Quantum Inf Process (2017) 16:280
DOI 10.1007/s11128-017-1709-5

Fundamental finite key limits for one-way information reconciliation in quantum key distribution

Marco Tomamichel[1] · **Jesus Martinez-Mateo**[2] · **Christoph Pacher**[3] · **David Elkouss**[4]

Received: 2 March 2016 / Accepted: 29 August 2017

Abstract The security of quantum key distribution protocols is guaranteed by the laws of quantum mechanics. However, a precise analysis of the security properties requires tools from both classical cryptography and information theory. Here, we employ recent results in non-asymptotic classical information theory to show that one-way information reconciliation imposes fundamental limitations on the amount of secret key that can be extracted in the finite key regime. In particular, we find that an often used approximation for the information leakage during information reconciliation is not generally valid. We propose an improved approximation that takes into account finite key effects and numerically test it against codes for two probability distributions, that we call binary–binary and binary–Gaussian, that typically appear in quantum key distribution protocols.

Keywords Quantum key distribution · Finite length · Low-density parity-check codes

Part of these results without the technical derivations were published in the proceedings of the International Symposium on Information Theory, Honolulu (2014) [44].

✉ Marco Tomamichel
marco.tomamichel@uts.edu.au

1 Centre for Quantum Software and Information, University of Technology Sydney, Sydney, NSW 2007, Australia

2 Center for Computational Simulation, Universidad Politecnica de Madrid, 28660 Boadilla del Monte, Spain

3 Digital Safety & Security Department, AIT Austrian Institute of Technology, Donau-City-Straße 1, 1220 Vienna, Austria

4 QuTech, Delft University of Technology, P.O. Box 5046, 2600 GA Delft, The Netherlands

Published online: 06 October 2017

1 Introduction

Quantum key distribution (QKD) [4,10] is a prime example of the interdisciplinary nature of quantum cryptography and the first application of quantum science that has matured into the realm of engineering and commercial development. While the security of the generated key is intuitively guaranteed by the laws of quantum mechanics, a precise analysis of the security requires tools from both classical cryptography and information theory (see [27,36] for early security proofs, and see [34] for a comprehensive review). This is particularly relevant when investigating the security of QKD in a practical setting where the resources available to the honest parties are finite and the security analysis consequently relies on non-asymptotic information theory.

In the following, we consider QKD protocols between two honest parties, Alice and Bob, which can be partitioned into the following rough steps. In the *quantum phase*, N physical systems are prepared, exchanged and measured by Alice and Bob. In the *parameter estimation (PE) phase*, relevant parameters describing the channel between Alice and Bob are estimated from correlations measured in the quantum phase. If the estimated parameters do not allow extraction of a secure key, the protocol aborts at this point. Otherwise, the remaining measurement data is condensed into two highly correlated bit strings of length n in the *sifting phase*—the *raw keys* X^n for Alice and Y^n for Bob [31]. We call n the block length, and it is the quantity that is usually limited by practical considerations (time interval between generated keys, amount of key that has to be discarded in case Alice and Bob create different keys, hardware restrictions). In the *information reconciliation (IR) phase*, Alice and Bob exchange classical information about X^n over a public channel in order for Bob to compute an estimate $\hat{X}^n$ of X^n. The *confirmation (CO) phase* ensures that $\hat{X}^n = X^n$ holds with high probability, or it aborts the protocol. Finally, in the *privacy amplification (PA) phase*, Alice and Bob distill a shared secret key of ℓ bits from X^n and $\hat{X}^n$. We say that a protocol is *secure* if (up to some error tolerance) both Alice and Bob hold an identical, uniform key that is independent of the information gathered by an eavesdropper during the protocol, for any eavesdropper with access to the quantum and the authenticated classical channel.

The ratio ℓ/N is constrained by the following effects: (1) Some measurement results are published for PE and subsequently discarded. (2) The sifting phase removes data that is not expected to be highly correlated, thus further reducing the length n of the raw key. (3) Additional information about the raw keys is leaked to the eavesdropper during the IR and CO phase. (4) To remove correlations with the eavesdropper, X^n and $\hat{X}^n$ need to be purged in the PA phase, resulting in a shorter key. Some of these contributions vanish asymptotically for large N while others approach fundamental limits.[1]

Modern tools allow to analyze QKD protocols that are secure against the most general attacks. They provide lower bounds on the number of secure key bits that can be extracted for a fixed block length, n. For the BB84 protocol, such proofs are, for example, given in [33,35] and [14]. These proofs were subsequently simplified

[1] Consider, for example, BB84 with asymmetric basis choice [25] on a channel with quantum bit error rate Q. Here, contributions (1) and (2) vanish asymptotically while contributions (3) and (4) converge to $h(Q)$.

to achieve better key rates in [43] and [17], respectively (see also [42] for a recent detailed proof). All results have in common that the key rate that can be achieved with finite resources is strictly smaller than the asymptotic limit for large n—as one would intuitively expect.

We are concerned with a complementary question: Given a secure but otherwise arbitrary QKD protocol for a fixed n, are there fundamental upper bounds on the length of the key that can be produced by this protocol? Such bounds are of theoretical as well as practical interest since they provide a benchmark against which contemporary implementations of QKD can be measured. In the asymptotic regime of large block lengths, such upper bounds have already been investigated, for example, in [29]. Here we limit the discussion to IR and focus on bounds that solely arise due to finite block lengths (Sect. 2). We complement the bounds with a numerical study of achievable leak values with LDPC codes (Sect. 5) and study some possible improvements and open issues (Sect. 6).

2 Fundamental limits for one-way reconciliation

We consider *one-way* IR protocols, where Alice first computes a syndrome, $M \in \mathcal{M}$, from her raw key, X^n, and sends it to Bob who uses the syndrome together with his own raw key, Y^n, to construct an estimate $\hat{X}^n$ of X^n. We will assume that X takes values in a discrete alphabet while we allow Y to take values in the real line. We are interested in the size of the syndrome (in bits), denoted $\log|\mathcal{M}|$, and the probability of error, $\Pr[X^n \neq \hat{X}^n]$. In most contemporary security proofs, $\log|\mathcal{M}|$ enters the calculation of the key rate rather directly.[2] More precisely, to achieve security it is necessary (but not sufficient) that

$$\ell \leq n - \mathrm{leak}_{\mathrm{EC}}, \tag{1}$$

where $\mathrm{leak}_{\mathrm{EC}}$ is the amount of information leaked to the eavesdropper during IR. Since it is usually impossible to determine $\mathrm{leak}_{\mathrm{EC}}$ precisely, this term is often bounded as $\mathrm{leak}_{\mathrm{EC}} \leq \log|\mathcal{M}|$. In the following, we are thus interested in finding lower bounds on $\log|\mathcal{M}|$.

Let f_{XY} be a probability density function. We say that an IR protocol is *ε-correct* on f_{XY} if it satisfies $\Pr[X^n \neq \hat{X}^n] \leq \varepsilon$ when X^n and Y^n are distributed according to $(f_{XY})^{\times n}$. Any such protocol (under weak conditions on f_{XY} and for small ε) satisfies $\frac{1}{n}\log|\mathcal{M}| \geq H(X|Y)_f$ [40]. Moreover, equality can be achieved for $n \to \infty$ [37]. On first sight, it thus appears reasonable to compare the performance of a finite block length protocol by comparing $\log|\mathcal{M}|$ with its asymptotic limit. In fact, for the purpose of numerical simulations, the amount of one-way communication from Alice to Bob required to perform IR is usually approximated as $\mathrm{leak}_{\mathrm{EC}} \approx \xi \times nH(X|Y)_f$, where $\xi > 1$ is the reconciliation efficiency. The constant ξ is often chosen in the range

[2] Recent works analyzing the finite block length behavior using this approximation include [1,5,7,17,24,35,43].

$\xi = 1.05$ to $\xi = 1.2$. However, this choice is scarcely motivated and independent of the block length, the bit error rate and the required correctness considered.

