DESIGN A HIGH EFFICIENT HYBRID POLAR CODES FOR CRYPTOGRAPHY

J. Praveen[1], Y. Kiran[2]
[1]*Dept. Of E.C.E, Hyderabad, Telangana, India*
[2]*Assistant Professor, Teegala Krishna Reddy Engineering College, Telangana, India*

Abstract- **To decode the capacity of polar codes we use two most popular soft-output BP algorithms. They are flooding belief propagation (FO-BP) algorithm and soft cancelation (SCAN) algorithm. The flooding belief propagation algorithm produces high signal to noise ratio and cost is also very high. Coming to the soft-output BP algorithm, it produces better result compared to the flooding belief propagation algorithm. Now in this paper, a proposed version of the BP algorithm is given as reduced complexity soft cancelation algorithm (RCSC). Compared to the SCAN the reduced complexity soft cancelation algorithm reduces the number of memory entries by 50%. we can observe that when signal to noise ratio is increased then the error performance improvement of the RCSC becomes more significant. To reduce the decoding latency and to increase the throughput of the RCSC algorithm we proposed a reduced latency soft cancelation (RLSC). At last the both RCSC and RLSC are used in optimized VLSI architectures.**

I. INTRODUCTION

In coding theory, polar code is very significant. Basically polar codes obtain their channel capacity by using two memory less channels. The two memory less channels are binary-input symmetric memory less channels and arbitrary discrete memory less channels. The block length N can be decoded by using successive cancelation algorithm having complexity O (N log N). But in SC algorithm it gives very low complexity for the polar codes. Now, belief propagation decoding is introduced in the polar codes. In this mainly two performances are analyzed one is message passing schedules and code performance under finite lengths. It not only analyzes the error performance but also it discuss about flooding schedule in BP algorithm.

The both processes of BP algorithms are known as flooding BP algorithms (FO-BP). The main intent of this FO-BP algorithm is that it produces high level of parallelism. Due to this high level of parallelism it produces high level of complexity. The number of memory entries required for this algorithm is given as 2N (log2 N + 1). In this algorithm the number of comparisons and additions are reduced. This is one type of decoder the another type of decoder is given as soft cancellation decoder (SCAN). Generally it is depend on the serial message update schedule. This serial decode message schedule resemble the SC decoding process. Compared to above FO-BP algorithm this SCAN decoder has less computational complexity and takes less memory. So from this we can say that SCAN is more faster than the SCAN.

Now, in this paper a reduced complexity soft-cancelation algorithm (RCSC) and a reduced latency soft-cancelation (RLSC) algorithm are proposed. Along with that they proposed the architectures of decoders. There are some contributions in this paper they are given below

1. Firstly, to simplify the calculations of logarithmic likelihood ratio (LLRs) a method is implemented that is simplified left message update (SLMU) method. When we compare this method with both SCAN and FO-BP algorithms this method first reduces the (N/2) (log2 N − 1) additions for each repeating process.
2. Now, coming to the RCSC algorithm it depends on the binary tree representation of the polar codes. This proposed RCSC algorithm reduces the number of memory entries. When FER is about 10^{-5} then the RCSC algorithm of FO-BP algorithm gives 0.7 dB and when FER is about 10^{-3} then the RCSC algorithm of SCAN algorithm gives 0.2 and 0.05 Db.
3. In the proposed RCSC algorithm, there is no need of the decoding performance degradation because of the adoption of the non recursive

expression. These are some contributions that are related to the proposed system.

II. PROPOSED RCSC AND RLSC DECODING ALGORITHMS

A. Simplified Left Message Update Method.

Basically, the message update of the both BP and SCAN algorithms are based on the binary-input symmetric memory less channels, arbitrary discrete memory less channels, message passing schedules and code performances under finite length. To compute the value of $L_{i,\,j}$ we proposed the simplified left message update method (SLMU). Now this method is modified to pass the message from particular schedules from i = 0 to i > 0. The entire process is shown in the below figure (1). From this figure we can observe the update of message when i=0 and i > 0. When i = 0 then SLMU method produces right LLR and coming to i > 0 then SLMU method produces left LLR.

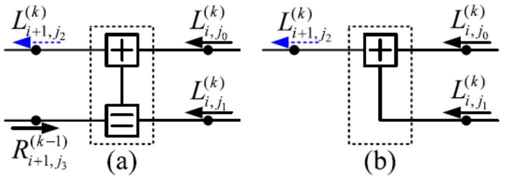


FIG. 1. UPDATE OF *LI*+1, *J*2 WHEN (A) *I* = 0 AND (B) *I* > 0.

B.

As discussed earlier that depending upon the SLMU method the RCSC algorithm gives binary tree representation of the polar code. The entire process of this binary tree representation when N=3 is shown in below figure (2). In this figure (2) there are white and black leaf nodes, in these leaf nodes it consists of both information and frozen bits. For every cycle the both left and right LLRs activates all the nodes in the tree.

