Time-Entanglement QKD: Secret Key Rates and Information Reconciliation Coding

Joseph J. Boutros, *Senior Member, IEEE*, and Emina Soljanin, *Fellow, IEEE*

***Abstract*— In time entanglement-based quantum key distribution (TE-QKD), Alice and Bob extract the raw key bits from the arrival times of entangled photon pairs. Each entangled pair can contribute to multiple key bits depending on how precisely Alice and Bob can measure the photon arrival times. Thus, TE-QKD can potentially increase the secret key rate compared to typical QKD implementations, which extract up to a bit per photon. Because of entanglement, the times of photon arrivals at Alice's and Bob's detectors and, thus, their raw keys should be identical. However, practical photon detectors suffer from time jitter errors. These errors cause discrepancies between Alice's and Bob's raw keys. Therefore, Alice must send information to Bob through the public channel to reconcile their raw keys. The amount of data sent for reconciliation represents a loss, rendering secret keys shorter than the raw keys. We compute the secret key rates possible in systems with detector jitter errors and show that they are much higher than those achievable in polarization entanglement-based QKD. We then construct codes for information reconciliation to approach these rates. We demonstrate that short and moderate-length standard error-correcting codes represent excellent information reconciliation choices, making TE-QKD a promising technology.**

***Index Terms*— Quantum key distribution, secret key rates, mutual information, time entanglement, time binning, jitter errors, soft-decision decoding.**

I. Introduction

SECRET key distribution protocols establish a shared sequence of bits between two (or more) distant parties, Alice and Bob, in the presence of an eavesdropper, Eve. The key consists of uniformly random independent bits known only to Alice and Bob. Quantum Key Distribution (QKD) starts by communicating quantum states over a quantum channel. The role of the quantum step is to 1) ensure that no eavesdropping goes undetected and 2) provide a source of perfect randomness in the entanglement-based systems.

There has been a significant effort to provide high key rates over long distances (see recent surveys [1], [2]). QKD schemes based on time-entangled photons have emerged as a promising technique primarily because each entangled photon pair can carry multiple key bits and thus potentially provide a higher secure key rate over long distances [3], [4].

TE-QKD schemes use Spontaneous Parametric Down-Conversion (SPDC) to generate entangled photon pairs according to a Poisson Process. One of the photons goes to Alice, and the other to Bob. Therefore, Alice and Bob ideally detect their photons simultaneously with exponentially distributed inter-arrival times. The most common single-photon detectors are Superconducting Nanowire Single-Photon Detectors (SNSPDs), which exhibit properties closest to ideal sensors. They have low dark count rates, meaning they rarely report photon detection without a photon arrival. Furthermore, they have low detector downtime d and slight detector timing jitter that manifests as Gaussian noise with zero mean and variance σ_d^2. Unfortunately, these imperfections are non-negligible: 1) detector jitters and dark counts cause disagreements between Alice's and Bob's keys since they detect photons at different times, and 2) the downtime introduces memory within the raw key bits since whether a photon is detected depends on whether another photon has been detected within the downtime of its arrival. For further discussion on the non-ideal properties and their implications, we refer the reader to the recent study [5].

At a high level, there are two main QKD steps. In the first step, Alice and Bob generate *raw key* bits using a quantum channel. Their respective raw keys may disagree at some positions, be partly known to Eve, and may not be uniformly random because of the aforementioned non-ideal detector properties. In the second step, Alice and Bob process the raw key to establish a shared *secret key*. They communicate through the public classical channel to reconcile differences between their raw keys, amplify the privacy of the key concerning Eve's knowledge, and compress their sequences to achieve uniform randomness. At the end of the protocol, Alice and Bob 1) have identical uniformly random (binary) sequences and 2) are confident the shared sequence is known only to them. Therefore the secret key is private and hard to guess. This paper focuses on the information reconciliation step.

Alice and Bob generate their secret keys from the correlated random photon arrivals. There are many ways to extract keys from this correlated information. One popular method is similar to Pulse Position Modulation (PPM); see, e.g., [6] and references therein. (Some recently proposed adaptive schemes

Manuscript received 30 January 2023; revised 18 June 2023; accepted 23 July 2023. Date of publication 4 August 2023; date of current version 19 December 2023. This research was based upon work supported by the National Science Foundation under Grant # FET-2007203. The associate editor coordinating the review of this article and approving it for publication was J. Zhang. *(Corresponding author: Joseph J. Boutros.)*

Joseph J. Boutros is with the Department of Electrical and Computer Engineering, Texas A&M University at Qatar, Doha, Qatar (e-mail: boutros@ieee.org).

Emina Soljanin is with the Department of Electrical and Computer Engineering, Rutgers, The State University of New Jersey, Piscataway, NJ 08854 USA.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCOMM.2023.3302135.

Digital Object Identifier 10.1109/TCOMM.2023.3302135

avoid discarding frames with multiple occupied bins [7], [8].) In PPM, Alice and Bob synchronize their clocks and discretize their timelines into time frames N time bins. In PPM, Alice and Bob agree to retain only time frames in which they both detect a single photon arrival and discard all other frames. This single photon is said to occupy a time bin depending on where within the frame it arrives. Since photon inter-arrival times follow an exponential distribution, each bin is occupied independently of other bins. Therefore, the number of raw key bits PPM decoding can extract from each frame equals $\log N$.

Alice and Bob obtain correlated bit streams (raw keys) by detecting the arrival times of their entangled photons. However, they must communicate over a public channel to agree on a key, i.e., reconcile their differences. Here, we consider one-way information reconciliation schemes in which Alice sends information about her sequence to Bob, who uses it to remove the differences between his and Alice's raw keys. After the information reconciliation, Alice and Bob share Alice's initial raw key. However, the shared key is not secret because of the public channel communication. Alice and Bob perform privacy amplification to correct that, establishing secrecy but shortening the key. Since Alice and Bob base their secret key generation on correlated photon arrival times, they follow what is known as the source model in Information Theory [9, Ch. 22.3]. The secrecy capacity for this model, when the eavesdropper has access to public communication but does not have correlated prior information, is equal to the mutual information between Alice's and Bob's observations (see, e.g., [9, p. 567]). The secrecy capacity is an achievable upper bound on the post-privacy amplification rate.

We focus on rate loss solely due to the communications over the classical public channel that has to be done since practical photon detectors exhibit time jitter. We compute the achievable secret key rates and construct codes for information reconciliation to approach these rates. Since no passive eavesdropping is possible on a quantum channel, Alice and Bob can detect the presence of Eve and discard the compromised frames. Analyzing rate loss due to eavesdropping on the quantum channel is beyond the scope of this paper.

This paper is organized as follows: Sec. II introduces notation and lists the paper's main contributions. Sec. III presents the TE-QKD channel model. Sec. IV computes the rates of raw key disagreement caused by detection jitter, and Sec. V derives the correlations between Alice's and Bob's raw keys. Sec. VI computes achievable information rates and the secrecy capacity of the TE-QKD channel. Sec. VII proposes and tests several coding schemes for information reconciliation. The final section draws the conclusions and lists the main contributions of this paper.

II. Notation

The number N of bins per time frame could be any positive integer greater than or equal to 2, our propositions, lemmas, and theorems have no other constraint on N. However, our numerical examples are given for $N = 2^m$, m integer, $m \geq 1$. The set $\mathbb{Z}_N$ denotes the set of N integers $\{0, 1, \ldots, N-1\}$.

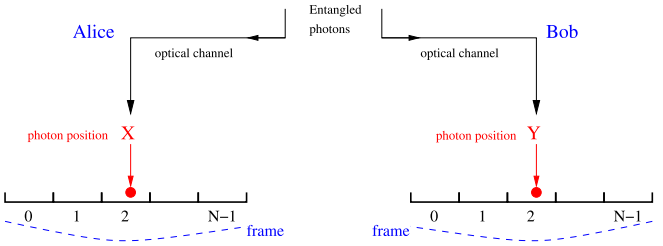

Fig. 1. QKD based on time entanglement with N bins per frame, $\log_2(N)$ binary digits per bin.

The notation $\lfloor x \rfloor$, known as the *floor of* x for $x \in \mathbb{R}$, is the largest integer smaller than or equal to x.

Letters such as X, Y, $\tilde{X}$, and $\tilde{Y}$ denote continuous random variables, while $\hat{X}$ and $\hat{Y}$ are discrete random variables. Then, $p(\hat{y}|\hat{x})$ denotes the conditional probability $\mathbb{P}(\hat{Y} = \hat{y}|\hat{X} = \hat{x})$. Also, $p(y|\hat{x})$ denotes the conditional density $p_{Y|\hat{X}}(y|\hat{x})$.

We use Bourbaki's notation for intervals on the real line, where a and b are two real numbers: the closed interval $[a, b] = \{x \in \mathbb{R} \ : \ a \leq x \leq b\}$, the half-open intervals $[a, b[= [a, b] \backslash \{b\}$ and $]a, b] = [a, b] \backslash \{a\}$, and the open interval $]a, b[= [a, b] \setminus \{a, b\}$.

We use the standard Bachmann-Landau big $\mathcal{O}$ notation:

The formal definition of $f(\sigma) = \mathcal{O}(g(\sigma))$ is: $\exists \alpha > 0$, $\exists \sigma_0 > 0$, $\forall \sigma < \sigma_0$, $|f(\sigma)| \leq \alpha |g(\sigma)|$.

In this paper, an expression such as $1 - \mathcal{O}(g(\sigma))$ or $1 + \mathcal{O}(g(\sigma))$ implicitly assumes that $g(\sigma) > 0$ in some open interval $]0, \sigma_0[$. Furthermore, we will frequently use $\gamma = 1/\sigma^2$, a signal-to-noise ratio defined as the inverse of the jitter variance, then we could write $f(\gamma) = \mathcal{O}(g(\gamma))$ in a similar situation when $\gamma \to \infty$.

Two functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ are asymptotically equivalent if $\lim_{\gamma \to \infty} \frac{f(\gamma)}{g(\gamma)} = 1$. In that case, we write $f(\gamma) \sim g(\gamma)$.

The function $Q(x) = \frac{1}{2} \operatorname{erfc}(\frac{x}{\sqrt{2}}) = \mathcal{O}(\exp(-x^2/2))$ is the Gaussian tail function. Recall the definition $Q(x) = \int_x^\infty \phi(t) dt$, where $\phi(t) = \frac{1}{\sqrt{2\pi}} \exp(-t^2/2)$ is the standard normal density. Furthermore, we recall the binary entropy function, $H_2(x) = -x \log(x) - (1 - x) \log(1 - x)$, and the symmetric ternary entropy function, $H_3(x) = -(1 - 2x) \log(1 - 2x) - 2x \log(x)$.

III. The PPM Channel Model

Let $\tilde{X}$ and $\tilde{Y}$ represent the time-position of the received photons at Alice's and Bob's sides, respectively. An illustration of this QKD scheme is given in Figure 1. Entangled photons are commonly generated by Spontaneous Parametric Down-Conversion (SPDC) sources, which can be collocated with one of the protocol participants. For more information about SPDC in the context of time entanglement QKD, we refer the reader to [5] and references therein.

We adopt the following mathematical model for the positions of two time-entangled photons:

$$\tilde{X} = U + Z_1, \quad \tilde{Y} = U + Z_2, \tag{1}$$

where Z_1 and Z_2 are independent identically distributed $\mathcal{N}(0, \sigma^2)$ additive Gaussian noises modeling the detection

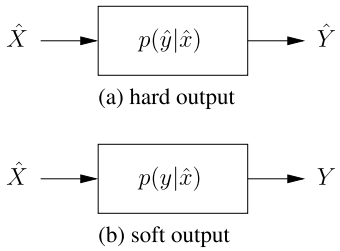

Fig. 2. TE-QKD channel models for hard-decision decoding (a) and soft-decision decoding (b).

jitter. U is a real uniform random variable in the interval $[0, N[$, where the integer $N = 2^m$ is the number of bins per frame, and m is the number of bits per photon. Alice and Bob communicate via a public channel and agree on a valid frame when $\tilde{X}$ and $\tilde{Y}$ fall in the interval $[0, N[$. They reject empty frames and frames with more than one received photon. Under the model defined by (1), the probability of a frame to be valid for both Alice and Bob is $\mathbb{P}(\tilde{X}, \tilde{Y} \in [0, N[)$. Let X and Y denote the instances of $\tilde{X}$ and $\tilde{Y}$ within the interval $[0, N[$, and let $\hat{X}$ and $\hat{Y}$ be the bin number inside a frame, i.e.,

$$\tilde{X} = X, \quad \text{for } \tilde{X} \in [0, N[, \qquad \tilde{Y} = Y, \quad \text{for } \tilde{Y} \in [0, N[, \tag{2}$$

$$\hat{X} = \lfloor X \rfloor \in \mathbb{Z}_N, \qquad \hat{Y} = \lfloor Y \rfloor \in \mathbb{Z}_N. \tag{3}$$

We distinguish two communication channels between Alice and Bob: (a) an algebraic (hard) output channel, (b) a real (soft) output channel, both having a discrete N-ary input $\hat{X}$ as shown in Figure 2.