Here, we argue that this approximation is unnecessarily rough in light of recent progress in non-asymptotic information theory. Strassen [38] already observed in the context of noisy channel coding that the asymptotic expansion of the fundamental limit for large n admits a Gaussian approximation. This approximation was recently refined by Polyanskiy et al. [32] (see also [16]). The problem of information reconciliation—also called source compression with side information—was investigated by Hayashi [15] and recently by Tan and Kosut [40]. Here we go slightly beyond this and provide bounds on the asymptotic expansion up to third order:

Theorem 1 *Let $0 < \varepsilon < 1$ and f_{XY} arbitrary. Then, for large n, any ε-correct IR protocol on f_{XY} satisfies*

$$\log |\mathcal{M}| \geq nH(X|Y) + \sqrt{nV(X|Y)}\, \Phi^{-1}(1-\varepsilon) - \frac{1}{2}\log n - O(1)\,.$$

Furthermore, there exists an ε-correct IR protocol with

$$\log |\mathcal{M}| \leq nH(X|Y) + \sqrt{nV(X|Y)}\, \Phi^{-1}(1-\varepsilon) + \frac{1}{2}\log n + O(1),$$

where Φ is the cumulative standard normal distribution,

$$H(X|Y) := \mathbb{E}\left[-\log \frac{f_{XY}}{f_Y}\right] \tag{2}$$

is the conditional entropy and

$$V(X|Y) := \mathrm{Var}\left[-\log \frac{f_{XY}}{f_Y}\right] \tag{3}$$

is the conditional entropy variance.

The proof uses standard techniques, namely Yassaee et al.'s achievability bounds [50] and an analogue of the meta-converse [32]. Note that the gap of $\log n$ between achievable and converse bounds for general distributions leaves room for improvements. In channel coding, the gap is at most $\frac{1}{2}\log n$, and constant for certain channels (see, e.g., [2,39,45] for recent work on this topic).

We are in particular interested in two situations that typically appear in QKD.

2.1 Binary variable QKD

We first look at binary variable protocols, such as BB84 [4] or the 6-state protocol [6], in the absence of an active eavesdropper. In this situation, the raw keys X and Y result from measurements on a channel with independent quantum bit error rate Q. The distribution $(P_{XY}^{Q})^n$, that we call the binary–binary distribution, describes a typical

manifestation of two random strings for which the expected bit error rate is Q. Here, we (at least) require ε-correctness for the distribution

$$P_{XY}^{Q}(0,0) = P_{XY}^{Q}(1,1) = \frac{1-Q}{2}, \qquad \text{and}$$
$$P_{XY}^{Q}(0,1) = P_{XY}^{Q}(1,0) = \frac{Q}{2}. \tag{4}$$

We show the following, specialized bounds:

Corollary 1 *Let* $0 < \varepsilon < 1$ *and let* $0 < Q < \frac{1}{2}$. *Then, for large n, any* ε*-correct IR protocol satisfies*

$$\log|\mathcal{M}| \geq \xi(n,\varepsilon;Q) \times nh(Q) - \frac{1}{2}\log n - O(1), \tag{5}$$

where

$$\xi(n,\varepsilon;Q) := 1 + \frac{1}{\sqrt{n}}\frac{\sqrt{v(Q)}}{h(Q)}\Phi^{-1}(1-\varepsilon).$$

Here, $h(x) = -x\log x - (1-x)\log(1-x)$ *and* $v(x) = x(1-x)\log^2\big(x/(1-x)\big)$. *Furthermore, there exists an* ε*-correct IR protocol with* $\log|\mathcal{M}| \leq \xi(n,\varepsilon;Q) \times nh(Q) + \frac{1}{2}\log n + O(1)$.

The proof of Eq. (5) follows by specializing Theorem 1 to the distribution P_{XY}^{Q}.

Moreover, numerical simulations reveal that the approximation in Corollary 1 is very accurate even for small values of n. More precisely, we find the following exact bound:

$$\log|\mathcal{M}| \geq nh(Q) + \left(n(1-Q) - F^{-1}\Big(\varepsilon\big(1+1/\sqrt{n}\big);n,1-Q\Big) - 1\right)\log\frac{1-Q}{Q} - \frac{1}{2}\log n - \log\frac{1}{\varepsilon}, \tag{6}$$

where $F^{-1}(\cdot\,;n,p)$ is the inverse of the cumulative distribution function of the binomial distribution. This bound can be evaluated numerically even for reasonably large n.

2.2 Continuous variable QKD

The second joint distribution of interest is the binary–Gaussian distribution:

$$f_{XY}(x,y) = \frac{1}{2\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(x-y)^2}{2\sigma^2}\right), \tag{7}$$

where $x \in \{-1,1\}$ and $y \in \mathbb{R}$.

In the absence of an active eavesdropper, this distribution arises in continuous variable QKD (CVQKD) with binary modulations [22,23] and can be induced in

the classical postprocessing of CVQKD with Gaussian modulation [19,21]. For this distribution, both the conditional entropy and the conditional entropy variance do not have known closed form formulas. Abusing notation we denote them again by $h(\sigma)$ and $v(\sigma)$, respectively. The conditional entropy is known to be [20]:

$$h(\sigma) = \int_{-\infty}^{\infty} \phi_\sigma(y) \log(\phi_\sigma(y)) \mathrm{d}y + \frac{1}{2} \log(8\pi e \sigma^2), \tag{8}$$

where

$$\phi_\sigma(y) = \frac{1}{\sqrt{8\pi\sigma^2}} \left(e^{-\frac{(y+1)^2}{2\sigma^2}} + e^{-\frac{(y-1)^2}{2\sigma^2}} \right).$$

The conditional entropy variance is easily found by applying Eq. (3)

$$v(\sigma) = e(\sigma) - h(\sigma)^2, \tag{9}$$

where

$$e(\sigma) = 2 \int_{-\infty}^{\infty} f_{XY}(1, y) \left(\log \left(\frac{f_{XY}(1, y)}{f_{XY}(1, y) + f_{XY}(-1, y)} \right) \right)^2.$$

These two integral forms can be solved numerically.

For this distribution, Theorem 1 yields the following bound:[3]

Corollary 2 *Let $0 < \varepsilon < 1$ and let $\sigma > 0$. Then, for large n, any ε-correct IR protocol satisfies*

$$\log |M| \geq \xi(n, \varepsilon; \sigma) \times n h(\sigma) - \frac{1}{2} \log n - O(1), \tag{10}$$

where

$$\xi(n, \varepsilon; \sigma) := 1 + \frac{1}{\sqrt{n}} \frac{\sqrt{v(\sigma)}}{h(\sigma)} \Phi^{-1}(1 - \varepsilon).$$

Furthermore, there exists an ε-correct IR protocol with $\log |\mathcal{M}| \leq \xi(n, \varepsilon; \sigma) \times n h(\sigma) + \frac{1}{2} \log n + O(1)$.

3 Notation and definitions

For a finite alphabet $\mathcal{X}$, we use $\mathcal{P}(\mathcal{X})$ to denote the set of probability distributions on $\mathcal{X}$. When $\mathcal{X}$ is the real line, $\mathcal{P}(\mathcal{X})$ denotes the set of distributions on the Borel sets of the reals. A channel is a probabilistic kernel $W : \mathcal{X} \to \mathcal{P}(\mathcal{Y})$, and we use $PW \in \mathcal{P}(\mathcal{Y})$ to denote the output distribution resulting from applying W to $P \in \mathcal{P}(\mathcal{X})$. We employ the ε-hypothesis testing divergence as defined in [9,45]. Let $\varepsilon \in (0, 1)$ and let $P, Q \in \mathcal{P}(\mathcal{Z})$. We consider binary (probabilistic) hypothesis tests $\xi : \mathcal{Z} \to [0, 1]$ and define the *ε-hypothesis testing divergence*

$$D_h^\varepsilon(P \| Q) := \sup \left\{ R \in \mathbb{R} \,\middle|\, \exists\, \xi :\ \mathbb{E}_Q\left[\xi(Z)\right] \leq (1 - \varepsilon) e^{-R} \ \wedge\ \mathbb{E}_P\left[\xi(Z)\right] \geq 1 - \varepsilon \right\}.$$

[3] We here apply Theorem 1 to distributions that are continuous in Y. Note that the proofs leading to Theorem 1 can easily be generalized to this setting.

Note that $D_h^\varepsilon(P\|Q) = -\log \frac{\beta_{1-\varepsilon}(P,Q)}{1-\varepsilon}$ where β_α is defined in Polyanskiy et al. [32]. It satisfies a data-processing inequality [49]

$$D_h^\varepsilon(P\|Q) \geq D_h^\varepsilon(PW\|QW)$$

for all channels W from $\mathcal{X}$ to $\mathcal{Y}$.

