International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 08
July 2017

Reliable Architecuture of Viterbi Technic for Cryptography Applications

B. Sunil Kumar[1] ; S. Butchi Babu[2] ; T.Prasad Babu [3]

[1-2]assistant Professor Dept Of E.C.E Sri Sarathi Institute Of Engineering And Technology Nuzvid. Andhra Pradesh
[3]head Of The Department Dept Of E.C.E B.V.S.R Engineering College Chimakurthy. Andhra Pradesh

ABSTRACT : *Cryptography codes are ECC codes and consequently data rate is more. They are linear error correcting codes for transmitting a message over a noisy transmission channel. Cryptography codes are finding the increase use in applications requiring reliable and highly efficient information transfer over noisy channels. These codes are capable of performing near to Shannon limit performance, Low Decoding Complexity. The main advantage of the parity check matrix is the decoder can correct all single-bit errors. In this Paper Cryptography encoder and decoder architecture for coding 3-bit message vector will be analyzed and also designed using verilog.*

KEYWORDS: Cryptography, Parity matrix, Generator matrix, Shannon's Coding Theorem

I. INTRODUCTION

CRYPTOGRAPHIC architectures provide protection for sensitive and smart infrastructures such as secure healthcare, smart grid, fabric, and home. Nonetheless, the use of cryptographic architectures does not guarantee immunity against faults occurring in these infrastructures.

Defects in VLSI systems may cause smart usage models to malfunction. Extensive research has been done for detecting such faults in the cryptographic algorithms such as elliptic curve cryptography and the Advanced Encryption Standard (AES).

Design for reliability and fault immunity ensures that with the presence of faults, reliability is provided for the aforementioned sensitive cryptographic architectures. The proposed work presents false-alarm sensitive fault detection schemes for crypto structures (we note that to have a thorough analysis, we choose the Pomaranch stream cipher also known as a cascade jump controlled sequence generator (CJCSG).

Such false alarms could be exploited to induce distrust to the user, i.e., repetitive false detections result in either ignoring the alarms by the user or abandoning the devices in which the cryptographic architectures are embedded. From a user's point of view, at the very least, this is uncomfortable; however, false alarms could lead to financial loss if abandoning the crypto-architectures happens. Finally, such a false detection would result in higher dynamic power consumption, resulting in extra energy depletion especially for constrained applications. The uneven architecture of this cipher presents unique challenges, which are motivations to its choice for the proposed work.

We would like to emphasize that the proposed work can be applied to similar ciphers and this paper does not intend to

benchmark the algorithmic attacks or the performance efficiency for a certain cipher.

Pomaranch is classified in the hardware profile of European Network of Excellence for Cryptology. This stream cipher includes an uneven substitution box and has been the center of attention to achieve efficient hardware architectures. Natural defects, which are inevitable in VLSI systems call for protecting these architectures through detection mechanisms to preserve their reliability.

II. PRELIMINARIES

The structure of a jump register section includes jump control in (JC*i*) and out (JC*o*) signals, which are fed into and out of the section. The substitution box is part of this unit which nonlinearly affects the jump control out signal which is used as an input of the following section. Fig. 1 shows the aforementioned sections cascaded nine times to contribute to the key stream of the cipher. As observed in this figure, this accumulated cascade jump control in key stream generation mode combines the outputs of the nine sections to reach to the key stream needed.

As part of its key generation process, Pomaranch uses eight uneven substitution boxes with a 9-bit input and a 7-bit output. Each substitution unit is based on the inverse modulo an irreducible polynomial of degree nine, i.e., $x9 + x + 1$, whose period is 73. The 9-bit output is then converted into a 7-bit one with deletion of the most significant and least significant bits of the result. For the hardware implementations of the uneven substitution box of Pomaranch, multiple instances (memories or lookup tables) are needed.

