International Journal of Computer and Communication Technology

Volume 1 | Issue 4 Article 3

October 2010

Cellular Automata Based Data Security Scheme in Computer Network using Single Electron Device

Jayanta Gope
1,2Research Scholar, Dept. of Electronics and Telecommunication Engineering Jadavpur University, Kolkata, India, jayantagope@rediffmail.com

Giriprakash H
1,2Research Scholar, Dept. of Electronics and Telecommunication Engineering Jadavpur University, Kolkata, India, giriprakash@rediffmail.com

Subir Kumar Sarkar
Professor (Dr.), Dept. of Electronics and Telecommunication Engineering Jadavpur University, Kolkata, India, subirkumar@rediffmail.com

Cellular Automata Based Data Security Scheme in Computer Network using Single Electron Device

Jayanta Gope[1], Giriprakash H[2]
[1,2]Research Scholar,
Dept. of Electronics and Telecommunication Engineering
Jadavpur University, Kolkata, India
jayantagope@rediffmail.com

Subir Kumar Sarkar
Professor (Dr.),
Dept. of Electronics and Telecommunication Engineering
Jadavpur University, Kolkata, India

Abstract— ***The internet conceptualized new ways of social interaction, activities globally. Internet serves billions of users worldwide. By the end of 2011it is expected that 22% of the world's population will regularly surf internet. Beside this, internet incorporated high risks for e-users by enabling intruders to gain access via security holes. Network security is a course of action for assuring data from illicit accessing, exploitation, exposure, damage, alteration, or disorders related to the impulsive growth of popularity of e-users. Cellular Automata (CA) has been recommended in favor of the potential usage of data security. Single Electron devices (SED) have unanimously contributed in significant reduction of size of electronic devices and are now weighed up as the best substitute of future device family. Here we address a novel adaptive method to assimilate CA using SED in data security.***

Keyword: Network Security, Cryptography, Cellular Automata, Single Electron device, Tunnel Junction

I. INTRODUCTION

Significant data security is generauirement for the network users. But networking remains vulnerable due to potential hacking and the virus entries, which are the genuine risk factors. e-hackers are deliberately creating viruses, worms, malware, spyware, bots, etc., to hack users connected to internet. Corporate Houses, Government Bureaus, Financial Bodies, Medical Organizations, Educational Institutes are mostly targeted. Every day, somehow and somewhere all over the world, networks and even hosts are being hacked by budding and potential hackers. Three main factors that are prerequisite in risk free or comparatively better networking are

- Confidentiality: - Data should be accessible to the entitled users solely.
- Integrity: - Data have to be modified only by the authorized user.
- Availability: - In time access of data to authorized and authenticated user.

Cryptography is emerging as one of the fundamental tools for maintaining confidentiality, access controlling, e-payments, commercial safekeeping, and innumerable supplementary meadow [1-5].

A distinctive array of equal and preset condition of automata whose subsequent state is regulated exclusively by their present status and the position of their neighbours are known to be CA. A set of cells in CA is formatted in a gridiron in such a way that each cell updates its position as a function of time in accordance to a definite set of rules, which control the circumstances of neighbouring cells. By developing apt set of laws into CA, we are capable of simulating a lot of complex behavior required in data security procedures [6 and 7].

SED has innovative physical effects of charge transport. The uncomplicated circuit configuration process exhibits single electron charging effects in the single electron box. A tunnel junction connects a metal granule in one side where electrons can tunnel in and out. The Coulomb interaction process of the single charge controls the correlated electron tunneling in small capacitance structures. For the fabrication process the size and capacitance C of the tunnel junction is reduced sufficiently, thus the tunneling of only one e generates a noticeable change e/C of the voltage across the junction. A single e is adequate to pile up information, which could not be achieved for Transistor or CMOS circuits; moreover, the circuit can provide enough means of reducing the power consumption. Within single electron devices, a few electrons represent one bit of information and the power consumption is drastically reduced. Single electron devices let the manipulation of individual electrons, which are ultimately utilized in the form of the electron devices. Their prospective assimilation level is exceptionally high owing to its small size. The momentum power product is forecasted to lie close to the quantum limit set by the Heisenberg's uncertainty principle. The processing speed of such device will be virtually equivalent to electronic speed. The delicate sensitivity is about five orders of degree enhanced than conventional solid-state MOSFET transistors [8-10].

