Novel Techniques for Information Reconciliation, Quantum Channel Probing and Link Design for Quantum Key Distribution

Marina Mondin[1], Fred Daneshgaran[2], Maria Delgado[1], and Fabio Mesiti[1]

[1] Politecnico di Torino, Dip. Di Elettronica, C.so duca degli Abruzzi 24, 10129, Torino, Italy
{marina.mondin,maria.delgadoalizo,fabio.mesiti}@polito.it
[2] California State Univ., ECE Dept., 5151 State Univ. Cr., Los Angeles, CA, 90032, USA
fdanesh@calstatela.edu

Abstract. In this manuscript, a novel technique for forward error correction based information reconciliation is proposed, exploiting capacity achieving soft-metric based iteratively decoded block codes. The availability of soft metric and information bits reliability is also employed to efficiently perform channel probing and privacy amplification.

Keywords: Information reconciliation, Low Density Parity Check codes, LDPC, soft metric, log likelihood ratios, QKD, Quantum Key Distribution.

1 Overview

Quantum computing and information processing is at the forefront of research and development and a multitude of organizations and research centers have been pursuing this area feverishly. In this field, quantum cryptography has emerged as one of the most important practical applications of non-classical or quantum theory. One-time pad (or Vernam cipher) requires that the key used to encode the message and hence render it illegible to unintended receiver, be as long as the message itself and this is often impractical and shorter keys are often used. While the security of the traditional cryptographic techniques is based on algorithmic complexity of solving certain mathematical problems (e.g., trap door one-way functions), the security of Quantum Cryptography (QC) is founded on basic physical principles. The best known example of traditional algorithmic method is multiplication of large numbers. In fact, the difficulty of prime factorization is at the basis of the most common public key cryptosystems. The problem from a cryptographic point of view is that the existence of a fast algorithm for factorization has not been ruled out; a sudden mathematical breakthrough would make many internet communications completely insecure. Even worse, it has been proven that the possible realization of a quantum computer would allow a fast algorithm for factorization. A secure cryptosystem can be achieved if one encodes information in a quantum system. To be more precise, quantum mechanics is able to generate perfectly secure, random keys which can then be used in standard secret-key protocols.

K. Sithamparanathan et al. (Eds.): PSATS 2010, LNICST 43, pp. 305–316, 2010.

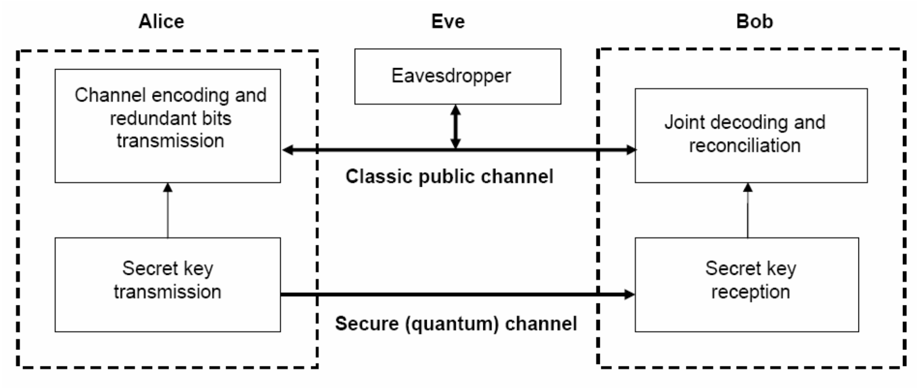

Fig. 1. Model of the secure and public channels involved in QKD communication

In the generic model of a secret-key cryptosystem shown in Figure 1, the sender Alice wants to transmit a plaintext message secretly to the receiver Bob. The secret key is transmitted on a secure (quantum) channel, which has typically high bit error rate (denoted QBER), so that a subsequent information reconciliation and privacy amplification operations need to be performed on a public channel. Once the secret key is known to Alice and to Bob (and only to them), Alice will encrypt the plaintext using the secret key according to the encryption rule of the system, and send the cryptogram to Bob, while Eve will not be able to recover the transmitted message. A multitude of attack strategies that could hypothetically be used by Eve have been identified and well documented in the literature. Note that the transmission rate on the QKD secret channel is generally very low (since the technology is very complex), while the actual data rate on the public channel can be very high. It is therefore important to analyze the achievable QKD rates. Furthermore, the bit error rate (BER) on the public channel is low, while the BER on the secret channel is high, and channel coding may be required to make the secret channel more reliable.

