International Journal of Research Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

A NOVEL SECURITY CRYPTOGRAPHY USING REVERSIBLE GATES

[1]PERAM VENKATESWARA REDDY , [2]SANKARA RAO KAMINENI
[1]M.TECH SCHOLAR, MALINENI PERUMALLU EDUCATIONAL SOCIETY'S GROUP OF INSTITUTIONS, GUNTUR
[2]PROFESSOR, MALINENI PERUMALLU EDUCATIONAL SOCIETY'S GROUP OF INSTITUTIONS, GUNTUR

ABSTRACT: In this paper, a novel architecture of encryption and decryption using high security technique for the VLSI implementation for encryption and decryption using reversible data. The pre-defined keys are required for each input for both encryption and decryption that are generated in real-time by the key-scheduler module by expanding the initial secret key and thus used for reducing the amount of storage for buffering. S-boxes are used for the implementation of the S.R, M.C and inverses S.R & M.C shared between encryption and decryption. The round keys needed for each round of the implementation are generated in real-time. The forward and reverse key scheduling is implemented on the same device, thus allowing efficient area minimization. Rather Than Using logical gates we are using PG gate for speed of operation. The pipelining is used after each standard round makes fast of operation to enhance the throughput and shift row mix column technique gives high security. The fault tolerance gives error free output than existed cryptography applications. These total design is designed with reversible gates to make less power for high speed applications.

Key words: reversible gate , Encryption, Decryption, S-box.

I.INTRODUCTION

Now-a-days, the power dissipation of devices is increasing with the technological advancement. Reversible logic gates attracted the attention of researchers due to its ability to reduce power dissipation.

Irreversible gates produce energy loss due to the information bits lost during computation process. Due to less no. of generated output signals information loss occurs than what is applied.

In 1961, According to R. Landauer's principle, irreversible logic gates dissipates KTln2 joules of energy for the loss of 1-bit information, where K is the Boltzmann constant and T is the absolute temperature. The operation performed is that the power dissipation is directly proportional to the number of information bit loss. In 1973, Charles Bennet proposed that, logic circuit must be built from reversible circuit to avoid heat dissipation; since there is no information loss occurs. Initially, in the design of reversible logic circuits, design was limited to combinational logic circuits. It was just because of the convention that the feedback is not allowed in the reversible computing. However, in 1980, Toffoli has shown that the feedback is allowed in reversible computing. According to Toffoli, a sequential network is reversible if its combinational part is reversible.

We proposed reversible realization of two shift registers naming Serial-in Serial-out and Serial-in Parallel-out for their application in designing sequence pulse generator. We also presented novel reversible architecture of Linear Feedback Shift Register (LFSR) and Parallel Signal Analyzer (PSA). The input bit of LFSR is a linear function of its last state in computing.

II. BRIEF OVERVIEW OF REVERSIBLE GATES

The laws of physics are essentially reversible. If any physical process (f) relates input (x, y) and outputs (z) such that, Z = f (x, y), the laws of reversibility verifies that for any given output z, the inputs, x & y are deductible. But the classical computers ignore this law of reversibility. For example, in an AND function, for output z = 0, the inputs cannot be exactly deducible as there 3 sets of inputs that make z = 0.

We assume the followings to describe a generalized reversible gate:

i) Set of domain variable = {x1, x2, …..,xn}

ii) Set of controls = C & the no. of elements in C defines the width of gate

iii) A Target = T

There are some reversible basic gates which we are going to use in design of Registers and are as follows:

A. NOT Gate

It is a simple 1 input and 1 output (1*1) reversible logic gate which implement inversion of input. It has unit quantum cost and unit delay.

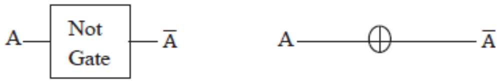


Fig 1. NOT gate and its quantum representation.

