High-Speed FPGA Implementation of LDPC Decoder for Quantum Key Distribution

Kazuaki Doi
Corporate Research & Development Center, Toshiba Corporation, 1, Komukai Toshiba-cho, Kawasaki-shi, Japan

Abstract：In research on quantum key distribution systems, research with a view to practical use is pursued as well as that in order to establish the theoretical proof of unconditional security. Improving the throughput of key distribution is cited as one of the important themes concerning practical use; the throughput of the signal process needs to be improved as well as that of quantum state transmission and the detection scheme. Low-Density Parity-Check (LDPC) Code is expected to be applied as an improved throughput method for the Error Correction (EC) process, and research on software-implemented LDPC Code, such as implementation in the CPU or the GPU, is underway. Here, we report the improvement of LDPC Decoding throughput to 200 Mbps without degrading the efficiency of the EC process by implementing the LDPC Decoder into the FPGA Board.

Keywords:：Quantum Key Distribution (QKD), Error Correction Code, LDPC, FPGA

Introduction：The BB84 scheme, proposed in 1984, is the classical QKD method. The Cascade protocol is used as the EC process in the BB84 scheme. In the Cascade protocol, the parity data corresponding to the quantum key is transmitted via a classical channel and the key data is corrected by using the parity data. But if the Cascade protocol is used, it is difficult to improve the throughput because repetitive and additional transmission of the parity data takes an extremely long time. Therefore, LDPC codes (1), which are the error correction codes of wireless communication systems and storage systems, are attracting attention and application of LDPC to QKD is being studied (2). If LDPC is used, it is easy to parallelize the decoding scheme and there is no need to repetitively and additionally transmit the syndrome data, which corresponds to the parity data in the Cascade protocol, and so throughput is expected to improve.

In QKD, since the efficiency with which syndrome data are used is strongly related to the security of the quantum key, error correction should be executed efficiently with as little usage of syndrome data as possible. Therefore the efficiency of the error correction ability of the LDPC decoding algorithm should be as high as possible. Sum-Product Algorithm (SPA), one of the commonly used LDPC decoding algorithms, has a very strong error correction ability, but it is difficult to implement SPA in FPGA while maintaining the decoding performance of SPA in floating-point operation because Gallager’s function ($\Phi(x)=-\log(\tanh(x))$) including hyperbolic functions is used in SPA. In this work, an LDPC decoder for high-speed QKD is implemented in FPGA and the performance is evaluated. As a result, FPGA-implemented decoder is found to have an error-correcting performance comparable with that of SPA in terms of floating-point operation and the throughput of the LDPC Decoder is improved to 200 Mbps while maintaining the error correction efficiency satisfactorily. This paper discusses the performance in detail.

FPGA implementation structure of LDPC Decoder：In one of the FPGA-implementation methods of SPA, Gallager’s f function is implemented as a table function (3). (In this paper, this method is called Table-SPA.) This method is easy to carry out but calculation of the periphery of the region such that $\Phi(x)$ is infinity at $x = 0$ cannot be reproduced, because the output of the table function in FPGA is limited. Therefore, Table-SPA causes an operation error if the calculation of the region is operated in the decoding algorithm, whereas SPA with using the floating-point operation does not. (In this paper, this method is called Floating-SPA.) The higher the absolute value of the input signal to LDPC Decoder, the higher the probability of this operation error becomes, and so if the iteration number of LDPC decoding is increased, the probability becomes higher.

Therefore, the LDPC decoder that selects the decoding algorithm according to the iteration number is proposed and implemented in FPGA as shown in Figure 1.