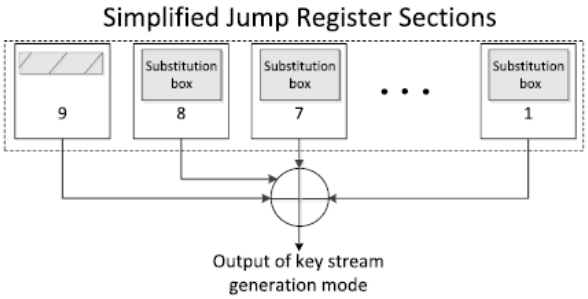

Fig. 1. Simplified accumulated cascade jump control.

In field-programmable gate array (FPGA) platforms, one needs to use block memories or distributed pipelined memories and in ASIC, memory macros or synthesized logic is needed which are not preferable for high-performance and low-complexity applications.

Thus, the inverse can be realized in composite fields such that the composite field $GF((23)3)$ is used through which the complexity of the operations needed for realizing the inverse is much reduced.The finite field $GF(29)$ is represented by elements (in terms of polynomials) of degree eight.

The field $GF(29)$ can also be represented as $GF((23)3)$, where, here, the elements of this composite field are given as polynomials of degree at most 2 with coefficients from $GF(23)$ [19]. We follow the representation in [19] and based on the search performed through the set of primitive polynomials of degree nine over $GF(2)$, it is determined that the polynomial $p(x) = x9+x7+x5+x+1$ is suitable for efficient architectures. Consequently, the polynomials $q(x) = x3+x+\gamma$ and $r(x) = x3+x+1$ are used as the

tower field polynomials for construction of the composite field operations. One can refer to [19] for detailed information and numeric examples. In this case, $(\alpha 7)9+\alpha 7+1 = 0$, eventually determining the linear transformation mapping polynomials modulo $x9 + x + 1$ to polynomials modulo $p(x)$.

In general, time and hardware redundancy are two main methods for fault diagnosis. Hardware redundancy adds hardware to the original structure for diagnosis and time redundancy repeats the operations two times for detection of transient faults.

Permanent faults through time redundancy can be detected using various methods which are, generally, denoted as recomputation with encoded operands. The fault diagnosis methods alarm the errors in the architectures; however, even if the overhead is acceptable, there could be a chance for false alarms, i.e., detection of faults that do not result in erroneous outputs. Such false alarms could be exploited to induce distrust to the user, i.e., repetitive, false detections result in either ignoring the alarms by the user or abandoning the devices in which the cryptographic architectures are embedded.

III. EFFICIENT ARCHITECTURES FOR THE SUBSTITUTION BOX

The substitution box is part of a unit in Pomaranch cipher which implements a key-dependent filter function, containing a 9-to-7-bit box and a balanced nonlinear Boolean function of seven variables. The 9-bit output of the substitution box is converted into a 7-bit one with deletion of the most significant and the least significant bits, as shown in Fig. 2. Composite fields can be utilized to realize the substitution box to achieve low-complexity architectures.

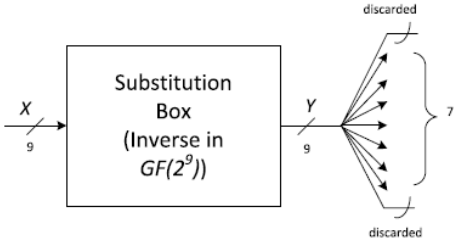

Fig. 2. 9-to-7 substitution box and its uneven structure.