Up to now, the most famous protocol suggested for QKD is the BB84 protocol. The BB84 protocol, using the *cascade reconciliation protocol*, performs error-correction by sending very little information over the public channel and was proposed by Gilles Brassard and Louis Salvail. The cascade protocol operates in a number of rounds, and requires interaction between transmitter and receiver (Alice and Bob).

From a practical point of view, most recent attempts at long distance free space QKD have focused on using Weak laser Pulses (WLP) as opposed to true single photon sources which are still in experimental development stages. With Decoy state QKD, clever eavesdropping strategies that may be adopted by Eve can no longer be used.

The focus of this paper is on pragmatic information reconciliation using novel soft information processing techniques. The proposed techniques can be applied to QKD schemes based both on Single Photon or WLP sources, with or without decoy states. The difference among the different schemes is the use of different channel metrics. Furthermore, the information reconciliation proposed here will only use feed-forward techniques, not requiring interaction between transmitter and receiver.

2 Quantum Channel Communication System

In reference to the model depicted in Figure 1, the practical implementations of QKD protocols rely on solutions that are low cost, offer high levels of security, and can be rapidly deployed requiring uncomplicated setups and conventional devices. In this regard, QKD using decoy states (henceforth referred to as DQKD) is currently the most promising technique.

Among the multitude of DQKD experimental techniques proposed in the literature, the technique described in [1], allows one to achieve the desired characteristics of DQKD, with a reduced cost and leading to a robust system. This technique amounts to what communication Engineers would refer to as Pulse Position Modulation (PPM) which allows the use of extremely simple measurements (the time of arrival of a pulse).

We propose to use a Photon Counting Detector (PCD) to generate soft information at the output of the quantum channel, as opposed to hard decisions about whether a given received signal is a logic-0 or a logic-1. Note that in its original form, the proposed BB84 technique does not require the use of PCD. Consider the application of soft coding to a specific scheme, i.e., the one of [1]. In this protocol Alice transmits attenuated coherent states (i.e., modulated pulses of a CW laser) that either she prepares with a mean photon number *N* or blocks such states and transmits vacuum pulses. The *k*-th logical bit is encoded in a two pulse temporal sequence,

$$|0_k\rangle = |\sqrt{N}\rangle_{2k-1}\,|0\rangle_{2k}$$
$$|1_k\rangle = |0\rangle_{2k-1}\,|\sqrt{N}\rangle_{2k}$$

The time of arrival allows an unambiguous discrimination of the logical qubit. In order to check the presence of an eventual eavesdropper Alice, with a small frequency *f*, transmits a decoy state,

$$|d_k\rangle = |\sqrt{N}\rangle_{2k-1}\,|\sqrt{N}\rangle_{2k}$$

Due to the coherence of the laser, the two component of the decoy state have a precise phase relation and thus they always exit a specific gate of an interferometer at Bob's side preceded by an unbalanced Beam Splitter (BS), with transmission t_B. Such correlation also exists across the boundary between two alternating bits as well. After measurements, Bob announces when the detector after interferometer clicked (set 1, bits for the check) and when the detector at the other exit of BS clicked (set 2, bits to be used for the key reconstruction). The effect of eavesdropping is a breaking of coherence and can be estimated by the measurement of the set 1. After this test, Alice and Bob run error correction and privacy amplification on set 2 thus obtaining the key.

The performance of the protocol is quantified by the achievable secret key rate

$$R_{sk} = [R + 2p_d(1-R)](1-f)\left(1-h(Q)-I_{Eve}\right)$$

Where, $R = 1-\exp\left(-N\,t\,t_B\eta\right)$ is the counting rate when the communication channel has a transmission *t*, p_d is the detector dark count rate, h(Q) is the binary entropy function and η is the detector quantum efficiency. By measuring the quantum bit error rate *Q*, Alice and Bob can estimate the fraction of information I_{Eve} known by Eve. Thus the protocol is based on on/off detection; either the state is observed or it is not.

Once the decoy states have been identified and erased from the useful transmitted sequence, the equivalent channel model is simply that of a binary symmetric channel with bit error probability equal to the quantum bit error rate *Q*, as shown in Figure 2-(a). However, in order to minimize the effect of dark counts, one can envisage more elaborate strategies based on "soft" encoding and decoding.