The following quantity, which characterizes the distribution of the log-likelihood ratio and is known as the *divergence spectrum* [13], is sometimes easier to manipulate and evaluate.

$$D_s^\varepsilon(P\|Q) := \sup\left\{R \in \mathbb{R} \;\middle|\; \Pr_P\left[\log\frac{P}{Q} \leq R\right] \leq \varepsilon\right\}.$$

It is intimately related to the ε-hypothesis testing divergence. For any $\delta \in (0, 1-\varepsilon)$, we have [41,45]

$$D_s^\varepsilon(P\|Q) - \log\frac{1}{1-\varepsilon} \leq D_h^\varepsilon(P\|Q) \leq D_s^{\varepsilon+\delta}(P\|Q) + \log\frac{1-\varepsilon}{\delta}. \tag{11}$$

For a joint probability distribution $P_{XY} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$, we define the Shannon conditional entropy

$$H(X|Y)_P := \mathbb{E}\left[-\log\frac{P_{XY}(X,Y)}{P_Y(Y)}\right] = \sum_{\substack{x\in\mathcal{X}\\ y\in\mathcal{Y}}} P_{XY}(x,y)\left(-\log\frac{P_{XY}(x,y)}{P_Y(y)}\right).$$

and its information variance

$$\begin{aligned} V(X|Y)_P &:= \mathrm{Var}\left[-\log\frac{P_{XY}(X,Y)}{P_Y(Y)}\right] \\ &= \sum_{\substack{x\in\mathcal{X}\\ y\in\mathcal{Y}}} P_{XY}(x,y)\left(-\log\frac{P_{XY}(x,y)}{P_Y(y)} - H(X|Y)_P\right)^2. \end{aligned}$$

We also employ the min-entropy, which is defined as

$$H_{\min}(X|Y)_P := -\log p_{\mathrm{guess}}(X|Y)_P,$$

where $p_{\mathrm{guess}}(X|Y)_P := \sum_{y\in\mathcal{Y}} \max_{x\in\mathcal{X}} P_{XY}(x,y)$.

4 Proofs

4.1 One-shot converse bound for general codes

A general (probabilistic) one-way IR code for a finite alphabet $\mathcal{X}$ is a tuple $\{\mathcal{M}, e, d\}$ consisting of a set of syndromes, $\mathcal{M}$, an encoding channel $e : \mathcal{X} \to \mathcal{P}(\mathcal{M})$, and a

decoding channel $d : \mathcal{Y} \times \mathcal{M} \to \mathcal{P}(\mathcal{X})$. We say that a code is ε-correct on a joint distribution $P_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ if

$$\Pr_{P_{XY}}\left[X = d(Y, e(X))\right] \geq 1 - \varepsilon.$$

The converse for probabilistic protocols clearly implies the converse for protocols where the encoder and decoder are deterministic as a special case.

We show the following one-shot lower bound on the size of the syndrome.

Proposition 1 *Any ε-correct one-way IR code for P_{XY} satisfies,*

$$\log|\mathcal{M}| \geq H_{\min}(X|Y)_Q - D_s^{\varepsilon+\delta}\left(P_{XY}\middle\|Q_{XY}\right) + \log\delta,$$

for any $\delta \in (0, 1-\varepsilon)$ and any $Q_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$.

Proof Let $P_{XYM\hat{X}}$ be the distribution induced by $P_{XY}, M \leftarrow e(X)$ and $\hat{X} \leftarrow d(Y, M)$. Analogously, $Q_{XYM\hat{X}}$ is induced by $Q_{XY} \in \mathcal{P}(\mathcal{X}\times\mathcal{Y})$, which we fix for the remainder. We then consider the hypothesis test $\xi(X, \hat{X}) = 1\{X = \hat{X}\}$ between $P_{X\hat{X}}$ and $Q_{X\hat{X}}$. We find

$$\mathbb{E}_P[\xi(X, \hat{X})] = \Pr_P[X = \hat{X}] \geq 1 - \varepsilon$$

and

$$\mathbb{E}_Q[\xi(X, \hat{X})] = \Pr_Q[X = \hat{X}] \leq |\mathcal{M}|\, p_{\text{guess}}(X|Y)_Q.$$

The first inequality holds by assumption that the code is ε-correct. The second inequality follows from the fact that $\Pr[X = \hat{X}] \leq p_{\text{guess}}(X|YM) \leq p_{\text{guess}}(X|Y)\,|\mathcal{M}|$.

By definition of the ε-divergence and the min-entropy, we thus have

$$D_h^{\varepsilon}(P_{X\hat{X}}\|Q_{X\hat{X}}) \geq H_{\min}(X|Y)_Q - \log|\mathcal{M}| + \log(1-\varepsilon). \tag{12}$$

Furthermore, Eq. (11) and the data-processing inequality with d and e yields

$$\begin{aligned} D_s^{\varepsilon+\delta}(P_{XY}\|Q_{XY}) + \log\frac{1-\varepsilon}{\delta} &\geq D_h^{\varepsilon}(P_{XY}\|Q_{XY}) \\ &\geq D_h^{\varepsilon}(P_{XYM}\|Q_{XYM}) \\ &\geq D_h^{\varepsilon}(P_{X\hat{X}}\|Q_{X\hat{X}}). \end{aligned}$$

Finally, the statement follows by substituting Eq. (12) and solving for $\log|\mathcal{M}|$. □

In the i.i.d. setting, it is sufficient to consider distributions of the form $Q_{XY} = U_X \times P_Y$, where U_X is the uniform distribution on $\mathcal{X}$. The bound in Proposition 1 then simplifies to

$$\log|\mathcal{M}| \geq \log|\mathcal{X}| - D_s^{\varepsilon+\delta}\left(P_{XY}\middle\|U_X \times P_Y\right) + \log\delta. \tag{13}$$

However, it is unclear whether choices of Q_{XY} that contain correlations between X and Y or are not uniform on X are useful to derive tight bounds in the finite block length regime.

4.2 Proof of Theorem 1

The problem of information reconciliation or source compression with side information has been studied by many authors in classical information theory. Recent work by Hayashi [15] as well as Tan and Kosut [40] considers the normal approximation of this problem. Here, in analogy with [45], we go one step further and also look at the logarithmic third-order term.

We consider the direct and converse parts of the theorem separately. Theorem 1 then follows as an immediate corollary. We prove slightly more precise converse and direct theorems by considering the special case where the information variance vanishes separately. Note that the bounds are tight in third order for this special case, whereas otherwise a gap of $\log n$ remains.

Theorem 2 (Converse for IR) *Let $0 < \varepsilon < 1$ and let P_{XY} be a probability distribution. Any ε-correct one-way IR protocol on P_{XY} satisfies the following bounds:*

- *If $V(X|Y)_P > 0$, we have*

$$\log|\mathcal{M}| \geq nH(X|Y)_P + \sqrt{nV(X|Y)_P}\,\Phi^{-1}(1-\varepsilon) - \frac{1}{2}\log n - O(1),$$

- *If $V(X|Y)_P = 0$, we have $\log|\mathcal{M}| \geq nH(X|Y)_P + \log(1-\varepsilon)$.*

Proof We consider an i.i.d. distribution $(P_{XY})^{\times n}$ and use Proposition 1, more precisely Eq. (13), to get

$$\begin{aligned}\log|\mathcal{M}| &\geq n\log|\mathcal{X}| - D_s^{\varepsilon+\delta}\left((P_{XY})^{\times n}\middle\|(U_X\times P_Y)^{\times n}\right) + \log\delta \\ &= -n\sup\left\{R\in\mathbb{R}\,\middle|\,\Pr\left[\frac{1}{n}\sum_{i=1}^{n}\log\frac{P_{XY}(X_i,Y_i)}{P_Y(Y_i)}\leq R\right]\leq\varepsilon+\delta\right\} + \log\delta\end{aligned} \tag{14}$$

for any $0 < \delta < 1-\varepsilon$. Note that we pulled $\log|\mathcal{X}|$ into the information spectrum to find (14). Next, observe that the random variables $Z_i = \log\frac{P_{XY}(X_i,Y_i)}{P_Y(Y_i)}$ follow an i.i.d. distribution, and satisfy $\mathbb{E}[Z_i] = -H(X|Y)_P$ and $\mathrm{Var}[Z_i] = V(X|Y)_P$. Let us first consider the special case where $V(X|Y)_P = 0$. This implies directly that $Z_i = -H(X|Y)_P$ with probability 1. Thus,

$$\Pr\left[\frac{1}{n}\sum_{i=1}^{n}Z_i\leq R\right] = \begin{cases}0 & \text{if } R < -H(X|Y)_P\\ 1 & \text{if } R\geq -H(X|Y)_P\end{cases}.$$

Hence, for any $\xi > 0$ and $\delta = 1-\varepsilon-\xi$, we find $\log|\mathcal{M}| \geq nH(X|Y)_P + \log(1-\varepsilon-\xi)$, proving the result in the limit $\xi\to 0$.

