DESIGN AN HIGH SECURITY CRYPTOGRAPHY USING GALIO FIELD

S. CHANDRIKA
M.TECH – SCHOLAR – E.C.E
Dept. of E.C.E
MALINENI LAKSHMAIAH WOMENS ENGENERING COLLEGE
GUNTUR DT.
K. RAVI KUMAR
ASSISTANT PROFESSOR
Dept. of E.C.E
MALINENI LAKSHMAIAH WOMENS ENGENERING COLLEGE
GUNTUR DT.

Abstract- This paper presents a new bit-parallel cryptography for the finite field GF (2m) generated with an irreducible all-one polynomial. Redundant representation adder is used to reduce the time delay of the proposed cryptography. In this project, we will propose an efficient VLSI architecture for cryptography implement it with an FPGA design methodology in order to provide a high-speed and last-effective cryptographic hardware.

I.INTRODUCTION

NONBINARY low-density parity-check (NB-LDPC) codes have become an interesting alternative to their binary counterparts for applications requiring small to moderate code word lengths and large rates. The main limitation of a wider use of NB-LDPC codes is that the complexity of the decoder limits the maximum throughput that can be achieved with their hardware implementations. NB-LDPC is lineal block codes characterized by a sparse parity check matrix H with *M* rows and *N* columns. Each nonzero element *hm,n* of H belongs to the Galois field GF*(q* = 2*p)*. In this paper, we only consider regular NB-LDPC codes with constant row weight *dc* and column weight *dv* . NB-LDPC codes can also be characterized by a bipartite graph called Tanner graph [1], where two types of nodes can be differentiated, the ones representing the rows of the parity check matrix called check nodes (CNs) and the ones that represent the columns in H, called variable nodes (VNs). Decoding algorithms for NB-LDPC codes use iterative message exchange between the CNs and the VNs and vice versa to estimate the most reliable code word from the noisy received sequence. Different decoding algorithms have been proposed since the Q-ary sum product algorithm (QSPA) [2]. The complexity of SPA is too large to be suitable for hardware implementations, and several approaches, such as fast Fourier transform- SPA [3], log-SPA, and max-log-SPA [4], were proposed to overcome its limitations. These solutions reduce the complexity of the CN processing equations without introducing any performance loss. In [5], an approximation of QSPA called extended min-sum (EMS) has been proposed, where the complexity of the CN is reduced considerably involving only comparisons and additions. Later, the min–max algorithm was proposed [6], which uses comparisons with compute the maximum reliability values instead of additions, unlike the EMS algorithm. This new solution helps preventing the growth of the data length of the decoder without introducing any performance loss with respect to the EMS algorithm. On the other hand, EMS and min–max algorithms still suffer from a bottleneck at the CN caused by the use of forward backward metrics for the extraction of check to variable messages. In [7], the trellis EMS (T-EMS) has been introduced, for computing the combination of the most reliable messages while avoiding the use of forward-backward metrics and, therefore, increasing the degree of parallelism. The decoder presented in [7] was improved in [8] where an extra column is added to the original trellis with the purpose of generating in a parallel way the check to variable messages. This algorithm allows to derive higher throughput architectures. The main drawback of the approach presented in [8] is that it requires a lot of area in its proposed structure, reducing the overall efficiency of the decoder. Today the communication has entered into our daily lives in many different forms; it is very difficult to lead a life without various appliances which plays a major role in communication. Conveying information through the exchange of thoughts, messages or information as by speech, visuals, signals, writing or behavior is the process of communication. Hence the need for efficient and reliable communication system has been rapidly rising in recent years. Hence several technologies have been developed in order to increase the long range communication and automatic data processing equipment. In recent years the need for efficient and reliable communication system is rising rapidly. So several technologies has been developed to achieve such communication system. The design should have high throughput and provide effective data transmission with minimum error rate. Many channels have been subjected to noise, thus errors may be introduced when it is transferred from sender to the receiver. Hence several error controlling techniques have been introduced in order to

detect and correct the error. One such technique is LDPC (Linear Density Parity Check). LDPC codes have the potential for highly parallel decoder implementation, and many high-throughputs LDPC decoders were reported. For a channel decoder used in mobile communications, the ability to support various levels of correction capabilities and code rates is a mandatory requirement. When designing an efficient multimode decoder, we must first find the similarity among different modes and then implement the common parts as reusable hardware components. Flexibility can be achieved by controlling the data flow through these reusable components. Since it is difficult to design a flexible architecture such that most hardware resources can be reused in different modes using a fully parallel architecture, a memory based partially parallel architecture is widely adopted in multimode LDPC decoder designs. Trellis modulation scheme is a modulation scheme which allows an efficient transmission of data over a band limited channels.