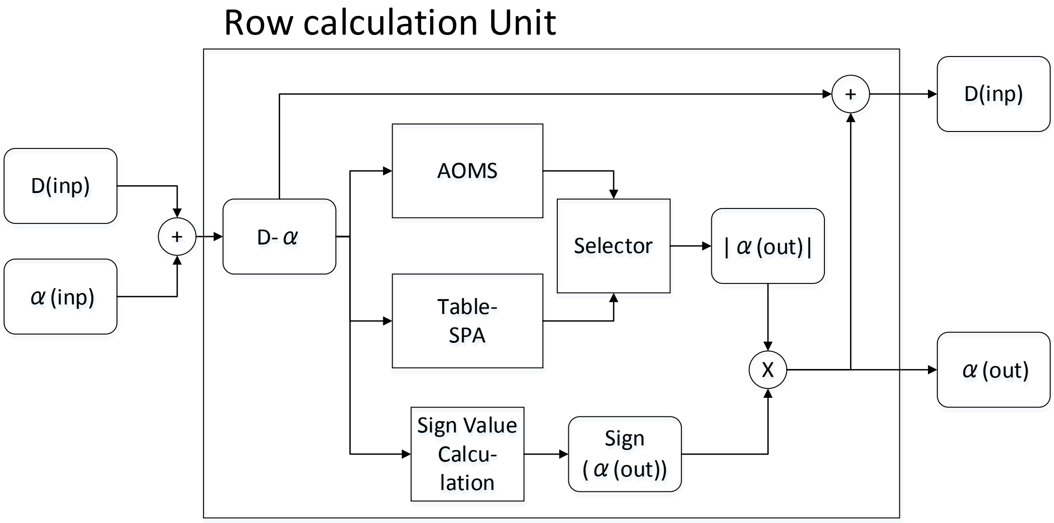

Figure 1 The construction of the proposed LDPC Decoder（Row Calculation Unit）

When the iteration number is small and the probability of operation error is small, Table-SPA is selected and when the iteration number is big and the probability of operation error is high, Adaptive Offset Min-Sum Algorithm (AOMS) (4) is selected. The maximum value of Φ(x) is infinity, and by contrast the maximum value of Φ(x) implemented into Table-function is limited, so if the operation error occurs, the output signal of Table-SPA becomes smaller than that of Floating-SPA. To solve the problem, AOMS, whose maximum value of output signal is bigger than that of Floating-SPA when implemented in FPGA and the decoding performance is guaranteed, is selected as the other decoding algorithm. In this FPGA implementation, if the iteration number is less than 30 Table-SPA is selected, and otherwise AOMS is selected.

Result : The verification of the performance of the proposed algorithm by using software simulation is explained. The QbER characteristic of the decoding failure rate is shown in Figure 2 and the efficiency characteristic of the decoding failure rate is shown in Figure 3.

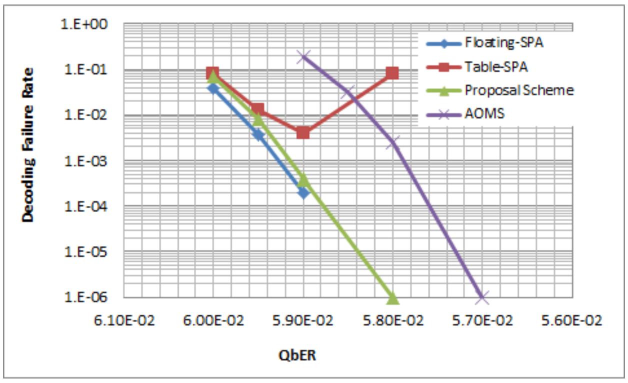

Figure 2 The QbER characteristic of the decoding failure rate of the decoding algorithm

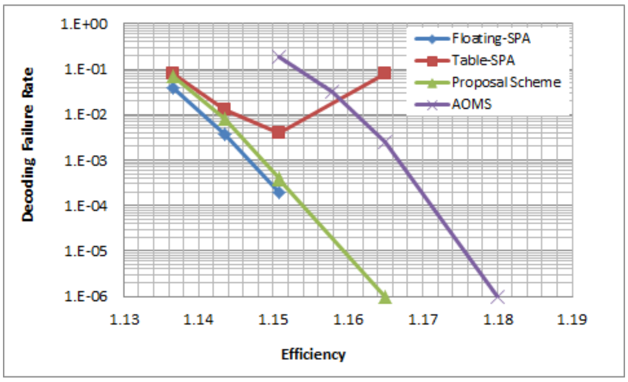

Figure 3 The efficiency characteristic of the decoding failure rate of the decoding algorithm