II. APPROACH OF DATA AUTHENTIFICATION TECHNIQUE USING CA

A data is authenticated only if it comes from its genuine source. Message authentification strategy should permit the user to verify about the unwanted occurrence of manipulation of the data. In this course of action a tag is generated at the sending node. The tag is the function of the secret key and the data to be sent. The sending node delivers the data & secret key consecutively in a proper cycle. In this process the sending node transmits the tags & data and the receiver separates them out sequentially at the receiving end. Next the tags & data are easily separated and are weighed against with the received tag. If they are equivalent then the data transferred amid the

transmitter and receiver is said to be authentic and bona fide. This process is given in fig.1which shows the state transition graph for the CA having characteristics matrix. The process of tag generation is described below. At the transmitting end let the key and data be defined as

$$key = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \text{ and } data = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

The tag is engendered using the rule90 and the rule150 on the key. The transmission end key is generated as following.

The rule150→ if at the 0^{th} column of any row, then perform
$tag\,[i] = key\,[i] \oplus key\,[i+1]$

If at the last [third here] column of any row, then perform
$tag\,[i] = key\,[i-1] \oplus key\,[i]$
Otherwise
$tag\,[i] = privatekey\ \ [i-1] \oplus privatekey\ \ [i] +$
$privatekey\ \ [i+1]$
The rule90→ if at the 0^{th} column of any row, then perform
$tag\,[i] = privatekey\ \ [i+1]$

If the last [third here] column of any row then perform
$tag\,[i] = privatekey\ \ [i-1]$

Otherwise,
$tag\,[i] = privatekey\ \ [i-1] \oplus privatekey\ \ [i+1]$

Using rule 150 and rule 90, the tag has been generated as

$$tag = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

Now the transmitted data is as follows:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

Tag Data

Now at the receiver side each part will be separated as

$$tag = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \text{ and } original\ data = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

Receiver should know the private key which is

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

The common practice is to send the tag, key and the original data which are matrices of same order sequentially at the receiving end. The user at the receiving end is familiar to the tag, secret key and the original data; hence separation is not a problem. However the secret key at the receiving end has to be similar with that of the transmitted key. By means of the secret key and the original data another tag is generated and is compared with that of the transmitted key. Now if they happen to be identical then the data transmission is authenticated since no one rather the sender and receiver is acquainted with their secret key.

The data recovery method from the tags is accomplished in the following mode. By the side of the transmitting end, every column of data matrix use the 90 and 150 rules in the similar approach as that of the authentication format stated above. The receiver after receiving the tags performs the comparative operation for each of the tags with the matrix generated by applying the 150 rule to the key. In fact all the row of the first tag is compared to recover the first column data vector. On behalf of data comparison in case of a match, a '1' is generated as data whereas '0' is generated for a mismatch. Later than comparing all the four tags the original data matrix is finally obtained. At the same time as only the tags are transmitted it is reasonably impossible to recuperate the data from the tags for an unauthorized user as the person doesn't know the key and the process of generating the tags. At the end, the confidentiality of the message is sustained [11-12].

III. CIRCUIT REALIZATION AND THE RESULTS OBTAINED

Rule 90 and 150 of CA are used here to apprehend the proposed SED based data security scheme. An individual cell of programmable CA is designed in fig.2 using SED. When rule line is high, the next state will follow the rule 150 but when rule line is low rule 90 will be considered. While the auto is low, the select line of the MUX is also low and the input I0 selected. Thus when auto is low the first bit is loaded into the cell. For better operation of CA auto is set to '1'. The Left data and the Right data are the inputs approaching from the neighboring cells. The SED based 4-bit 90-150 PCA is shown in fig.3. The complete SED based 4-bit 90-150 PCA is shown in fig.4 along with its corresponding timing diagram in fig.5. It

is evident that the circuit implemented at this point using single electron devices are in a 2D pattern. Binary information is programmed by SED orientation of electron devices. For the period of transmission 'M' is set to zero, the data is loaded into data register, and the consequence is that the PCA is set either to rule 90 or 150. Here we included two lines in favor of output: while M=0; it is transmission of data and the output is obtained from the 4-bit PCA for each one of the tags produced. When M=1; it is reception of data, the recovered data is drawn together from the output of the four D-flip flops connected at the bottom of the figure. For a (4X4) data matrix, this process cycles four times consecutively. For our design expediency, we used the same data as in the specified example. We observed that the correct data is recovered.