Without error-correcting codes, the information rate on these channels is $\log_2(N) = m$ bits per channel use (bpcu). The main channel parameter γ is a signal-to-noise ratio parameter (SNR) defined as

$$\gamma = \frac{E_s}{\sigma^2} = \frac{1}{\sigma^2}, \tag{4}$$

where the average energy per symbol $E_s = 1$ is a normalized energy per transmitted photon. Another QKD channel parameter is $\overline{\gamma}$, referred to as the normalized signal-to-noise ratio, where the standard deviation of the additive Gaussian noise is normalized by the frame length N, hence its definition is

$$\overline{\gamma} = \frac{1}{(\sigma/N)^2} = \frac{N^2}{\sigma^2}, \quad \overline{\gamma}(dB) = \gamma(dB) + 20\log_{10}(N). \tag{5}$$

We express the error probability and the information rate as functions of N and the SNR γ or the normalized SNR $\overline{\gamma}$. The bin width is set to 1 to simplify the analysis, i.e., the frame width is N, except for Section VI-B. The conversion of this mathematical model into a physical model representing a laboratory experiment is straightforward after introducing a time scale to convert γ and N into physical parameters. In Section VI-B, the number of bins is infinite (it's a continuum of bins), the frame has a unit length and $\gamma = \overline{\gamma}$ in that special QKD channel with both soft input and soft output.

IV. Rate of Raw Key Disagreement Under Detection Jitter

We consider the probability of error $P_e(\gamma) = \mathbb{P}(\hat{X} \neq \hat{Y})$. The probability P_e characterizes the quality of channel (a) in Figure 2 defined by its transition probabilities $p(\hat{y}|\hat{x})$. The latter will be entirely determined in Section VI. In the current section, we are interested in determining the expression of $P_e(\gamma)$ as a function of the signal-to-noise ratio γ, for a given number of bins N per frame.

Let $\pi_i = \mathbb{P}(\hat{X} = i)$, $i \in \mathbb{Z}_N$, be the *a priori* probability of the unique frame photon to fall in bin number i. Then, the exact expression of the probability of error is

$$\begin{aligned} P_e(\gamma) &= \sum_{i=0}^{N-1} \pi_i \sum_{\substack{j=0 \\ j\neq i}}^{N-1} p(\hat{y} = j|\hat{x} = i) \\ &= \frac{1}{N} \sum_{i=0}^{N-1} \mathbb{P}(\hat{Y} \neq \hat{X}|\hat{U} = i), \end{aligned} \tag{6}$$

where $\hat{U} = \lfloor U \rfloor$. Since U is uniform in $[0, N)$, we get $\mathbb{P}(\hat{U} = i) = \mathbb{P}(U \in [i, i+1)) = \frac{1}{N}$ which explains the factor in the last equality above. As a first step, in the current section, we solve $P_e(\gamma)$ from the most right equality in (6) via the conditioning over $\hat{U}$. To avoid cumbersome expressions, exact expressions as established in Sections V&VI, we assume that γ is large enough (σ^2 is small enough) so we can neglect the border effects in the frame. Hence, we make no difference here between $\tilde{X}$ and X (resp. $\tilde{Y}$ and Y), and we use the approximation that both X and Y are i.i.d. Gaussian when conditioning on U.

Proposition 1: The probability of symbol error $P_e(\gamma) = \mathbb{P}(\hat{X} \neq \hat{Y})$ as a function of the SNR γ and the number N of bins per frame is given by the expression

$$P_e(\gamma) = \frac{2}{\sqrt{\pi}} \times \left(1 - \frac{1}{N}\right) \times \gamma^{-\frac{1}{2}} + \mathcal{O}(\exp(-\frac{\gamma}{4})). \tag{7}$$

Proof: Set $V = U - \hat{U}$, so V is Uniform$[0, 1]$. Let $p(i \to j|v)$ be the probability of falling in bin j given that $\hat{U} = i$ and $V = v$, where $i, j \in \mathbb{Z}_N$. A symbol error occurs if $X = U + Z_1$ remains in bin i but $Y = U + Z_2$ leaves to bin j, $j \neq i$. The probability of such an event is $p(i \to i|v) \times p(i \to j|v)$, given that both additive Gaussian noises Z_1 and Z_2 are independent. Also, an error occurs if both X and Y leaves to two different bins ℓ and j, with probability $p(i \to \ell|v) \times p(i \to j|v)$. Then, the conditional symbol error probability becomes

$$\begin{aligned} P_e(i, v) = 2 \sum_{\substack{j=0 \\ j\neq i}}^{N-1} p(i \to i|v)p(i \to j|v) + \\ 2 \sum_{\substack{\ell=0 \\ \ell\neq i}}^{N-1} \sum_{\substack{j=0 \\ j\neq i, j\neq \ell}}^{N-1} p(i \to \ell|v)p(i \to j|v) \end{aligned}$$

The factor of 2 is due to the symmetry if the two letters X and Y are switched. As illustrated in Figure 3, we will neglect bins beyond the left and the right bin. The neglected bins are at least at distance 1.0 from the bin $\hat{U} = i$. They correspond

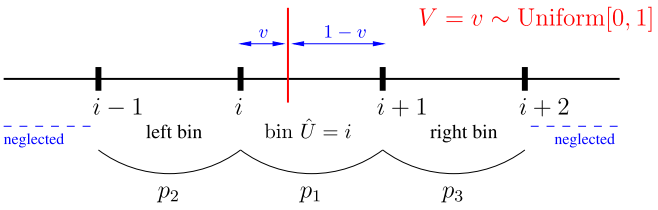

Fig. 3. Illustration of the probability of error in bin position.

to a probability of error $Q(1/\sigma) = \mathcal{O}(\exp(-1/(2\sigma^2))) = \mathcal{O}(\exp(-\frac{\gamma}{2}))$. To further simplify the notations, define p_1, p_2, and p_3, where

$$p_1 = p(i \to i|v) = 1 - Q\left(\frac{v}{\sigma}\right) - Q\left(\frac{1-v}{\sigma}\right), \quad (8)$$

$$p_2 = p(i \to i-1|v) = Q\left(\frac{v}{\sigma}\right), \quad (9)$$

$$p_3 = p(i \to i+1|v) = Q\left(\frac{1-v}{\sigma}\right). \quad (10)$$

We obtain that $P_e(i,v)$ equals

$$\mathcal{O}(\exp(-\frac{\gamma}{2})) + \begin{cases} \{2[p_1p_2 + p_1p_3 + p_2p_3], \\ \qquad \text{for } i = 1,\ldots,N-2, \\ 2p_1p_3, \text{ for } i = 0, \\ 2p_1p_2, \text{ for } i = N-1. \end{cases} \quad (11)$$

Now, integrate over v, $\mathbb{P}(\hat{Y} \neq \hat{X}|\hat{U}=i) = \int_0^1 P_e(i,v)\ dv$. Then, apply (6) and use the equality $\int_0^1 p_1p_2dv = \int_0^1 p_1p_3dv$ to finally reach

$$P_e(\gamma) = \frac{1}{N}\sum_{i=0}^{N-1}\int_0^1 P_e(i,v)\ dv = 4\left(1-\frac{1}{N}\right)\int_0^1 p_1p_2\ dv + 2\left(1-\frac{1}{N}\right)\int_0^1 p_2p_3\ dv\ + \mathcal{O}(\exp(-\frac{\gamma}{2})). \quad (12)$$

The two integrals in (12) include three types of integrals. Let us process them step by step.

$$I_1 = \int_0^1 Q\left(\frac{v}{\sigma}\right)\ dv = \frac{\sigma(1-e^{-1/2\sigma^2})}{\sqrt{2\pi}} + Q\left(\frac{1}{\sigma}\right) = \frac{\sigma}{\sqrt{2\pi}} + \mathcal{O}(\exp(-\frac{\gamma}{2})).$$

$$I_2 = \int_0^1 \left[Q\left(\frac{v}{\sigma}\right)\right]^2 dv = \frac{(\sqrt{2}-1)\sigma}{2\sqrt{\pi}} + \mathcal{O}(\exp(-\gamma)).$$

$$I_3 = \int_0^1 Q\left(\frac{v}{\sigma}\right)\ Q\left(\frac{1-v}{\sigma}\right)\ dv \leq \int_0^1 \exp\left(\frac{-v^2-(1-v)^2}{2\sigma^2}\right)\ dv\ =\ \mathcal{O}(\exp(-\frac{\gamma}{4})),$$

since $v^2+(1-v)^2 \geq \frac{1}{2}$ for $v \in [0,1]$. I_1 and I_2 were solved via integration by parts using the fact that $\frac{dQ(x)}{dx} = -\phi(x)$. I_3 has no simpler form. Our upper bound of I_3 brings a sufficient answer to the current proposition. After substituting I_1, I_2, and I_3 into (12), we get (7) as stated by the proposition. □

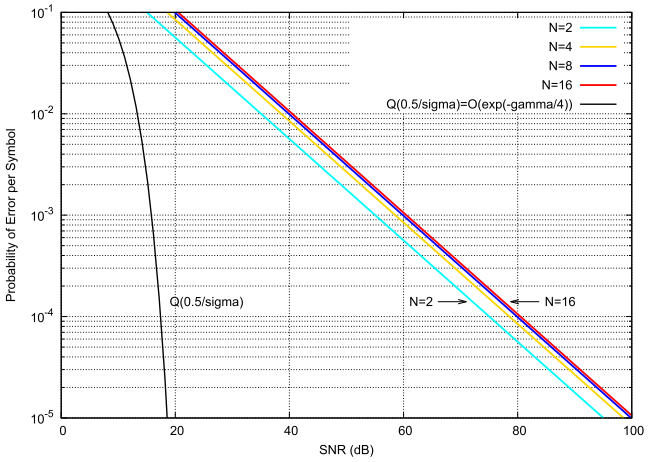

Fig. 4. Probability of symbol error versus signal-to-noise ratio, for $\log_2(N)$ bits per photon and no coding.

The expression $\frac{2}{\sqrt{\pi}} \times \left(1-\frac{1}{N}\right) \times \gamma^{-\frac{1}{2}}$ perfectly fits the Monte Carlo simulation of $\mathbb{P}(\hat{Y} \neq \hat{X})$ even for a signal-to-noise ratio as low as 20dB (error rate close to 10^{-1}). Figure 4 shows the plots of the probability of error $P_e(\gamma)$ for different number of bins per frames, from 1 bit per photon up to 4 bits per photon. The plots of the probability of error versus the normalized SNR, $P_e(\overline{\gamma})$, are obtained from Figure 4 after shifting right each curve by $20\log_{10}(N)$ decibels as per (5). When the error rate scales as $1/\gamma^d$, we say that the system is exhibiting an order-d diversity [10]. In standard communication systems with frequency-selective, space-selective, or time-selective channels, the diversity order is a positive integer. Diversity takes non-integer values when the fading distribution is non-standard, e.g., a Nakagami distribution. Proposition 1 shows that uncoded TE-QKD has a diversity order of $1/2$. The photon positions near a bin boundary behave like a deep fading, i.e., a small measurement jitter creates an error. Then, the combination of the uniform and the Gaussian distributions achieves an order-$1/2$ diversity such as in integrals I_1 and I_2.

V. Correlation Between Raw Keys

The conditional densities of $\tilde{X}$ is directly derived from (1),

$$p_{\tilde{X}|U}(\tilde{x}|u) = \frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(\tilde{x}-u)^2}{2\sigma^2}\right), \quad \tilde{x} \in \mathbb{R}. \quad (13)$$

Conditioned on $U=u$, $\tilde{X}$ and $\tilde{Y}$ are independent. Then, after integrating (13),

$$\mathbb{P}(\tilde{X},\tilde{Y} \in [0,N[|u) = \mathbb{P}(\tilde{X} \in [0,N[|u)^2 = \left[Q\left(-\frac{u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right]^2.$$

The probability that Alice's and Bob's frames are valid is

$$\mathbb{P}(\tilde{X},\tilde{Y} \in [0,N[) = \int_0^N \left[Q\left(-\tfrac{u}{\sigma}\right) - Q\left(\tfrac{N-u}{\sigma}\right)\right]^2\ p_U(u)du = \frac{1}{N}\int_0^N \left[Q\left(-\tfrac{u}{\sigma}\right) - Q\left(\tfrac{N-u}{\sigma}\right)\right]^2\ du. \quad (14)$$

The density of $\tilde{X}$ is also derived by integrating over u, which is equivalent to convolving the densities of U and Z_1, we get

$$p_{\tilde{X}}(\tilde{x}) = \int_0^N p_{\tilde{X}|U}(\tilde{x}|u)\frac{1}{N}\,du = \frac{1}{N}\left[Q\left(\frac{-\tilde{x}}{\sigma}\right) - Q\left(\frac{N-\tilde{x}}{\sigma}\right)\right], \quad \tilde{x}\in\mathbb{R}. \tag{15}$$

Since X is a version of $\tilde{X}$ truncated to the interval $[0, N[$, conditioning on $U + Z_1 \in [0, N[$, the density of X is determined by scaling the density of $\tilde{X}$, namely, for $x, u \in [0, N[$,

$$p_{X|U}(x|u) = \frac{p_{\tilde{X}|U}(x|u)}{\int_0^N p_{\tilde{X}|U}(t|u)dt} = \frac{\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(x-u)^2}{2\sigma^2}\right)}{\left[Q\left(-\frac{u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right]} \tag{16}$$

and, for $x \in [0, N[$,

$$p_X(x) = \frac{p_{\tilde{X}}(x)}{\int_0^N p_{\tilde{X}}(t)dt} = \frac{Q\left(-\frac{x}{\sigma}\right) - Q\left(\frac{N-x}{\sigma}\right)}{\int_0^N \left[Q\left(-\frac{t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right]dt} \tag{17}$$

By symmetry from (1), $p_{\tilde{Y}|U}(\tilde{y}|u)$, $p_{\tilde{Y}}(\tilde{y})$, $p_{Y|U}(y|u)$, and $p_Y(y)$ have expressions identical to (13), (15), (16), and (17) respectively, for $\tilde{y} \in \mathbb{R}$ and $y \in [0, N[$. The bins *a priori* probabilities $\pi_i = \mathbb{P}(\hat{X} = i) = \mathbb{P}(X \in [i, i+1])$ become

$$\int_i^{i+1} p_X(x)dx = \frac{\int_i^{i+1}\left[Q\left(\frac{-x}{\sigma}\right) - Q\left(\frac{N-x}{\sigma}\right)\right]dx}{\int_0^N \left[Q\left(-\frac{t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right]dt}. \tag{18}$$

At high SNR, for $\sigma^2 \ll 1$, we have $\pi_i \approx 1/N$, $\forall i$, because the truncation to the interval $[0, N[$ has less effect in the small-noise regime. Numerical examples are given in Table I, for $N = 8$ bins per frame. The entropy of $\hat{X}$ is very stable, as listed in the last column of the table, $H(\hat{X}) = -\sum_{i=0}^{N-1}\pi_i \log_2(\pi_i) \approx \log_2(N)$ at low and high signal-to-noise ratios.