The LDPC used in the simulation is irregular LDPC, whose codeword length is 84608 bits, syndrome length is 31488 bits, row weight is from 11 to 14, and column weight is from 2 to 12. In this simulation, Floating-SPA, Table-SPA implemented alone in FPGA, AOMS implemented alone in FPGA, and the proposed algorithm implemented in FPGA were compared. The horizontal axis of Figure 2 denoted QbER is the bit error rate of quantum channel and the vertical axis of Figure 2 is the decoding failure rate. The horizontal axis of Figure 3 denoted Efficiency is the ratio of the length of syndrome data for error correcting to the minimum bound length of syndrome data based on Shannon's theory. The vertical axis of Figure 3 is the decoding failure rate. As shown in Figure 2 and 3, the proposed algorithm has the same decoding performance as Floating-SPA and the decoding failure rate is below 1e-4 if the efficiency is more than 1.16.

Next, the result of implementation in Altera Stratix V 5SGXA7 is explained. The logistic usage amount is approximately 63 K (ALMs) and the memory block size is approximately 27.2 Mbit. Since the logic utilization rate is approximately 30% and the memory block utilization rate is approximately 50%, the moving frequency of FPGA-implemented LDPC Decoder becomes approximately 200 MHz. And next, decoding throughput is examined. The Efficiency characteristic of the average iteration number for error correcting is shown in Figure 4. As shown in the figure, if Efficiency becomes bigger, the average iteration number for error correcting is reduced, and if Efficiency is more than 1.15, the decoding throughput reaches 200 Mbps.

Conclusion : In this paper, FPGA-implementation of LDPC Decoder for high-speed QKD is proposed and the performance is evaluated. As a result, the proposed algorithm implemented in FPGA is found to have the same decoding performance as Sum-Product Algorithm in floating-point operation. And as a result of implementing LDPC Decoder in the FPGA board mounting Altera Stratix V, the decoding throughput becomes 200 Mbps and the efficiency is 1.15. In the future, the FPGA LDPC Decoder will be implemented in a QKD system and the throughput of the entire EC process will be evaluated.

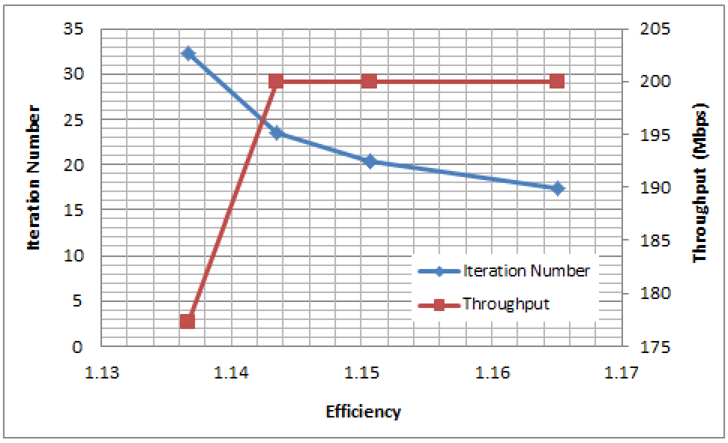

Figure 4 The Efficiency characteristic of the average iteration number and the decoding throughput

References :

1. R.G.Gallager, Low-Density-Parity-Check-Codes, M.I.T. Press, 1963
2. A.R.Dixon, High speed and adaptable error correction for megabit/s rate quantum key distribution, Scientific Reports 4, 2014
3. A High Performance and Programmable decoder VLSI for Structured LDPC Codes, ISCIT 2006
4. Adaptive Offset Min-Sum Algorithm for Low-Density Parity Check Codes, IEEE COMMUNICATIONS LETTERS, Vol.10, No.6