IV. CONCLUSION

The modus operandi of the circuit is rather speedy and it can accomplish a very high density of integration. Thus, the objective of reducing the size is achieved. The compactness and very less power consuming characteristics are very much intended and thereby rendering it appropriate for the utilization in present communication systems.

REFERENCES

[1] P.Kumar and A. Sinha, "Survey of Intrusion Detection Systems and Security Audit Analysis", Intl. Conf. on Quality, Reliability and Information Technology, Dec.21-23, New Delhi, 2000.

[2] A. Tanenbaum,"Computer Networks", 4th ed., Prentice Hall of India Pvt. Ltd., 2003.

[3] W. Sta;llings, "Data and Computer Communications,"7th ed., Perason Education Inc., 2006.

[4] Mark Curtin, "Introduction to Network Security"March 1997.

[5] Mark J. Cox, "Classification of Security Issues," 2005.

[6] D. R Stinson,"Cryptography: Theory and Practice, "CRC Press, 1995.

[7] W. Stallings,"Cryptography and Network Security – Principles and Practice", Prentice Hall, 2000.

[8] Subir Kumar Sarkar, **Anup Kumar Biswas**, P.C. Pradhan and N.R. Bandyopadhyay: " Single Electron devices and next generation digital electronics" International Conference on Computers and Devices For communication. CODEC-04, January, 1-3, 2004, Hyatt Regency Kolkata, India

[9] Prasanna Kumar Sahu, Anup Kumar Biswas and Subir Kumar Sarkar: " Realization of Fast Switching, Low power and Less apace Consuming Logic Circuits Using Single Electron devices" International Journal opf information and computing Sciences Vol. 7, June 2004, pp 54-66

[10] Subir Kumar Sarkar, Samir Kumar Sarkar, Jayanta Gope, Tarun Kumar Chatterjee, Senthil Kumar and Gautam .M.A "Single Electron Device Based Application Specific Integrated Circuit Design for Use in Stock Market" In National Conference on Advanced Computing and Computer Networks (NCACCN 2007), Vikhe Patil College of Engineering, Ahmednagar, Maharasthtra on 9-10 March 2007.

[11] David g. Green. "Cellular Automata", 1993

[12] Subir Kumar Sarkar, G.C.Manna, S.S.Sing, T.Dutta, Samir kumar sarkar and P. K. Naskar, "CDMA Technology Based Reliable Wireless Mobile Communication System on a single chip using Cellular Automata Concept", Journal of Engineering, computing & Architecture, vol.2 issue-1, 2008.