One of the main ideas of our paper is that of using a detector discriminating the number of incident photons characterized by a certain set of *n*-photon dark count probabilities $p_{d,n}$. We note that we can generate and use a form of soft information even if a PCD is not used. The key attribute in using PCD is that we can generate soft information associated with the key data transmitted on the quantum channel.

For every number of detected photons one can associate a weight by comparing $p_{d,n}$ with the probability $p_n = \dfrac{\exp(-\mu)\mu^n}{n!}$ expected for the attenuated coherent state with average photon number μ.

Let *N* be the theoretical number of photons transmitted for every information bit, N_{max} the maximum number of photons that can be detected in one symbol interval, with the positive sign the transmission or reception of a logic-0 and with the negative sign the transmission or reception of a logic-1, then we can model the discrete channel generated by QKD transmission using weak laser pulses as shown in Figure 2 (b), with an input random variable *Xw* which at the generic k-th instant may assume the values $Xw_k \in (-N,+N)$, and an output random variable *Yw* which at the generic k-th instant may assume the values $Yw_k \in (-N_{\max},\ldots,-2,-1,0,1,2,\ldots,+N_{\max})$, where $N_{\max} > N$. Note that the model below is associated with transmission of one information bit which corresponds to two time slots (hence, the positive-negative designation in the probabilistic channel model), even though the number of photons detectable in a given slot is obviously only a positive quantity.

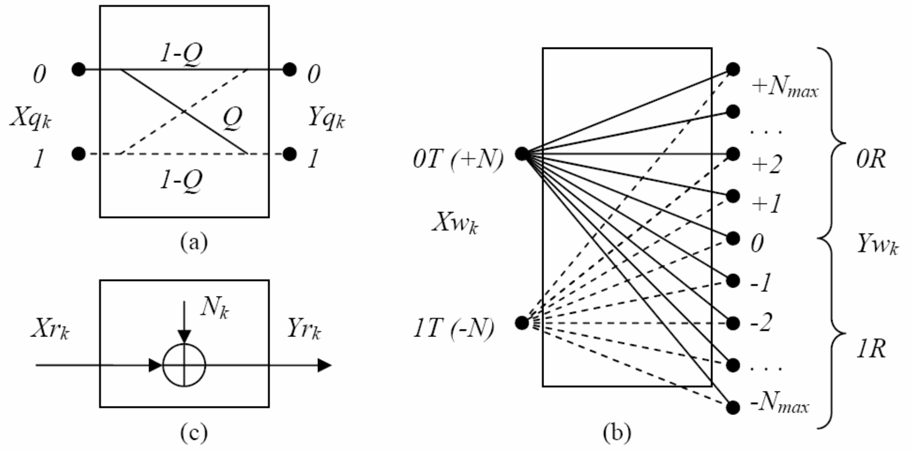

Fig. 2. Equivalent model for the single photon quantum channel (a), when WLP are used (b), and for the public channel (c)

The section about soft-metric based post-processing will describe how to extract useful soft metric values from the channel models of Figure 2 (a) and (b), and how to use them during the decoding and information reconciliation phases.

3 Classic Communication System

The public channel uses classic communication schemes, typically a radiofrequency link. Since very strong coding is allowed, the bit error rate of the classic channel is generally extremely small. Since the use of an optical link implies the presence of line of sight (LOS) between transmitter and receiver, fading can be excluded, and additive white Gaussian noise (AWGN) is generally the predominant impairment, so that the equivalent channel model shown in Figure 2 (c) can be used. In this figure, Xr_k is the k-th transmitted symbol, $N_k \in \mathcal{N}(0,\sigma^2)$ is a Gaussian random variable with zero mean and variance $\sigma^2 = N_0/2 = E_b/2\eta_S$, where $\eta_S = E_b/N_0$ is the wireless link signal-to-noise ratio, and Yr_k is the real sample obtained at the output of the public channel detector. If a bipolar transmission scheme is used, we can set $Xr_k \in (-\sqrt{E_b},+\sqrt{E_b})$.