The following lemma helps understand the behavior of (14)-(18) at high SNR ($\sigma^2 \ll 1$), which are most commonly addressed scenarios in experimental systems (see e.g., [6]) and can be inferred from detector specification sheets such as [11].

Lemma 1: Let $f_\sigma(x) = Q\left(-\frac{x}{\sigma}\right) - Q\left(\frac{1-x}{\sigma}\right)$. *For* $\sigma > 0$ *and* $\gamma = 1/\sigma^2$, *given the properties of the Gaussian tail function* $Q(x)$, *the difference function* $f_\sigma(x)$ *satisfies*

a) $\forall x \in \mathbb{R}, f_\sigma(x) = f_\sigma(1-x) \in]0, 1[$. *Also,* $f_\sigma(0) = f_\sigma(1) = \frac{1}{2} - \mathcal{O}(\exp(-\frac{\gamma}{2}))$.

b) For $x \in]0, 1[$, $f_\sigma(x) = 1 - \mathcal{O}(\exp(-\min^2(x, 1-x)\frac{\gamma}{2}))$.

c) For $x < 0$, *we have* $f_\sigma(x) = \mathcal{O}(\exp(-x^2\frac{\gamma}{2}))$, *and* $f_\sigma(x) = \mathcal{O}(\exp(-(x-1)^2\frac{\gamma}{2}))$ *for* $x > 1$.

d) Integrating f_σ *and* f_σ^2, *we get* $\int_0^1 f_\sigma(x)\,dx = 1 - \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{\gamma}} + \mathcal{O}(\exp(-\frac{\gamma}{2})) = 1 - \mathcal{O}(\frac{1}{\sqrt{\gamma}})$ *and* $\int_0^1 f_\sigma^2(x)\,dx = 1 - \frac{1+\sqrt{2}}{\sqrt{\pi}}\frac{1}{\sqrt{\gamma}} + \mathcal{O}(\exp(-\frac{\gamma}{4})) = 1 - \mathcal{O}(\frac{1}{\sqrt{\gamma}})$.

e) $\int_{i/N}^{(i+1)/N} f_\sigma(x)\,dx = \frac{1}{N} - \mathcal{O}(\frac{1}{\sqrt{\gamma}})$ *for* $i = 0$ *and* $i = N-1$ *(the two extreme bins in a frame of* N *bins).* $\int_{i/N}^{(i+1)/N} f_\sigma(x)\,dx = \frac{1}{N} + \mathcal{O}(\exp(-\beta\gamma))$ *for* $i = 1 \ldots N-2$ *(the inner bins), where the exponent constant is* $\beta = \frac{1}{2}\min^2(\frac{i}{N}, 1 - \frac{i+1}{N})$.

The proof of Lemma 1 is found in the appendix. The convergence of $f_\sigma(x)$ is not uniform in the interval $[0, 1]$. The point-wise convergence of $f_\sigma(x)$ to 0 (outside $[0, 1]$) or to 1 (inside $[0, 1]$) is very slow in the neighborhood of the points $x = 0$ and $x = 1$. At high SNR, the difference of the two $Q()$ functions behaves as a square function and its integral slowly approaches 1 at a rate of $1/\sqrt{\gamma}$.

Applying Lemma 1 to (14)-(18), after substituting u/N to u and σ/N to σ, proves the following equalities where $\tilde{x}, x, u \in]0, N[$ and $i \in \mathbb{Z}_N$:

$$\begin{aligned}
\mathbb{P}(\tilde{X}, \tilde{Y} \in [0, N[) &= 1 - \mathcal{O}(\frac{1}{\sqrt{N^2\gamma}}) = 1 - \mathcal{O}(\frac{1}{\sqrt{\overline{\gamma}}}),\\
p_{\tilde{X}}(\tilde{x}) &= \frac{1}{N} - \mathcal{O}(\exp(-\min^2(\frac{\tilde{x}}{N}, 1 - \frac{\tilde{x}}{N})\frac{\overline{\gamma}}{2})),\\
p_{X|U}(x|u) &= \frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(x-u)^2}{2\sigma^2}\right)\\
&\quad (1 + \mathcal{O}(\exp(-\min^2(\frac{u}{N}, 1 - \frac{u}{N})\frac{\overline{\gamma}}{2})),\\
p_X(x) &= \frac{1}{N}(1 - \mathcal{O}(\exp(-\min^2(\frac{x}{N}, 1 - \frac{x}{N})\frac{\overline{\gamma}}{2}))\\
&\quad (1 + \mathcal{O}(\frac{1}{\sqrt{\overline{\gamma}}})),\\
\pi_i &= (\frac{1}{N} \pm \mathcal{O}(g(\overline{\gamma})))(1 + \mathcal{O}(\frac{1}{\sqrt{\overline{\gamma}}})),
\end{aligned}$$

where the vanishing rate of $g(\overline{\gamma})$ depends on i as stated by the Lemma. The high SNR behavior of many expressions below could be determined via the application of the results listed in Lemma 1.

To complete our analysis of the QKD channel between Alice and Bob, it is necessary to find the likelihoods $p_{Y|\hat{X}}(y|\hat{x})$ and the transition probabilities $p_{\hat{Y}|\hat{X}}(\hat{y}|\hat{x})$ for the soft-output and the hard-output mathematical models illustrated in Figure 2. We proceed in a similar manner as from (13) to (17), by first integrating over U, then truncating over the interval $[0, N[$.

Lemma 2: Given Alice's frame is valid, i.e. $\tilde{X} \in [0, N[$, *the density of* U *becomes*

$$p_{U|\tilde{X}\in[0,N[}(u) = \frac{Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)}{\int_0^N \left[Q\left(\frac{-t}{\sigma}\right)Q\left(\frac{N-t}{\sigma}\right)\right]dt} = p_{U|\tilde{Y}\in[0,N[}(u), \quad u \in [0, N[, \tag{19}$$

where $p_{U|\tilde{Y}\in[0,N[}(u)$ *is the density of* U *given that Bob's frame is valid. Furthermore, the* a priori *probabilities* $\{\hat{\pi}_i\}_{i=0}^{N-1}$ *when both frames are valid are given by*

$$\hat{\pi}_i = \mathbb{P}(\hat{X} = i|\tilde{Y} \in [0, N[) = \frac{\int_0^N \left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right]\left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right]du}{\int_0^N \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right]^2 du} \tag{20}$$

The proof of Lemma 2 is found in the appendix. The lemma tells that invalidating the cases where the photon falls outside the frame converts the uniform density $p_U(u) = \frac{1}{N}$ into a non-uniform density in (19). Furthermore, the *a priori* probability π_i of (18) becomes $\hat{\pi}_i$ of (20) when adding the condition that Bob's frame is valid. π_i and $\hat{\pi}_i$ already consider that Alice has a valid frame. The next lemma leads to establishing the channel likelihood expression.

TABLE I
A PRIORI PROBABILITIES OF PHOTON BINS FOR $N = 8$ BINS PER FRAME

SNR	$\pi_0, \ldots, \pi_7$	$H(\hat{X})$ (bits)
10 dB	0.112796, 0.129062, 0.129071, 0.129071, 0.129071, 0.129071, 0.129062, 0.112796	2.997655
25 dB	0.122885, 0.125705, 0.125705, 0.125705, 0.125705, 0.125705, 0.125705, 0.122885	2.999931
40 dB	0.124626, 0.125125, 0.125125, 0.125125, 0.125125, 0.125125, 0.125125, 0.124626	2.999998

Lemma 3: The conditional density of U given $\hat{X} = i$, for $u \in [0, N[$ and $i \in \mathbb{Z}_N$, is

$$p(u|\hat{X} = i) = \frac{Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)}{\int_0^N \left[Q\left(\frac{i-t}{\sigma}\right) - Q\left(\frac{i+1-t}{\sigma}\right)\right] dt} \tag{21}$$

Furthermore, when Bob gets a valid frame, the density of U conditioned on Alice's bin number is

$$p(u|\hat{X} = i, \tilde{Y} \in [0, N[) = \frac{\left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right]\left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right]}{\int_0^N \left[Q\left(\frac{i-t}{\sigma}\right) - Q\left(\frac{i+1-t}{\sigma}\right)\right]\left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right] dt}. \tag{22}$$

The proof of Lemma 3 is found in the appendix. The existence of Y assumes that $\tilde{Y} \in [0, N[$, as we mentioned for X in the proof of Lemma 3. In the sequel, we remind the reader of the condition $\tilde{Y} \in [0, N[$ in the subscript of the likelihood function.

Theorem 1: When both Alice and Bob get valid frames, the soft-output QKD channel model likelihood, $p(y|\hat{x}) = p_{Y|\hat{X},\tilde{Y}\in[0,N[}(y|\hat{x})$, has the following expression

$$\frac{\int_0^N \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-u)^2}{2\sigma^2}} \left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right] du}{\int_0^N \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right]\left[Q\left(\frac{i-t}{\sigma}\right) - Q\left(\frac{i+1-t}{\sigma}\right)\right] dt}, \tag{23}$$

for $\hat{x} = i = 0, \ldots, N-1$, $y \in [0, N[$. For simplicity, the likelihood in (23) will be denoted by $p(y|\hat{X} = i)$.

Proof: We drop the subscripts in the density functions, when possible, to simplify the notations. We start by a marginalization before truncating $p(\tilde{y}|u)$:

$$\begin{aligned} &p(y|\hat{X} = i, \tilde{Y} \in [0, N[) \\ &= \int_0^N p(y, u|\hat{X} = i, \tilde{Y} \in [0, N[) du \\ &= \int_0^N p(y|u, \hat{X} = i, \tilde{Y} \in [0, N[) p(u|\hat{X} = i, \tilde{Y} \in [0, N[) du \\ &= \int_0^N p(y|u) p(u|\hat{X} = i, \tilde{Y} \in [0, N[) du. \end{aligned} \tag{24}$$

The left factor $p(y|u)$ inside the integral in (24) is given by the truncation of the density in (13) (replace x by y) and the right factor was solved by Lemma (3).

$$\begin{aligned} &p(y|\hat{X} = i, \tilde{Y} \in [0, N[) = \\ &\int_0^N \frac{p(\tilde{y} = y|u)}{\int_0^N p(\tilde{y}|u) d\tilde{y}} p(u|\hat{X} = i, \tilde{Y} \in [0, N[) du, = \\ &\int_0^N \frac{\frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(y-u)^2}{2\sigma^2}\right)}{Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)} \cdot \\ &\frac{\left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right]\left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right]}{\int_0^N \left[Q\left(\frac{i-t}{\sigma}\right) - Q\left(\frac{i+1-t}{\sigma}\right)\right]\left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right] dt} du. \end{aligned}$$

After simplifying the term $Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)$ we reach the announced result. □

The transition probabilities $p_{i,j} = \mathbb{P}(\hat{Y} = j|\hat{X} = i)$ of the hard-output QKD channel are directly derived by integrating the conditional density function of the soft output Y established by the previous theorem.

Corollary 1: The probability that Bob's photon falls in bin $j \in \mathbb{Z}_N$ given that Alice's photon fell in bin $i \in \mathbb{Z}_N$ is

$$p_{ij} = \mathbb{P}(\hat{Y} = j|\hat{X} = i) = \frac{\int_0^N \left[Q\left(\frac{j-u}{\sigma}\right) - Q\left(\frac{j+1-u}{\sigma}\right)\right]\left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right] du}{\int_0^N \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right]\left[Q\left(\frac{i-t}{\sigma}\right) - Q\left(\frac{i+1-t}{\sigma}\right)\right] dt}. \tag{25}$$

Proof: Integrate (23) over Bob's photon position y from j to $j+1$, then switch the two integrals to get the result announced by this corollary. □

We complete this section by establishing the expression of the *a posteriori* probability useful for soft-decision decoding, e.g., for belief-propagation decoding of low-density parity-check codes, for ordered-statistics decoding of linear block codes, or Viterbi decoding of convolutional codes. Let $APP(i) = APP(\hat{X} = i) = \mathbb{P}(\hat{X} = i|Y = y)$ be the *a posteriori* probability of Alice's photon bin number i, for $i = 0 \ldots N-1$. The next theorem gives the expression $APP(i)$, which is used in our proposed coding/decoding schemes in Section VII.