B. Controlled-V and Controlled-V+ Gate

Controlled V and V+ are the basic gates. In the controlled-V gate when the control signal A = 0, then the input B on target line will pass through the controlled part unchanged, that is Q = B. When A = 1, then the unitary operation V is applied to the input B, and output will be Q = V(B).

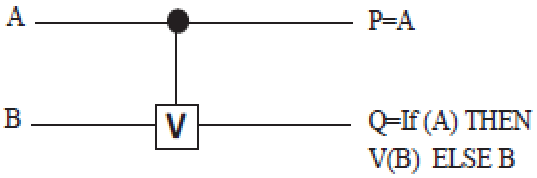


Fig 2. Quantum representation of Controlled-V.

In the controlled-*V+* gate when the control signal A = 0, then the input B will pass through the controlled part unchanged, that is Q = B. When A = 1, then the unitary operation *V+= V-*1 is applied to the input B, that is, Q = *V+*(B).

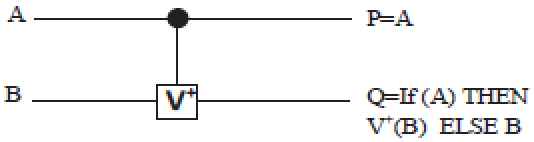


Fig 3. Quantum representation of Controlled-V$^+$.

The V and *V+* gates have the following properties:

$$V \times V = NOT$$
$$V \times V+ = V+ \times V = I$$
$$V+ \times V+ = NOT$$

C. Controlled-NOT Gate/ Feynman Gate

It is a 2*2 reversible logic gate. CNOT Gate, also known as FEYNMAN Gate. It is used to overcome the fan-out problem since it can be used for copying the information. CNOT gate has unit quantum cost and unit delay.

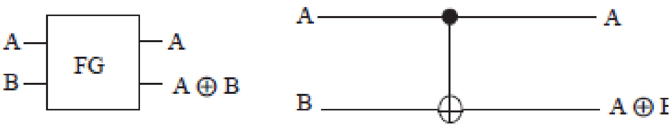


Fig.4 Feynman gate & its quantum representation.

D. Toffoli Gate

Toffoli gate is a 3*3 reversible gate with quantum cost of 5 and delay of 5Δ. It is called also universal reversible gate.

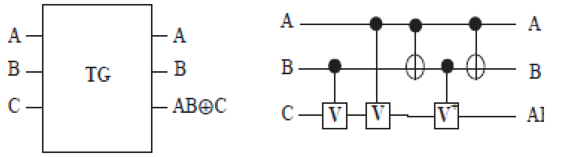


Fig.5 Toffoli gate and its quantum representation.

E. Fredkin Gate

Fredkin Gate is also a 3*3 gate. It has 5 quantum cost and delay is 5Δ. When A = 0, the other two inputs B and C is simply copied to the output. But when A = 1, B and C is swapped in the output. Hence, it is also denominated as a controlled swap gate. Basic logic function can be implemented using this gate and called universal reversible gate.

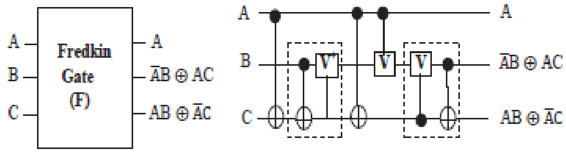


Fig 6. Fredkin gate and its quantum representation.

F. Peres Gate

Peres gate is a 4-input and 4-output (4*4) reversible gate. It has a minimum quantum cost among the 4*4 reversible gate and is equal to 4 and delay is 4Δ.

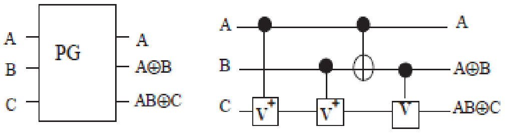


Fig 7. Peres gate and its quantum representation.