In the following, we may therefore assume that $V(X|Y)_P > 0$, which allows for a simple application of the Berry–Esseen theorem, which states that

$$\forall R \in \mathbb{R} : \left| \Pr\left[\frac{1}{n}\sum_{i=1}^{n} Z_i \leq R\right] - \Phi\left(\sqrt{n}\,\frac{R + H(X|Y)_P}{\sqrt{V(X|Y)_P}}\right)\right| \leq \frac{B}{\sqrt{n}}\,,$$

where

$$B := B_0 \frac{T(X|Y)_P}{\left(\sqrt{V(X|Y)_P}\right)^3}$$

and $B_0 \leq \frac{1}{2}$ is a the Berry–Esseen constant [46] and $T(X|Y)_P := \mathbb{E}\left[\left|\log \frac{P_Y}{P_{XY}} - H(X|Y)_P\right|^3\right] < \infty$ is the third moment of the information spectrum. Since $0 < B < \infty$ is finite, we find

$$\begin{aligned}
\log|\mathcal{M}| &\geq -n \sup\left\{R \in \mathbb{R} \,\middle|\, \Phi\left(\sqrt{n}\,\frac{R + H(X|Y)_P}{\sqrt{V(X|Y)_P}}\right) \leq \varepsilon + \frac{B+1}{\sqrt{n}}\right\} - \frac{1}{2}\log n \\
&= nH(X|Y)_P - \sqrt{nV(X|Y)_P} \times \sup\left\{r \in \mathbb{R} \,\middle|\, \Phi(r) \leq \varepsilon + \frac{B+1}{\sqrt{n}}\right\} - \frac{1}{2}\log n \\
&= nH(X|Y)_P - \sqrt{nV(X|Y)_P}\,\Phi^{-1}\left(\varepsilon + \frac{B+1}{\sqrt{n}}\right) - \frac{1}{2}\log n\,.
\end{aligned}$$

Here, we chose $\delta = 1/\sqrt{n}$, implicitly assuming that $n > (B+1)^2(1-\varepsilon)^{-2}$ is sufficiently large. Since Φ^{-1} is continuously differentiable except at the boundaries, there exists a constant γ such that

$$\Phi^{-1}\left(\varepsilon + \frac{B+1}{\sqrt{n}}\right) \leq \Phi^{-1}(\varepsilon) + \gamma\,\frac{B+1}{\sqrt{n}}.$$

Since $V(X|Y)_P < \infty$, this then leads to the desired bound

$$\begin{aligned}
\log|\mathcal{M}| \geq\; & nH(X|Y)_P - \sqrt{nV(X|Y)_P}\,\Phi^{-1}(\varepsilon) - \frac{1}{2}\log n \\
& -\gamma\left(B_0\frac{T(X|Y)_P}{V(X|Y)_P} + \sqrt{V(X|Y)_P}\right).
\end{aligned} \tag{15}$$

□

The constant term in (15) can be simplified when $\varepsilon < \frac{1}{2}$ and $n > (B+1)^2(\frac{1}{2}-\varepsilon)^{-2}$. We get

$$\begin{aligned}
\log|\mathcal{M}| \geq\; & nH(X|Y)_P - \sqrt{nV(X|Y)_P}\,\Phi^{-1}(\varepsilon) - \frac{1}{2}\log n \\
& -\frac{1}{\varphi(\Phi^{-1}(\varepsilon))} \times \frac{3T(X|Y)_P}{2V(X|Y)_P},
\end{aligned}$$

where we used that $B_0 \leq \frac{1}{2}$ and $\left(\sqrt{V(X|Y)_P}\right)^3 \leq T(X|Y)_P$. Moreover, we note that the choice $\gamma = \frac{\mathrm{d}\,\Phi^{-1}}{\mathrm{d}\,\varepsilon}\big|_\varepsilon = \frac{1}{\varphi(\Phi^{-1}(\varepsilon))}$ is sufficient (and also necessary for large n) due to concavity of Φ^{-1} on $(0, \frac{1}{2})$. Here, $\varphi(x) = \frac{\mathrm{d}\,\Phi}{\mathrm{d}\,x}\big|_x = \frac{1}{\sqrt{2\pi}} \exp\left(-x^2/2\right)$ denotes the probability density function of the standard normal distribution. The constant term behaves very badly for small ε, e.g., we find

$$\frac{1}{\varphi\left(\Phi^{-1}\left(10^{-4}\right)\right)} \approx 2.5 \times 10^3$$

for a typical value of ε. Nonetheless, the normal approximation in Theorem 2 is often very accurate.

Theorem 3 (Achievability for IR) *Let $0 < \varepsilon < 1$ and let P_{XY} be a probability distribution. There exists an ε-correct one-way IR protocol with the following property:*

- *If $V(X|Y)_P > 0$, we have*

$$\log|\mathcal{M}| \leq nH(X|Y)_P + \sqrt{nV(X|Y)_P}\,\Phi^{-1}(1-\varepsilon) + \frac{1}{2}\log n + O(1).$$

- *If $V(X|Y)_P = 0$, we have $\log|\mathcal{M}| \leq nH(X|Y)_P - \log\varepsilon$.*

Proof We employ a one-shot achievability bound due to [50] (we use the variant in [3, Corollary 12]), which, for every $0 < \delta < \varepsilon$, ensures the existence of an ε-correct protocol with

$$\log|\mathcal{M}| \leq n\log|\mathcal{X}| - D_s^{\varepsilon-\delta}\left((P_{XY})^{\times n} \,\middle\|\, (U_X \times P_Y)^{\times n}\right) - \log\delta + 1.$$

The remaining steps are exactly analogous to the steps taken in the proof of the converse asymptotic expansion, and we omit them here. □

4.3 Proof of Corollary 1

The corollary is a trivial specialization of Theorem 1, and it only remains to evaluate $H(X|Y)_P$ and $V(X|Y)_P$ for the distribution in Eq. (4). We find

$$\begin{aligned} H(X|Y)_P &= -\sum_{x,y} P_{XY}(x,y)\log\frac{P_{XY}(x,y)}{P_Y(y)} \\ &= -Q\log Q - (1-Q)\log(1-Q) =: h(Q), \end{aligned}$$

and

$$\begin{aligned} V(X|Y)_P &= \sum_{x,y} P_{XY}(x,y)\left(\log\frac{P_{XY}(x,y)}{P_Y(y)} + h(Q)\right)^2 \\ &= Q\left((1-Q)\log Q - (1-Q)\log(1-Q)\right)^2 \\ &\quad + (1-Q)\left(Q\log(1-Q) - Q\log Q\right)^2 \\ &= \left(Q(1-Q)^2 + (1-Q)Q^2\right)\left(\log Q - \log(1-Q)\right)^2 \\ &= Q(1-Q)\left(\log\frac{Q}{1-Q}\right)^2 =: v(Q). \end{aligned}$$

4.4 Exact converse bound for (ε, Q)-correct codes

Let us state a more precise lower bound on $\log|\mathcal{M}|$ that is valid for all n and can be evaluated numerically for large n. This bound has the advantage that it does not contain unspecified contributions of the form $O(1)$. In particular, it does not suffer from the problem of potentially large constant terms as discussed above.

Proposition 2 *Let $0 < \varepsilon < 1$ and let $0 < Q < \frac{1}{2}$. Then, any (ε, Q)-correct one-way error correction code on a block of length n satisfies*

$$\begin{aligned} \log|\mathcal{M}| \geq nh(Q) + \left(n(1-Q) - F^{-1}\left(\varepsilon\left(1+1/\sqrt{n}\right); n, 1-Q\right) - 1\right)\log\frac{1-Q}{Q} \\ - \frac{1}{2}\log n - \log\frac{1}{\varepsilon}, \end{aligned}$$

where $F^{-1}(\,\cdot\,; n, p)$ is the inverse of the cumulative distribution function of the binomial distribution, i.e., $F(k; n, p) := \sum_{\ell=0}^{k}\binom{n}{\ell}p^\ell(1-p)^{n-\ell}$ and $F^{-1}(\varepsilon; n, p) := \max\{k \in \mathbb{N} \mid F(k; n, p) \leq \varepsilon\}$.

