IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 June 2024, accepted 10 July 2024, date of publication 15 July 2024, date of current version 29 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3428571

RESEARCH ARTICLE

Simultaneous Basis and Information Reconciliation in Quantum Key Distribution

JESUS MARTINEZ-MATEO[1] **AND DAVID ELKOUSS**[2], **(Member, IEEE)**

[1]Departamento de Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones, Universidad Politécnica de Madrid, 28040 Madrid, Spain
[2]Networked Quantum Devices Unit, Okinawa Institute of Science and Technology, Graduate University, Okinawa 904-0412, Japan

Corresponding author: Jesus Martinez-Mateo (jesus.martinez.mateo@upm.es)

This work was supported in part by the JST Moonshot Research and Development Program under Grant JPMJMS226C.

ABSTRACT We consider in this paper the practical implementation of a siftingless quantum key distribution protocol. The protocol is considered siftingless since it combines sifting and error correction in a single step for basis and information reconciliation, respectively. The protocol can be efficiently implemented even assuming the existence of errors in the communication. In this case, the correlations between the legitimate parties can be modeled by a binary symmetric channel with erasures. Specific codes for this channel are included and simulated for intermediate block lengths. Simulation results show that a key reconciliation step carrying simultaneously both basis and information reconciliation can be efficiently implemented.

INDEX TERMS Forward error correction, information reconciliation, quantum key distribution, siftingless.

I. INTRODUCTION

Quantum key distribution (QKD) is probably one of the most interesting applications of quantum information [1]. It allows the exchange of an information-theoretically secure key between two distant parties, traditionally named Alice and Bob. In the original QKD protocol proposed by Bennett and Brassard in 1984 (BB84) [2], Alice encodes a bit into a quantum state choosing randomly and uniformly from two mutually orthogonal bases and sends it to Bob through a quantum channel. Bob is able to recover the original bit with certainty —assuming no errors in the communication— only if he measures using the same basis. In the BB84 protocol, both parties agree on a common raw key discarding the states from those measurements that do not produce a conclusive result. This procedure, known as basis reconciliation or key *sifting*, takes place through a classical public, noiseless and authenticated channel that guarantees the legitimacy of the communication between Alice and Bob.

In a practical implementation there are errors in the raw key. That is, after the use of the quantum channel, Alice and Bob have two strings that are classically correlated but not identical. In addition, for the sake of security, these errors are paranoically attributed to the action of an eavesdropper—Eve's knowledge. Thus, a key distillation process has to be performed by both parties in order to convert the noisy raw key into a shared, error free, secret key. Again, a public and authenticated discussion is carried out by the legitimate parties to distill a secret key. This is usually implemented in two steps: information reconciliation (error correction) and privacy amplification [3], [4], [5]. The first one produces a common string and the second one outputs a shorter, but secret, key.

Several strategies have been proposed in the literature to improve the practical implementation of the sifting step in a QKD protocol. In [6] the authors demonstrate that the BB84 protocol continues being secure even when bases for the encoding are asymmetrically chosen, that is, with different probability. In the asymptotic regime, the efficiency of the sifting procedure can be therefore made as close to 1 as desired by biasing the basis choice without compromising the security. Asymmetric BB84 protocols have also been considered for practical implementations in the finite-key regime [7], [8]. In this case the bias of the encoding choice is

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

limited by the need to characterize the error rate in both bases; the key is obtained from the values encoded in one of the basis, while the values in the other basis are used to estimate the error rate in the quantum channel or quantum bit error rate. However, the choice of basis should not leak information of whether a quantum state will be used as key material or for error estimation, as this can compromise security [9], [10]. Another simple modification of the BB84 protocol is proposed in [11] and improved in [12] that leads to a method of key expansion in which no public discussion of bases is required, and in which a portion of the distributed key is left to be used as a basis sequence later. Obviously, further public discussion for error correction and privacy amplification are still required.

A different approach was adopted in [13], [14]. In these works, it is described a simplified version of the BB84 protocol where basis and information reconciliation (sifting and error correction, respectively) are combined in a single key reconciliation step. Therefore, instead of comparing the bases used by the parties in a key sifting (or basis reconciliation) step, the parties attempt to correct those errors caused by preparing and measuring quantum states using different bases, taking into account that in such a case the outcomes are completely unknown. In coding theory this inconclusive result is commonly referred to as an erasure, and it is well-known that asymptotically n additional bits are required to correct n erasures in a binary erasure channel (BEC) [15], thus sifting can be equivalently replaced[1] by an error correction procedure on the BEC. However, in practice we have errors caused by basis mismatch and errors in the communication that must be reconciled together in a single step. The protocol is considered *siftingless* since no symbols are sifted away after the use of the quantum channel. Although this approach remains largely unexplored, we show here that its postprocessing can be easily implemented with high efficiency for all relevant quantum bit error rate values. For this, we develop novel error correcting codes for the binary erasure symmetric channel which can be of independent interest.