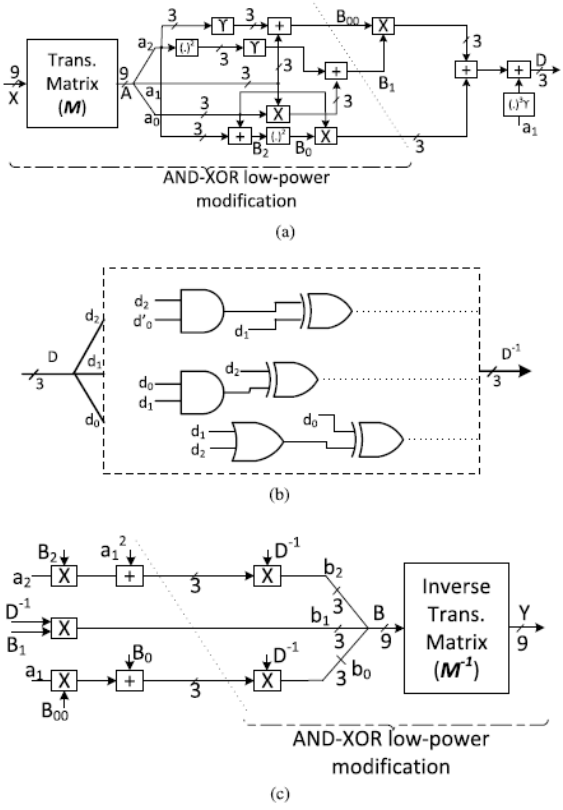

Fig. 3. Architectures for the composite field substitution box and the presented low-power modifications, (a) first subpart, (b) second subpart, and (c) third subpart.

The structure of the substitution box using composite fields is shown in Fig. 3. As shown in Fig. 3(a) and (c), a transformation matrix (M) transforms the elements in the binary field to the composite field $GF((2)3)$. Then, the operations are done in composite fields to achieve the inverse which is then retransformed to binary field using an inverse transformation matrix ($M-1$).

Eventually, the two most and least significant bits are discarded to get to the uneven structure of the substitution box of Pomaranch. The resulting transformation matrix M and its inverse $M-1$ are given in [19] (mapping vectors in $GF(2)$ defined by $x9+x+1$ to vectors in $GF((2)3)$ defined by $p(x)$ and $\gamma = \alpha 73$).

The operations used in composite fields include addition, multiplication (including multiplication with constant γ), squaring, cubing, and inversion in $GF(2)$. The architecture of the substitution box in Fig. 3 includes a first subpart [Fig. 3(a)] which contains the transformation matrix M whose input is shown by $X \in GF(2)$ to get an output of $A \in GF((2)3)$.

This 9-bit element is then divided into 3-bit elements denoted by $a2$, $a1$, $a0$ which are then processed to get the output of this subpart, i.e., $D \in GF(2)$. In Fig. 3(b) (second subpart), the inversion operation in $GF(2)$ is shown which yields to $D-1 \in GF(2)$. Finally, as shown in Fig. 3(c) (third subpart), $D-1 \in GF(2)$ is further modified to obtain 3-bit elements denoted by $b2$, $b1$, $b0$ in Fig. 3(c) and eventually $B \in GF((2)3)$, which is then retransformed by the inverse transformation matrix $M-1$ to get the output $Y \in GF(2)$ in the binary field, which is discarded eventually to a 7-bit output.

A. Low-Power Architectures

The substitution box occupies much of the area and consumes much of the power in Pomaranch. Based on our ASIC synthesis, the S-boxes occupy around 91% of the top-level key map and roughly 88% of the top-level power is consumed by the S-boxes. One needs to carefully pinpoint the approaches for realizing this unit so that the eventual architecture is usable for sensitive applications in various constrained smart infrastructures.

To reduce the dynamic hazards in the hardware implementations of the substitution box of the Pomaranch stream cipher for low-power designs, one can base the architectures devised on the propagation probability of signal transitions [20]. One observation is that XOR gates can increase the power consumption due to the fact that such logic gates have the probability of signal propagation of one and thus propagating all the hazards, increasing the power consumed. To achieve more low-power architectures for the substitution box of the Pomaranch stream cipher, we have restructured it so that a two-level logic, i.e., AND–XOR structure, is obtained for subparts one and three of composite field realization of the substitution box, i.e., Fig. 3(a) and (c), respectively. Specifically, in Fig. 3(a), the combined restructured

transformation matrix and part of logic gates in composite fields [specified in Fig. 3(a) by the curly bracket] are modified to achieve an AND–XOR structure.

