and subsequently p) too high without also taking the effects of down-time into account.

V. Conclusion

The conclusion goes here. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Appendix A
Dark Count Model–Not Organized

The arrivals of these dark counts are distributed according to a Poisson process much like the entangled photon arrivals but with a different rate parameter for each arm of the experiment. We will refer to these rates for Alice and Bob respectively, using the parameters λ_A^{dc} and λ_B^{dc}.

The frame-coincident dark count arrivals also contribute to the observed jitter error distribution. As shown earlier, when two dark counts arrive in the same frame Alice and Bob see this frame as PPM valid. Dark counts are uniformly distributed within a given time frame. Thus, to determine the distribution of the observed jitter from coincident dark counts, we convolve two uniform distributions over the time frame width. The convolution of two uniform distributions results in the triangular distribution with a peak at jitter value 0 $\mathrm{Tri}(f) = \frac{1}{f} - \frac{1}{f^2}|x|$. We consider this as a different type of observed jitter error and better model the observed error statistics that we see in experimental results. As such we can write the distribution of observed jitter errors as a weighted sum of the distribution of pure jitter errors and jitter errors due to coincident dark counts.

The weighting term is a function of the frame size as it represents the ratio between the probability that a frame is PPM valid due to an SPDC photon pair to the total probability that a frame is PPM valid. Given a specific frame size parameter, we get:

$$\begin{aligned}
p(t_j) &= c(f_{size})N(0,\sigma_d^2) + (1 - c(f_{size}))\,\mathrm{Tri}(f_{size}) \\
p_{frame}^{spdc} &= \lambda_p f_{size}\exp\left(-\lambda_p f_{size}\right) \\
p_{frame}^{dc} &= \lambda_{A/B}^{dc} f_{size}\exp\left(-\lambda_{A/B}^{dc} f_{size}\right) \\
c(f_{size}) &= \frac{p_{ppm}^{spdc}}{p_{ppm}^{total}} \\
&= \frac{p_{ppm}^{spdc}}{p_{ppm}^{spdc} + p_{ppm}^{DC} - p_{ppm}^{spdc} p_{ppm}^{DC}}.
\end{aligned}$$

Using what we know about photon arrivals already we can model what we expect our detectors to see as a combination of the model of SPDC arrivals and the model of dark counts. This allows us to find the probability of detecting a PPM valid time frame and can help to optimize our time frame size before trying to optimize our bin size.

Given our arrival rates, we know that the probability of detecting a PPM valid frame due to SPDC generated entangled photons is,

$$p_{ppm}^{spdc} = \lambda_p f_{size}\exp\left(-\lambda_p f_{size}\right).$$

Likewise, the probability that a PPM valid frame is detected due to dark counts alone is,

$$p_{ppm}^{DC} = \lambda_A^{dc}\lambda_B^{dc} f_{size}^2 \exp\left(-(\lambda_A^{dc} + \lambda_B^{dc}) f_{size}\right).$$

Thus, The total probability that a time frame is PPM valid is,

$$p_{ppm}^{total} = p_{ppm}^{spdc} + p_{ppm}^{DC} - p_{ppm}^{spdc} p_{ppm}^{DC}.$$

To maximize the photon utilization, we must maximize the probability that each frame is PPM valid. We also must balance this optimization with the fact that the PPM valid frames due to dark counts are unusable and contribute a large number of errors. For this reason, it is extremely important to get dark counts as low as possible in experiments.

Appendix B

Notes

How are λ_p and t_c related? Why?

How are T_f and t_c related? Why?

1) Chris: Suppose we observe the system for some long period of time $T = m \cdot T_f$. Then $T\lambda_p$ photons will arrive whp. In polarization based QKD, we will get $T\lambda_p$ bits (1 bit per photon).

Any time entanglement based scheme with bin size τ_b, can give us at most $h(p_b)$ bits per bin where $p_b = 1 - e^{-\lambda_p \tau_b}$. With bin size τ_b and n bins per frame, we have nm bins in the interval $T = T_f m$ Therefore, we get at most

$$\frac{h(p_b) \cdot nm}{T_f m \lambda_p} = \frac{h(p_b)}{\tau_b \lambda_p}$$

bits per photon. Consequently, we need

$$\tau_b \lambda_p > h(p_b)$$

to be better than polarization based systems. This is what Chris has in the poster.

How many bits do we get with PPM if $T = m \cdot T_f$ as a function of bin size $\tau_b = T_f/n$? We have $p_b = 1 - e^{-\lambda_p \tau_b}$. The number of bits accumulated over time T is whp

$$\log n \cdot n p_b (1 - p_b)^{n-1} \cdot m,$$

Recall that the source emitted $T_f m \lambda_p$ photons on average. Therefore, we get

$$\log \frac{T_f}{\tau_b} \cdot \frac{p_b}{\tau_b \lambda_p} e^{-\lambda_p \tau_b (n-1)}$$

bits per photon.

2) Nick: With the system parameters and T_f given, the raw key rate depends on τ_b. The jitter error depend on τ_b and σ_d. For a given σ_d, find τ_b that maximizes the post-reconciliation key rate ?

Write system model.

Describe the noise in a section

from 12/13/21: Semi provocative title Say in passing that ppm may be suboptimal

Model of eve— assume no quantum eve. Only leakage through reconciliation One hot encoding

Future work maybe has dark counts stuff

Key extraction as it's own section

Mention briefly in eve model info Rec

Have a qkd prelims section

Maybe a summary of results section and problem formulation

Parameters and notation

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.