In this work we combine two of the approaches described above: bases are asymmetrically chosen and bases reconciliation is combined with information reconciliation in a single reconciliation step. The protocol analyzed is, in essence, an asymmetric version of the four-state protocol from the family of siftingless protocols proposed by Grosshans in [13]. The aim of this work is to examine the classical postprocessing step of a siftingless protocol in a practical setting, with a numerical simulation of the key reconciliation efficiency using real postprocessing algorithms [16], [17], [18].

The paper is organized as follows. In Section II the protocol is described and information leakage in the simplified key reconciliation step analyzed. A family of codes and their performance is described in Section III. Finally, conclusions are presented in Section IV.

II. SIFTING-LESS QUANTUM KEY DISTRIBUTION

A. PROTOCOL

We consider here a siftingless version of BB84. This protocol is defined in the following steps.

Step 1. State Preparation. Alice chooses uniformly at random the string of bits $(x_i)_{i\in\mathbb{N}}$ and a second bit string $(a_i)_{i\in\mathbb{N}}$ following a Bernoulli process with probability $\Pr(a_i = 0) = p_x$. For each index in the string Alice prepares and sends the state $|x_i\rangle_{a_i}$ to Bob, where a_i selects the encoding basis, zero indicates the computational basis and one the Hadamard basis, and x_i encodes the logical bit to transmit into one of the eigenvectors of the chosen basis.

Step 2. Measurement. For simplicity, we assume that all the states reach Bob's measuring device. On the receiving side Bob chooses the binary string $(b_i)_{i\in\mathbb{N}}$ following a Bernoulli process with the same probability $\Pr(b_i = 0) = p_x$. The measurement basis for the incoming states are selected between the computation and Hadamard basis following b_i. The outcomes of the measurements are stored in the binary string $(y_i)_{i\in\mathbb{N}}$.

Step 3. Parameter Estimation. Alice and Bob choose a random subset of size t of their strings, for encoding and measurement bases, and exchange their values on the public channel. Let $(n_1, \ldots, n_t)$ be the indexes associated with the published values and $M = \{j : a_{n_j} = b_{n_j}\}$, that is, the positions where the encoding and measurement basis coincide. Then, they can compute the quantum bit error rate (QBER) as follows:

$$Q = \frac{1}{|M|}\sum_{i\in M} x_i \oplus y_i \tag{1}$$

We denote by X, A and Y, B the strings of bit and basis values available to respectively Alice and Bob after shrinking the original ones to eliminate the published positions.

Step 4. Partial Basis Reconciliation. Alice sends A to Bob, that is, she informs Bob of the basis choice for every state prepared and sent in Step 1. After this message the correlations between Alice and Bob are as follows: for every position i such that $A_i = B_i$ Bob knows that his bit value should coincide with Alice's except with probability Q, and for every i such that $A_i \neq B_i$ Bob knows that his bit and Alice's are completely independent, that is, this corresponds to an erasure which we denote by e.

This description effectively allows to consider the bit strings of Alice and Bob as the input and output, respectively, of a binary erasure symmetric channel (BESC) as shown in Fig. 1. Note that, when there are no erasures in the considered channel (since a full basis reconciliation, or sifting, was

[1] Note that, assuming perfect error correction in the reconciliation of bases and there are no other errors, the amount of information required to reconcile those inconclusive results caused by a basis mismatch is equal to the number of basis mismatches. Since the information disclosed during this procedure is later discarded in the privacy amplification, then the raw key length remains the same after a key sifting procedure or the proposed error correction on the BEC.

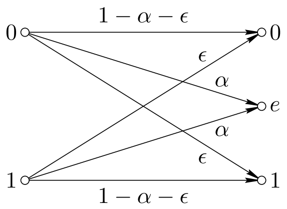


FIGURE 1. Channel model for the BESC with erasure probability α and crossover probability ϵ. In the analyzed siftingless protocol α is the probability that there is a basis mismatch. The quantum bit error rate Q is determined from the crossover probability $\epsilon = Q(1-\alpha)$.

carried out), it reduces to the binary symmetric channel (BSC), that is, the channel used to model the correlations between the bit strings of the legitimate parties in BB84 [16].