Theorem 2: Given the photon position $Y = y$ on Bob's side, the probability for Alice's photon to belong to bin number $i \in \mathbb{Z}_N$ is

$$APP(i) = \frac{\int_0^N \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-u)^2}{2\sigma^2}} \left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right] du}{\int_0^N \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-t)^2}{2\sigma^2}} \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right] dt}. \tag{26}$$

Proof: Given that $\tilde{X}, \tilde{Y} \in [0, N[$, we apply Bayes' rule to get

$$\mathbb{P}(\hat{X} = i|Y = y) = \frac{p(y|\hat{X} = i)\mathbb{P}(\hat{X} = i)}{p(y)}.$$

The result of Theorem 2 is found in three steps: (i) Use (23) from Theorem 1 for $p(y|\hat{X} = i)$. (ii) Use (20) for the a priori $\mathbb{P}(\hat{X} = i)$. (iii) Finally, $p(y) = p_{Y|\tilde{X}\in[0,N)}(y) = p_{\tilde{Y}|\tilde{X}\in[0,N)}(\tilde{y} = y) / \int_0^N p_{\tilde{Y}|\tilde{X}\in[0,N)}(t) dt$ after truncating the density of $\tilde{Y}$. The density $p_{\tilde{Y}|\tilde{X}\in[0,N)}(\tilde{y})$ is found in (54) while switching the letters x (resp. X) and y (resp. Y), in conjunction with (13) and (19),

$$p(y) = \frac{\int_0^N \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-u)^2}{2\sigma^2}} \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right] du}{\int_0^N \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right]^2 dt}, \tag{27}$$

which ends the proof of Theorem 2. □

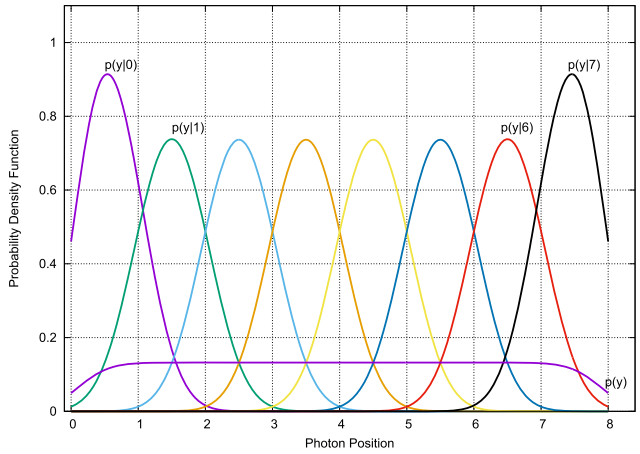

Fig. 5. Soft-Output channel likelihoods, N=8 bins per frame, SNR=10 dB.

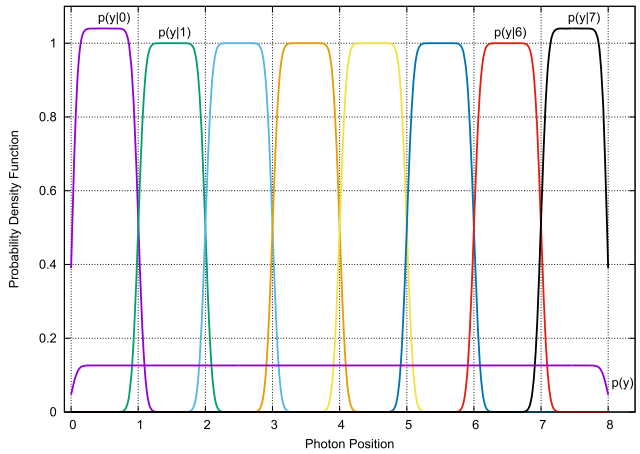

Fig. 6. Soft-Output channel likelihoods, N=8 bins per frame, SNR=25 dB.

For consistency, the reader could check that $p(y)$ given at the end of the proof of Theorem 2 is also equal to $\sum_{i=0}^{N-1} \hat{\pi}_i p(y|\hat{X}=i)$ from (20) and (23). Figures 5 and 6 plot the likelihoods $p(y|\hat{X}=i)$ at low SNR $\gamma = 10$ dB (low photon detector precision) and a relatively higher SNR $\gamma = 25$ dB (higher photon detector precision), respectively. At low SNR, $p(y|\hat{X}=i)$ has a Gaussian shape. The shape tends to become square at high SNR. The *a posteriori* probabilities $APP(i)$, $i \in \mathbb{Z}_N$, have a plot similar to the channel likelihoods.

VI. Secret Key Information Rates

A. Mutual Information Between Raw Keys

Firstly, we consider the mutual information of the algebraic hard-output channel defined by the transition probability $p(\hat{y}|\hat{x}) = \mathbb{P}(\hat{Y}=\hat{y}|\hat{X}=\hat{x})$. In Corollary 1, the expression of $p_{ij} = p(\hat{Y}=j|\hat{X}=i)$ was established. Hence, we can directly compute the mutual information $I(\hat{X};\hat{Y})$ as follows:

$$H(\hat{Y}) - H(\hat{Y}|\hat{X}) = -\sum_{i=0}^{N-1} \mathbb{P}(\hat{Y}=i)\log(\mathbb{P}(\hat{Y}=i)) + \sum_{i=0}^{N-1} \mathbb{P}(\hat{X}=i) \sum_{j=0}^{N-1} \mathbb{P}(\hat{Y}=j|\hat{X}=i)$$

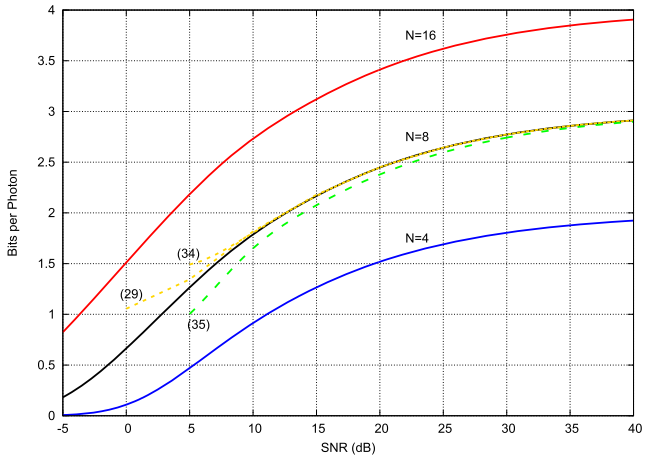

Fig. 7. Mutual information $I(\hat{X};\hat{Y})$ of the algebraic hard-output TE-QKD channel, for $N=4$ (blue), $N=8$ (black), $N=16$ bins per frame (red). The two dotted yellow curves and the dotted green curve correspond respectively to high-SNR approximations of $I(\hat{X};\hat{Y})$ given by (34), (29), and (35) for $N=8$ bins per frame.

$$\log(\mathbb{P}(\hat{Y}=j|\hat{X}=i)) = -\sum_{i=0}^{N-1} \hat{\pi}_i \log(\hat{\pi}_i) + \sum_{i=0}^{N-1} \hat{\pi}_i \sum_{j=0}^{N-1} p_{ij}\log(p_{ij}), \tag{28}$$

where the *a priori* $\hat{\pi}_i$ of $\hat{X}$ and $\hat{Y}$ is found in (20). The plot of $I(\hat{X};\hat{Y})$ expressed in bits versus the signal-to-noise ratio is depicted in Figure 7, for 2, 3, and 4 coded bits per transmitted photon. As expected, the curves go towards the asymptote $H(\hat{X})$ at high signal-to-noise ratio. In fact, the entropy $-\sum_{i=0}^{N-1} \hat{\pi}_i \log(\hat{\pi}_i)$ is very stable even at low SNR and could be well approximated by $\log(N)$. The summation in (28) could be truncated to neighboring bins or to bins within an integer distance less than D,

$$I(\hat{X};\hat{Y}) \approx \log(N) + \frac{1}{N} \sum_{|i-j|\le D} p_{ij}\log(p_{ij}). \tag{29}$$

The simplification (29) is an excellent approximation down to $\gamma \ge 10$ dB for $D=1$ only and it extends to $\gamma \ge 5$ dB for $D=2$. The next proposition gives more insight into the behavior of the *a priori* and the transition probabilities, and the discrete channel mutual information in the low-noise regime.

Proposition 2: At high signal-to-noise ratio, when $\sigma^2 \ll 1$, we have the following results:

a) The transition probability of the hard-output QKD channel established in Corollary 1 satisfies:

At the two extremal bins, $i=0$ and $i=N-1$, we have

$$p_{0,1} = \frac{\frac{\sigma}{\sqrt{\pi}} + \mathcal{O}(e^{-\frac{\gamma}{4}})}{1 - \frac{1+\sqrt{2}}{2\sqrt{\pi}}\sigma + \mathcal{O}(e^{-\frac{\gamma}{4}})}, \tag{30}$$

where $p_{0,1} = p_{N-1,N-2} = 1 - p_{0,0} = 1 - p_{N-1,N-1}$, and $\sigma = 1/\sqrt{\gamma}$.

At the middle bins, $i = 1 \dots N-2$, we have

$$p_{1,2} = \frac{\frac{\sigma}{\sqrt{\pi}} + \mathcal{O}(e^{-\frac{\gamma}{4}})}{1 - \mathcal{O}(e^{-\frac{\gamma}{4}})}, \tag{31}$$

where $p_{1,2} = p_{i,i+1} = p_{i,i-1} = (1 - p_{i,i})/2$. All other transition probabilities $p_{i,j}$ for $|i-j| \geq 2$ are $\mathcal{O}(e^{-\frac{\gamma}{4}})$ and can be forced to 0 in any numerical calculation at high SNR.

b) The a priori *probabilities established in Lemma 2 satisfy*

At the two extremal bins, $i = 0$ and $i = N-1$, we have

$$\hat{\pi}_0 = \hat{\pi}_{N-1} = \frac{1 - \frac{1+\sqrt{2}}{2\sqrt{\pi}}\sigma + \mathcal{O}(e^{-\frac{\gamma}{4}})}{N\left[1 - \frac{1+\sqrt{2}}{\sqrt{\pi}}\overline{\sigma} + \mathcal{O}(e^{-\frac{\gamma}{4}})\right]}, \tag{32}$$

where the numerator includes σ but the denominator involves $\overline{\sigma} = \sigma/N$. For the middle bins, with $i = 1 \dots N-2$, we have

$$\hat{\pi}_i = \frac{1 - \mathcal{O}(e^{-\frac{\gamma}{4}})}{N\left[1 - \frac{1+\sqrt{2}}{\sqrt{\pi}}\overline{\sigma} + \mathcal{O}(e^{-\frac{\gamma}{4}})\right]}. \tag{33}$$

c) Following a) and b), the mutual information $I(\hat{X};\hat{Y})$ of the discrete-input discrete-output QKD channel given by (28) becomes

$$\frac{N - 2\beta\sigma}{N(1-2\beta\overline{\sigma})}\log\left[N(1-2\beta\overline{\sigma})\right] - \frac{2(1-\beta\sigma)}{N(1-2\beta\overline{\sigma})}\log(1-\beta\sigma) - \frac{2(1-\beta\sigma)}{N(1-2\beta\overline{\sigma})}H_2\left(\frac{\sigma/\sqrt{\pi}}{1-\beta\sigma}\right) - \frac{(N-2)}{N(1-2\beta\overline{\sigma})}H_3\left(\frac{\sigma}{\sqrt{\pi}}\right) + \mathcal{O}(e^{-\frac{\gamma}{4}}), \tag{34}$$

where $\beta = \frac{1+\sqrt{2}}{2\sqrt{\pi}}$, $\sigma = 1/\sqrt{\gamma}$, and $\overline{\sigma} = \sigma/N$.

The proof of Proposition 2 is found in the appendix. At high signal-to-noise ratio, this proposition shows how fast $p_{i,j}$ converges to $\frac{\sigma}{\sqrt{\pi}}$. The latter is a one-sided probability of error and it is half the double-sided probability of error stated in Proposition 1. As expected, $\hat{\pi}_i$ converges to $1/N$ much faster for inner bins as found in Proposition 2-b). The high-SNR expression of $I(\hat{X};\hat{Y})$ established in Proposition 2-c) perfectly fits the exact mutual information of the discrete channel down to $\gamma = 10$ dB and then diverges at low SNR below 10 dB. The binary entropy function represents the extremal bins error. The ternary entropy function carries the inner bins error. Expression (34) is a quick method to evaluate $I(\hat{X};\hat{Y})$ at moderate and high signal-to-noise ratios without performing any integration.

One could ask how good is the approximated mutual information if the TE-QKD discrete channel is assumed to have a circular transition probability matrix. Under the assumptions of Proposition 1, we take: 1- X and Y are Gaussian, 2- all bins are equiprobable, and 3- the error probability of the discrete-input discrete-output channel is dominated by events where X and Y are separated by one or two bins only. According to Theorem 7.2.1 in [12, Ch. 7.2], the expression for a circular discrete channel is

$$I(\hat{X};\hat{Y}) \approx \log(N) + \sum_{j=-2}^{2} p_{0j}\log_2(p_{0j}), \tag{35}$$

where $p_{01} = p_{0,-1} \approx \int_0^1 2p_1p_2\ dv = 2(I_1 - I_2 - I_3)$, $p_{02} = p_{0,-2} \approx \int_0^1 2p_2p_3\ dv = 2I_3$, and $p_{00} = 1 - 2p_{01} - 2p_{02}$.

