Time-Entanglement Based QKD

Time-entanglement is a promising way to address the photon-starved conditions that limit key rate in polarization-entanglement [2]. With arbitrary precision, we could extract arbitrarily many bits from a single photon arrival time. In practice, precision is limited, so to extract bits from timing information, what we do is divide the time into discrete bins, which are then grouped into frames. Frames can be thought of as encoded binary words, where each bin corresponds to a 1 when occupied by at least one photon and 0 otherwise.

Detector Recovery-Time

In the figure above, a blue dot indicates an occupied bin, so the first frame will be interpreted as containing at least one photon and the second frame is unoccupied. Frames can be thought of as encoded binary words, where each bin corresponds to a single bit of information, what we do is divide time into discrete and equal-size frames and resolve the number of occupied bins inside the frame, minus one if \( d \geq 0 \). The expression under each identifier is the transition probability of all transitions into that state.

Markov Chain Representation

Because of memory between the frames, we model the system by a Markov Chain (MC). The raw key rate is equal to the entropy rate of the MC \( R = -\sum_{i,j} P_{ij} \log P_{ij} \) bits/s, where \( P_{ij} \) is the stationary probability vector and \( P \) is the transition matrix.

An Upper Bound on the Key Rate

Here, the recovery-time is in bins so if \( k = 1 \) ps, and recovery-time is 2ps, then \( d = 2 \).

In the case of Non-Optimal Schemes

For typical \( n \) (1024, 4096), calculating \( R_p \) using an MC state for each of the \( 2^n \) frames is impractical. To address this problem, we have developed a way to combine states so that the total number of states increases polynomially with \( n \), with negligible loss of accuracy in \( R_p \) and \( R_t \). The idea is to combine "similar" states and \( y \) where states \( s \) and \( y \) are similar if the distance between \( P_{xy} \) and \( P_{y’} \) is small. For example, MC generated using our method and the corresponding rates' plot is shown below. Does Time-Entanglement Entangle up to its Promise?

The two variables – entangled pair production rate \( h_p \) and bin width \( \tau \) – as we have described them so far, would, in theory, allow designers to arbitrarily increase the key rate. In practice, decreasing \( \tau \) too far may overwhelm the system by jitter errors, and increasing \( \tau \) too far reduces the system efficiency because of the detector recovery-time. Additionally, note that by \( \tau = 0 \), we are back to extracting at most one bit per photon arrival. This is predicted by the formula for maximum photon utilization:

\[
R = \frac{h_p}{\tau} - \frac{h_p - \exp(-\frac{h_p}{\tau})}{\tau} \text{ bits/time.}
\]

Detector recovery-time is a time interval following a photon detection during which the detector is unresponsive to any subsequent photon arrivals.

This recovery-time is not restricted by time resolution and may be much greater than the finest distinguishable time unit. This means that photon arrivals can no longer be modeled as i.i.d.; rather than as an exponential distribution, photon interarrival times are better modeled as a shifted exponential distribution, where the shift corresponds with the recovery time. This introduction of memory leads to reductions in \( R_t \) and \( R_p \). Calculating Information Rate

We will focus on two variables which affect how key generation rate is calculated.

The Rate at Which Entangled Photon Pairs are Generated

We model the duration between consecutive entangled photon pair production times as exponential with the rate \( h_p \). From \( h_p \), we can find the probability that a bin is occupied, \( P = 1 - \exp(-\frac{h_p}{\tau}) \), where \( \tau \) is the bin width in time. Therefore, the maximum number of bits per bin is \( N_p = \frac{h_p}{P(1 - \exp(-\frac{h_p}{\tau}))} \). The binary entropy function.

Detector Resolution / Bin Width

Increasing detector resolution means more bits available for us to decode per unit time, which compensates for the resulting decrease in \( h_p \). The entropy extracted per time is:

\[
R = \log_2(\frac{h_p}{P(1 - \exp(-\frac{h_p}{\tau}))}) \text{ bits/time.}
\]

For example, if we halve the bin width and use \( \tau = \frac{1}{2} \) instead of \( \tau \), we will extract a maximum of \( 2N_p = \log_2(\frac{2h_p}{P(1 - \exp(-\frac{h_p}{\tau}))}) \) bits per time, which is strictly greater than \( N_p \) except at \( \tau = 0 \). In theory, if we can arbitrarily decrease bin width, we can also arbitrarily increase \( R_p \). Note that while improvements in \( h_p \) also benefit key rates from polarization entanglement, improvements in detector resolution mostly only benefit key rates from time-entanglement.

Jitter Error and Associated Rate Cost

Jitter errors caused by the detector imperfections follow a Gaussian distribution. These errors are different from errors introduced through dark counts, which produce a triangular distribution (the convolution of two uniform distributions over the frame width). Around 42% of jitters are expected to be less than 100 ps in magnitude for this frame configuration. The plot below shows the direct relation between detector jitter variance and key rate loss generated using the error channel characterization above.

Secret key rate in bits per frame when frame size is 4096 ps and we use 16 bits per frame

Jitter Error Reference

Each state contains an identifier \((d_0, d_1, d_2, q_0)\), where \( d_0 \) and \( d_1 \) are recovery-time into and out of the frame, respectively, and \( q_0 \) is the number of occupied bins inside the frame, minus one if \( d_1 d_2 \geq 0 \). The expression under each identifier is the transition probability of all transitions into that state.

References