.II. EXISTED SYSTEM

In this section, the design of the CN unit based on TMM algorithm is explained. Where parallel processing is adopted to generate the output messages *Rm,n(a)*. The first step in the CN processing requires transformation from the normal domain to the delta domain. This delta domain transformation is made using a permutation network similar to the one proposed in [14]. This network requires $q \cdot \log2(q)$ multiplexors of two inputs to perform the delta domain transformation of each input vector message Qm,n. Therefore, the CN requires *dc* permutation networks where multiplexors are addressed by tentative hard decision symbols *zn*. The same structure is used for inverse transformation to normal domain applied to output messages *_Rm,n(a)*, where instead of addressing multiplexors using tentative hard decisions symbols, $zn + \beta$ sum is applied. The CN syndrome β is calculated adding all *dc* tentative hard decision symbols.

This is performed using a GF adder in a tree structure fashion. The next step of the CN processing involves the implementation of the function ψ, which extracts the two most reliable messages for each symbol $a \in GF(q)$.

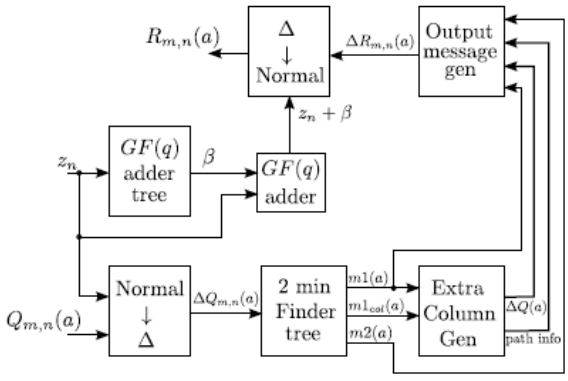

FIG.1 EXISTED SYSTEM

This function is implemented using a 2-min finder tree structure where also the position of the first minimum is extracted. Only $q-1$ cellsare required to implement all functions, because in delta domain messages the most reliable symbols remains on $\eta j = 0$ in the delta domain and their magnitudes are equal to zero. Each ψ function requires *dc* inputs because of the processing based on the trellis reordering of the delta messages. The approach followed to implement the ψ function is the tree structure proposed on since it provides a good tradeoff between the area and latency.

III. PROPOSED SYSTEM

Substitution in DES is done by S-boxes. A 6-bit value with a 4-bit value is substituted by each box. We need eight S-boxes to create a 32-bit half block. Substitution in AES is done through Sub Bytes transformation that transforms a whole state to another state. However, we can say that Sub Bytes actually substitutes 16 bytes with new 16 bytes. The Sub Bytes transformation is repeated in each round. So we have *Nr* of this transformation. Sub Bytes Transformation The Sub Bytes transformation is a non - linear byte substitution that operates independently on each byte of the State using a substitution table (S-box). This S box which is invertible is constructed by composing two transformations.

SHIFT ROW TRANSFORMATION:

This implies that the action of shifting rows is particularly simple, just performing left circular shifts of rows 1, 2 and 3, by amounts of 1, 2, and 3 bytes respectively. Row 0 is not changed. In the decryption process, the action of inverse shifting rows is particularly simple, just performing right circular of rows 1, 2, and 3, by amounts of 1, 2, and 3 bytes. Row 0 is not changed.

These circular shifts in the opposite direction for each of the last three rows (the first row was unaltered to begin with) is performed by the Inverse Shift Row(known as Inv Shift Row). This operation may not appear to do much but if you think about how the bytes are ordered within state then it can be seen to have far more of an impact. It should be remembered that it is treated as an array of four byte columns, i.e. the bytes 1, 2, 3 and 4 actually represents the first column. A linear distance of four bytes is a one byte shift.

The four bytes of one column are spread out to four different columns and it is ensured by the transformation. The Shift Rows column is depicted here as a linear shift which gives a better idea how this section helps in the encryption.

G.F. ADDER:

The Galois field multiplier and adder are elaborated in detail, while the circuits that perform the other operations are described briefly. The proposed implementations are compared to binary versions and to those MVL versions that can be obtained using known synthesis methods. The chapter is concluded with remarks about the possible systematic synthesis methods that would employ the techniques introduced while developing these circuits.

Galois field circuits are useful in many applications, from error correcting code encoders to cryptographic protection devices to interleaved memory controllers. Many researchers have invested the Binary Galois field circuits . Much less work has been done on MVL versions of such circuits We will give an informal introduction to Galois fields in this section; for a thorough treatment the reader can consult the literature.