Step 5. Information Reconciliation. Alice sends to Bob an encoding of her bit string X that allows Bob to correct the discrepancies between X and Bob's Y. This encoding should be as short as possible in order to disclose the minimum amount of information.

Step 6. Privacy Amplification. Alice selects randomly a function f_H from a family of universal hash functions. She sends the selected function to Bob and they extract a secret key K of length l by applying f_H to the reconciled key.

The classical postprocessing or key distillation process in the BB84 protocol corresponds to steps 5 and 6 (after a full basis reconciliation step), and errors in the communication are modeled by a BSC with crossover probability Q (QBER). On the other hand, in the siftingless version the key distillation includes steps 4, 5 and 6, and errors are modeled by a BESC (as depicted in Fig. 1) with erasure probability α and crossover probability ϵ.

The novelty of this siftingless protocol with respect to BB84 is that both reconciliation steps, bases and information reconciliation, are joined logically into a single one. Alice sends her string of basis and the information reconciliation messages together since no feedback is expected from Bob. This differs from the one in [13] in the reconciliation step since for simplicity we consider forward error correction instead of reverse reconciliation. On the other hand, schemes for privacy amplification can be used without modification by plugging in the appropriate parameters.

B. RECONCILIATION EFFICIENCY

As a result of the given QKD siftingless protocol, the bit strings or keys belonging to Alice and Bob can be considered as the output of two correlated sources. Let X and Y be two correlated discrete random variables taking values in the binary alphabets $\mathcal{X} = \{0, 1\}$ and $\mathcal{Y} = \{0, 1, e\}$, respectively. Both variables can be regarded as the input and output of a BESC with input distribution $\Pr(X = 0) = \Pr(X = 1) = 1/2$. The channel parameters are: α the symmetric probability of a transition to the erasure symbol, and ϵ the probability also symmetric of bit flipping. For the former, the transition to the erasure symbol corresponds to the event $A_i \neq B_i$ (basis mismatch) with probability $\alpha = 1 - p_x^2 - (1-p_x)^2$. For the latter, the protocol allows to compute the QBER using Eq. (1), then simply $\epsilon = Q(1-\alpha)$.

The problem of reconciling discrepancies (errors) between two correlated sources is equivalent to a particular case of source coding with side information, also known as Slepian-Wolf coding [19], where X is the source and Y the side information. Accordingly, given the source X and a decoder with access to side information Y, no encoding of X shorter than $H(X|Y)$ allows for a reliable decoding. This is the minimum information that should be given to Bob that holds the side information Y in order to allow him to recover X. Then, the efficiency of an information reconciliation procedure can be defined as:

$$f_{\mathrm{IR}} = \frac{m}{nH(X|Y)} \tag{2}$$

where m is the length of the bit string message exchanged for reconciling the errors in a key of length n. Note that, it holds that $f_{\mathrm{IR}} \geq 1$, and $f_{\mathrm{IR}} = 1$ stands for perfect reconciliation.

We can calculate the conditional entropy $H(X|Y)$ for the given BESC as:

$$\begin{aligned} H(X|Y) &= \sum_{y \in Y} p(y) H(X|Y=y) \\ &= \frac{1-\alpha}{2} H(X|Y=0) \\ &\quad + \frac{1-\alpha}{2} H(X|Y=1) + \alpha H(X|Y=e) \\ &= (1-\alpha) h(\frac{\epsilon}{1-\alpha}) + \alpha \\ &= \alpha + (1-\alpha) h(Q) \end{aligned} \tag{3}$$

where $h(p)$ is the binary Shannon entropy function given by $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$.

Note that, the BESC capacity is then given by $C = 1 - \alpha - (1-\alpha)h(Q)$. Therefore, when $\alpha = 0$ it holds $C = 1 - h(Q)$, and when $\epsilon = 0$ it holds $C = 1 - \alpha$, that is, the capacities of binary symmetric and binary erasure channels, respectively.