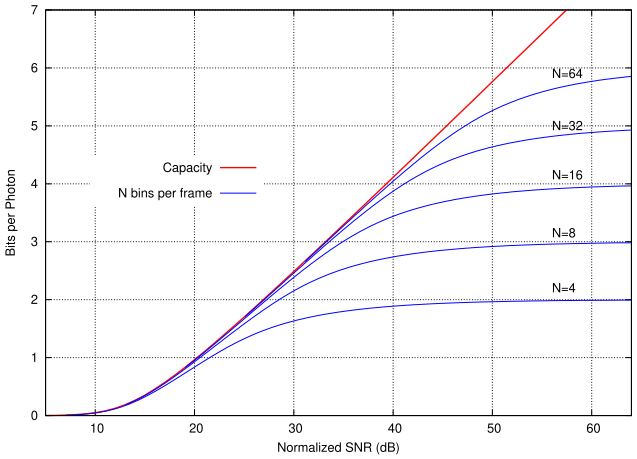

Fig. 8. Mutual information $I(\hat{X};Y)$ of the soft-output TE-QKD channel, for $N = 4 - 64$ bins per frame, i.e., $2 - 6$ bits per photon.

All three high-SNR approximations (34), (29) with $D = 2$, and (35) are respectively shown in dotted lines from top to bottom on Figure 7 for $N = 8$ bins per frame. (34) and (29) follows the exact mutual information $I(\hat{X};\hat{Y})$ at high SNR. (35) is not tight enough at $N = 8$ but becomes tighter for $N \geq 16$ bins per frame.

The second step is to compute the mutual information for the soft-output TE-QKD channel. We have $I(\hat{X};Y) = H(\hat{X}) - H(\hat{X}|Y)$. The second expression after flipping X and Y based on differential entropy, it is also equivalent from a numerical stability point of view and has all its terms established in the previous section. We prefer the mutual information where the high-SNR asymptote is visible, hence

$$I(\hat{X};Y) = H(\hat{X}) - H(\hat{X}|Y) = H(\hat{X}) + \sum_{i=0}^{N-1}\hat{\pi}_i\int_0^N p(y|\hat{x}=i)\log_2(APP(i))\ dy, \tag{36}$$

where the *a priori* $\hat{\pi}_i$ is from (20), the likelihood $p(y|\hat{x}=i)$ is from (23), and the *a posteriori* $APP(i)$ is from (26). Figure 8 shows the mutual information $I(\hat{X};Y)$ versus normalized SNR $\overline{\gamma}$ for different number of bins per frame. The red upper envelope is established by Theorem 3 in the next section. It corresponds to the maximal mutual information achievable on the TE-QKD channel.

B. Maximal Secrecy Rate

The random variables X, $\hat{X}$, and Y form a Markov chain $X \rightarrow \hat{X} \rightarrow Y$. Therefore, the data processing inequality [12, Ch. 2] yields

$$I(\hat{X};Y) \leq I(X;Y), \quad \forall\ N \geq 2. \tag{37}$$

Consequently, for any value of the number N of bins per frame, the rate of our channel $p_{Y|\hat{X}}(y|\hat{x})$ is always bounded from above by the rate of the continuous-input continuous-output channel $p_{Y|X}(y|x)$ corresponding to a continuum of zero-measure bins in Alice's frame. Thus, by determining the mutual information $I(X;Y)$ we get the maximal secrecy rate of the photon channel between Alice and Bob.

Without loss of generality, assume that the frame size is 1, instead of N. Now, the problem is to find $I(X;Y)$ where X and Y are truncated versions of the original photon positions, $X = \tilde{X} \in [0,1), Y = \tilde{Y} \in [0,1)$. The model in (1) becomes $\tilde{X} = U + \mathcal{N}(0,\sigma^2)$, $\tilde{Y} = U + \mathcal{N}(0,\sigma^2)$, U is uniform in $[0,1)$, and the two additive Gaussian noises are independent. The normalized signal-to-noise ratio is naturally defined by $\gamma = \overline{\gamma} = 1/\sigma^2$ under this context of infinite number of bins and a frame of unit length.

Theorem 3: The maximal secrecy rate is given by

$$I(X;Y) = h(Y) - h(Y|X) \tag{38}$$

$$= -\int_0^1 p(y)\ \log(p(y))\ dy + \int_0^1 p(x) \int_0^1 p(y|x)\ \log(p(y|x))\ dydx \tag{39}$$

where $p(x)$ and $p(y)$ are from (27) after replacing the frame size N by 1, $p(x) = p_{X|\tilde{X},\tilde{Y}\in[0,1)}(x)$ is

$$\frac{\int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-u)^2}{2\sigma^2}} \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{1-u}{\sigma}\right)\right] du}{\int_0^1 \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{1-t}{\sigma}\right)\right]^2 dt}, \tag{40}$$

$p(y) = p_{Y|\tilde{X},\tilde{Y}\in[0,1)}(y)$ *is*

$$\frac{\int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-u)^2}{2\sigma^2}} \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{1-u}{\sigma}\right)\right] du}{\int_0^1 \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{1-t}{\sigma}\right)\right]^2 dt}, \tag{41}$$

and the conditional density $p(y|x)$ is

$$\frac{1}{\sqrt{4\pi\sigma^2}} e^{-\frac{(y-x)^2}{4\sigma^2}} \frac{\left[Q\left(\frac{0-(x+y)/2}{\sigma/\sqrt{2}}\right) - Q\left(\frac{1-(x+y)/2}{\sigma/\sqrt{2}}\right)\right]}{\int_0^1 \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-u)^2}{2\sigma^2}} \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{1-u}{\sigma}\right)\right] du}. \tag{42}$$

Proof: We complete the proof by finding the expression of the conditional density $p(y|x)$. Indeed, we can write after marginalizing and applying Bayes' rule

$$p(y|x) = p_{Y|X,\tilde{X},\tilde{Y}\in[0,1)}(y|x) = \int_0^1 p(y,u|x)\ du = \int_0^1 \frac{p(u)p(x|u)p(y|u)}{p(x)} du. \tag{43}$$

In the above integral expression we used the fact that $p(x,y|u) = p(x|u)p(y|u)$ as a result of the model defined by (1). In (43), both $p(x|u)$ and $p(y|u)$ are from (16), $p(x)$ is from (27), and finally $p(u) = p_{U|\tilde{X},\tilde{Y}\in[0,1)}(u)$ is found in (56), all after substituting 1 to N. After simplifying the integrand of (43), we get $p(y|x)$ as stated by (42). □

Corollary 2: At high signal-to-noise ratio, i.e., $\gamma = \frac{1}{\sigma^2} \gg 1$, the maximal secrecy rate satisfies

$$I(X;Y) = (1 + \mathcal{O}(\tfrac{1}{\sqrt{\gamma}}))\frac{1}{2}\log\left(\frac{\gamma}{4\pi e}\right) + \mathcal{O}\left((\tfrac{1}{\sqrt{\gamma}})^{\alpha}\right) \sim \frac{1}{2}\log\left(\frac{\gamma}{4\pi e}\right), \quad \forall \alpha \in]0,1[. \tag{44}$$

Proof: The proof is based on a Babylonian approach with heavy calculus. Let us give a sketch on how the limit is guessed. By applying Lemma 1 and some extra algebra, when $\gamma \gg 1$, we get that $p(x) \to 1$, $p(y) \to 1$, and $p(y|x) \to \frac{1}{\sqrt{4\pi\sigma^2}} e^{-\frac{(y-x)^2}{4\sigma^2}}$, in (40), (41), and (42) respectively, for $x, y \in]0,1[$. Then, the differential entropy $h(Y) \to 0$, $h(Y|X) \to h(\mathcal{N}(0,2\sigma^2)) = \frac{1}{2}\log(4\pi e\sigma^2)$, so the maximal secrecy rate satisfies $I(X;Y) = h(Y) - h(Y|X) \to \frac{1}{2}\log\left(\frac{\gamma}{4\pi e}\right)$. The detailed rigorous proof is found in [13]. □

The Gaussian differential entropy (44) is very close to $I(X;Y)$ above 2 bits per photon and becomes very accurate beyond 3 bits per photon where it coincides with the red upper envelope in Figure 8 at a high signal-to-noise ratio. The double variance $2\sigma^2$ in (44), originally found in (42), comes from the superposition of the variances of Z_1 and Z_2 in the system model defined by (1). After canceling U, the model becomes $\tilde{Y} = \tilde{X} + Z_1 - Z_2$. $\tilde{X}$ and Z_1 are correlated, making the density expression relatively complicated when conditioning on X. In the small-noise regime, this correlation fades away, and the variance $2\sigma^2$ of the total additive Gaussian noise $Z_1 - Z_2$ dominates the mutual information as in (44). At low and very low signal-to-noise ratios, one should use exact density expressions from Theorem 3 and proceed via numerical integration to get exact values of $I(X;Y)$ and the corresponding SNR limits if the user accepts to apply a relatively low coding rate which is not the trend in TE-QKD where coding rates above $1/2$ are preferred which places us in the moderate and the high SNR region.

VII. Key-Reconciliation Codes

Following the complete characterization in Sections V-VI-B of the TE-QKD channel model described in Section III, we next introduce error-correcting codes to bring the error-rate performance as close as possible to the information-theoretic limits corresponding to maximal achievable rates.

A. Reed-Solomon (RS) Codes

We consider the famous family of Reed-Solomon codes with an application to a frame of $N = 2^m$ bins, i.e. m coded bits per photon. In order to chose a high enough error-correction capacity, an RS code over $\mathbb{F}_q$ is considered, where q is large enough. Each finite field element corresponds to $\log_2(q)/m$ photons. For simplicity, assume that $q = 2^{\ell m}$, for some positive integer ℓ. The RS code has length $n = q - 1$ (primitive) and dimension $k = n - 2t$, so the targeted rate is $m \times \frac{k}{n}$ information bits per photon. One codeword of this $\mathcal{C}[n,k,t]_q$ RS code requires the transmission of a total of $n \times \log_2(q)/m$ photons to Alice and $n \times \log_2(q)/m$ photons to Bob, all with valid frames. After receiving the $n \times \log_2(q)/m$ valid frames, Alice converts the $n \times \log_2(q)$ bits received on the quantum channel into a length-n word denoted by $c + e$, where $c \in \mathcal{C}$ and $e \in \mathbb{F}_q^n$. Similarly, Bob converts his $n \times \log_2(q)$ received bits into $c + e'$, where $e' \in \mathbb{F}_q^n$. In the hard-output channel model of Section III, $c + e$ is written at the input $\hat{X}$ and $c + e'$ is read from the output $\hat{Y}$. On the public channel, Alice sends to Bob the syndrome $s = (c+e)H^t$, $s \in \mathbb{F}_q^{n-k}$, where H is the parity-check matrix of $\mathcal{C}$. Given s and given $c+e'$, the reconciliation performed by Bob is equivalent to finding Alice's word $c+e$. Bob proceeds as follows:

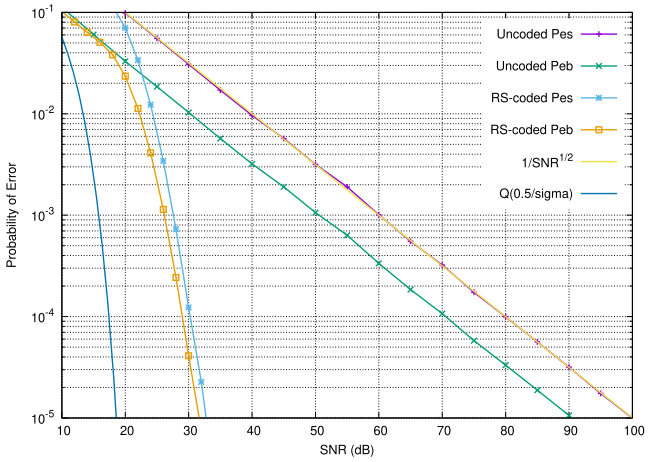

Fig. 9. Performance of the RS code $[63, 43, t = 10]_{64}$ on the hard-output time-entanglement QKD channel, for $N = 8$ bins per frame, transmitting 2.05 information bits per photon.

- Compute a syndrome $s' = (c + e')H^t$.
- Feed $s' - s$ to an algebraic (Berlekamp-Massey [14]) decoder to find $e' - e$.
- Subtract the error $e' - e$ from Bob's word to get $c + e' - (e' - e) = c + e$ the $\mathbb{F}_q^n$ word possessed by Alice. Replace all subtractions by additions in usual finite fields of characteristic 2.

The performance of RS $\mathcal{C}[n = 63, k = 43, t = 10]_{q=64}$ code is shown in Figure 9. One codeword requires the transmission of a total of 126 photons, where one field element carries two photons. The results show a large gain, e.g., about 58 dB of gain for a bit error-rate $P_{eb} = 10^{-5}$ after reconciliation.

The analysis of the algebraic decoder is easy thanks to its bounded-distance decoding in the Hamming space. A decoding error occurs each time the channel adds more than t errors in $\mathbb{F}_q$. A simple union bound for the RS code is obtained by summing from $t + 1$ to n errors. We proceed as follows:

a) The uncoded symbol error probability over the TE-QKD channel is $P_e(\gamma) = \frac{2}{\sqrt{\pi}}(1 - \frac{1}{N})\frac{1}{\sqrt{\gamma}}$.

b) For the RS code, the input probability of error per finite-field element is $P_{in}(\gamma) = 1 - (1 - P_e(\gamma))^{\ell}$.

c) The bound on the probability of error in $\mathbb{F}_q$ after decoding becomes

$$P_{eRS}(\gamma) = \sum_{i=t+1}^{n} \frac{i}{n}\binom{n}{i} P_{in}^i(\gamma)(1 - P_{in}(\gamma))^{n-i}. \quad (45)$$

d) The symbol (per photon) error probability after decoding is then $P_{eOut}(\gamma) = 1 - (1 - P_{eRS}(\gamma))^{1/\ell}$.

e) The probability of error per bit after Reed-Solomon decoding, given a Gray labeling of the bins, is well estimated by $P_{ebRS}(\gamma) = \frac{1}{\log_2(N)} P_{eOut}(\gamma)$.