Let us discuss this process in detail manner. Let us consider a node v and during the k $_{th}$ iteration all the LLRs vectors get updated then the node v gets activated. Once node v is activated then it calculates soft vector message sends to its left child as well as it calculates soft vector message sends to its right child. In this RCSC and SCAN algorithms it have same activated nodes as well as decoding latency.

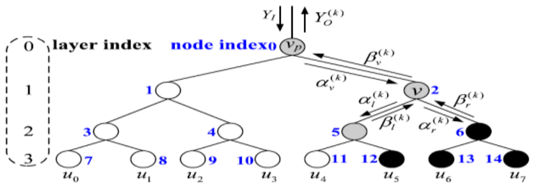


FIG. 2. MESSAGE PASSING ON THE TREE REPRESENTATION OF A POLAR CODE.

To reduce decoding algorithm and error performance degradation in RCSC algorithm we proposed the RLSC algorithm. Basically, when an arbitrary rate node is activated then this proposed RLSC algorithm accelerates returned LLR vector.

1.Simplified LLR Computation for Arbitrary Rate Nodes:

As discussed earlier that in binary tree representation it consists of both information bits and frozen bits. Now in this the frozen bit pattern vector is denoted as p_v and the main purpose of this is to indicate the location of leaf nodes. In this frozen bit pattern vector it consists of N_v letters. Each letter consists of F and D, this indicates the leaf nodes that are associated with information bits. To illustrate the RLSC algorithm we use two algorithms. Algorithm 1 and algorithm 2 are the leaf nodes in proposition 1. Here the FO-BP algorithm is proposed to calculate the returned LLRs from SPC node.

In algorithm 1 the node v is activated then returned LLR vector value is calculated and it consists of seven different frozen bit pattern vectors. Coming to the algorithm 2 it consists of LLC algorithm which computes the returned LLC vector when arbitrary rate node is activated. This arbitrary vector node when N=16 falls into three categories. They are one of the child node is a rate-0 node, one of the child node is rate-1 node, and both the left and the right child nodes are arbitrary rate nodes.

2.Proposed Tree Pruning Method:

Up to now we have discussed about the binary tree representation but in this we are going to discuss about the pruning tree. The proposed RLSC algorithm works on this pruning tree representation. There are mainly three steps in the pruning process which are given below

1. First remove all the child nodes in both rate-0 node and rate-1 node.
2. Next remove all the child nodes in the SPC and REP node $N_v \leq N_T$. Here N_T is a

predefined parameter and it denotes the number of leaf nodes belonging to node v.

3. Next remove all child nodes of arbitrary rate node with N=16.

To improve the speed of calculation some of the constituents are proposed they are SPC, REP and REP-SPC. The main purpose of this REP-SPC node is to increase the throughput of SC decoder. Coming to the proposed RLSC algorithm frozen bit distribution is proposed to improve the throughput of soft output decoder.

D. Storage Requirements

From all this we can know that RLSC and RCSC algorithms require less memory entries than SCAN and FO-BP algorithms. For an every entry it stores LLR. They reduce the memory entries by 57% and 23%. From this we can say that as the value of N increases then the reduction of memory entries will also increases.

III. PROPOSED CRYPTOGRAPHY ARCHITECTURES

The below figure 3 shows the proposed architecture of the cryptography. In this they are five LLR memories they are given as LMem, RMeml, RMemr, Channel Memory (CMEM), and Soft-Output Memory (SMEM). In this the channel memory stores the channel inputs as well as soft output memory stores the right LLRs sent from the root node. In this structure the both SPC and REP implements the functions of spcc and repc. ET unit gives the proposed ET schemes coming to the HD unit; it produces p bits in parallel.

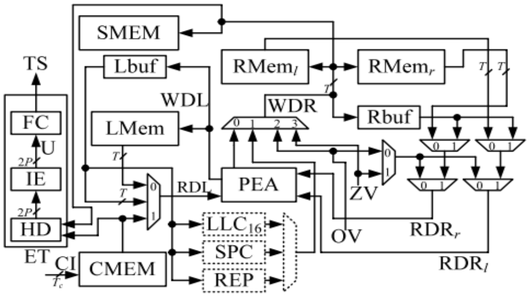


FIG. 3. CRYPTOGRAPHY TOP ARCHITECTURE.

