Design of Partially Parallel Polar Encoder Architecture

A.Balaji[1] M.Srujana[2]
[1]M.Tech. Student [2]Associate Professor
[1,2]Department of Electronics & Communication Engineering
[1,2]Pathfinder Engineering College (PECH), Thimmapur, Hanamkonda, Warangal Telangana, India

Abstract— The polar writing was one among the most effective error correcting code attributable to the channel achieving property. The prevailing parallel encoder was additionally higher and simple to implement however it's not applicable for long polar codes as a result of it needed Brobdingnagian space quality. During this paper it consist a main purpose of encryption method with terribly giant scale integration it proposes a re-placement encryption style which might applicable for long polar codes. because the projected polar encoder will applicable for any style and any polar code with high performance and fewer hardware quality.

Key words: ECC, Encoding, Parallel Processing, Butterfly Architecture

I. INTRODUCTION

POLAR CODE is also a brand new class of error-correcting codes that incontrovertibly achieves the potential of the underlying channels. additionally, concrete algorithms for constructing, encoding, and cryptography the code unit all developed. as a results of the data rate achieving property, the polar code is presently thought of as a significant breakthrough in committal to writing theory, and additionally the relevance of the polar code is being investigated in many applications, as well as information storage devices.

Although the polar code achieves the underlying channel capacity, the property is asymptotical since a good error correcting performance is obtained once the code length is sufficiently long. To be close to the information rate, the code length got to be a minimum of 220 bits, and many of literature works introduced polar codes ranging from 210 to 215 to achieve sensible error-correcting performances in observe. in addition, the dimensions of a message protected by associate error-correcting code in storage systems is mostly 4096 bytes, i.e., thirty 2 768 bits, and is predicted to be long to 8192 bytes or sixteen 384 bytes inside the close to future. although the polar code has been thought-about being related to low quality, such associate degree extended polar code suffers from severe hardware quality and long latency. Therefore, associate degree style which will efficiently beware of long polar codes is critical to make the very-large-scale integration (VLSI) implementation attainable. varied divinatory aspects of the polar code, in conjunction with code construction and secret writing algorithms, square measure investigated in previous works, and economical secret writing structures are studied. ordered cancelation (SC) secret writing has been traditionally used , and advanced secret writing algorithms like belief propagation secret writing, list secret writing, and simplified SC square measure recently utilized. On the alternative hand, hardware architectures for polar coding have rarely been mentioned. Among several manuscripts coping with hardware implementation, given a straightforward coding style that processes all the message bits throughout a completely parallel manner. The wholly parallel style is intuitive and simple to implement, but it isn't acceptable for long polar codes as a results of excessive hardware quality. additionally, the partial total network (PSN) for associate SC decoder is taken into account a polar encoder. as a results of the character of ordered secret writing, however, the number of inputs is severely restricted inside the PSN, one or a try of bits at a time. Since a polar encoder sometimes takes the inputs from a buffer or memory of that bit dimension is far larger, the PSN is not acceptable for coming up with a general polar cryptography style. For the first time, this temporary analyzes the cryptography methodology inside the point of view of VLSI implementation and proposes a partially parallel style. The planned encoder is very participating in implementing a protracted polar encoder as a result of it will do a high turnout with tiny hardware quality.

II. POLAR ENCODING

The polar code utilizes the channel polarization development that each channel approaches either a superbly reliable or a completely screaming channel because the code length goes to eternity over a combined channel created with a collection of N identical sub channels. because the dependableness of every sub channel is thought a priori, K most reliable sub channels area unit accustomed transmit data, and the remaining sub channels area unit set to preset values to construct a polar (N, K) code. Since the polar code belongs to the category of linear block codes, the secret writing method may be characterized by the generator matrix. The generator matrix GN for code length N or 2n is obtained by applying the ordinal mathematician power to the kernel matrix

Given the generator matrix, the code word is computed by x = uGN, wherever u and x represent information and code word vectors, severally. Throughout this brief, we have a tendency to assume that data vector u is organized in a existence, whereas code word vector x is organized in an exceedingly bit-reversed order to alter the reason on the secret writing process. an easy totally parallel secret writing design was bestowed, that has secret writing quality of O(N log N) for a polar code of length N and takes n stages when N = 2n. for instance, a polar code with a length of sixteen is enforced with thirty two XOR gates and processed with four stages within the totally parallel encoder, the whole secret writing method is completed in an exceedingly cycle. The totally parallel encoder is intuitively designed supported the generator matrix, however implementing such associate encoder becomes a significant burden once an extended polar code is employed to realize a good error-correcting performance. In sensible implementations, the memory size and also the range of XOR gates increase as the code length will increase. None of the previous works has deeply studied the way to write the polar code with efficiency, although varied trade-offs

area unit doable between the latency and the hardware quality.