The probability or error P_{ebRS} obtained from (45) perfectly fits the Monte Carlo method in the area where this method is tractable on a computer, i.e. for error rates in the interval $[10^{-7}, 10^{-1}]$. At $P_{ebRS} = 10^{-10}$, the coding gain over the uncoded probability of error per bit is 158 dB! Such a huge gain is explained by the diversity order of the TE-QKD channel. The diversity order is defined as $d = \lim_{\gamma\to\infty} \frac{-\log(P_e)}{\log(\gamma)}$ [10, Chapters 13-14]. From Proposition 1 we know that the TE-QKD has a diversity order of $\frac{1}{2}$, it behaves like a half-diversity Nakagami fading channel. The error-correcting code increases the diversity order which is equivalent to increasing the slope of $P_e(\gamma)$. An additive Gaussian noise channel without fading has infinite diversity, with or without coding, making all curves look parallel. In presence of fading, a high diversity converts the channel into a Gaussian channel [15]. In practice, a diversity order beyond 8 could be barely distinguished from the local slope of $e^{-\gamma}$ on a Gaussian channel. In our case, from (45), we deduce that the diversity order after algebraic RS decoding is $(t + 1)/2$. There is no asymptotic coding on the TE-QKD channel. The coding gain increases if measured at a lower probability of error.

B. Binary Bose-Chaudhuri-Hocquenghem (BCH) Codes

The TE-QKD channel does not generate error bursts. Errors are independent and the most common event is one erroneous bit per photon before decoding. In other words, the binary-burst error-correcting capability of Reed-Solomon codes is not exploited. Hence, we suggest to utilize a binary BCH code of the same binary length as the RS$[63, 43]_{64}$, which is $63 \times 6 = 378$ binary digits. We start from a primitive length of 511 and shorten down to 378. At $t = 13$ the binary BCH code has a dimension $k = 261$. This BCH$[378, 261, t = 13]_2$ code yields a diversity order $(t+1)/2 = 7$ better than the 5.5 order of the RS code shown in the previous section. The number of information bits per photon is $261/378 \times 3 = 2.07$ bits for $N = 8$ bins per frame.

Without adding any extra figure to this sub-section, the Monte Carlo simulation and the analytical bound show that the binary BCH$[378, 261, t = 13]$ code beats the RS$[63, 43]_{64}$ code by 3 dB in signal-to-noise ratio at $P_{ebRS} = P_{ebBCH} = 10^{-5}$. To get the coding gain at a lower probability of error, we propose the following very tight union bound:

a) The uncoded symbol error probability over the TE-QKD channel is $P_e(\gamma) = \frac{2}{\sqrt{\pi}}(1 - \frac{1}{N})\frac{1}{\sqrt{\gamma}}$. Below 10^{-1} a maximum of one bit error occurs in a block of $m = \log_2(N)$ coded bits thanks to Gray labeling. There are n/m such blocks per BCH codeword involving individual binary errors.

b) The bound on the probability of error in $\mathbb{F}_2$ after BCH decoding becomes

$$P_{ebBCH}(\gamma) = \sum_{i=t+1}^{n/m} \frac{i}{n}\binom{\frac{n}{m}}{i} P_e^i(\gamma)(1 - P_e(\gamma))^{\frac{n}{m}-i}. \quad (46)$$

At $P_{ebRS} = P_{ebBCH} = 10^{-10}$, the binary BCH$[378, 261, t = 13]$ code beats the RS$[63, 43]_{64}$ code by 5 dB. This value corresponds to a 163 dB of BCH coding gain with respect to the uncoded photons at $N = 8$ bins per frame. Notice that the reconciliation at Bob's side for BCH codes (binary or non-binary) is identical to the reconciliation described in the previous section for Reed-Solomon codes where the syndrome $s' - s$ is fed to a Berlekamp-Massey decoder.

C. Low-Density Parity-Check (LDPC) Codes

The significant impact of the graph-based LDPC codes on the performance of polarization-based QKD systems was

already demonstrated in [16] for the reconciliation of discrete random variables with a binary symmetric channel (BSC) model. Low-density parity-check codes [17], [18] are flexible regarding length, coding rate, and decoding methods. As usual, the LDPC code parity-check matrix is the adjacency matrix of a bipartite Tanner graph with n variable nodes and $n-k$ check nodes, assuming that the graph is (d_v, d_c)-regular. For finite fields $\mathbb{F}_q$ with $q>2$, non-zero elements of the adjacency matrix are replaced by elements from $\mathbb{F}_q \setminus \{0\}$. The standard method for decoding LDPC codes is belief propagation (BP), i.e., iterative probabilistic decoding. Codes over a large field F_q or a large ring $\mathbb{Z}/q\mathbb{Z}$ could be considered [19] to minimize the loss during the symbol-to-bit soft values conversion. It is also possible to use joint local-global LDPC codes with optimized bin mapping to achieve good performance [20] or apply multilevel coding as in [21]. However, these papers consider a different QKD channel model. This paper shows the impact of LDPC codes on TE-QKD with a $(3,9)$-regular binary LDPC code only. The coding rate is $2/3$ guaranteeing 2 exchanged bits per photon when the frame has 8 bins. However, we consider a short length $n=384$ (64×6) comparable to the RS and BCH codes given in the previous sub-sections and a longer code with $n=9999$ to illustrate a performance close enough to the Shannon limit.

The symbol/bin APP is found via (26), where $APP(i) = APP(\hat{X}=i)$ is the *a posteriori* probability of bin number i, $i\in\mathbb{Z}_N$. Then the APP of binary digit b_ℓ, where $\ell\in\mathbb{Z}_m$, $m=\log_2(N)$, is derived by the following marginalization

$$APP(b_\ell) = \sum_{i\in\mathbb{Z}_N \,:\, b_\ell} APP(\hat{X}=i). \tag{47}$$

The above marginalization depends on the type of binary labeling. Our paper considers N bins per frame with Gray labeling of $\log_2(N)$ bits per bin. Figure 10 shows the bit-error-rate versus γ for the binary LDPC code on the TE-QKD soft-output channel at $n=384$ bits and $n=9999$ bits. They respectively gain 12 and 16 dB compared to the BCH$[378,261]$ code, at a bit error probability of 10^{-5}. Compared to the uncoded TE-QKD, the coding gain is 73 dB and 77 dB, respectively. At length $n=9999$, the LDPC code is on top of the Shannon limit for a TE-QKD hard-output channel ($\gamma_{limit}=12.61$ dB) and is 2 dB only from the Shannon limit of the soft-output TE-QKD channel ($\gamma_{limit}=10.45$ dB). We see no reason for using longer LDPC codes to catch an extra 1-2 dB, given that the total coding gain compared to the no-coding case already equals 77 dB!

If a lab system implementation requires a less complex expression for $APP(\hat{X}=i)$ without the erfc()/Q() function and integration, (26) can be simplified by assuming that the Gaussian density has the effect of a Dirac impulse at small σ and using the $\propto$ symbol (proportional to) since the denominator does not depend on the index i, we get that $APP(i)$ is $\propto$

$$\int_0^N \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-u)^2}{2\sigma^2}} \left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right] du \propto \left[Q\left(\frac{i-y}{\sigma}\right) - Q\left(\frac{i+1-y}{\sigma}\right)\right].$$

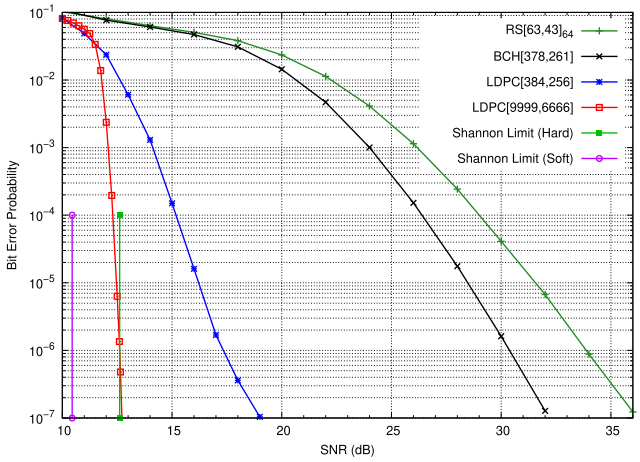

Fig. 10. Performance of the $(3,9)$-regular binary LDPC code at length $n=384$ and $n=9999$ bits on the soft-output time-entanglement QKD channel, for $N=8$ bins per frame, transmitting 2.0 information bits per photon.

Then, depending on the sign of the arguments $i-y$ and $i+1-y$, we approximate $Q(x)$ by $\frac{1}{2}e^{-\frac{x^2}{2}}$ (if $x\geq 0$) and by $1-\frac{1}{2}e^{-\frac{x^2}{2}}$ (if $x<0$). Let $j=\lfloor Y \rfloor$ be the bin position of Y on Bob's side, i.e. $Y\in[j, j+1[$. The simplified APP expressions become:

$$\text{If } i=j, \quad APP(i) \propto \left[1 - \tfrac{1}{2}e^{-\frac{(y-i)^2}{2\sigma^2}} - \tfrac{1}{2}e^{-\frac{(y-i-1)^2}{2\sigma^2}}\right], \tag{48}$$

$$\text{If } i\neq j, \quad APP(i) \propto sign(j-i)\left[\tfrac{1}{2}e^{-\frac{(y-i-1)^2}{2\sigma^2}} - \tfrac{1}{2}e^{-\frac{(y-i)^2}{2\sigma^2}}\right]. \tag{49}$$

When (48)-(49) are utilized in the BP decoder of the binary LDPC code over the TE-QKD soft-output channel, the loss is limited to 0.25-0.30 dB with respect to the exact expression (26). This is a minuscule loss when dealing with coding gains above 50 dB.

Notice that we are not showing a performance of the LDPC code over a hard-output channel. Indeed, optimal BP decoding is identical whether the channel output is soft or not, i.e., the BP decoder is the same decoder on both a Gaussian-like channel and a BSC-like channel. The gap between hard and soft is about 8.5 dB for the LDPC$[384,256]$ and about 4 dB for the LDPC$[9999,6666]$ at a bit error rate of 10^{-5}. Suppose the system implementation possesses an optimal BP decoder, but the exact photon position is unavailable; only the bin number is available. In such a case, the lab implementation is forced to use LDPC codes on a hard-output channel, and the binary digits APP expression (47) becomes

$$APP(b_\ell) \propto \sum_{i\in\mathbb{Z}_N \,:\, b_\ell} \hat{\pi}_i \times p_{i,j}, \tag{50}$$

where $j=\lfloor Y \rfloor$, $\hat{\pi}_i$ is given by (20) or (32)-(33) at small σ, and $p_{i,j}$ is given by (25) or (30)-(31) in the small σ regime. Coding theorists and practitioners could also use convolutional codes, turbo codes, polar codes, and other binary or non-binary

TABLE II
INFORMATION THEORETICAL (SHANNON) LIMITS FOR TE-QKD

N bins per frame	Bits per photon	$R = k/n$ code rate	SNR limit hard	σ/N hard	SNR limit soft	σ/N soft
8	2.0	2/3	12.61 dB	0.029269	10.45 dB	0.037533
16	3.0	3/4	13.29 dB	0.013532	10.85 dB	0.017922
32	3.0	3/5	3.88 dB	0.019992	3.46 dB	0.020982
32	4.0	4/5	13.61 dB	0.0065215	11.04 dB	0.0087670
64	4.0	2/3	4.01 dB	0.0098474	3.58 dB	0.010347
64	5.0	5/6	13.77 dB	0.0032012	11.13 dB	0.0043383
8 Uncoded	3.0	1	90.34 dB $P_{eb} = 10^{-5}$	0.0000038 achieved		
8 BCH, n=378	2.0	2/3	28.49 dB $P_{eb} = 10^{-5}$	0.0047034 achieved		
8 LDPC, n=9999	2.0	2/3			12.47 dB $P_{eb} = 10^{-5}$	0.029745 achieved

algebraic codes with short or moderate length to achieve large coding gains on the TE-QKD channel.

D. A Summary of Capacity Limits at Different Frame Sizes

We complete the current section by a table summarizing important information theoretical limits on the time-entanglement QKD channel, with both hard and soft output. Shannon limit in terms of SNR is the value of the non-normalized signal-to-noise ratio γ such that mutual information is equal to the targeted information exchange rate, $I(\hat{X};\hat{Y}) = \frac{k}{n}\log_2(N)$ for a hard output and $I(\hat{X};Y) = \frac{k}{n}\log_2(N)$ for a soft output. Table II has seven columns with parameters covering 8 bins per frame up to 64 bins per frame. The last two rows correspond to SNR and standard deviation values achieved by the BCH and the LDPC codes as found in sub-sections VII-B and VII-C.

The signal-noise ratio soft-decoding limits listed in Table II appear to be close to two values, one SNR of around 10-11 dB and a lower SNR around 3.5 dB. The hard-decoding limits are higher than soft-decoding limits, because $I(\hat{X};\hat{Y}) \leq I(\hat{X};Y)$, the gap depends on the frame size and the coding rate. Of course, the hard-soft gap vanishes at small coding rates (below $1/2$) and increases at high coding rates when mutual information approaches the asymptote $\log_2(N)$.