G. Proposed Modified Fredkin (MF) Gate

It is the proposed modified version of 3*3 Fredkin gate with a quantum cost of 4 and a delay of 4Δ. When A = 0, it is the same as Fredkin Gate, but when A = 1, B and complement of C is swapped in the output. Quantum representation of this gate is

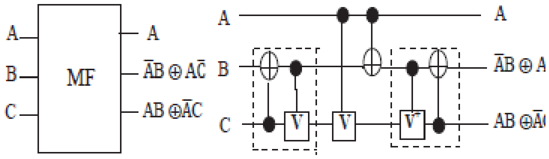


Fig 8. MF gate and its quantum representation.

III.PROPOSED SYSTEM

The fig: 9 shows the encryption block diagram with high security implementation. The initial stage having input and initial key goes under PG operation for less power consumption. This conversion of binary data to a matrix is totally carried out by byte sub transformation. Now the total matrix consisting of row and columns by using these we implemented the security by the hybrid crossbar technique.

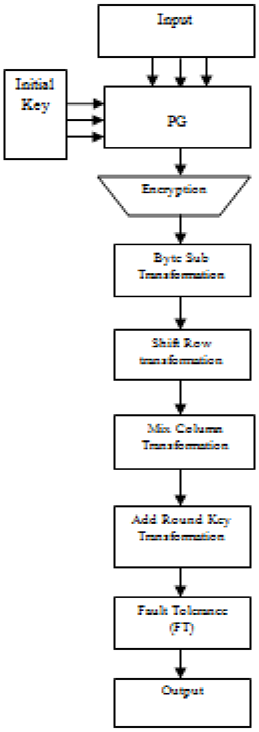


Fig 9. PROPOSED SYSTEM

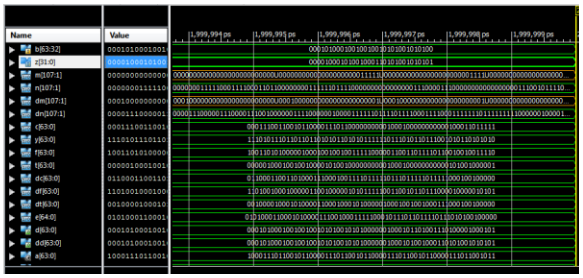
Shift Row transformation is one of the technique for security i.e. the total row is matrix is shifted to another row and with vice and versa. The second technique is mix column transformation it gives two columns into a single column to reduce the size. In another way we can make as comparison of two columns into a single column.

The add round key transformation is used rounding the nearest value of matrix. This represents the rounded output taken as 'e' for encryption block. After that Add round key is given to the Fault Tolerance. Next it is given to the output. The total encryption block is used in the transmitter side. The output of encryption block given to input to decryption block.
Similarly decryption block consisting of sub blocks as encryption with small inversion. So the input 'e' taken as input for decryption the input 'e' and final key goes under decryption with hybrid crossbar technique and the output of the decryption given to input as for inverse byte sub transformation. The inverse byte sub transformation divide the matrix representation into binary representation.

IV. RESULTS

The encryption and decryption is designed by using reversible gates. The total input bits of proposed encryption are multiplexed with the initial key by using Reversible gates. After that the encryption and by sub transformation, shift row mix column, add round key will be given to the input and output pins. Finally, the DD is the output as shown in the graphical representation of fig10.

The total operations of Byte sub transformation, Shift row transformation, Mix column transformation, Add round key transformation and Fault tolerance are operated with reversible gates to make the operation accurately and takes less power for high speed application.



```
Name          Value
b[63:32]      0001010001001
z[31:0]       0000100010100
m[107:1]      0000000000000
n[107:1]      0000000111110
dm[107:1]     0001000000000
dn[107:1]     0000111000001
c[63:0]       0001110011001
y[63:0]       1110101110110
f[63:0]       1001101010000
t[63:0]       0000010001001
dc[63:0]      0110001100110
df[63:0]      1101001000100
dt[63:0]      0010000100010
e[64:0]       0101000110001
d[63:0]       0001010001001
dd[63:0]      0001010001001
a[63:0]       1000111011001
```