On the public link, no information bits can be transmitted, so only the redundant information of the considered feed-forward systematic block channel code with rate R_b will be transmitted. If we denote by n_q the number of information q-bits and by r the number of redundant bits, in order to minimize the quantity of information derived by Eve from the public channel, r must be minimized, and therefore the code rate,

$$R_c = \frac{n_q}{n_q + r}$$

must be maximized. For this reason, the use of long information blocks is required and Low density parity check codes (LDPC) with iterative soft decoding meet this criterion. For such codes, the information blocks of length $n = n_q + r$ in the order of tens of thousands can be used. In spite of the large block length (which guarantees high coding rate), the use of iterative soft decoding allows for acceptable decoding complexity.

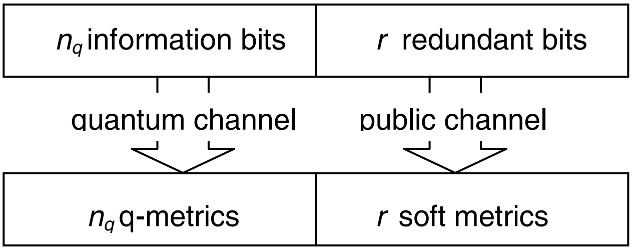

Fig. 3. Available bits and metrics at transmitter and receiver

Given the previous hypotheses, and denoting as b_k the k-th redundant bit, we can write $Xr_k = \sqrt{E_b}(2b_k - 1)$ and $Yr_k = \sqrt{E_b}(2b_k - 1) + N_k$, where Yr_k has a conditional probability density function

$$f_Y(Yr_k \mid b_k) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(- \frac{\left(Yr_k - \sqrt{E_b}(2b_k - 1)\right)^2}{2\sigma^2} \right)$$

The corresponding Log-Likelihood Ratio (LLR) value is,

$LLR(Yr_k) = \log\left[P(Yr_k \mid b_k = 1) / P(Yr_k \mid b_k = 0)\right]$ is $LLR(Yr_k) = \dfrac{2Yr_k\sqrt{E_b}}{\sigma^2}$.

This is the soft metric that will later be used by the post-processing block for the k-th redundant bit with sample value at the output of the detector equal to Yr_k.

3.1 Soft-Metric Based Post-Processing

Soft metric processing will be used for error correction, eavesdropping detection and privacy amplification, exploiting all the information available from the detectors at the output of the public and the quantum channels. This corresponds to using in the post processing algorithms not only the raw received information and redundancy bits, but all the soft information extracted from the channels, i.e., the log-likelihood ratios or LLRs [2], also denoted *soft metrics* in what follows.

Evaluation of soft metrics for different channels

As far as the redundant bits are concerned, the real received signal samples $Yr_k \in R$ can be used to generate the soft metrics,

$$LLR(Yr_k) = 2Yr_k\sqrt{E_b} / \sigma^2 .$$

As far as the information bits are concerned, when single photon transmission is used (or no soft information is extracted from a WLP based quantum channel in the absence of photon counting detector), the channel model shown in Figure 2 (a) must be considered, with transmitted bits $Xq_k \in GF(2) = \{0,1\}$ and received bits $Yq_k \in GF(2) = \{0,1\}$, whose soft metrics are [2] ,

$$LLR(Yq_k) = \begin{cases} \log[(1-Q)/Q] & \text{if} \quad Yq_k = 1 \\ \log[Q/(1-Q)] & \text{if} \quad Yq_k = 0 \end{cases}.$$

In the case of WLP transmission, however, when a photon counter is available at the receiver, additional soft information can be extracted, as previously discussed. In this case, the equivalent channel model shown in Figure 2(b) must be considered, and the soft likelihood metrics

$$\begin{aligned} LLR(Yw_k) &= \log\left[P(Yw_k \mid b_k = 1) / P(Yw_k \mid b_k = 0)\right] \\ &= \log\left[P(Yw_k \mid Xw_k = 1) / P(Yw_k \mid Xw_k = 0)\right] \end{aligned}$$

can be expressed as

$$LLR(Yw_k = Yw(j)) =$$
$$\log\left[P(Yw_k = Yw(j) \mid Xw_k = 1) / P(Yw_k = Yw(j) \mid Xw_k = 1)\right]$$