Finally, in the case of a BESC the reconciliation efficiency is given by:

$$f_{\mathrm{BESC}} = \frac{1-R}{\alpha + (1-\alpha)h(Q)} \tag{4}$$

III. RESULTS

In this section we study the key reconciliation efficiency of the siftingless QKD protocol, and compare it with the efficiency of the common BB84 protocol with sifting, that is, where bases are reconciled separately. As representative situations, we consider symmetric and asymmetric versions of a siftingless protocol with the computational basis chosen with probability $p_x = 0.5$ and $p_x = 0.9$, respectively. The strings that Alice and Bob hold after the fourth step can be regarded as the input and output of a BESC, respectively. Therefore, the symmetric and asymmetric version of the siftingless correspond to a BESC with different erasure parameter: $\alpha = 0.5$ and $\alpha = 0.18$, respectively.

TABLE 1. Ensembles of LDPC codes for reconciling errors in the BSC and BESC.

R	α	ϵ_{th}	Generating polynomials
0.4	0	0.12905	$\lambda(x) = 0.27607x + 0.284x^2 + 0.12098x^4 + 0.17623x^9 + 0.14272x^{14}$
0.5	0	0.09994	$\lambda(x) = 0.23802x + 0.20997x^2 + 0.03492x^3 + 0.12015x^4 + 0.01587x^6 + 0.00480x^{13} + 0.37627x^{14}$
0.6	0	0.0707	$\lambda(x) = 0.15596x + 0.3482x^2 + 0.15943x^{13} + 0.33641x^{14}$
0.7	0	0.04705	$\lambda(x) = 0.13046x + 0.28919x^2 + 0.11962x^{10} + 0.18365x^{12} + 0.27708x^{14}$
0.8	0	0.02711	$\lambda(x) = 0.1209x + 0.27376x^2 + 0.11513x^5 + 0.26113x^{10} + 0.22908x^{14}$
0.2	0.5	0.06649	$\lambda(x) = 0.34535x + 0.30047x^2 + 0.00153x^3 + 0.03001x^4 + 0.05209x^6 + 0.0622x^8 + 0.15314x^{13}$ $+0.05521x^{14}$
0.25	0.5	0.04911	$\lambda(x) = 0.29461x + 0.31147x^2 + 0.02619x^6 + 0.09763x^8 + 0.00039x^{12} + 0.26971x^{13}$
0.3	0.5	0.03493	$\lambda(x) = 0.28648x + 0.29861x^2 + 0.01865x^4 + 0.03605x^5 + 0.08488x^9 + 0.19943x^{13} + 0.0759x^{14}$
0.35	0.5	0.02266	$\lambda(x) = 0.26827x + 0.27609x^2 + 0.07527x^4 + 0.03865x^8 + 0.00612x^{11} + 0.11442x^{12} + 0.22118x^{14}$
0.3	0.18	0.12295	$\lambda(x) = 0.29916x + 0.29341x^2 + 0.02963x^3 + 0.04413x^7 + 0.11139x^9 + 0.11326x^{10} + 0.10902x^{12}$
0.4	0.18	0.08724	$\lambda(x) = 0.23264x + 0.27205x^2 + 0.04311x^3 + 0.01965x^4 + 0.00563x^6 + 0.0111x^8 + 0.1277x^9$ $+0.01882x^{11} + 0.19036x^{13} + 0.07894x^{14}$
0.5	0.18	0.05797	$\lambda(x) = 0.22101x + 0.23206x^2 + 0.14413x^4 + 0.02782x^5 + 0.05917x^{12} + 0.12996x^{13} + 0.18585x^{14}$
0.6	0.18	0.03405	$\lambda(x) = 0.18632x + 0.25482x^2 + 0.0401x^3 + 0.09578x^5 + 0.14295x^9 + 0.02251x^{13} + 0.25752x^{14}$
0.7	0.18	0.01482	$\lambda(x) = 0.15322x + 0.32204x^2 + 0.0422x^5 + 0.00627x^7 + 0.04001x^8 + 0.23397x^{11} + 0.20229x^{13}$