IV. RESULTS

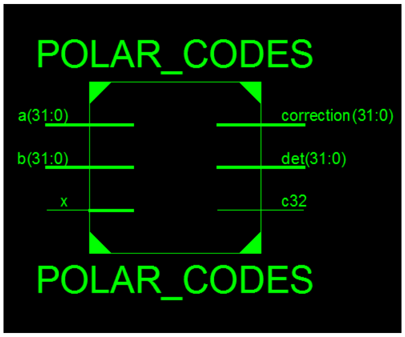


Fig. 4. RTL SCHEMATIC

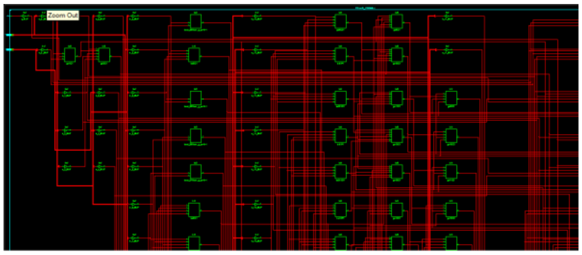
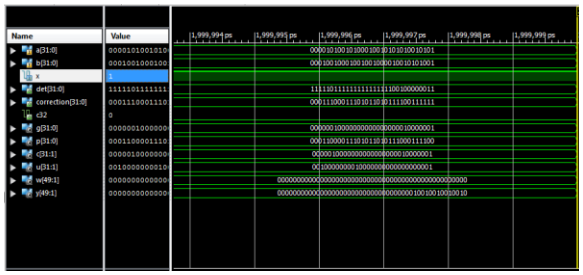


Fig. 5. TECHNOLOGY SCHEMATIC



```
Name              Value
a[31:0]           0000101001010     00001010010100010010101010010101
b[31:0]           0001001000100     00010010001001001000010010101001
x                 1
det[31:0]         1111101111111     11111011111111111111100100000011
correction[31:0]  0001110001110     00011100011101011010111100111111
c32               0
g[31:0]           0000001000000     00000010000000000000000010000001
p[31:0]           0001100001110     00011000011101011010111000111100
c[31:1]           0000010000000     0000010000000000000000010000001
u[31:1]           0010000000010     0010000000010000000000000000001
w[49:1]           0000000000000     0000000000000000000000000000000000000000000000000
y[49:1]           0000000000000     0000000000000000000000000000000000000100100100100 10
```

Fig. 6. OUTPUT WAVEFORM

V. CONCLUSION

In this paper we have discussed about the flooding belief propagation (FO-BP) algorithm and soft cancelation (SCAN) algorithm which has high signal to noise ratio. There are two efficient algorithms in SCAN they are RLSC and RCSC. These are proposed for the purpose of decoding algorithms. some of the VLSI architectures are given with particular length. The speed of this proposed algorithms are different they are for RLSC algorithm the speed is slow and coming to the RCSC algorithm the speed is fast.

REFERENCES

[1] J. Lin, C. Xiong, and Z. Yan, “A high throughput list decoder architecture for polar codes,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 24,

no. 6, pp. 2378–2391, Jun. 2016, doi: 10.1109/TVLSI.2015. 2499777.

[2] B. Yuan and K. K. Parhi, "Early stopping criteria for energy-efficient low-latency belief-propagation polar code decoders," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6496–6506, Dec. 2015.

[3] G. D. Forney, Jr., "Codes on graphs: Normal realizations," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 520–548, Feb. 2001.

[4] N. Hussami, S. B. Korada, and R. Urbanke, "Performance of polar codes for channel and source coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, South Korea, Jun./Jul. 2009, pp. 1488–1492.

[5] A. Eslami and H. Pishro-Nik, "On finite-length performance of polar codes: Stopping sets, error floor, and concatenated design," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 919–929, Mar. 2013.

[6] U. U. Fayyaz and J. R. Barry, "Low-complexity soft-output decoding of polar codes," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 5, pp. 958–966, May 2014.

[7] J. Xu, T. Che, and G. Choi. (2015). "XJ-BP: Express journey belief propagation decoding for polar codes." [Online]. Available: http://arxiv.org/abs/1504.06025

[8] S. M. Abbas, Y. Fan, J. Chen, and C.-Y. Tsui, "Low complexity belief propagation polar code decoders," in *Proc. IEEE Workshop Signal Process. Syst. (SiPS)*, May 2015, pp. 1–6. [Online]. Available: http://arxiv.org/abs/1505.04979

[9] Y. S. Park, Y. Tao, S. Sun, and Z. Zhang, "A 4.68 Gb/s belief propagation polar decoder with bit-splitting register file," in *Symp. VLSI Circuits Dig. Tech. Papers*, Jun. 2014, pp. 1–2.

[10] E. ¸Sa¸so˘glu, E. Teltar, and E. Arıkan, "Polarization for arbitrary discrete memoryless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, South Korea, Jun. 2009, pp. 144–148.

[1]**J. PRAVEEN** Completed M.Tech degree in VLSI System Design from Briilaint Institute Of Engineering Techonolgy, Jntu, Hyderabad. received the b.tech degree in Electronics And Communication Engineering from Teegala Krishna Reddy College Of Engineering And Techonolgy, Jntu, Hyderabad, in 2010, His area of interest is Low Power V.L.S.I, and Digital communication.

[2]Y.KIRAN working as Assistant professor in Teegala Krishna Reddy Engineering College. Completed M.Tech degree in VLSI System Design from Jawaharlal Nehru Institute of Technology, JNTU, Hyderabad, Received the B.Tech degree in Electronics and Communication Engineering from Scient Institute of Technology, JNTU, Hyderabad, in 2010, research interests include VLSI System design, Low Power VLSI.