Joint use of metrics from different channels

In the decoding of LDPC for the information bits $Xq_k \in GF(2) = \{0,1\}$, we will use the soft metrics of the received raw bits $Yq_k \in GF(2) = \{0,1\}$

$$LLR(Yq_k) = \begin{cases} \log[(1-Q)/Q] & \text{if } \; Yq_k = 1 \\ \log[Q/(1-Q)] & \text{if } \; Yq_k = 0 \end{cases},$$

while, as far as the redundant bits $Xr_k \in GF(2) = \{0,1\}$ are concerned, we are dealing with the real received signal samples Yr_k with soft metrics

$$LLR(Yr_k) = 2Yr_k\sqrt{E_b}/\sigma^2 \; .$$

These metrics must be jointly used and compared in the LDPC decoder. To achieve this, the metrics need to be compatible and comparable. Let us suppose that the equivalent Binary Symmetric Channel (BSC) model used in the quantum channel is obtained using 2 PAM as the modulation scheme with transmitted levels $\sqrt{Ep_b}(2b_k - 1)$, where b_k are the transmitted bits, $\hat{b}_k$ are the decided raw bits, Ep_b is the energy per bit and σ_p^2 is the noise variance per dimension (see Figure 4). Let us also denote the equivalent received sample as $Yp_k = \sqrt{Ep_b}(2b_k - 1) + Np_k$, so that

$$P(b_k \text{in error}) = \frac{1}{2} erfc\left(\frac{\sqrt{Ep_b}}{\sqrt{2}\sigma_p}\right) = Q$$

where, the transmitted levels are $\pm\sqrt{Ep_b}$ and $Np_k \in \mathcal{N}(0,\sigma_p^2)$

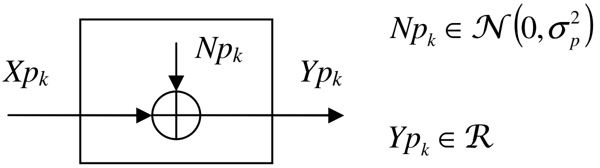

Fig. 4. Equivalent model for the single photon quantum channel when using an equivalent 2 PAM modulation scheme

At this point we can assume that the noise is negligible, (i.e., that $Yp_k \cong \sqrt{Ep_b}(2b_k - 1) \cong \sqrt{Ep_b}(2\hat{b}_k - 1)$), allowing us to write the soft metric of the equivalent 2 PAM channel as,

$$LLR(Yp_k) = \frac{4Yp_k\sqrt{Ep_b}}{2\sigma_p^2} = \frac{4Ep_b(2\hat{b}_k - 1)}{2\sigma_p^2} =$$

$$= 4erfc^{-1}(2Q)(2\hat{b}_k - 1) = \begin{cases} +4erfc^{-1}(2Q) \text{ if } \hat{b}_k = 1 \\ -4erfc^{-1}(2Q) \text{ if } \hat{b}_k = 0 \end{cases}$$

The metric for the equivalent BSC Quantum channel shown in the last formula can be jointly used with the metric of the 2 PAM public channel for decoding.

Iterative soft forward error correction

Once the appropriate soft (quantized on more than 1 bit) metrics have been associated with the various (information and redundant) bits, the situation is as depicted in Figure 3, and a soft metric based block decoder must be identified. Considering the basic result of Shannon's theorem that indicates that the longer the considered block length in Forward Error Correction (FEC) channel code, the larger its minimum distance and/or the higher its rate, we desire to use a very large block length $n_q + r$, which can pose huge constraints on the decoding complexity. To overcome this, Low Density Parity Check (LDPC) codes provide a viable solution.

In fact, in contrast to many classic codes, LDPC codes allow very fast iterative probabilistic decoding algorithms, in addition to being a class of linear capacity achieving codes. This makes LDPC codes attractive from both a theoretical and a practical point of view.

Finally, we can notice that the suggested decoding algorithm offers a soft-output, so that the decoded bits, obtained after a suitable and possibly variable number of iterations, are paired with their associated soft metrics as well, which can be used as an indicator on the reliability of the decoded bits.

Convergence analysis

A typical decoded bit error performance curve of an iteratively decoded capacity achieving code transmitted over a binary symmetric channel (BSC), as a function of the transition probability P of the BSC, is illustrated in Figure 5. The performance of the code is divided into three regions: the low-performance region, the waterfall region and the (optional) error floor region.

The low-performance region is the region where transition probability P is higher than the minimum value required for the iterative decoding to converge. The value of the threshold transition probability P* depends on the size of considered code.