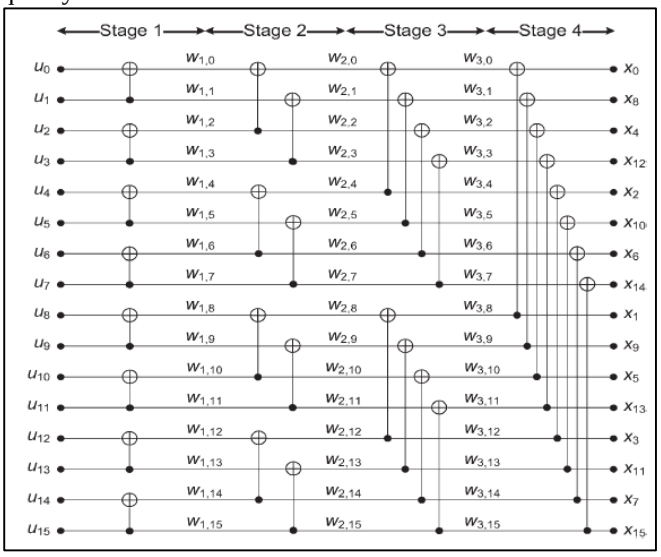

Fig. 1: Fully parallel architecture for encoding a 16-bit polar code

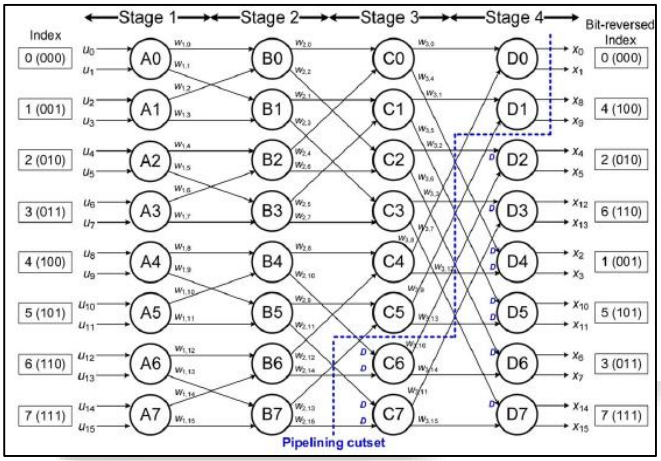

Fig. 2: DFG of 16-bit polar encoding

III. PROPOSED POLAR ENCODER

The approach and therefore the thanks to work the planning, a 4-parallel secret writing style for the 16-bit polar code is exemplified thoroughgoing. The all parallel secret writing style is initial transformed to a sunburst kind, therefore the period analysis and register allocation unit applied to the sunburst style. Lastly, the planned parallel style for long polar codes is portrayed

A. Folding Transformation

The folding transformation is wide accustomed save hardware resources by time-multiplexing several operations on a helpful unit. associate degree info flow graph (DFG) hold dear the absolutely parallel secret writing technique for 16-bit polar codes is shown in where a node represents the kernel operation F, and wij denotes the jth edge at the ith stage. Note that the DFG of the all parallel polar encoder is comparable to it of the quick Fourier work except that the polar encoder employs the kernel matrix instead of the butterfly operation. Given the 16-bit DFG, the 4-parallel folded style that processes four bits at a time is accomplished with swing two useful units in each stage since the helpful unit computes two bits at a time. among the folding transformation, decisive a folding set, that represents the order of operations to be dead in associate degree extremely helpful unit, is that the most crucial vogue issue. To construct economical folding sets, all operations with-in the absolutely parallel secret writing unit of measurement initial classified as separate folding sets. Since the input is in associate degree extremely cosmos, it's cheap to as an alternative distribute the operations among the consecutive order.