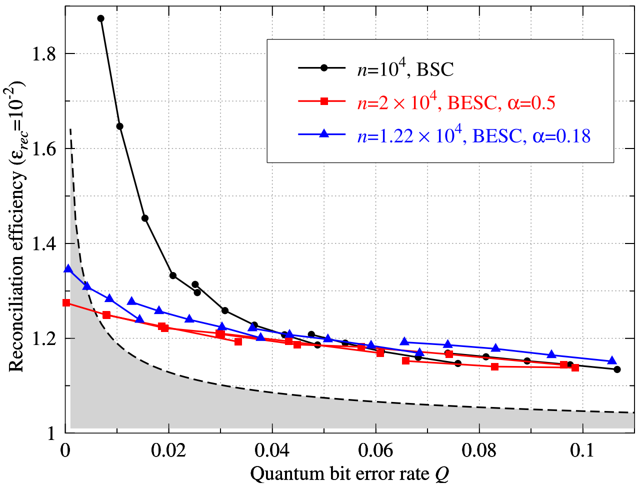


FIGURE 2. (Color online) Reconciliation efficiency using the rate-adaptive method described in [16]. The reconciliation method is also suited for the BESC channel (siftingless reconciliation). LDPC codes of 10^4, 2×10^4 and 1.22×10^4 bits length are compared, for BB84 (black dots), symmetric siftingless (red boxes) and asymmetric siftingless reconciliation (blue triangles), respectively. The fundamental limit [20] for the efficiency of one-way information reconciliation with a finite block length code of 10^4 bits is also depicted (black dashed line). The efficiencies correspond to a frame error rate of $\varepsilon_{\text{rec}} = 10^{-2}$.

We implemented the rate-adaptive reconciliation method based on low-density parity-check (LDPC) codes described in [16]. These error correcting codes are extremely efficient only for a specific type of noise [21]. In order to assess the achievable key rate with real postprocessing, we design and construct codes adapted to the correlations produced by the BB84 and siftingless protocols. First, we designed families of irregular LDPC codes using a differential evolution algorithm as in [22]. The codes designed (see Table 1) have thresholds (ϵ_{th}) —which were computed using the discretized density evolution algorithm described in [23]— close to the capacity of the BESC. Next, we constructed instances of the code ensembles described in Table 1 using the progressive edge-growth algorithm [24]. The length of the codes was chosen so that it allows to directly compare BB84 with the siftingless protocol. In consequence, we chose codes of 10^4, 2×10^4 and 1.22×10^4 bits length for BB84, symmetric siftingless and asymmetric siftingless, respectively. Note that, in all three cases, the key string to reconcile without erasures is close to 10^4 bits length. Indeed, in the symmetric siftingless version (with $\alpha = 0.5$) there are approximately 10^4 erasures, while in the asymmetric siftingless ($\alpha = 0.18$) it is near 2200.

As suggested in [16], 10% of the code symbols were used for code rate modulation, using intentional puncturing [17] and shortening techniques. For each mother code, and different proportions of punctured and shortened symbols, we computed the maximum crossover probability ϵ that can be corrected assuming a frame error rate of $\varepsilon_{\text{rec}} = 10^{-2}$. This frame error rate value was used since it provides a better compromise between reconciliation efficiency and secret key rate for intermediate block length codes as argued in [18]. The numerical results[2] shown in Fig. 2 report the reconciliation efficiency of these codes in the QBER range $Q \in [0.01, 0.1]$, where a secret key could be distilled. The efficiency for the BB84 (BSC channel for reconciliation), symmetric siftingless (BESC channel with $\alpha = 0.5$) and asymmetric siftingless (BESC with $\alpha = 0.18$) overlap in the range from 4%, whereas in the low QBER region the efficiency of a siftingless reconciliation is better. Fig. 2 also shows the fundamental limit for one-way information reconciliation over the BSC with finite resources [20], that is, the optimal efficiency when reconciling errors in BB84 with a linear code of finite block length (10^4 bits)

IV. CONCLUSION

In this paper we have studied a siftingless QKD protocol. That is, a protocol in which there are no symbols discarded after the use of the quantum channel. The advantage of such a protocol is that both reconciliation steps, bases and

[2] Numerical results were computed using iterative LDPC decoding. For decoding we used a sum-product algorithm with serial schedule and a maximum of 200 decoding iterations.

information reconciliation, can be joined into a single one. We have computed the impact of a realistic postprocessing scenario with a rate-adaptive reconciliation procedure based on LDPC codes. For the implementation of the reconciliation protocol we have designed and constructed families of LDPC codes for the BESC with thresholds close to the optimal value. Simulated results show a good average efficiency even in the low error rate region.

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014.

[3] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, no. 2, pp. 210–229, Apr. 1988.

[4] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. Eurocrypt'93, Workshop Theory Appl. Cryptograph. Techn. Adv. Cryptol.*, in Lecture Notes in Computer Science, vol. 765. New York, NY, USA: Springer, 1994, pp. 410–423.

[5] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Sep. 1995.

[6] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *J. Cryptol.*, vol. 18, no. 2, pp. 133–165, Apr. 2005.