The performance region where a small decrease in the transition probability P results in a considerable improvement in the error probability is called the waterfall region, or sometimes the turbo cliff region when its slope is particularly steep.

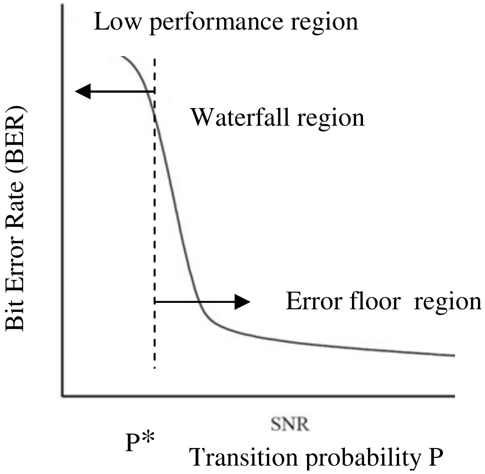

Fig. 5. Typical decoded BER performance curve of an iteratively decoded capacity achieving code

In the error floor region, when present, the performance does not improve significantly as the transition probability P decreases further, or however it decreases with a slope much smaller than in the waterfall region. We must note that the error floor region typically does not show a horizontal floor, but a change in slope with respect to the waterfall region.

Given these general characteristics of an LDPC code performance, and knowing that a quantum channel has a typical quantum BER $Q \approx 0.11$ or lower, and that the channel is not considered reliable because of eavesdropping if $Q > Q^* \approx 0.3$, i.e., if the QBER is larger than a given threshold Q^*, if an LDPC code is selected with threshold transition probability $P^* \approx Q^*$, the decoding process will not converge if the quantum channel is unreliable. The non-convergence could be detected by observing the erratic behavior of the decoded sequence reliability, allowing the use of the decoded codeword reliability monitoring as a form of quantum channel probe. Hence, we have a novel mechanism of detecting eavesdropping on the fly based on the inherent characteristics of the codes employed for information reconciliation.

Privacy amplification

The availability of soft output information, where the decoded bits are paired with the associated reliability, offers an instrument for performing efficient and selective privacy amplification, deleting from the decoded sequence (i.e., form the quantum key), the bits with low reliability, maintaining the most trusted information. This allows for a variable rate security key generation protocol which again to the best of our knowledge is entirely novel.

Simulation Results

We have conducted simulations using LDPC codes with rate 0.5 and various block lengths. Weighed q-metric values $\alpha LLR(Yp_k)$ have been considered, with $0 < \alpha \leq 1$. The parameter α has been inserted in order to optimize the contribution of the information derived from the q-bits, which should not be too high since the q-bits are generally not very reliable, but should also not be too low, due to the fact that some information can however be extracted from them.

In Figure 6 and Figure 7 we report the simulated Bit Error Rate (BER) and Frame Error Rate (FER) of a LDPC code with $n=n_q+r=504$, $r=252$ and $R_c=0.5$ decoded with 100 iterations, for different values of the QBER parameter Q in the range 0.1 to 0.5, as a function of the weigh parameter α. It can be observed how an optimal value of α in the order of 0.5 can be identified, which however depends on the QBER parameter Q. Optimizing α allows for a strong performance improvement, lowering the achievable error rates up to three orders of magnitude.

It can also be observed that the decoder performance converges to low BER and FER values only if Q is smaller than roughly 0.15, allowing for reliability control, as previously described.

Finally, in Figure 8, the BER values of a $n=n_q+r=504$, $r=252$ and $R_c=0.5$ code are compared with those of a $n=n_q+r=1000$, $r=500$ and $R_c=0.5$ code, one for Q in the range 0.12-0.5, showing that as expected, longer code blocks (and higher complexity) allow for better decoding performances.