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$D(w_{1j})$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$D(w_{2j})$	1	1	2	2	0	0	1	1	1	1	-2	-2	0	0	-3	-3
$D(w_{3j})$	2	2	-2	-2	-0	-0	-0	-0	0	0	0	0	-2	-2	2	2
$D'(w_{1j})$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$D'(w_{2j})$	1	1	2	2	0	0	1	1	1	1	2	2	0	0	1	1
$D'(w_{3j})$	2	2	2	2	4	4	4	4	0	0	0	0	2	2	2	2

Fig. 3: Original delay requirements $D(w_{ij})$ and recalculated delay requirements $D^{'}(w_{ij})$

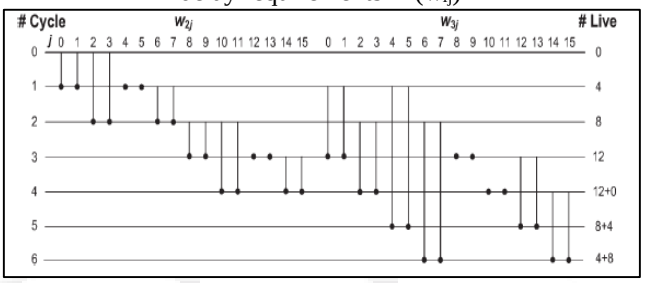

Fig. 4: Linear lifetime chart for w_{2j} and w_{3j}

Thus, each stage consists of two folding sets, each of that contains entirely odd or maybe operations to be performed by a separate unit. Considering the four-parallel input sequence in associate degree extremely natural order, stage one has two folding sets of associate degree. each folding set contains four parts, and therefore the position of a part represents the operational order among the corresponding helpful unit. two helpful units for stage one execute A0 and A1 at an equivalent time at the beginning and A2 and A3 at later cycle, so forth. The folding sets of stage a try of have identical order as those of stage one, i.e., and since the four-parallel input sequence of stage a try of is equal to that of stage one. what's a lot of, to envision the folding sets of another stage s, the property that the functional unit processes a mix of inputs whose indices disagree by 2s−1 is exploited. among the case of stage 3, two info whose indices disagree by four unit of measurement processed on, which suggests that the operational distance of the corresponding info is two as a result of the kernel helpful unit computes two info at a time. as associate degree example, w2,0 and w2,4 that come from B0 and B2 unit of measurement used as a result of the inputs to C0. Since every inputs got to be valid to be processed during a helpful unit, the operations in stage 3 unit of measurement aligned to the late input data. Cyclic shifting the folding sets right by one, which might be accomplished by inserting a delay of one live, is to vary full utilization of the helpful units by overlapping adjacent iterations. As a result, the folding sets of stage 3 area unit determined to and, where C6 among this iteration is overlapped with A0 and B0 among consecutive iteration. Among an equivalent manner, the property that the helpful unit processes a mix of inputs whose indices dissent by eight is exploited in stage

four. The folding sets of stage four area unit and , that unit of measurement obtained by cyclic shifting the previous folding sets of stage 3 by 2.

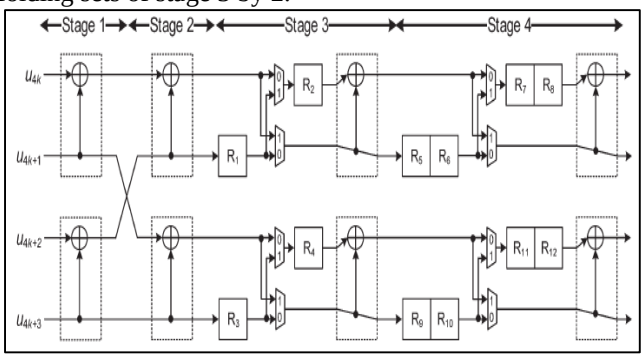

Fig. 6: Proposed 4-Parallel folded architecture for encoding the polar(16,K) codes

Sometimes speaking, a stage whose index s may be a smaller quantity than or equal to log2 P, where P is that the extent of correspondence, has an equivalent folding sets determined by equally interleaving the operations among the consecutive order, and another stage whose index s is larger than log2 P has the folding sets obtained by cyclic shifting the previous folding sets of stage s − one right by s − log2 P. Now, permit U.S. to have faith in the delay parts required among the folded style plenty of specifically. once a position wij from functional unit S to purposeful unit T incorporates a delay of d, the delay wants for wij among the F-folded style could also be calculated as