Proof We repeat Eq. (14), where we found

$$\log|\mathcal{M}| \geq -\sup\left\{R \in \mathbb{R} \;\middle|\; \Pr\left[\sum_{i=1}^{n} \underbrace{\log\frac{P_{XX'}(X_i, X_i')}{U_{X'}(X_i')}}_{=:Z_i} \leq R\right] \leq \varepsilon + \delta\right\} + \log\delta\,.$$

for any $0 < \delta < 1 - \varepsilon$. Here, we further used that $P_{X'}$ is uniform so that the random variables Z_i are of the simple form

$$\Pr_P\left[Z_i = \log Q\right] = Q \quad \text{and} \quad \Pr_P\left[Z_i = \log(1-Q)\right] = 1 - Q\,.$$

When $Q \neq \frac{1}{2}$, we can rescale this into a Bernoulli trial:

$$B_i = \left(Z_i - \log Q\right)\left(\log \frac{1-Q}{Q}\right)^{-1}.$$

Thus, by an appropriate change of variable, we get

$$\begin{aligned}
\log|M| &\geq -\left(n \log Q + \log \frac{1-Q}{Q} \times \sup\left\{k \in \mathbb{N} \,\middle|\, \Pr\left[\sum_{i=1}^{n} B_i \leq k\right] \leq \varepsilon + \delta\right\}\right) + \log \delta \\
&= nh(Q) + \left(n(1-Q) - \max\left\{k \in \mathbb{N} \,\middle|\, F(k-1; n, 1-Q) \leq \varepsilon + \delta\right\}\right) \log \frac{1-Q}{Q} + \log \delta \\
&= nh(Q) + \left(\min\left\{k \in \mathbb{N} \,\middle|\, F(k; n, Q) \geq 1 - \varepsilon - \delta\right\} - nQ\right) \log \frac{1-Q}{Q} + \log \delta.
\end{aligned} \tag{16}$$

The remaining optimizations over k and δ can be done numerically. Alternatively, we are free to choose $\delta = \frac{\varepsilon}{\sqrt{n}}$ in Eq. (16) to conclude the proof. □

4.5 Proof of Corollary 2

In order to prove Corollary 2, we just need to evaluate the conditional entropy and entropy variances for the binary–Gaussian distribution Eq. (7). For the sake of completeness, we do the explicit calculations. For the conditional entropy, we obtain

$$\begin{aligned}
H(X|Y)_f &= -\int_{-\infty}^{\infty} \mathrm{d}y \sum_{x \in \{-1,1\}} f_{XY}(x, y) \left(\log \frac{f_{XY}(x, y)}{f_Y(y)}\right) \\
&= -\int_{-\infty}^{\infty} \mathrm{d}y \sum_{x \in \{-1,1\}} f_{XY}(x, y) \left(\log f_{XY}(x, y)\right) \\
&\quad + \int_{-\infty}^{\infty} \mathrm{d}y f_Y(y) \log\left(f_Y(y)\right).
\end{aligned} \tag{17}$$

Let us expand separately the first term in Eq. (17):

$$\begin{aligned}
&\int_{-\infty}^{\infty} \mathrm{d}y \sum_{x \in \{-1,1\}} f_{XY}(x, y) \left(\log f_{XY}(x, y)\right) \\
&= \int_{-\infty}^{\infty} \sum_{x \in \{-1,1\}} \mathrm{d}y \frac{1}{\sqrt{8\pi\sigma^2}} \exp\left(-\frac{(x-y)^2}{2\sigma^2}\right) \left(\log \frac{1}{\sqrt{8\pi\sigma^2}} \exp\left(-\frac{(x-y)^2}{2\sigma^2}\right)\right) \\
&= \int_{-\infty}^{\infty} \sum_{x \in \{-1,1\}} \mathrm{d}y \frac{1}{\sqrt{8\pi\sigma^2}} \exp\left(-\frac{(x-y)^2}{2\sigma^2}\right) \left(-\frac{1}{2} \log 8\pi\sigma^2 - \frac{(x-y)^2}{2\sigma^2} \log e\right)
\end{aligned}$$

$$
\begin{aligned}
&= -\frac{1}{2}\log 8\pi\sigma^2 - \frac{\log e}{2\sigma^2}\int_{-\infty}^{\infty}\sum_{x\in\{-1,1\}} \mathrm{d}y \frac{1}{\sqrt{8\pi\sigma^2}}\exp\left(-\frac{(x-y)^2}{2\sigma^2}\right)(x-y)^2 \\
&= -\frac{1}{2}\log 8\pi\sigma^2 - \frac{\log e}{2\sigma^2}\int_{-\infty}^{\infty} \mathrm{d}y \frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{y^2}{2\sigma^2}\right)y^2 \\
&= -\frac{1}{2}\log 8\pi\sigma^2 e. \qquad (18)
\end{aligned}
$$

The marginal on Y can be found to be:

$$
\begin{aligned}
f_Y(y) &= \sum_{x\in\{-1,1\}} f_{XY}(x,y) \\
&= \frac{1}{\sqrt{8\pi\sigma^2}}\left(\exp\left(-\frac{(y+1)^2}{2\sigma^2}\right)+\exp\left(-\frac{(y-1)^2}{2\sigma^2}\right)\right). \qquad (19)
\end{aligned}
$$

It follows that $H(X|Y)_f = h(\sigma)$ by plugging Eq. (18) and (19) back into Eq. (17). Now let us prove that the conditional entropy variance is given by Eq. (9).

$$
\begin{aligned}
V(X|Y)_f &:= \mathrm{Var}\left[-\log\frac{f_{XY}}{f_Y}\right] \\
&= \mathbb{E}\left[\left(-\log\frac{f_{XY}}{f_Y}\right)^2\right] - \left(\mathbb{E}\left[-\log\frac{f_{XY}}{f_Y}\right]\right)^2 \\
&= \mathbb{E}\left[\left(-\log\frac{f_{XY}}{f_Y}\right)^2\right] - (h(\sigma))^2. \qquad (20)
\end{aligned}
$$

We conclude by identifying the first term in the right hand side of Eq. (20) with $e(\sigma)$:

$$
\begin{aligned}
\mathbb{E}\left[\left(-\log\frac{f_{XY}}{f_Y}\right)^2\right] &= \int_{-\infty}^{\infty}\mathrm{d}y\sum_{x\in\{-1,1\}} f_{XY}(x,y)\left(-\log\frac{f_{XY}(x,y)}{f_Y(y)}\right)^2 \\
&= 2\int_{-\infty}^{\infty}\mathrm{d}y f_{XY}(1,y)\left(-\log\frac{f_{XY}(1,y)}{f_Y(y)}\right)^2,
\end{aligned}
$$

where the last equality follows because $f_{XY}(1,y) = f_{XY}(-1,-y)$.

5 Numerical results

As shown above, $\log|\mathcal{M}| \approx \xi(n,\varepsilon;\cdot)nh(\cdot)$ is theoretically achievable for both binary–binary and binary–Gaussian distributions, and optimal up to additive constants. However, this implies that, for instance in the binary–binary case, the approximation $\log|\mathcal{M}| \approx 1.1nh(Q)$ is provably too optimistic if $\xi(n,\varepsilon;Q) > 1.1$, e.g., for $n \leq 10^4$,

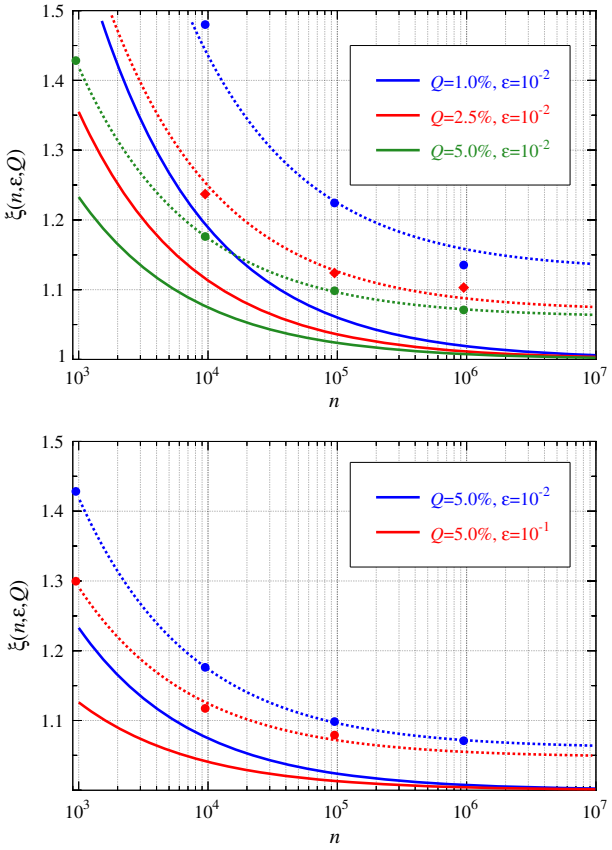

Fig. 1 Solid lines show the fundamental limit of the efficiency for the binary–binary distribution, $\xi(n, \varepsilon; Q)$, as a function of n for different values of Q and ε. The dotted lines show fits (see Table 1) to Eq. (21) for simulated LDPC codes (marked with symbols)

$Q \geq 2.5\%$, and $\varepsilon = 10^{-2}$. The function $\xi(\cdot, \varepsilon; Q)$ is plotted in Fig. 1 for different values of ε and Q.