The two typical values of soft-decoding SNR limits are explained or interpreted for small σ via (44):

$$\frac{1}{2}\log\left(\frac{\overline{\gamma}}{4\pi e}\right) = \log_2(N) - b, \tag{51}$$

where $\overline{\gamma} = N^2\gamma$ and b is a backoff value. Here, $b = 1$ bit or $b = 2$ bits in Table II. Then, solving (51) yields $\gamma = (4\pi e)/2^{2b}$. We get $\gamma = 9.31$ dB for $b = 1$ and $\gamma = 3.29$ for $b = 2$. The difference with the values in the 6th column of Table II is due to $I(\hat{X};Y)$ going away from the envelope $I(X;Y)$ to follow its own asymptote. We hope that SNR limits given in Table II will be useful to physicists and coding theorists working in this QKD field.

VIII. CONCLUSION

In TE-QKD, the photon arrival detector jitter leaves Alice and Bob with correlated but not identical keys. To obtain a shared secret key, Alice must send information to Bob over a public channel, thus lowering their shared key rate. We presented a rigorous analysis of secret key information rates and proposed and tested several codes for information reconciliation to approach the maximum secret key rates. These achievable secret key rates are much higher than the maximum possible by polarization entanglement-based QKD.

The main contributions of this paper constitute a full characterization of the time-entanglement QKD channel from information theory and coding theory points of view:

- We derive the error rates of the TE-QKD channel, and prove that the TE-QKD channel behaves like a $1/2$-diversity Nakagami fading channel, see Proposition 1.
- We find the exact *a priori* probability of bins given that both Alice's and Bob's frames are valid; see Lemma 2.
- We establish the exact conditional density of Bob's photon position given Alice's for a soft-output TE-QKD channel; see Theorem 1. The output density expression is also determined; see (27).
- We determine the expression of the transition probabilities of the discrete (hard-output) TE-QKD channel; see Corollary 1.
- We give the exact expression of the *a posteriori* probability for the soft-output TE-QKD channel, see Theorem 2.
- We derive the exact formula for the mutual information $I(\hat{X};\hat{Y})$ (hard-output) and find simplified expressions in the small-noise regime, see (28), (29), (35), and Proposition 2-c.
- The exact formula for the mutual information $I(\hat{X};Y)$ (soft-output) is given, see (36). We also determine all densities needed to compute the maximal rate $I(X;Y)$, and we give a nice log-formula expression in the small-noise regime, see Theorem 3 and Corollary 2.
- We demonstrate that huge coding gains can be obtained by short and moderate-length error-correcting codes such as the well-known RS, BCH, and LDPC codes under algebraic hard-decision decoding and probabilistic soft-decision decoding.

Practical photon detectors suffer from other impairments, e.g., dark currents and downtime, which may cause further rate loss. These impairments should be a subject of future work.

For an extensive list of open problems and future directions in TE-QKD, we refer the reader to the expository article [22].

APPENDIX

This appendix includes the proofs of Lemmas 1, 2, 3, and Proposition 2.

A. Proof of Lemma 1

For a), let G be a standard normal random variable. The finite interval $[-x, 1-x]$ is never reduced to a single point. We get $f_\sigma(x) = \mathbb{P}(G \in [-x, 1-x]) \in]0,1[$. Then, $f_\sigma(1-x) = Q\left(-\frac{(1-x)}{\sigma}\right) - Q\left(\frac{x}{\sigma}\right) = 1 - Q\left(\frac{1-x}{\sigma}\right) - 1 + Q\left(-\frac{x}{\sigma}\right) = f_\sigma(x)$, using the property $Q(-x) = 1-Q(x)$. Finally $f_\sigma(0) = Q(0) - Q\left(\frac{1}{\sigma}\right) = \frac{1}{2} - \mathcal{O}(\exp(-\frac{\gamma}{2}))$.

For b), we write $f_\sigma(x) = 1 - Q\left(\frac{x}{\sigma}\right) - Q\left(\frac{1-x}{\sigma}\right)$. Then $Q\left(\frac{x}{\sigma}\right) + Q\left(\frac{1-x}{\sigma}\right) \leq \frac{1}{2}\exp(-x^2/(2\sigma^2)) + \frac{1}{2}\exp(-(1-x)^2/(2\sigma^2)) \leq \exp(-\min^2(x, 1-x)\gamma/2)$ which yields the announced result. This inequality is only useful to us for $x \in]0,1[$ to keep the exponential decay.

For c), $x < 0$, so $1-x > -x > 0$. Then $f_\sigma(x) \leq Q\left(\frac{-x}{\sigma}\right) \leq \frac{1}{2}\exp(-x^2/(2\sigma^2)) = \mathcal{O}(\exp(-x^2\gamma/2))$. The proof is similar for $x > 1$.

As mentioned for I_1 in the proof of Proposition 1, the anti-derivative of $Q(ax)$, $a, x \in \mathbb{R}$, is determined after integration by parts. We get

$$\int Q(ax)dx = xQ(ax) - \frac{1}{\sqrt{2\pi a^2}}\exp(-a^2x^2/2) + c, \quad (52)$$

where c is the integration constant.

For d), $\int_0^1 f_\sigma(x)\ dx = \int_0^1 \left[1 - Q\left(\frac{x}{\sigma}\right) - Q\left(\frac{1-x}{\sigma}\right)\right] dx = 1 - 2I_1 = 1 - \sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{\gamma}} + \mathcal{O}(\exp(-\frac{\gamma}{2}))$, where I_1 is solved thanks to (52).

As mentioned for I_2 in the proof of Proposition 1, the anti-derivative of $[Q(ax)]^2$, $a, x \in \mathbb{R}$, is also determined by integration by parts and the application of (52). We get

$$\int Q^2(ax)dx = xQ^2(ax) - \sqrt{\frac{2}{\pi a^2}}Q(ax)\exp(-a^2x^2/2) + \frac{1}{\sqrt{\pi a^2}}Q(ax\sqrt{2}) + c. \quad (53)$$

Then, $\int_0^1 f_\sigma^2(x)dx = 1 - 4I_1 + 2I_2 + 2I_3 = 1 - 4 \times \frac{\sigma}{\sqrt{2\pi}} + 2 \times \frac{\sqrt{2}-1}{2\sqrt{\pi}}\sigma + \mathcal{O}(\exp(-\frac{\gamma}{4}))$, where I_2 is solved thanks to (53) and $I_3 = \mathcal{O}(\exp(-\frac{\gamma}{4}))$ as shown before. This completes the proof of d).

The proof of e) is mainly based on (52), after taking care of the bin position within the frame. We have

$$\begin{aligned} I_4 &= \int_{i/N}^{(i+1)/N} f_\sigma(x)\ dx \\ &= \int_{i/N}^{(i+1)/N} \left[1 - Q\left(\frac{x}{\sigma}\right) - Q\left(\frac{1-x}{\sigma}\right)\right] dx \\ &= \frac{1}{N} - \int_{i/N}^{(i+1)/N} Q\left(\frac{x}{\sigma}\right) dx - \int_{1-(i+1)/N}^{1-i/N} Q\left(\frac{x}{\sigma}\right) dx \\ &= \frac{1}{N} - \left[\frac{(i+1)}{N}Q\left(\frac{i+1}{N\sigma}\right) - \frac{i}{N}Q\left(\frac{i}{N\sigma}\right)\right. \\ &\quad \left. - \frac{\sigma}{\sqrt{2\pi}}e^{-\frac{\gamma}{2}\frac{(i+1)^2}{N^2}} + \frac{\sigma}{\sqrt{2\pi}}e^{-\frac{\gamma}{2}\frac{i^2}{N^2}}\right] \\ &\quad - \left[(1 - \frac{i}{N})Q\left(\frac{1-\frac{i}{N}}{\sigma}\right) - (1 - \frac{i+1}{N})Q\left(\frac{1-\frac{i+1}{N}}{\sigma}\right)\right. \\ &\quad \left. - \frac{\sigma}{\sqrt{2\pi}}e^{-\frac{\gamma}{2}(1-\frac{i}{N})^2} + \frac{\sigma}{\sqrt{2\pi}}e^{-\frac{\gamma}{2}(1-\frac{i+1}{N})^2}\right]. \end{aligned}$$

If $i = 0$ or $i = N-1$, $I_4 = \frac{1}{N} - \frac{\sigma}{\sqrt{2\pi}} = 1 - \mathcal{O}(\frac{1}{\sqrt{\gamma}})$, all terms with exponential decay are absorbed by the $\mathcal{O}(\frac{1}{\sqrt{\gamma}})$. For middle bins, $i = 1 \ldots N-2$, $I_4 = \frac{1}{N} + \mathcal{O}(e^{-\frac{\gamma}{2}\frac{i^2}{N^2}}) + \mathcal{O}(e^{-\frac{\gamma}{2}(1-\frac{i+1}{N})^2})$, all terms of higher decay are absorbed by these two big $\mathcal{O}$. Hence, $I_4 = \frac{1}{N} + \mathcal{O}(e^{-\beta\gamma})$, where the exponent constant is $\beta = \frac{1}{2}\min^2(i/N, 1-(i+1)/N)$. □

B. Proof of Lemma 2

Let us apply Bayes' rule, while dropping the subscripts to simplify the notation:

$$p(u|\tilde{X} \in [0, N[) = \frac{\mathbb{P}(\tilde{X} \in [0, N[|u) \times p_U(u)}{\mathbb{P}(\tilde{X} \in [0, N[)}.$$

From (13), we get $\mathbb{P}(\tilde{X} \in [0, N[|u) = Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)$.

From (15), we get the expression $\mathbb{P}(\tilde{X} \in [0, N[) = \frac{1}{N}\int_0^N \left[Q\left(\frac{-t}{\sigma}\right) - Q\left(\frac{N-t}{\sigma}\right)\right] dt$. Finally, plugging $p_U(u) = 1/N$ leads to the result announced by the lemma in (19). The equality $p_{U|\tilde{X}\in[0,N[}(u) = p_{U|\tilde{Y}\in[0,N[}(u)$ is the result of the symmetry between Alice and Bob in our model.

The *a priori* probability $\hat{\pi}_i$ is derived after establishing the density of $\tilde{X}$ conditioned on a valid frame for Bob, $\tilde{Y} \in [0, N[$. By marginalisation over U, we have

$$\begin{aligned} p_{\tilde{X}|\tilde{Y}\in[0,N[}(\tilde{x}) &= \int_0^N p_{\tilde{X}|U,\tilde{Y}\in[0,N[}(\tilde{x}|u)p_{U|\tilde{Y}\in[0,N[}(u)\ du \\ &= \int_0^N p_{\tilde{X}|U}(\tilde{x}|u)p_{U|\tilde{Y}\in[0,N[}(u)\ du, \end{aligned} \quad (54)$$

where the two factors are given by (13) and (19) respectively. The *a priori* probability $\hat{\pi}_i = \mathbb{P}(X \in [i, i+1[|\tilde{Y} \in [0, N[)$ becomes, for $i = 0, \ldots, N-1$,

$$\begin{aligned} \hat{\pi}_i &= \int_i^{i+1} p_{X|\tilde{Y}\in[0,N[}(x)\ dx \\ &= \int_i^{i+1} \frac{p_{\tilde{X}|\tilde{Y}\in[0,N[}(x)}{\int_0^N p_{\tilde{X}|\tilde{Y}\in[0,N[}(\tilde{x})\ d\tilde{x}}\ dx \\ &= \frac{\int_{x=i}^{i+1}\int_{u=0}^N p_{\tilde{X}|U}(x|u)p_{U|\tilde{Y}\in[0,N[}(u)\ du\ dx}{\int_{\tilde{x}=0}^N\int_{u=0}^N p_{\tilde{X}|U}(\tilde{x}|u)p_{U|\tilde{Y}\in[0,N[}(u)\ du\ d\tilde{x}} \\ &= \frac{\int_{u=0}^N \left[Q\left(\frac{i-u}{\sigma}\right) - Q\left(\frac{i+1-u}{\sigma}\right)\right] p_{U|\tilde{Y}\in[0,N[}(u)\ du\ dx}{\int_{u=0}^N \left[Q\left(\frac{-u}{\sigma}\right) - Q\left(\frac{N-u}{\sigma}\right)\right] p_{U|\tilde{Y}\in[0,N[}(u)\ du\ d\tilde{x}}. \end{aligned}$$

We obtain (20) after replacing $p_{U|\tilde{Y}\in[0,N[}(u)$ by its expression from (19). □

C. Proof of Lemma 3

The existence of X and $\hat{X}$, e.g. when writing $\hat{X} = i$, requires that $\tilde{X} \in [0, N[$. This hidden assumption should not

be forgotten. By applying Bayes' rule,

$$p(u|\hat{X}=i) = p(u|\hat{X}=i, \tilde{X}\in[0,N[) = \frac{\mathbb{P}(\hat{X}=i|u,\tilde{X}\in[0,N[)\times p(u|\tilde{X}\in[0,N[)}{\pi_i}.$$

The first term in the numerator can be developed as follows

$$\mathbb{P}(\hat{X}=i|u,\tilde{X}\in[0,N[) = \mathbb{P}(X\in[i,i+1[|u,\tilde{X}\in[0,N[) = \frac{\mathbb{P}(\tilde{X}\in[i,i+1[|u)}{\mathbb{P}(\tilde{X}\in[0,N[|u)} = \frac{Q\left(\frac{i-u}{\sigma}\right)-Q\left(\frac{i+1-u}{\sigma}\right)}{Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)}.$$