$$D(wij) = Fd + t - s \quad (1)$$

Where t and s denote the position among the folding set such as T and S, severally. Note that (1) may well be a simplified delay equation derived with assumptive that the kernel purposeful unit is not pipe-lined. The delay wants of the 4-folded design, i.e., D(wij) for one ≤ i ≤ 3 and nil ≤ j ≤ fifteen, area unit summarized in Fig. 3. as associate degree example, w2,0 from B0 to C0 demands one delay since d = zero, t = 1, and s = 0. Note that some edges indicated by circles have negative delays. For the folded style to be potential, the delay wants ought to be larger than or adequate zero for all the sides. Pipe lining or re temporal order techniques could also be applied to the all parallel DFG so as to create positive that its folded hardware has and delays. each edge with a negative delay got to be paid by inserting a minimum of 1 delay part to create the price of not negative. we've to create positive that the two inputs of associate degree operation undergo constant type of delay components from the start points. If they are utterly completely different, additional delay parts sq. live inserted to create the ways in which has constant delay parts. In Fig. 3, as associate degree example, four edges with zero delays area unit specially marked with negative zeros since additional delays area unit necessary due to the try of the quantity of delay parts. The DFG is pipe lined by inserting delay components, as shown in Fig. 2, where the line indicates the pipeline cut set associated with twelve delay components. The de-lay wants of the pipe lined DFG D(wij) unit of measurement recalculated supported and shown at all-time low of Fig. 3. As a result, eight purposeful units and forty eight delay components in total unit of measurement enough to implement the 4-parallel 4-folded coding style supported the folding sets.

B. Period Analysis and Register Allocation

Allocated at the corresponding cycle. With taking into thought the 4-parallel method, variables ar strictly assigned to registers in associate degree extremely forward manner. In Fig. 5, Associate in Nursing arrow dictates that a variable detain associate degree extremely register is migrated to a distinct register, and a circle indicates that the variable is consumed at the cycle. for instance, w2,0 and w2,4 area unit consumed in associate degree extremely sensible unit to execute operation C0 that generates w3,0 and w3,4. At an equivalent time, w2,1 and w2,5 ar consumed in another sensible unit to execute operation C1 that produces w3,1 and w3,5. The migration of the other variables springs by following the register allocation table. Finally, the following 4-parallel pipe lined structure projected to encrypt the 16-bit polar code is illustrated in Fig. 6, that consists of eight sensible units and twelve delay parts. A try of 2 sensible units takes guilty of one stage, and thus the delay parts area unit to store variables in line with the register allocation table. The hardware structures for stages one and some of is foursquare accomplished as no delay parts ar necessary in those stages, whereas for stages 3 and 4, several multiplexers area unit placed before of some sensible units to assemble the inputs of the sensible units. The projected style ceaselessly processes four samples per cycle in line with the folding sets and thus the register allocation table. Note that the projected encoder takes a attempt of inputs in associate degree extremely world associate degreed generates a attempt of outputs in an extremely bit-reversed order, as shown in Fig. 2. as a result of the sensible unit among the projected style processes a attempt of 2 bits at a time, the projected style maintains the consecutive order at the input aspect and thus the bit reversed order at the output aspect if a attempt of consecutive bits is considered one entity

IV. SYNTHESIS &SIMULATION RESULTS

In this paper I have designed the proposing technique. This process is designed using Verilog HDL. The RTL description is synthesised and simulated in Xilinx ISE 13.2i. The simulated wave forms are presented below.