Moreover, theoretical achievability only ensures the existence of an information reconciliation (error correcting) code without actually constructing it. In fact, it is not known if efficient codes used in practical implementations can achieve the above bound. Hence, the approximation given in Corollaries 1 and 2 is generally too optimistic and must be checked against what can be achieved using state-of-the-art codes.

We suggest that practical information reconciliation codes for finite block lengths should be benchmarked against the fundamental limit for that block length, and not against the asymptotic limit. Moreover, we conjecture that, for some constants $\xi_1, \xi_2 \geq 1$ depending only on the coding scheme used, the leaked information due to information reconciliation can be approximated well by

$$\text{leak}_{\text{EC}} \approx \xi_1 \times nh(Q) + \xi_2 \times \sqrt{nv(Q)}\, \Phi^{-1}(1-\varepsilon) \tag{21}$$

for a large range of n and Q (σ for binary–Gaussian distributions) as long as ε is small enough. Here, ξ_1 measures how well the code achieves the asymptotic limit (first order) whereas ξ_2 measures the second-order deficiency.

In the following, we test this conjecture against some state-of-the-art error correcting codes (designed for the binary symmetric and additive white Gaussian channels, BSC and AWGN, respectively). More precisely, we study several scenarios where we fix two of the parameters in (21)—the failure probability ε, the block length n, the leakage and the noise parameter—and explore the trade-off between the two free parameters. In each scenario, we construct codes that verify the two fixed parameters and fit ξ_1 and ξ_2 according to (21). For this numerical analysis, we have chosen low-density parity-check (LDPC) codes following several recent implementations [26,30,48].

We constructed two sets of LDPC codes with the progressive edge algorithm (PEG) [18]. We constructed the first set of codes using the following degree polynomials for the BSC:

$$\begin{aligned}\lambda_1(x) &= 0.1560x + 0.3482x^2 + 0.1594x^{13} + 0.3364x^{14}\\ \lambda_2(x) &= 0.1305x + 0.2892x^2 + 0.1196x^{10} + 0.1837x^{12} + 0.2770x^{14}\\ \lambda_3(x) &= 0.1209x + 0.2738x^2 + 0.1151x^5 + 0.2611x^{10} + 0.2291x^{14},\end{aligned}$$

where $\lambda_1(x)$, $\lambda_2(x)$ and $\lambda_3(x)$ were designed for coding rates 0.6, 0.7 and 0.8, respectively [8].

And we constructed the second set of codes using these polynomials for the AWGN channel:

$$\begin{aligned}\lambda_4(x) &= 0.16988x + 0.29342x^2 + 0.1633x^6 + 0.15835x^{11} + 0.21505x^{28}\\ \lambda_5(x) &= 0.13372x + 0.2689x^2 + 0.00358x^6 + 0.15093x^7 + 0.01572x^8\\ &\quad + 0.04647x^9 + 0.0001x^{10} + 0.00228x^{19} + 0.08615x^{24} + 0.02173x^{25}\\ &\quad + 0.27025x^{27} + 0.00017x^{29}\\ \lambda_6(x) &= 0.10462x + 0.31534x^2 + 0.26969x^8 + 0.00933x^{19} + 0.02778x^{21}\\ &\quad + 0.00803x^{24} + 0.23115x^{26} + 0.03406x^{29}\end{aligned}$$

with code rates 0.6, 0.7 and 0.8, for $\lambda_4(x)$, $\lambda_5(x)$ and $\lambda_6(x)$, respectively.

Figures 3 and 4 show the block error rate as a function of Q (the crossover probability in BSC) and SNR $= 1/\sigma^2$ (the signal-to-noise ratio in the AWGN) for codes with rates 0.6, 0.7, 0.8, and lengths 10^3, 10^4. The thick lines connect the simulated points, while the dotted lines represent a fit following Eq. (21). (The fit values are shown in Table 1.) The fit perfectly reproduces the so-called waterfall region of the codes. However, Eq. (21) drops sharply with Q for $Q \in [0, 0.1]$ and with σ for $\sigma \in [0, 4]$ while LDPC codes experience an error floor. In this second region, the fit cannot approximate the behavior of the codes.

In Fig. 1, we plot the function $\xi(n, \varepsilon; Q)$ and the efficiency results obtained with LDPC codes for reconciling strings following a binary–binary distribution. We chose as representative lengths 10^3, 10^4, 10^5, and 10^6. For every block length, we constructed

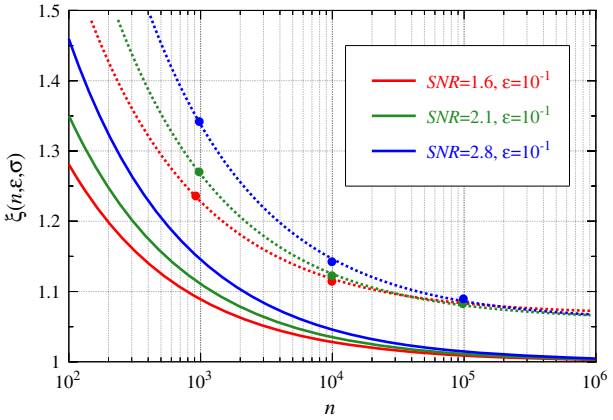

Fig. 2 As in Fig. 1 the solid lines show the fundamental limit of the efficiency but for the binary–Gaussian distribution, $\xi(n, \varepsilon; \sigma)$, as a function of n for different signal-to-noise ratios (SNR) and ε values

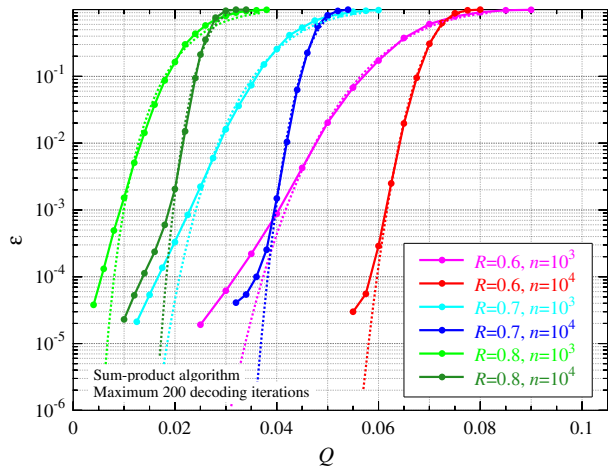

Fig. 3 Simulated block error rates ε of LDPC codes of length $n = 10^3$ and $n = 10^4$ and code rates $R = 0.6$, $R = 0.7$ and $R = 0.8$ as a function of quantum bit error rate Q

codes of rates 0.6, 0.7 and 0.8 following $\lambda_1(x)$, $\lambda_2(x)$, and $\lambda_3(x)$. The points in the figure were obtained by puncturing and shortening the original codes [11,12] until the desired block error rate was obtained. The results show an extra inefficiency due to the use of real codes. This inefficiency shares strong similarities with the converse bound, its separation from the asymptotic value is greater for lower values of Q, block error rates and lengths and fades as these parameters increase. For example, for $n = 10^4$, $Q = 1.0\%$ and $\varepsilon = 10^{-2}$ the extra inefficiency due to the use of real codes is over 1.2, while for $n = 10^6$, $Q = 5.0\%$ and $\varepsilon = 10^{-1}$ the extra inefficiency is close to 1.05.

