Efficient Information Reconciliation for Continuous-Variable QKD using Non-Binary Low-Density Parity-Check Codes

Christoph Pacher, Jesus Martinez-Mateo, Jörg Duhme, Fabian Furrer, Vitus Händchen, Tobias Gehring, Reinhard F. Werner, Roman Schnabel

In typical discrete-variable (DV) QKD protocols each transmitted signal, that is not discarded during the key generation process, is usually decoded to a single bit of the raw key. For DVQKD, reconciliation methods like Cascade [1] and rate-adapted low-density parity-check (LDPC) codes [2], typically operating on the binary alphabet, have been shown to be efficient and high-throughput approaches.

On the other hand, in continuous-variable (CV) QKD the situation is significantly different: the transmitted continuous signals potentially have uncountably many different outcomes. Nevertheless, the measurement process converts those signals into discrete values (symbols), albeit typically distinguishing between much more than two different outcomes. Thus, for the key generation process of CVQKD larger alphabets can be considered, e.g. the set $\{0,1\}^p$ with $p > 1$, which allows for a binary representation of each symbol, i.e. such that p bits are generated per non-discarded symbol.

We present here an information reconciliation method [3], [4] and demonstrate for the first time that it can achieve efficiencies close to 0.98 [4]. This method is based on the belief propagation decoding of non-binary LDPC codes over finite (Galois) fields. In particular, for convenience and faster decoding we only consider power-of-two Galois fields.

Quantization phase.—A cut off parameter α defines the boundaries of a key generation grid in the phase space. The interval $[-\alpha, \alpha]$ is uniformly partitioned by choosing a spacing value δ such that the number of sub-intervals (bins) is equal to 2^p. From each continuous measurement outcome we obtain one raw key symbol by binning.

Reconciliation phase.— We chose the binary representation for each symbol and write Alice's and Bob's quantized outcomes as $x_A, x_B \in \{0,1\}^p = \{0,1\}^d \times \{0,1\}^q$, such that $x_A = \check{x}_A \| \hat{x}_A$ and $x_B = \check{x}_B \| \hat{x}_B$, where $\check{x}_A, \check{x}_B \in \{0,1\}^d$ denote the d least significant bits of x_A, x_B, resp., $\cdot\|\cdot$ denotes concatenation, and $\hat{x}_A, \hat{x}_B \in \{0,1\}^q$ denote respectively the remaining bits of x_A, x_B.

The reconciliation involves then the following steps:

1) Alice and Bob construct frames consisting of n quantized symbols each: $X_A := (x_A^1, \ldots, x_A^n)$, $X_B := (x_B^1, \ldots, x_B^n)$.

2) Alice sends through a noiseless channel the d least significant bits of each symbol in X_A, i.e. $\check{X}_A := (\check{x}_A^1, \ldots, \check{x}_A^n)$ to Bob who reconciles $\check{X}_B := (\check{x}_B^1, \ldots, \check{x}_B^n)$ by setting $\check{X}_B = \check{X}_A$. Note that this step corresponds to a coding process with rate $R = 0$.

3) Finally, the proposed reconciliation method concludes using a non-binary LDPC code with frame length n over a Galois field of order 2^q to reconcile errors in the q most significant bits of each symbol in X_A and X_B, i.e. in $\hat{X}_A := (\hat{x}_A^1, \ldots, \hat{x}_A^n)$ and $\hat{X}_B := (\hat{x}_B^1, \ldots, \hat{x}_B^n)$. Assuming direct reconciliation, $\hat{X}_B$ is the symbol frame to be reconciled. To this end, Alice computes a syndrome of $\hat{X}_A$ and sends it to Bob through a noiseless channel. For an optimal reconciliation, the length of this syndrome must be adapted to the correlation between $\hat{X}_A$ and $\hat{B}_B$. Bob begins then the decoding process using an iterative belief propagation based algorithm, initialized with an estimation of the a-priori probability for each symbol $\hat{x}_A^i$ based on his corresponding measurement outcome x_B^i and the corrected $\check{x}_B^i$. After both steps Alice and Bob share the same reconciled key with high probability.

We constructed regular and irregular non-binary LDPC codes over $GF(2^q)$ and performed simulations to analyze their efficiency [4]. Non-binary LDPC decoding over $GF(2^q)$ is performed with a sum-product (belief propagation based) algorithm using the q-dimensional Hadamard transform with a maximum of 50 decoding iterations.

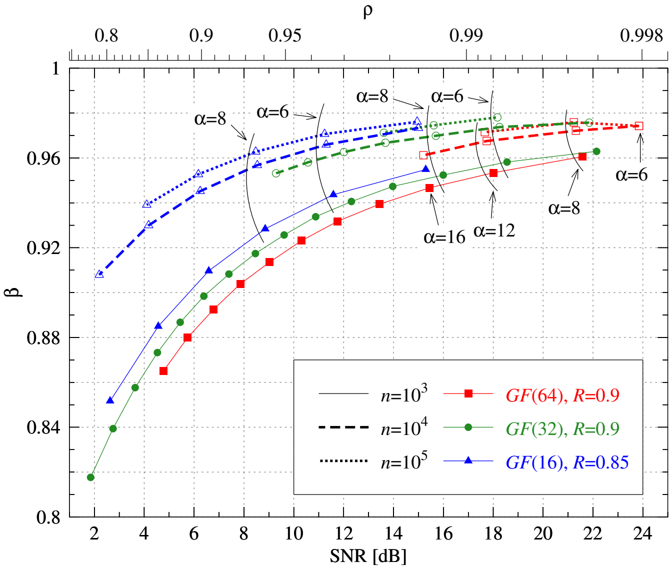

Fig. 1. Reconciliation efficiency β as a function of signal-to-noise ratio (bottom) and correlation coefficient (top) for non-binary LDPC decoding over different Galois fields varying the interval half width α for fixed-rate codes.

Fig. 1 shows the reconciliation efficiency as a function of the SNR for different half widths α of the reconciliation interval. Increasing α values were considered for a constant coding rate R. Then we compared the reconciliation efficiency of several coding rates over different Galois fields. In this case, the total number of sub-intervals of the reconciliation interval remains constant 2^9. Consequently, the number d of disclosed bits differs for each Galois field, i.e. $d = 5$, 4, and 3 for decoding over $GF(2^4)$, $GF(2^5)$, and $GF(2^6)$, respectively. Several curve points corresponding to low values of α are labeled in the figure. Note that the interval half width of two consecutive points on a curve differs by 2 or 4. As shown, the efficiency considering a frame length of $n = 10^4$ bits is over 0.9 in the SNR range from 2 to 24 dB and approaches 0.98 for $n = 10^5$ and SNR > 14 dB.

References

[1] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol Cascade," *Quantum Inform. Comput.*, vol. 15, no. 5&6, pp. 453–477, 2015.

[2] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Key Reconciliation for High Performance Quantum Key Distribution," *Sci. Rep.*, vol. 3, no. 1576, pp. 1–6, 2013.

[3] C. Pacher, J. Duhme, F. Furrer, V. Händchen, T. Gehring, and R. F. Werner, "Reconciliation for Continuous Variable Quantum Key Distribution With Non-Binary LDPC Codes," *QCrypt Poster #74*, 2014.

[4] C. Pacher, J. Martinez-Mateo, J. Duhme, and F. Furrer, "Information reconciliation for continuous-variable quantum key distribution using non-binary low density parity check codes," *to appear*, 2015.