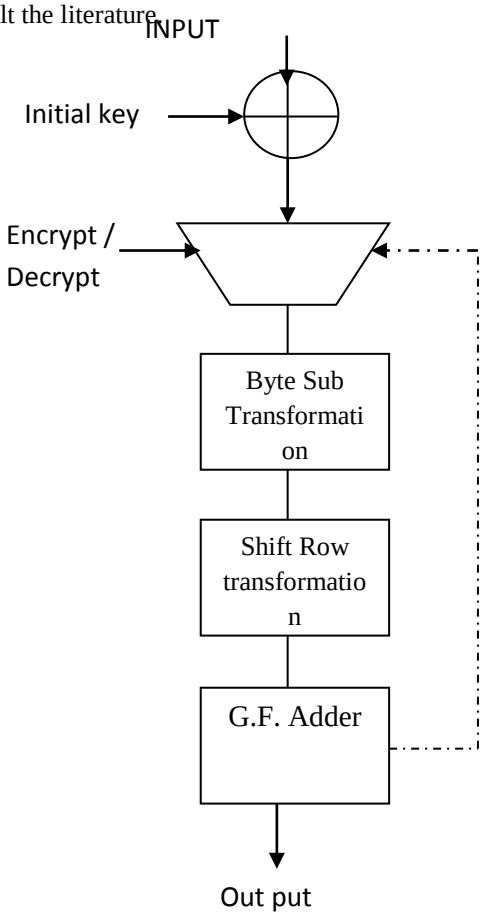

FIG.2 PROPOSED SYSTEM

Text on the topic Several MVL current-mode CMOS GF4 circuits are presented in this section. An adder and a multiplier are described in detail, while less commonly used division and exponentiation circuits are described briefly. We will use the fact that GF4 is of characteristic two to derive a simple implementation of the addition circuit. Note that the absolute difference circuit will produce the output with diagonal elements equal to zero. We can see, the addition differs from the absolute difference in only two entries of the addition table. Therefore, an attractive realization of the addition operation is to use the absolute difference plus a correction circuit for the two entries outlined. We have considered another implementation of the GF4 adder, which uses a pass-transistor network design style. The GF4 adder function can be implemented by decomposing.

IV RESULT

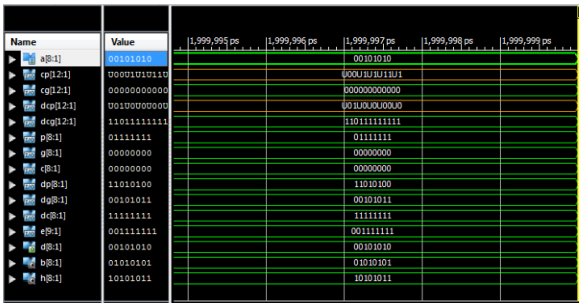

FIG.3 OUTPUT GRAPH

V CONCLUSION

In this paper, a new bit-parallel cryptography architecture for all-one polynomial is proposed. Redundant representation adder is used to reduce the time delay of the proposed cryptography. In this project, we implemented an efficient VLSI architecture for cryptography implement it with an FPGA design methodology in order to provide a high-speed and last-effective cryptographic hardware.

REFERENCES

[1] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

[2] M. C. Davey and D. MacKay, "Low-density parity check codes over GF(q)," *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 165–167, Jun. 1998.

[3] L. Barnault and D. Declercq, "Fast decoding algorithm for LDPC over GF(2*q*)," in *Proc. IEEE Inf. Theory Workshop*, Mar./Apr. 2003, pp. 70–73.

[4] H. Wymeersch, H. Steendam, and M. Moeneclaey, "Log-domain decoding of LDPC codes over GF(q)," in *Proc. IEEE Int. Conf. Commun.*, vol. 2. Jun. 2004, pp. 772–776.

[5] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over GF(q)," *IEEE Trans. Commun.*, vol. 55, no. 4, pp. 633–643, Apr. 2007.

[6] V. Savin, "Min-max decoding for non binary LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 960–964.

[7] E. Li, K. Gunnam, and D. Declercq, "Trellis based extended min-sum for decoding nonbinary LDPC codes," in *Proc. 8th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Nov. 2011, pp. 46–50.

[8] E. Li, D. Declercq, and K. Gunnam, "Trellis-based extended min-sum algorithm for non-binary LDPC codes and its hardware structure," *IEEE Trans. Commun.*, vol. 61, no. 7, pp. 2600–2611, Jul. 2013.

[9] F. Cai and X. Zhang, "Relaxed min-max decoder architectures for nonbinary low-density parity-check codes," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 21, no. 11, pp. 2010–2023, Nov. 2012.

[10] C. Poulliat, M. Fossorier, and D. Declercq, Design of regular (2,d*c*)-LDPC codes over GF(q) using their binary images," *IEEE Trans. Commun.*, vol. 56, no. 10, pp. 1626–1635, Oct. 2008.