Similarly, in Fig. 2 we plot $\xi(n, \varepsilon; \sigma)$ and the efficiency obtained with LDPC codes when reconciling strings following binary–Gaussian distributions. Representative lengths were also chosen 10^3, 10^4 and 10^5. Codes of rates 0.6, 0.7, and 0.8,

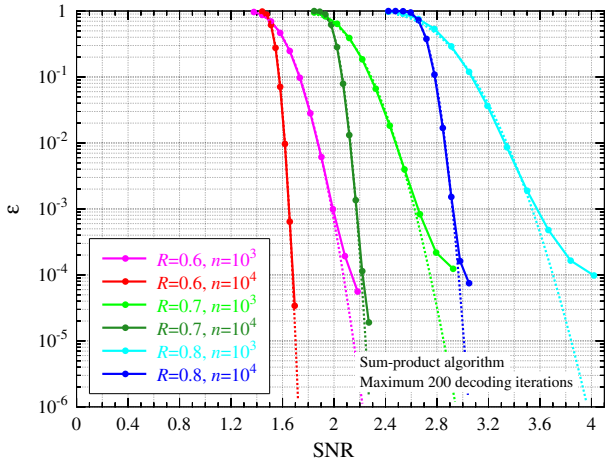

Fig. 4 Simulated block error rates ε of LDPC codes of length $n = 10^3$ and $n = 10^4$ and code rates $R = 0.6$, $R = 0.7$ and $R = 0.8$ as a function of SNR

Table 1 Values of ξ_1 and ξ_2 for the fitted curves in Figs. 1, 3 and 5

n	Q	ε	Leak	ξ_1	ξ_2
–	0.010	10^{-2}	–	1.13	3.82
–	0.025	10^{-2}	–	1.07	3.71
–	0.050	10^{-2}	–	1.06	3.54
–	0.050	10^{-1}	–	1.05	2.41
10^3	–	–	4×10^2	1.11	1.39
10^3	–	–	3×10^2	1.12	1.45
10^3	–	–	2×10^2	1.13	1.69
10^4	–	–	4×10^3	1.07	1.41
10^4	–	–	3×10^3	1.08	1.44
10^4	–	–	2×10^3	1.11	1.89
10^3	0.015	–	–	1.16	1.52
10^3	0.030	–	–	1.16	1.31
10^4	0.025	–	–	1.14	1.26
10^4	0.040	–	–	1.07	1.58

following $\lambda_5(x)$, $\lambda_6(x)$ and $\lambda_7(x)$, respectively, were punctured until the desired block error rate was obtained ($\varepsilon = 10^{-1}$). As in Fig. 1, the results show an additional inefficiency due to the use of real codes.

Finally, we address the design question posed above, that is, we study the efficiency variation as a function of the block error rate for fixed n and noise parameter. We have performed this study only for the binary–binary distribution for computational reasons, but we expect similar results to hold for the binary–Gaussian. In this setting, we need code constructions that allow to modulate the rate with fixed block length. The most

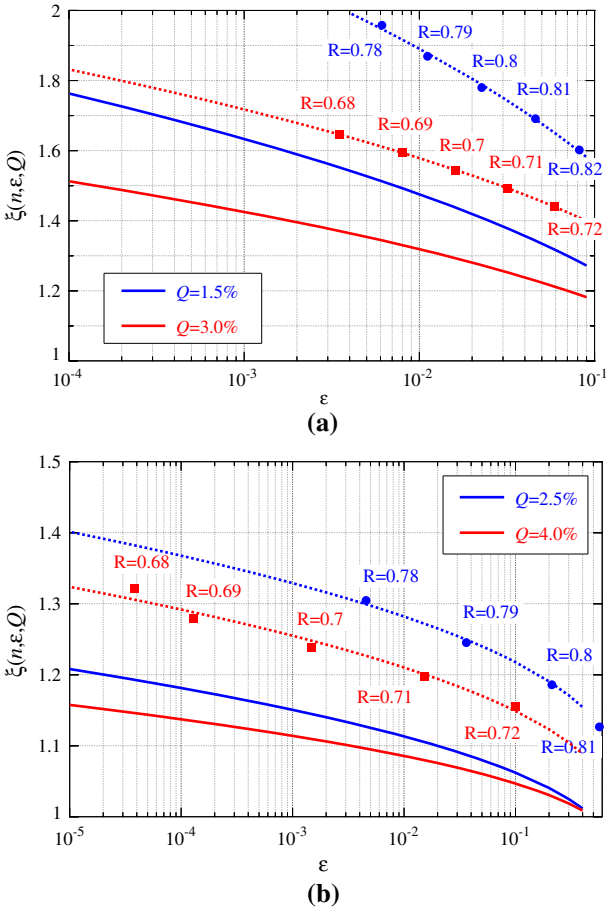

Fig. 5 Ratio between the leakage and the asymptotical optimum in several scenarios as a function of the block error rate ε. Subfigures **a** and **b** show results for block lengths 10^3 and 10^4, respectively. In each subfigure, the solid lines show the converse bound from Corollary 1, while the dotted lines show the values achieved with actual LDPC codes

natural modulating option would have been to construct codes for every n of interest and augment [28] the codes, that is, eliminate some of the restrictions that the code words verify. However, it is known that LDPC codes do not perform well under this rate adaptation technique [47]. In consequence, we constructed a different code with the PEG algorithm for every rate. In order to obtain a smooth efficiency curve, we used the degree polynomials $\lambda_1(x)$, $\lambda_2(x)$ and $\lambda_3(x)$ for constructing all codes even with coding rates different to the design rate.

Figure 5 shows the efficiency as a function of the block error rate. Each of the two subfigures (a) and (b) shows the simulation results for codes of length 10^3 and 10^4, respectively. Colors blue and red correspond to $Q = 1.5\%$ and 3.0% in subfigure (a) and to 2.5% and 4.0% in subfigure (b). The solid lines show the bound given by Corollary 1, similar to Fig. 1 we observe that, ceteris paribus, lower values of Q

Table 2 Values of ξ_1 and ξ_2 for the fitted curves in Fig. 2 and Fig. 4

n	SNR	ε	Leak	ξ_1	ξ_2
–	1.6	10^{-1}	–	1.07	2.58
–	2.1	10^{-1}	–	1.06	2.67
–	2.8	10^{-1}	–	1.06	2.74
10^3	–	–	4×10^2	1.11	1.23
10^3	–	–	3×10^2	1.12	1.34
10^3	–	–	2×10^2	1.13	1.40
10^4	–	–	4×10^3	1.08	1.27
10^4	–	–	3×10^3	1.07	1.42
10^4	–	–	2×10^3	1.08	1.33

imply higher values of ξ. The points show values achieved by LDPC codes: each point represents the block error rate of a different parity-check modulated code. Finally, the dotted lines show the best least squares fit to Eq. 21, the values of ξ_1 and ξ_2 are given in Table 1. From these curves, we can extract some useful design information, (1) if the target failure probability is very high [26], then the gain obtained by increasing the block length is modest; (2) if the target failure probability is low (below 10^{-4}), the leakage is over a fifty percent larger than the optimal one for moderate block lengths; and (3) for block length 10^5, the largest length for which we could compute simulations in the whole block error rate region, we were unable to consistently offer efficiency values below 1.1 and furthermore we report no point with f below 1.05.

Tables 1 and 2 show the values of ξ_1 and ξ_2 used in Figs. 1, 2, 3, 4 and 5 respectively, to fit the data points obtained from the simulations. In these curves, ξ_1 is—independently of ε, n, Q, σ—in the range [1.05, 1.16], while the second-order deficiency ξ_2 is more sensible to the parameter variations. In the first four rows of Table 1, that correspond to Fig. 1 with fixed Q and ε, ξ_2 is in the range [2.41, 3.82], for the middle six rows, that correspond to Fig. 3 with fixed n and leak, ξ_2 is in the range [1.49, 1.96], while for the last four rows, that correspond to Fig. 5 with fixed n and Q, ξ_2 is in the range [1.26, 1.58]. In the first three rows of Table 2, that correspond to Fig. 2 with fixed σ and ε, ξ_2 is in the range [2.58, 2.71], while in the last six rows, that correspond to Fig. 4 with fixed n and leak, ξ_2 is in the range [1.07, 1.42]. Note that for each scenario, the averages in these ranges could safely be used for system design purposes since necessarily codes with those ξ_1 and ξ_2 values or better exist.

6 Conclusion

In this paper, we studied the fundamental limits for one-way information reconciliation in the finite key regime. These limits imply that a commonly used approximation for the information leakage during information reconciliation is too optimistic for a range of error rates and block lengths. We proposed a two-parameter approximation that takes into account finite key effects.

We compared the finite length limits with LDPC codes and found a consistent range of achievable finite length efficiencies. These efficiencies should be of use to the quantum key distribution systems designer. One question that we leave open is the study of these values for different coding families.

Finally, it is clear that PE and PA also contribute to finite length losses in the QKD key rate. While it seems possible to investigate fundamental limits in PA based on the normal approximation of randomness extraction against quantum side information [41] as a separate problem, we would in fact need to investigate it jointly with IR since there is generally a trade-off between the two tasks that needs to be optimized over.

Acknowledgements MT thanks N. Beaudry, S. Bratzik, F. Furrer, M. Hayashi, C.C.W. Lim, and V.Y.F. Tan for helpful comments and pointers to related work. MT is supported by an Australian Research Council Discovery Early Career Researcher Award (DECRA) fellowship. JM has been funded by the Spanish Ministry of Economy and Competitiveness through project Continuous Variables for Quantum Communications (CVQuCo), TEC2015-70406-R. CP has been funded by the Vienna Science and Technology Fund (WWTF) through project ICT10-067 (HiPANQ). DE was supported via STW and the NWO Vidi grant "Large quantum networks from small quantum devices".