The second term in the numerator is given in (19) in Lemma 2. After substituting the expression of π_i from (18), we get

$$p(u|\hat{X}=i) = \frac{Q\left(\frac{i-u}{\sigma}\right)-Q\left(\frac{i+1-u}{\sigma}\right)}{\int_i^{i+1}\left[Q\left(\frac{-t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]dt},$$

The reader is invited to prove via a change of variable that

$$\int_i^{i+1}\left[Q\left(\frac{-t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]dt = \int_0^{N}\left[Q\left(\frac{i-t}{\sigma}\right)-Q\left(\frac{i+1-t}{\sigma}\right)\right]dt. \quad (55)$$

which leads to the result announced by the lemma in (21). The proof of (22) follows similar steps as for the proof of (21). Firstly, using Bayes' rule and (14) we get a conditional density of U,

$$p(u|\tilde{X},\tilde{Y}\in[0,N[) = \frac{\left[Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]^2}{\int_0^N\left[Q\left(\frac{-t}{\sigma}\right)-Q\left(\frac{N-t}{\sigma}\right)\right]^2 dt}. \quad (56)$$

Secondly, we solve the conditional probability of Alice's photon bins,

$$\mathbb{P}(\hat{X}=i|u,\tilde{X},\tilde{Y}\in[0,N[) = \frac{\mathbb{P}(\tilde{X}\in[i,i+1[,\tilde{Y}\in[0,N[|u)}{\mathbb{P}(\tilde{X},\tilde{Y}\in[0,N[|u)} = \frac{\left[Q\left(\frac{i-u}{\sigma}\right)-Q\left(\frac{i+1-u}{\sigma}\right)\right]\left[Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]}{\left[Q\left(\frac{-u}{\sigma}\right)-Q\left(\frac{N-u}{\sigma}\right)\right]^2}.$$

Finally, we use the above expressions of $\mathbb{P}(\hat{X}=i|u,\tilde{X},\tilde{Y}\in[0,N[)$ and $p(u|\hat{X},\tilde{Y}\in[0,N[)$, and (20) from Lemma 2 in

$$p(u|\hat{X}=i,\tilde{Y}\in[0,N[) = \frac{\mathbb{P}(\hat{X}=i|u,\tilde{X},\tilde{Y}\in[0,N[)\times p(u|\tilde{X},\tilde{Y}\in[0,N[)}{\hat{\pi}_i}$$

to reach (22) in this lemma. □

D. Proof of Proposition 2

For the sake of space, we only show the detailed proof for the denominator of $p_{0,1}$ (also equal to the numerator of $\hat{\pi}_0$). All other results are found using similar calculus techniques. The denominator of $p_{0,1}$ from Corollary 1 ($i=0, j=1$) is equal to the integral

$$\begin{aligned}
I_5 &= \int_0^N\left[Q\left(\tfrac{-t}{\sigma}\right)-Q\left(\tfrac{N-t}{\sigma}\right)\right]\left[Q\left(\tfrac{-t}{\sigma}\right)-Q\left(\tfrac{1-t}{\sigma}\right)\right]dt\\
&= \int_0^N\left[1-Q\left(\tfrac{t}{\sigma}\right)-Q\left(\tfrac{N-t}{\sigma}\right)\right]\left[Q\left(\tfrac{t-1}{\sigma}\right)-Q\left(\tfrac{t}{\sigma}\right)\right]dt\\
&= \int_0^N Q\left(\tfrac{t-1}{\sigma}\right)dt - \int_0^N Q\left(\tfrac{t}{\sigma}\right)dt + \int_0^N Q^2\left(\tfrac{t}{\sigma}\right)dt\\
&- \int_0^N Q\left(\tfrac{t}{\sigma}\right)Q\left(\tfrac{t-1}{\sigma}\right)dt - \int_0^N Q\left(\tfrac{N-t}{\sigma}\right)Q\left(\tfrac{t-1}{\sigma}\right)dt\\
&+ \int_0^N Q\left(\tfrac{N-t}{\sigma}\right)Q\left(\tfrac{t}{\sigma}\right)dt\\
&= \underbrace{\int_{-1}^0 Q\left(\tfrac{t}{\sigma}\right)dt}_{(i)} - \underbrace{\int_{N-1}^N Q\left(\tfrac{t}{\sigma}\right)dt}_{(ii)} + \underbrace{\int_0^N Q^2\left(\tfrac{t}{\sigma}\right)dt}_{(iii)}\\
&- \underbrace{\int_0^1 Q\left(\tfrac{t}{\sigma}\right)\left(1-Q\left(\tfrac{1-t}{\sigma}\right)\right)dt}_{(iv)} - \underbrace{\int_1^N Q\left(\tfrac{t}{\sigma}\right)Q\left(\tfrac{t-1}{\sigma}\right)dt}_{(v)}\\
&- \underbrace{\int_0^1 Q\left(\tfrac{N-t}{\sigma}\right)\left(1-Q\left(\tfrac{1-t}{\sigma}\right)\right)dt}_{(vi)}\\
&- \underbrace{\int_1^N Q\left(\tfrac{N-t}{\sigma}\right)Q\left(\tfrac{t-1}{\sigma}\right)dt}_{(vii)} + \underbrace{\int_0^N Q\left(\tfrac{N-t}{\sigma}\right)Q\left(\tfrac{t}{\sigma}\right)dt}_{(viii)}.
\end{aligned}$$

Now we solve the elementary integrals (i)-$(viii)$ one by one.

Using (52), $(i) = 0 - \frac{\sigma}{\sqrt{2\pi}} + Q(\frac{-1}{\sigma}) + \frac{\sigma}{\sqrt{2\pi}}e^{-\frac{\gamma}{2}} = 1 - \frac{\sigma}{\sqrt{2\pi}} + \mathcal{O}(e^{-\frac{\gamma}{2}})$. Using the fact that $Q(x)$ is a monotone decreasing function, then $(ii) = \mathcal{O}(e^{-(N-1)^2\frac{\gamma}{2}})$. The third integral is directly solved via (53): $(iii) = NQ^2(\frac{N}{\sigma}) - \sigma\sqrt{\frac{2}{\pi}}Q(\frac{N}{\sigma})e^{-N^2\frac{\gamma}{2}} + \frac{\sigma}{\sqrt{\pi}}Q(\frac{N\sqrt{2}}{\sigma}) - 0 + \sigma\sqrt{\frac{2}{\pi}}\frac{1}{2} - \frac{\sigma}{\sqrt{\pi}}\frac{1}{2}$. Then we find $(iii) = \left(\frac{\sqrt{2}-1}{2\sqrt{\pi}}\right)\sigma + \mathcal{O}(e^{-N^2\frac{\gamma}{2}})$. $(iv) = I_1 - I_3 = \frac{\sigma}{\sqrt{2\pi}} + \mathcal{O}(e^{-\frac{\gamma}{4}})$. For (v), $t^2+(t-1)^2 \geq 1$ in the interval $[1,N]$, then we have $(v) = \mathcal{O}(e^{-\frac{\gamma}{2}})$. The first part of (vi) is $\mathcal{O}(e^{-(N-1)^2\frac{\gamma}{2}})$ and the second part is also $\mathcal{O}(e^{-(N-1)^2\frac{\gamma}{2}})$ because $(N-t)^2+(1-t)^2 \geq (N-1)^2$ in the interval $[0,1]$. So $(vi) = \mathcal{O}(e^{-(N-1)^2\frac{\gamma}{2}})$. Applying similar arguments, we get $(vii) = \mathcal{O}(e^{-(N-1)^2\frac{\gamma}{4}})$ and $(viii) = \mathcal{O}(e^{-N^2\frac{\gamma}{4}})$. Combining (i)-$(viii)$ yields $I_5 = 1 - \frac{1+\sqrt{2}}{2\sqrt{\pi}}\sigma + \mathcal{O}(e^{-\frac{\gamma}{4}})$ as stated. □

REFERENCES

[1] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *NPJ Quantum Inf.*, vol. 2, no. 1, p. 16025, Nov. 2016.

[2] R. Nandal, A. Nandal, K. Joshi, and A. Rathee, "A survey and comparison of some of the most prominent QKD protocols," *SSRN Electron. J.*, vol. 1, pp. 238–272, Jan. 2021.

[3] C. Lee et al., "High-rate field demonstration of large-alphabet quantum key distribution," Defense Tech. Inf. Center, Fort Belvoir, VA, USA, Tech. Rep., 2016.

[4] M. C. Sarihan et al., "High dimensional quantum key distribution with biphoton frequency combs through energy-time entanglement," in *Proc. Conf. Lasers Electro-Optics (CLEO)*, May 2019, pp. 1–2.

[5] D. Birnie, C. Cheng, and E. Soljanin, "Information rates with non ideal photon detectors in time-entanglement based QKD," *IEEE Trans. Commun.*, vol. 71, no. 4, pp. 2246–2259, Apr. 2023.

[6] T. Zhong et al., "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," *New J. Phys.*, vol. 17, Feb. 2015, Art. no. 022002.

[7] H. Zhou and G. Wornell, "Adaptive pulse-position modulation for high-dimensional quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory*, Istanbul, Turkey, Jul. 2013, pp. 359–363.

[8] E. Karimi, E. Soljanin, and P. Whiting, "Increasing the raw key rate in energy-time entanglement based quantum key distribution," in *Proc. 54th Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, USA, Nov. 2020, pp. 433–438.
[9] A. E. Gamal and Y. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[10] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2008.
[11] *Superconducting Nanowire Single-Photon Detectors*, Photon Spot Inc., Monrovia, CA, USA, 2022.
[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.
[13] J. J. Boutros and E. Soljanin, "Time-entanglement QKD: Secret key rates and information reconciliation coding," 2023, *2301.00486v1*.
[14] R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[15] J. J. Boutros and E. Viterbo, "Signal space diversity: A power- and bandwidth-efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. Inf. Theory*, vol. 42, pp. 502–518, Jul. 1998.
[16] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, South Korea, Jun. 2009, pp. 1–11.
[17] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA, USA: MIT Press, 1963.
[18] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[19] J. J. Boutros, U. Erez, J. V. Wonterghem, G. I. Shamir, and G. Zèmor, "Geometric shaping: Low-density coding of Gaussian-like constellations," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Guangzhou, China, Nov. 2018, pp. 1–5.
[20] S. Yang, M. C. Sarihan, K.-C. Chang, C. W. Wong, and L. Dolecek, "Efficient information reconciliation for energy-time entanglement quantum key distribution," in *Proc. 53rd Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, USA, Nov. 2019, pp. 1364–1368.
[21] H. Zhou, L. Wang, and G. Wornell, "Layered schemes for large-alphabet secret key distribution," in *Proc. Inf. Theory Appl. Workshop (ITA)*, San Diego, CA, USA, Feb. 2013, pp. 1–10.
[22] L. Dolecek and E. Soljanin, "QKD based on time-entangled photons and its key-rate promise," 2023, *arXiv:2303.01973*.

Joseph J. Boutros (Senior Member, IEEE) received the M.S. degree in electrical engineering and the Ph.D. degree from École Nationale Supérieure des Télécommunications (ENST, Télécom Paris), Paris, France, in 1992 and 1996, respectively. From 1996 to 2006, he was an Associate Professor with the Department of Communications and Electronics, ENST. He was a member of the Research Unit UMR-5141 with the French National Scientific Research Center (CNRS), Paris. In 2007, he joined Texas A&M University at Qatar, as a Professor of electrical engineering. He teaches courses in signal processing, communication theory, probability theory, neural networks, and computer programming. His mathematical approach for teaching communication theory is combined with a strong practical computing component. He has been a Scientific Consultant with Alcatel Space, Philips Research, and Motorola Semiconductors, and a member of the Digital Signal Processing Team, Juniper Networks Cable. In 2019, he was a appointed holder of the Occidental Petroleum Professorship in STEM Leadership. He is a co-inventor of 14 industrial patents, including algorithms and techniques in channel coding and digital communications. His research interests include codes on graphs, sphere packing and lattices, iterative decoding, codes for security, and connections between coding theory and other areas, such as cryptography and machine learning. His research is mainly performed under grants and tight collaboration with private companies and public institutions, such as Mitsubishi Electric; Europe, Rennes, France; Google Pittsburgh, USA; Nokia Bell-Labs Paris, France; and the Qatar National Research Fund. He is the General Chair and the Organizer of the 2003 and the 2023 IEEE Information Theory Workshop at La Sorbonne and at Saint-Malo, France.

Emina Soljanin (Fellow, IEEE) received the European Diploma in electrical engineering from the University of Sarajevo, Bosnia, in 1986, and the Ph.D. and M.S. degrees in electrical engineering from Texas A&M University, College Station, TX, USA, in 1989 and 1994, respectively. She is currently a Distinguished Professor of electrical and computer engineering at Rutgers, The State University of New Jersey. Before moving to Rutgers, The State University of New Jersey in January 2016, she was a member of Technical Staff (Distinguished) for 21 years in various incarnations of the Mathematical Sciences Research Center, Bell Labs. Her interests and expertise are broad and currently range from distributed computing to quantum information science. Over the past quarter of the century, she has participated in numerous research and business projects, including power system optimization, magnetic recording, color space quantization, hybrid ARQ, network coding, data and network security, distributed systems performance analysis, and quantum information theory. She was an outstanding alumnus at the Texas A&M School of Engineering, the 2011 Padovani Lecturer, the 2016 and 2017 Distinguished Lecturer, and the 2019 IEEE Information Theory Society President.