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

Christoph Pacher[1†], Jesus Martinez-Mateo[2], Jörg Duhme[3], Fabian Furrer[4], Vitus Händchen[5], Tobias Gehring[5,6], Reinhard F. Werner[3], and Roman Schnabel[5]

[1] Digital Safety & Security Department, AIT Austrian Institute of Technology GmbH, 1220 Vienna, Austria
[2] Madrid Center for Computational Simulation, Universidad Politécnica de Madrid, 28660 Boadilla del Monte, Spain
[3] Institut für Theoretische Physik der Leibniz Universität Hannover, Appelstraße 2, 30167 Hannnover, Germany
[4] Department of Physics, Graduate School of Science, University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan, 113-0033
[5] Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut) and
Institut für Gravitationsphysik der Leibniz Universität Hannover, Callinstraße 38, 30167 Hannover, Germany
[6] Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kgs. Lyngby, Denmark
[†] e-mail: Christoph.Pacher@ait.ac.at

ABSTRACT.— We report on an efficient information reconciliation method for correcting errors in a continuous-variable quantum key distribution system. It consists of several steps. First, in a quantization phase, the continuous result of a measurement is discretized into 2^p intervals, each one corresponding to a different symbol. Next, in the reconciliation phase, Alice transmits the d least significant bits of the binary representation of her symbol to Bob. This allows Bob to reduce the number of possible symbols by a factor of 2^d. Finally, a non-binary low-density parity-check code over a Galois field of order 2^{p-d} is used to reconcile a frame with the remaining discrepancies in the $p-d$ most significant bits of the binary representation of each symbol.

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

METHOD.

A. Quantization phase.—The continuous result of a measurement is discretized into 2^p intervals, each one corresponding to a different symbol. A cut off parameter $\pm\alpha$ defines the boundaries of a key generation grid around the origin of the phase space. The interval $[-\alpha,\alpha]$ is uniformly partitioned by choosing an spacing value δ such that the number of subintervals (bins) is equal to 2^p. Symbols in the raw keys are then obtained by binning the measurement outcomes, where the representative values for each interval are chosen from the elements of a finite (Galois) field of order 2^p, $GF(2^p)$.

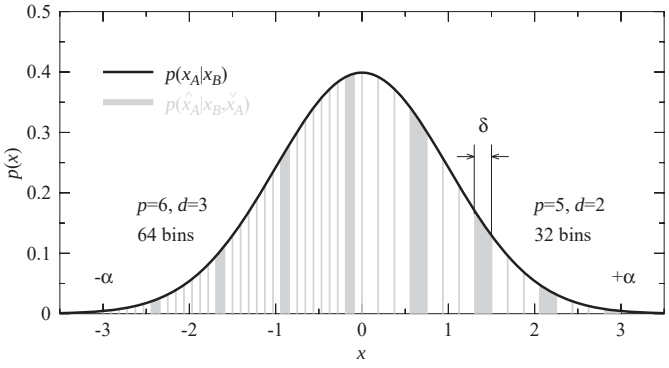

Fig. 1. Quantization or key generation grid.

B. Reconciliation phase.— We chose the binary representation for each symbol and rewrite Alice's and Bob's quantized outcomes by considering $x_A, x_B \in GF(2^d)\otimes GF(2^q) = GF(2^p)$, such that $x_A = \hat{x}_A \| \check{x}_A$ and $x_B = \hat{x}_B \| \check{x}_B$, where $x\|y$ denotes the concatenation of two binary sequences, x and y, the former x representing the least significant bits of the sequence. The reconciliation involves then the following steps:

Step B.1) Alice sends through a noiseless channel her d least significant bits of the binary representation of her symbol $\{\check{x}_A\}$ to Bob who rewrites his quantized outcome by equaling with those bits received from Alice, $\check{x}_B = \check{x}_A$.

Step B.2) Finally, the proposed reconciliation method concludes using a non-binary LDPC code over a Galois field of order 2^q (1) to reconcile a frame with the remaining discrepancies in the q most significant bits of the binary representation of each symbol.

The efficiency of the proposed two-steps information reconciliation method is defined as

$$\beta = \frac{H(Q(X_A)) - \ell}{I(X_A;X_B)}, \qquad (1)$$

where ℓ is total leakage per symbol that can be bounded, given the coding rate R of the non-binary LDPC code used, by $\ell = d + q(1-R)$.

RESULTS.

Fig. 2 shows the reconciliation efficiency as a function of the signal-to-noise ratio (SNR) for different half widths of the reconciliation interval α. Increasing α values were considered for a constant coding rate R. It was then compared the reconciliation efficiency of several coding rates over different Galois fields. In this case, the number of sub-intervals of the reconciliation interval remain constant to 2^9, such that the number of disclosed bits differs for each Galois field, i.e. $d = 5$, 4, and 3 for decoding over $GF(16)$, $GF(32)$, and $GF(64)$, respectively. The smallest interval half width (i.e. $\alpha = 4$ and $\alpha = 6$) are labeled in the figure. Note that the interval half width of two consecutive points on a curve differs by 2 ($GF(64)$) or 4 ($GF(16)$, $GF(32)$). As shown, the efficiency considering a frame length of $n = 10^4$ bits is over 0.9 in the range from 2 to 24 dB.

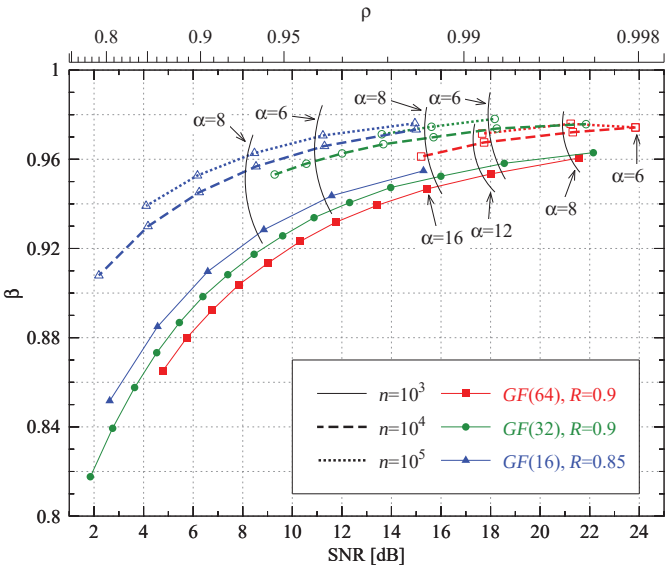

Fig. 2. Reconciliation efficiency for fixed-rate non-binary LDPC decoding over different Galois fields varying the interval half width α.

CONCLUSIONS.— We propose an efficient information reconciliation method (2) that directly operates on symbols of a key generation alphabet, instead of using the binary representation for each symbol. This method, novelty proposed for CVQKD, is based on the belief propagation decoding of non-binary LDPC codes over $GF(q)$ with $q > 2$.

ACKNOWLEDGMENTS.— Partially supported by the projects Hybrid Quantum Networks, TEC2012-35673, funded by *Ministerio de Economía y Competitividad*, Spain, and HiPANQ, ICT10-067, Vienna Science and Technology Fund (WWTF).

REFERENCES.

(1) L. Barnault and D. Declercq, "Fast decoding algorithm for LDPC over GF(2^q)," in *ITW 2003, IEEE Inf. Theory Workshop*. IEEE, Mar. 2003, pp. 70–73.

(2) 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," *in preparation*, 2015.