References

1. Abruzzo, S., Mertz, M., Kampermann, H., Bruss. D.: Finite-key analysis of the six-state protocol with photon number resolution detectors. In: Proceedings of SPIE, pp. 818917. Prague (2011)
2. Altug, Y., Wagner, A. B.: The third-order term in the normal approximation for singular channels. In: IEEE International Symposium on Information Theory (ISIT), 2014, pp. 1897–1901. IEEE, (2014)
3. Beigi, S., Gohari, A.: Quantum achievability proof via collision relative entropy. IEEE Trans. Inf. Theory **60**(12), 7980–7986 (2014)
4. Bennett, C. H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computer System Signal Processing, pp. 175–179, IEEE, Bangalore (1984)
5. Bratzik, S., Mertz, M., Kampermann, H., Bruß, D.: Min-entropy and quantum key distribution: nonzero key rates for small numbers of signals. Phys. Rev. A **83**(2), 022330 (2011)
6. Bruß, D.: Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett. **81**(14), 3018–3021 (1998)
7. Cai, R.Y.Q., Scarani, V.: Finite-key analysis for practical implementations of quantum key distribution. New J. Phys. **11**(4), 045024 (2009)
8. Chung, S.-Y., Forney, G.D., Richardson, T.J., Urbanke, R.: On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit. IEEE Commun. Lett. **5**(2), 58–60 (2001)
9. Dupuis, F., Kraemer, L., Faist, P., Renes, J. M., Renner, R.: Generalized entropies. In: Proceedings of XVIIth International Congress on Mathematical Physics, pp. 134–153, Aalborg, Denmark (2012)
10. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
11. Elkouss, D., Martinez-Mateo, J., Martin, V.: Information reconciliation for quantum key distribution. Quantum Inf. Comput. **11**(3), 226–238 (2011)
12. Elkouss, D., Martinez-Mateo, J., Martin, V.: Untainted puncturing for irregular low-density parity-check codes. IEEE Wirel. Commun. Lett. **1**(6), 585–588 (2012)
13. Han, T.S.: Information-Spectrum Methods in Information Theory. Springer, Berlin (2003)
14. Hayashi, M.: Practical evaluation of security for quantum key distribution. Phys. Rev. A **74**(2), 022307 (2006)
15. Hayashi, M.: Second-order asymptotics in fixed-length source coding and intrinsic randomness. IEEE Trans. Inf. Theory **54**(10), 4619–4637 (2008)
16. Hayashi, M.: Information spectrum approach to second-order coding rate in channel coding. IEEE Trans. Inf. Theory **55**(11), 4947–4966 (2009)
17. Hayashi, M., Tsurumaru, T.: Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths. New J. Phys. **14**(9), 093014 (2012)

18. Hu, X.-Y., Eleftheriou, E., Arnold, D.-M.: Regular and irregular progressive edge-growth tanner graphs. IEEE Trans. Inf. Theory **51**(1), 386–398 (2005)
19. Jouguet, P., Kunz-Jacques, S., Leverrier, A.: Long-distance continuous-variable quantum key distribution with a Gaussian modulation. Phys. Rev. A **84**(6), 062317 (2011)
20. Leverrier, A.: Theoretical study of continuous-variable quantum key distribution. Ph.D. thesis, Telecom ParisTech, Paris, France, (2009)
21. Leverrier, A., Alléaume, R., Boutros, J., Zémor, G., Grangier, P.: Multidimensional reconciliation for continuous-variable quantum key distribution. Phys. Rev. A **77**, 042325 (2008)
22. Leverrier, A., Grangier, P.: Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys. Rev. Lett. **102**(18), 180504 (2009)
23. Leverrier, A., Grangier, P.: Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. Phys. Rev. A **83**(4), 042312 (2011)
24. Lim, C.C.W., Portmann, C., Tomamichel, M., Renner, R., Gisin, N.: Device-independent quantum key distribution with local Bell test. Phys. Rev. X **3**(3), 031006 (2013)
25. Lo, H.-K., Chau, H., Ardehali, M.: Efficient quantum key distribution scheme and a proof of its unconditional security. J. Cryptol. **18**(2), 133–165 (2004)
26. Martinez-Mateo, J., Elkouss, D., Martin, V.: Key reconciliation for high performance quantum key distribution. Sci. Rep. **3**(1576), 1–6 (2013)
27. Mayers, D.: Unconditional security in quantum cryptography. J. ACM **48**(3), 351–406 (2001)
28. Morelos-Zaragoza, R.H.: The Art of Error Correcting Coding. Wiley, Hoboken (2006)
29. Moroder, T., Curty, M., Lütkenhaus, N.: One-way quantum key distribution: simple upper bound on the secret key rate. Phys. Rev. A **74**(5), 052301 (2006)
30. Pacher, C., Lechner, G., Portmann, C., Maurhart, O., Peev, M.: Efficient QKD Postprocessing Algorithms. In: QCrypt 2012, Singapore, (2012)
31. Pfister, C., Coles, P. J., Wehner, S., Lütkenhaus, N.: Sifting attacks in finite-size quantum key distribution. arXiv preprint arXiv:1506.07502 (2015)
32. Polyanskiy, Y., Poor, H.V., Verdú, S.: Channel coding rate in the finite blocklength regime. IEEE Trans. Inf. Theory **56**(5), 2307–2359 (2010)
33. Renner, R.: Security of Quantum Key Distribution. Ph.D. thesis, ETH Zurich, (2005)
34. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**(3), 1301–1350 (2009)
35. Scarani, V., Renner, R.: Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. Phys. Rev. Lett. **100**(20), 200501 (2008)
36. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
37. Slepian, D., Wolf, J.: Noiseless coding of correlated information sources. IEEE Trans. Inf. Theory **19**(4), 471–480 (1973)
38. Strassen, V.: Asymptotische Abschätzungen in Shannons Informationstheorie. In: Transactions of the Third Prague Conference on Information Theory, pp. 689–723. Prague (1962)
39. Tan, V., Tomamichel, M.: The third-order term in the normal approximation for the AWGN channel. IEEE Trans. Inf. Theory **61**(5), 2430–2438 (2015)
40. Tan, V.Y., Kosut, O.: On the dispersions of three network information theory problems. IEEE Trans. Inf. Theory **60**(2), 881–903 (2014)
41. Tomamichel, M., Hayashi, M.: A hierarchy of information quantities for finite block length analysis of quantum tasks. IEEE Trans. Inf. Theory **59**(11), 7693–7710 (2013)
42. Tomamichel, M., Leverrier, A.: A rigorous and complete proof of finite key security of quantum key distribution. arXiv preprint arXiv:1506.08458 (2015)
43. Tomamichel, M., Lim, C.C.W., Gisin, N., Renner, R.: Tight finite-key analysis for quantum cryptography. Nat. Commun. **3**, 634 (2012)
44. Tomamichel, M., Martinez-Mateo, J., Pacher, C., Elkouss, D.: Fundamental finite key limits for information reconciliation in quantum key distribution. In: IEEE International Symposium on Information Theory (ISIT), 2014, pp. 1469–1473. IEEE (2014)
45. Tomamichel, M., Tan, V.Y.F.: A tight upper bound for the third-order asymptotics for most discrete memoryless channels. IEEE Trans. Inf. Theory **59**(11), 7041–7051 (2013)
46. Tyurin, I.: A refinement of the remainder in the Lyapunov theorem. Theory Probab. Appl. **56**(4), 693–696 (2010)

47. Varodayan, D., Aaron, A., Girod, B.: Rate-adaptive codes for distributed source coding. Signal Process. **86**(11), 3123–3130 (2006)
48. Walenta, N., Burg, A., Caselunghe, D., Constantin, J., Gisin, N., Guinnard, O., Houlmann, R., Junod, P., Korzh, B., Kulesza, N., Legré, M., Lim, C.W., Lunghi, T., Monat, L., Portmann, C., Soucarros, M., Thew, R.T., Trinkler, P., Trolliet, G., Vannel, F., Zbinden, H.: A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. New J. Phys. **16**(1), 013047 (2014)
49. Wang, L., Colbeck, R., Renner, R.: Simple channel coding bounds. In: Proceedings of IEEE ISIT, pp.1804–1808. IEEE, (2009)
50. Yassaee, M.H., Aref, M.R., Gohari, A.: A technique for deriving one-shot achievability results in network information theory. In: Proceedings of IEEE ISIT, (2013)