Moreover, in Fig. 3(c), the combined restructured inverse transformation matrix and part of logic gates [shown in Fig. 3(c) by the curly bracket] are transformed into an AND–XOR structure for power preservation.

The original composite field structure and the two modified low-power ones [one with only the AND–XOR structure, as shown in Fig. 3(c), and the other with both of the modified architectures in Fig. 3(a) and (c)] are synthesized in ASIC and the area and power consumptions are derived and compared. We note that composite field realization is of paramount benefit for low-complexity architectures compared with memorymacros or synthesized registers on the ASIC platform. Moreover, power preservation will lead to low-energy solutions for sensitive and constrained, battery-powered embedded systems.

The proposed low-power architectures increase the area with the benefit of much decrease in power consumption. Indeed, based on the synthesis results, the power savings are much higher than the induced area for the structures. Specifically, at a typical working frequency, although the composite field architecture is 7% and 24% more area efficient than the proposed architectures, respectively, its power consumption is 19% and 47% higher compared with the proposed low-power structures, respectively (without much difference in the delay and thus frequency and throughput).

Specifically, the power consumption corresponding to the original architecture is 14.5 nW, which is reduced to 11.75 nW (at the expense of a 7% increase in area and a saving of 19% in power) and to 7.69 nW (at the expense of a 7% increase in area and a saving of 19% in power).

IV. PROPOSED SYSTEM

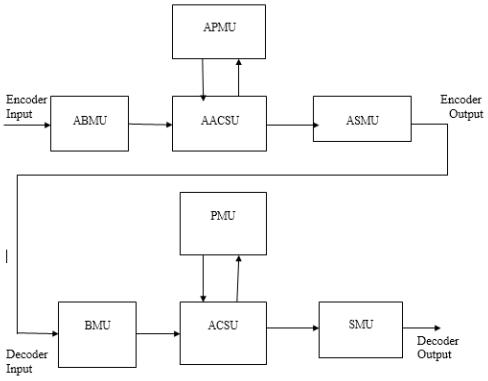

Fig. 4. Block Diagram Of Modified Cryptography

Modified cryptography consists of both encoder and decoder. Encoder converts the digital signal in to the analog signal. Decoder converts the analog signal into digital signal.

Encoder usually consists of the following major blocks:

4.1. Branch Metric Unit (ABMU)

4.2. Path Metric Unit (APMU)

4.3. Add–Compare–Select Unit (AACSU)

4.4. Survivor Management Unit (ASMU)

Encoder output is given as input to the decoder of the modified cryptography. cryptography algorithm for decoding a bit stream that has been encoded using convolution code or trellis code. A hardware cryptography decoder for basic code usually consists of the following major blocks:

4.1. Branch Metric Unit (BMU)

4.2. Path Metric Unit (PMU)

4.3. Add–Compare–Select Unit (ACSU)

4.4. Survivor Management Unit (SMU)

4.1. Branch metric unit (BMU)

A branch Metric Unit's function is to calculate branch metrics, which are normed distances between every possible symbol in the code alphabet, and the received symbol. There are hard decision and soft decision cryptography decoders. A hard decision cryptography decoder receives a simple bit stream on its input, and a Hamming distance is used as a metric. A soft decision cryptography decoder receives a bit stream containing information about the reliability of each received symbol.

4.2. Path metric unit (PMU)

A path Metric Unit summarizes branch metrics to get metrics for paths, where K is the constraint length of the code, one of which can eventually be chosen as optimal. Every clock it makes decisions, throwing off wittingly non optimal paths. The core elements of a PMU are ACS (Add-Compare-Select) units. The way in which they are connected between themselves is defined by a specific code's trellis diagram.

4.3. Add–Compare–Select Unit(ACSU)

The add–compare–select unit(ACSU) which selects the survivor paths for each trellis state, also finds the minimum path metric of the survivor paths.