Fig 10. OUTPUT WAVEFORM

V.CONCLUSION

A novel architecture of encryption and decryption using high security technique for the VLSI implementation using Reversible gates is implemented. The pre-defined keys are required for each input for both encryption and decryption that are generated in real-time by the key-scheduler module by expanding the initial secret key and thus used for reducing the amount of storage for buffering. S-boxes are used for the implementation of the S.R, M.C and inverses S.R & M.C shared between encryption and decryption. The round keys needed for each round of the implementation are generated in real-time. The forward and reverse key scheduling is implemented on the same device, thus allowing efficient area minimization. The fault tolerance circuit gives error free output than existed cryptography application. The total design is designed with reversible gates to make less power for high speed application.

VI.REFERENCES

[1] J. Rose *et al.*, "The VTR project: Architecture and CAD for FPGAs from verilog to routing," in *Proc. ACM/SIGDA FPGA*, 2012, pp. 77–86.
[2] Y. Hara, H. Tomiyama, S. Honda, and H. Takada, "Proposal and quantitative analysis of

the CHStone benchmark program suite for practical C-based high-level synthesis," *J. Inf. Process.*, vol. 17, pp. 242–254, Oct. 2009.

[3] A. Canis *et al.*, "LegUp: High-level synthesis for FPGA-based processor/accelerator systems," in *Proc. ACM/SIGDA FPGA*, 2011, pp. 33–36.

[4] E. Ahmed and J. Rose, "The effect of LUT and cluster size on deepsubmicron FPGA performance and density," *IEEE Trans. Very Large Scale Integr. (VLSI)*, vol. 12, no. 3, pp. 288–298, Mar. 2004.

[5] J. Rose, R. Francis, D. Lewis, and P. Chow, "Architecture of fieldprogrammable gate arrays: The effect of logic block functionality on area efficiency," *IEEE J. Solid-State Circuits*, vol. 25, no. 5, pp. 1217–1225, Oct. 1990.

[6] H. Parandeh-Afshar, H. Benbihi, D. Novo, and P. Ienne, "Rethinking FPGAs: Elude the flexibility excess of LUTs with and-inverter cones," in *Proc. ACM/SIGDA FPGA*, 2012, pp. 119–128.

[7] J. Anderson and Q. Wang, "Improving logic density through synthesisinspired architecture," in *Proc. IEEE FPL*, Aug./Sep. 2009, pp. 105–111.

[8] J. Anderson and Q. Wang, "Area-efficient FPGA logic elements: Architecture and synthesis," in *Proc. ASP DAC*, 2011, pp. 369–375.

[9] J. Cong, H. Huang, and X. Yuan, "Technology mapping and architecture evalution for k/m-macrocell-based FPGAs," *ACM Trans. Design Autom. Electron. Syst.*, vol. 10, no. 1, pp. 3–23, Jan. 2005.

[10] Y. Hu, S. Das, S. Trimberger, and L. He, "Design, synthesis and evaluation of heterogeneous FPGA with mixed LUTs and macro-gates," in *Proc. IEEE ICCAD*, Nov. 2007, pp. 188–193.

[11] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," *Commun. ACM*, vol. 56, no. 10, pp. 35–37, Oct. 2013.

[12] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

AUTHORS DETAILS:

Venkateswara Reddy Peram has completed her B.Tech in Electronics and Communication Engineering from Chinthalapudi Engineering College,J.N.T.U.K affiliated college in 2013.He is pursuing her M.Tech in VLSI from Malineni Perumallu Educational Society , J.N.T.U.K affiliated college.

Sankara Rao Kamineni is an Professor at Malineni Perumallu Educational Society Group of Institutions, Guntur. M.Tech, ECE from Sree Kavitha Engineering College, Karepalli, Khammam(Dt).