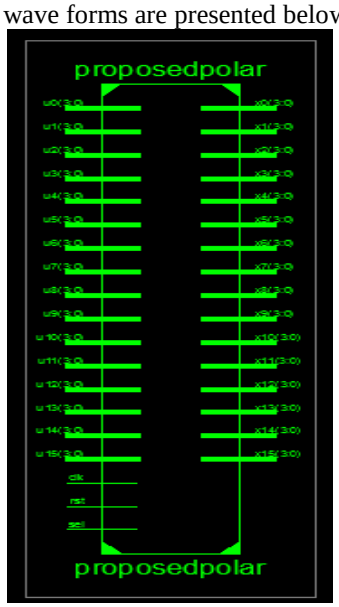

Fig. 7: Top level RTL schematic diagram

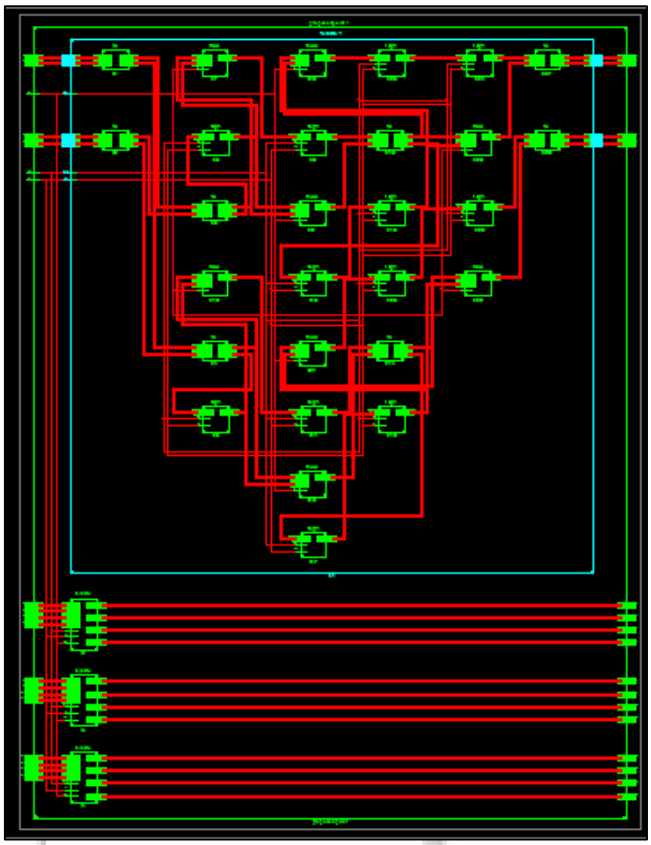

Fig. 8: Internal architecture of RTL schematic

Synthesis Results

polarcode1 Project Status (05/30/2016 - 21:40:09)			
Project File:	polarencoding.xise	**Parser Errors:**	No Errors
Module Name:	polarcode1	**Implementation State:**	Synthesized
Target Device:	xc7z010-3clg400	**• Errors:**	No Errors
Product Version:	ISE 14.5	**• Warnings:**	5 Warnings (2 new)
Design Goal:	Balanced	**• Routing Results:**	
Design Strategy:	Xilinx Default (unlocked)	**• Timing Constraints:**	
Environment:	System Settings	**• Final Timing Score:**	

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice LUTs	52	17600	0%
Number of fully used LUT-FF pairs	0	52	0%
Number of bonded IOBs	96	100	96%

Detailed Reports					[-]
Report Name	**Status**	**Generated**	**Errors**	**Warnings**	**Infos**
Synthesis Report	Current	Mon May 30 21:40:08 2016	0	5 Warnings (2 new)	4 Infos (4 new)
Translation Report					
Map Report					

```
Timing Details:
---------------
All values displayed in nanoseconds (ns)

=========================================================================
Timing constraint: Default path analysis
  Total number of paths / destination ports: 180 / 48
-------------------------------------------------------------------------
Delay:               1.106ns (Levels of Logic = 4)
  Source:            u14<3> (PAD)
  Destination:       x<47> (PAD)

  Data Path: u14<3> to x<47>
                                Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     IBUF:I->O             6   0.000   0.451  u14_3_IBUF (u14_3_IBUF)
     LUT3:I0->O            1   0.043   0.289  x<47>_SW0 (N01)
     LUT6:I5->O            1   0.043   0.279  x<47> (x_47_OBUF)
     OBUF:I->O                 0.000          x_47_OBUF (x<47>)
    ----------------------------------------
    Total                      1.106ns (0.086ns logic, 1.020ns route)
                                       (7.8% logic, 92.2% route)

=========================================================================

Cross Clock Domains Report:
--------------------------
```

Fig. 9: Simulation Result

V. CONCLUSION

This transient has conferred a current half parallel encoder style developed for long polar codes. Many improvement techniques area unit applied to derive the planned style. Experimental results show that the planned style can save the hardware compared therewith of the whole parallel style. Finally, the link between the hardware quality and conjointly the throughput's is analyzed to select out the foremost applicable style for a given application. Therefore, the planned style provides a wise resolution for writing associate degree extended polar code.

REFERENCES

[1] Hoyoung Yoo, Student Member, IEEE, and In-Cheol Park, Senior Member, IEEEPartially Parallel Encoder Architecture for Long Polar Codes

[2] E. Arikan, "Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels," IEEE Trans. Inf. Theory, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[3] R.Mori and T. Tanaka, "Performance of polar codes with the construction using density evolution," IEEE Commun. Lett., vol. 13, no. 7, pp. 519– 521, Jul. 2009.
[4] S. B. Korada, E. Sasoglu, and R. Urbanke, "Polar codes: Characterization of exponent, bounds, constructions," IEEE Trans. Inf. Theory, vol. 56, no. 12, pp. 6253–6264, Dec. 2010.
[5] I. Tal and A. Vardy, "List decoding of polar codes," in Proc. IEEE ISIT, 2011, pp. 1–5.
[6] K. Chen, K. Niu, and J. Lin, "Improved successive cancellation decoding of polar codes," IEEE Trans. Commun., vol. 61, no. 8, pp. 3100–3107, Aug. 2013.