4.4. Survivor Management Unit (SMU)

The survivor management unit (SMU) that is responsible for selecting the output based on the minimum path metric. Cryptography algorithm is called optimum algorithm since it minimizes the probability of error.

V. RESULT

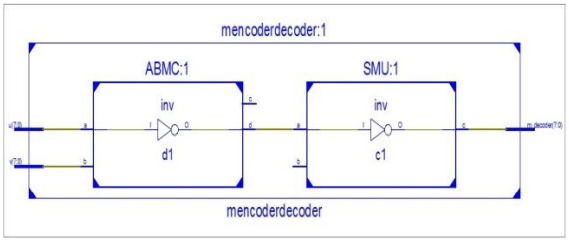

Fig. 5. RTL Schematic Diagram

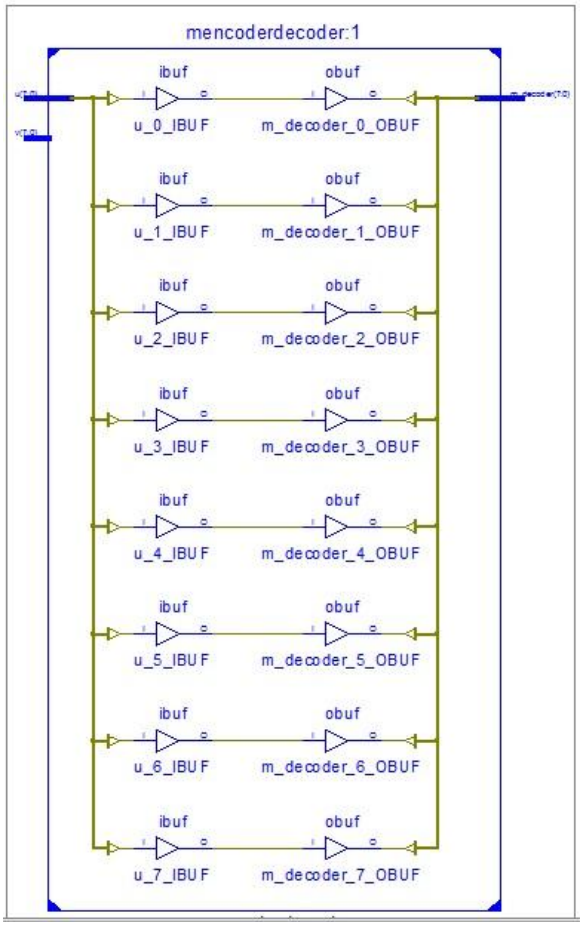

Fig. 6. Technologic Schematic

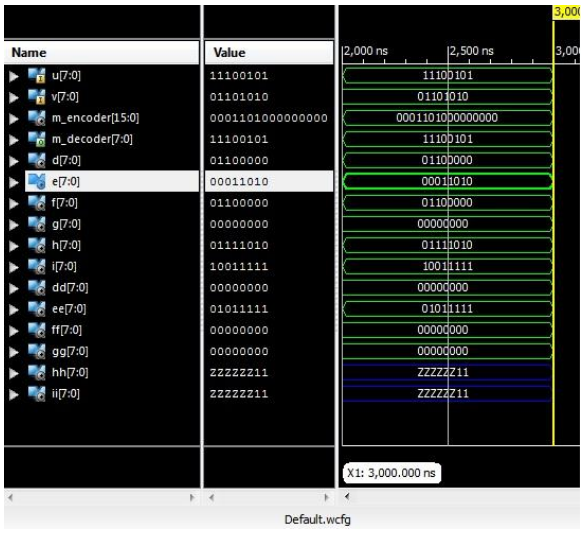

Fig. 7. Output Waveform

VI. CONCLUSION

Cryptography is a superior error correcting coding technique which allows further error modification and hence data rate of transmission is elevated. In this paper Design of Encoder, channel and Decoder is for a cryptography codes is presented. Coding is done using (7, 3) cryptography. Coding is done on HDL Designer Series and simulation results are obtained from Xilinx 14.7.