[7] R. Y. Q. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045024.

[8] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Commun.*, vol. 3, no. 1, pp. 1–6, Jan. 2012.

[9] C. Pfister, N. Lütkenhaus, S. Wehner, and P. J. Coles, "Sifting attacks in finite-size quantum key distribution," *New J. Phys.*, vol. 18, no. 5, Apr. 2016, Art. no. 053001.

[10] K. Tamaki, H.-K. Lo, A. Mizutani, G. Kato, C. C. W. Lim, K. Azuma, and M. Curty, "Security of quantum key distribution with iterative sifting," *Quantum Sci. Technol.*, vol. 3, no. 1, Jan. 2018, Art. no. 014002.

[11] W. Y. Hwang, I. G. Koh, and Y. D. Han, "Quantum cryptography without public announcement of bases," *Phys. Lett. A*, vol. 244, no. 6, pp. 489–494, Aug. 1998.

[12] Q. Jia, K. Xue, Z. Li, M. Zheng, D. S. L. Wei, and N. Yu, "An improved QKD protocol without public announcement basis using periodically derived basis," *Quantum Inf. Process.*, vol. 20, no. 2, p. 69, Feb. 2021.

[13] F. Grosshans, "Robust and efficient sifting-less quantum key distribution protocols," 2009, *arXiv:0907.2897*.

[14] F. Grazioso and F. Grosshans, "Quantum-key-distribution protocols without sifting that are resistant to photon-number-splitting attacks," *Phys. Rev. A, Gen. Phys.*, vol. 88, no. 5, Nov. 2013, Art. no. 052302.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley-Interscience, 1991.

[16] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Information reconciliation for quantum key distribution," *Quantum Inf. Comput.*, vol. 11, no. 3, pp. 226–238, Mar. 2011.

[17] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Untainted puncturing for irregular low-density parity-check codes," *IEEE Wireless Commun. Lett.*, vol. 1, no. 6, pp. 585–588, Dec. 2012.

[18] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Key reconciliation for high performance quantum key distribution," *Sci. Rep.*, vol. 3, no. 1, pp. 1–6, Apr. 2013.

[19] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 4, pp. 471–480, Jul. 1973.

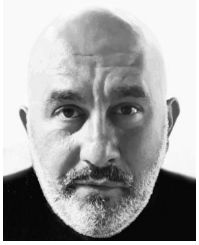
[20] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, "Fundamental finite key limits for one-way information reconciliation in quantum key distribution," *Quantum Inf. Process.*, vol. 16, no. 11, p. 280, Nov. 2017.

[21] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Nov. 2001.

[22] A. Shokrollahi and R. Storn, "Design of efficient erasure codes with differential evolution," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 2000, pp. 1–5.

[23] S.-Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Commun. Lett.*, vol. 5, no. 2, pp. 58–60, Feb. 2001.

[24] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.



JESUS MARTINEZ-MATEO received the B.S. degree in computer science, the M.S. degree in computational mathematics, and the Ph.D. degree in computer science from Universidad Politécnica de Madrid, Spain, in 2008, 2009, and 2011, respectively. He was a member with the Research Group on Quantum Information and Computation, from 2009 to 2018, and an Academic Secretary with the Research Center for Computational Simulation, from 2016 to 2018. He is currently an Associate Professor with Departamento de Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones, Universidad Politécnica de Madrid. He is involved with post-processing in quantum key distribution, and holds four patents and one software registration. His research interests include information and communication theory, fuzzy set theory, and scientific computing.

DAVID ELKOUSS (Member, IEEE) received the Ph.D. degree from Universidad Politécnica de Madrid (UPM) and the master's degree in electrical engineering from Telecom Paris, UPM. He is currently an Associate Professor with Okinawa Institute of Science and Technology, where he leads the Networked Quantum Devices Unit. Before, he was an Assistant Professor with TU Delft and held a postdoctoral position with Universidad Complutense de Madrid and TU Delft. He is interested in developing theoretical tools for enabling near-term quantum devices to perform communications, computational, and cryptographic tasks. He has served in several conferences, including cochairing technical program tracks (IEEE QCE, IEEE QCNC) and chairing the organizing committee of TQC. He serves as an Associate Editor for IEEE/ACM Transactions on Networking and *ACM Transactions on Quantum Computing*. He has been the Guest Editor for IEEE Wireless Communications and IEEE Journal on Selected Areas in Communications.