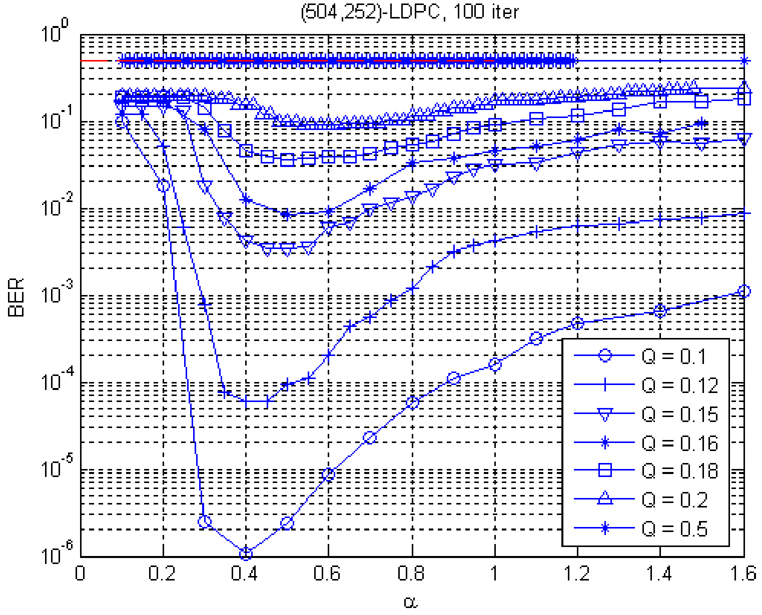

Fig. 6. BER performance of a LDPC code with $n=n_q+r$=504, $r=252$ and $R_c=0.5$, decoded with 100 iterations as a function of Q and α

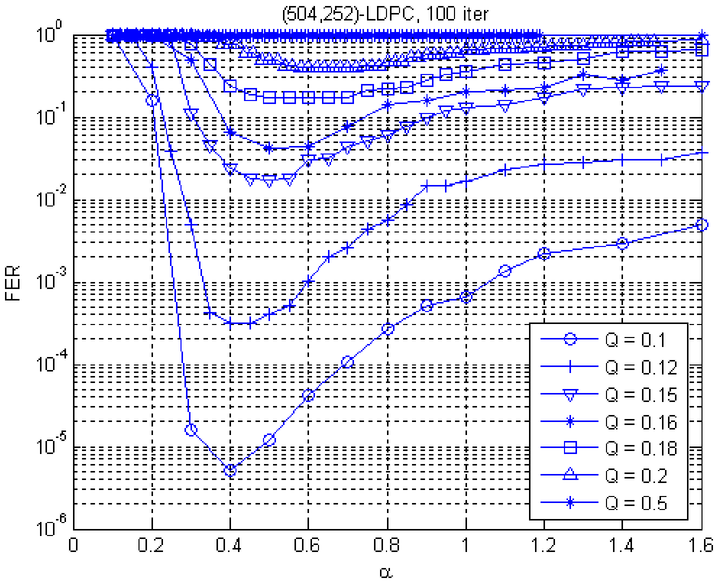

Fig. 7. FER performance of a LDPC code with $n=n_q+r=504$, $r=252$ and $R_c=0.5$, decoded with 100 iterations as a function of Q and α

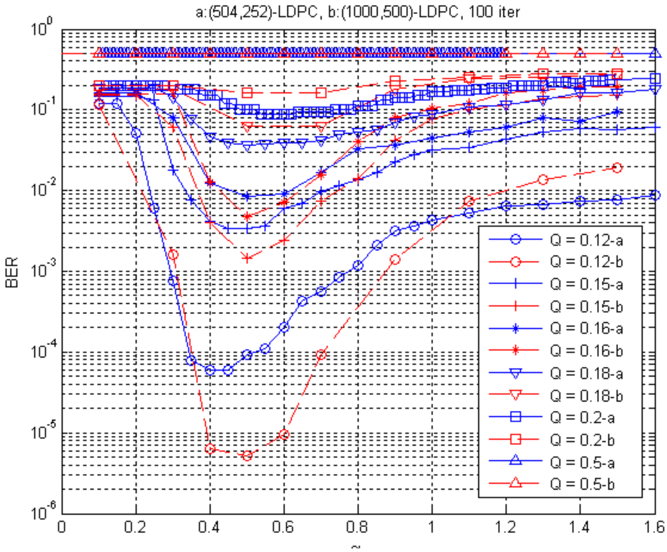

Fig. 8. Comparison between the BER performance of two LDPC codes with $R_c=0.5$, one with $n=n_q+r=504$, $r=252$ and one with $n=n_q+r=1000$, $r=500$ as a function of Q and α

References

1. Stucki, D., et al.: Appl. Phys. Lett. 87, 194108 (2005)
2. Proakis, J.G., Salehi, M.: Digital Communications, 5th edn. McGraw-Hill, New York (2006)