VII. REFERENCES

[1] SatyabrataSarangi and Swapna Banerjee, "Efficient Hardware Implementation of Encoderand Decoder for Golay Code", IEEE Transactions On Very Large Scale Integration (VLSI) Systems 2014. [2] Xiao-Hong Peng, Member, IEEE, and Paddy G. Farrell, Life Fellow, IEEE, "On Construction of the (24, 12, 8) Golay Codes", IEEE Manuscript received January 19, 2005; revised July 7, 2005 and December15, 2005, respectively.

[3] W. Cao, "High-speed parallel hard and soft-decision Golay decoder: Algorithm and VLSI-architecture," in Proc. IEEE Int. Conf. Acoust.,Speech, Signal Process. (ICASSP)., vol. 6. May 1996, pp. 3295–3297.

[4] Ayyoob D. Abbaszadeh and Craig K. Rushforth, Senior Member, IEEE, "VLSI Implementation of a MaximumLikelihood Decoder for the Golay (24, 12) Code", IEEE Journal on Selected Areas in Communications. VOL. 6, NO. 3, APRIL 1988.

[5] W. Cao, "High-speed parallel VLSI-architecture for the (24, 12) Golay decoder with optimized permutation decoding," in Proc. IEEE Int. Symp.Circuits Syst. (ISCAS), Connecting World, vol. 4. May 1996, pp. 61–64.

[6] P. Adde, D. G. Toro, and C. Jego, "Design of an efficient maximum likelihood soft decoder for systematic short block codes," IEEE Trans.Signal Process. vol. 60, no. 7, pp. 3914–3919, Jul. 2012.

[7] B. Honary and G. Markarian, "New simple encoder and trellis decoder for Golay Codes", ELECTRONICS LETTERS 9th December 1993 Vol. 29 No. 25.

[8] Michael Sprachmann, "Automatic Generation of Parallel CRC Circuits", 0740-7475/01/$10.00 © 2001 IEEE.

[9] Giuseppe Campobello, Giuseppe Patane`, and Marco Russo, "Parallel CRC Realization", IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 10, OCTOBER 2003.

[10] G. Solomon, "Golay encoding/decoding via BCH-hamming," Comput.Math. Appl., vol. 39, no. 11, pp. 103–108, Jun. 2000.

[11] I. Boyarinov, I. Martin, and B. Honary, "High-speed decoding of extended Golay Code," IEE Proc. Commun., vol. 147, no. 6, pp. 333–336, Dec. 2000. [12] D. C. Hankersonet al., Coding Theory and Cryptography The Essentials, 2nd ed. New York, NY, USA: Marcel Dekker, 2000.

[13] M.-H. Jing, Y.-C. Su, J.-H. Chen, Z.-H. Chen, and Y. Chang,"High-speed low-complexity Golay decoder based on syndromeweight determination," in Proc. 7th Int. Conf. Inf., Commun., SignalProcess. (ICICS), Dec. 2009, pp. 1–4.

[14] T.-C. Lin, H.-C. Chang, H.-P. Lee, and T.-K. Truong, "On the decoding of the (24, 12, 8) Golay Code," Inf. Sci., vol. 180, no. 23, pp. 4729–4736, Dec. 2010.

B. SUNIL KUMAR[1] working as Assistant Professor in S.S.I.E.T, nuzvid. He has 10 years of teaching experience. His area of interest is V.L.S.I Design.

S. BUTCHI BABU[2] working as Assistant Professor in S.S.I.E.T, Nuzvid. He has 3 years of teaching experience with research interest designing of circuits.

T.PRASAD BABU[3] working as Associate Professor & H.O.D in B.V.S.R Engineering College, Chimakurthy. He has 14 years of teaching experience. His area of interest is V.L.S.I Frontend Design.