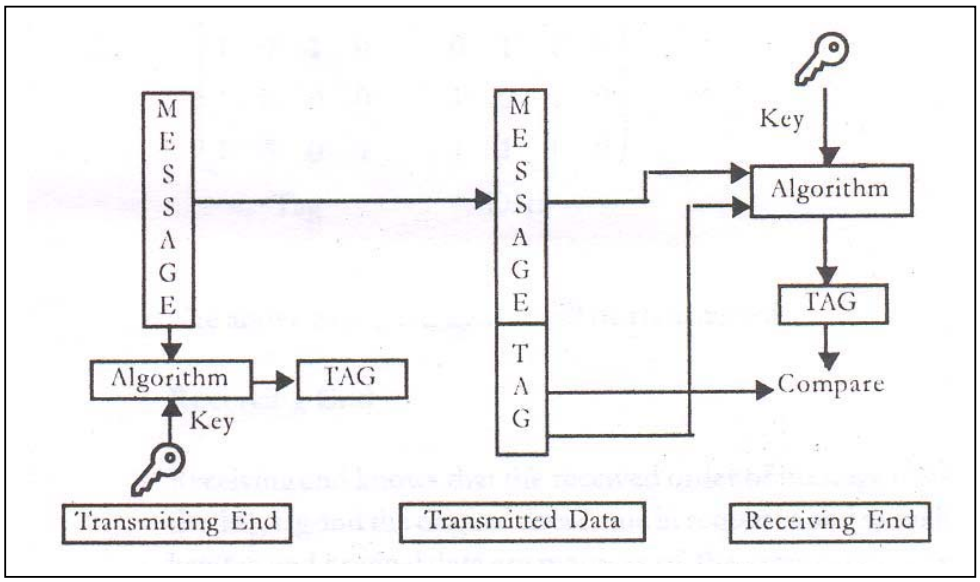

Fig. 1: Message Authentification Technique

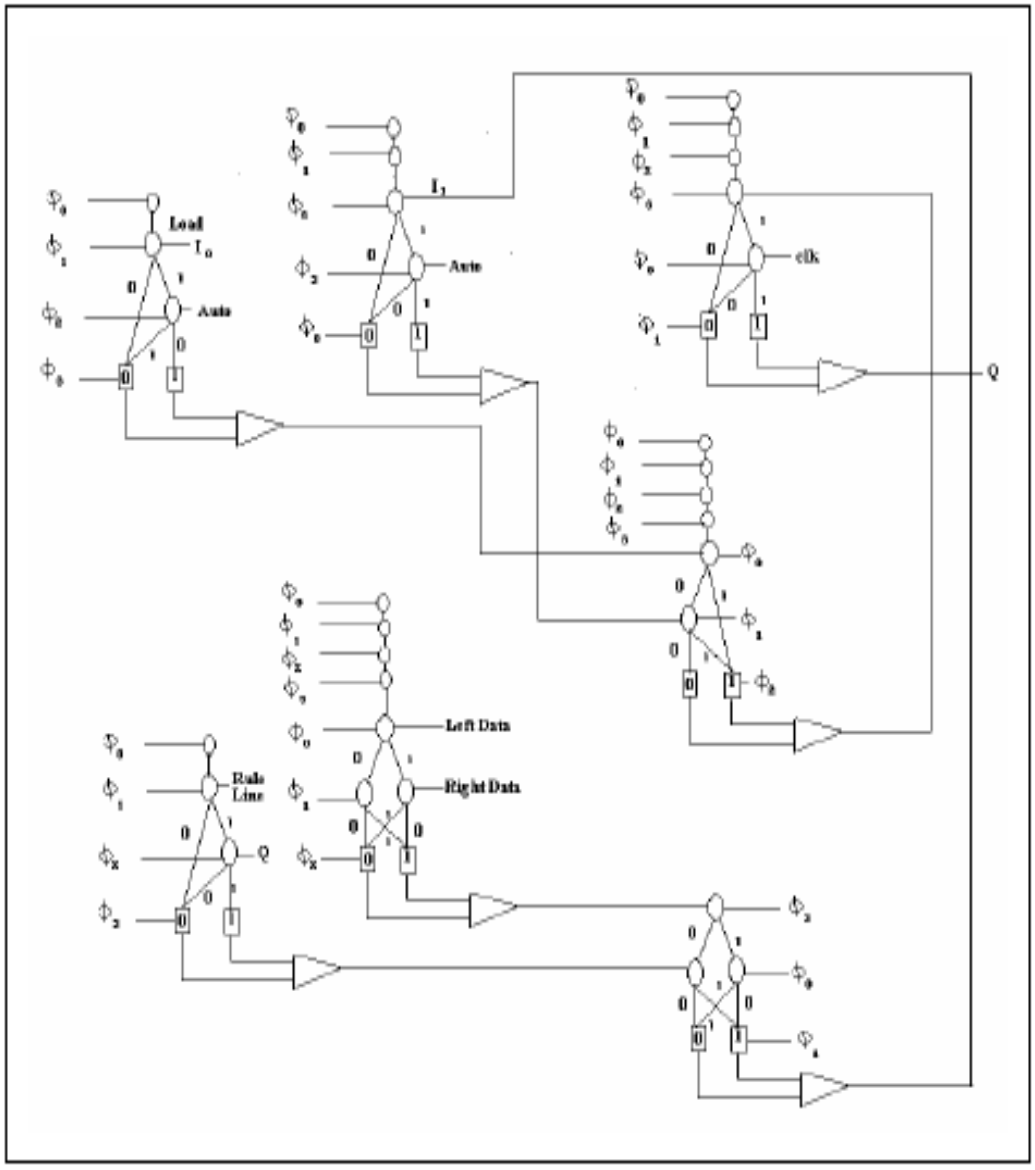

Fig. 2 SED Based Single Bit PCA

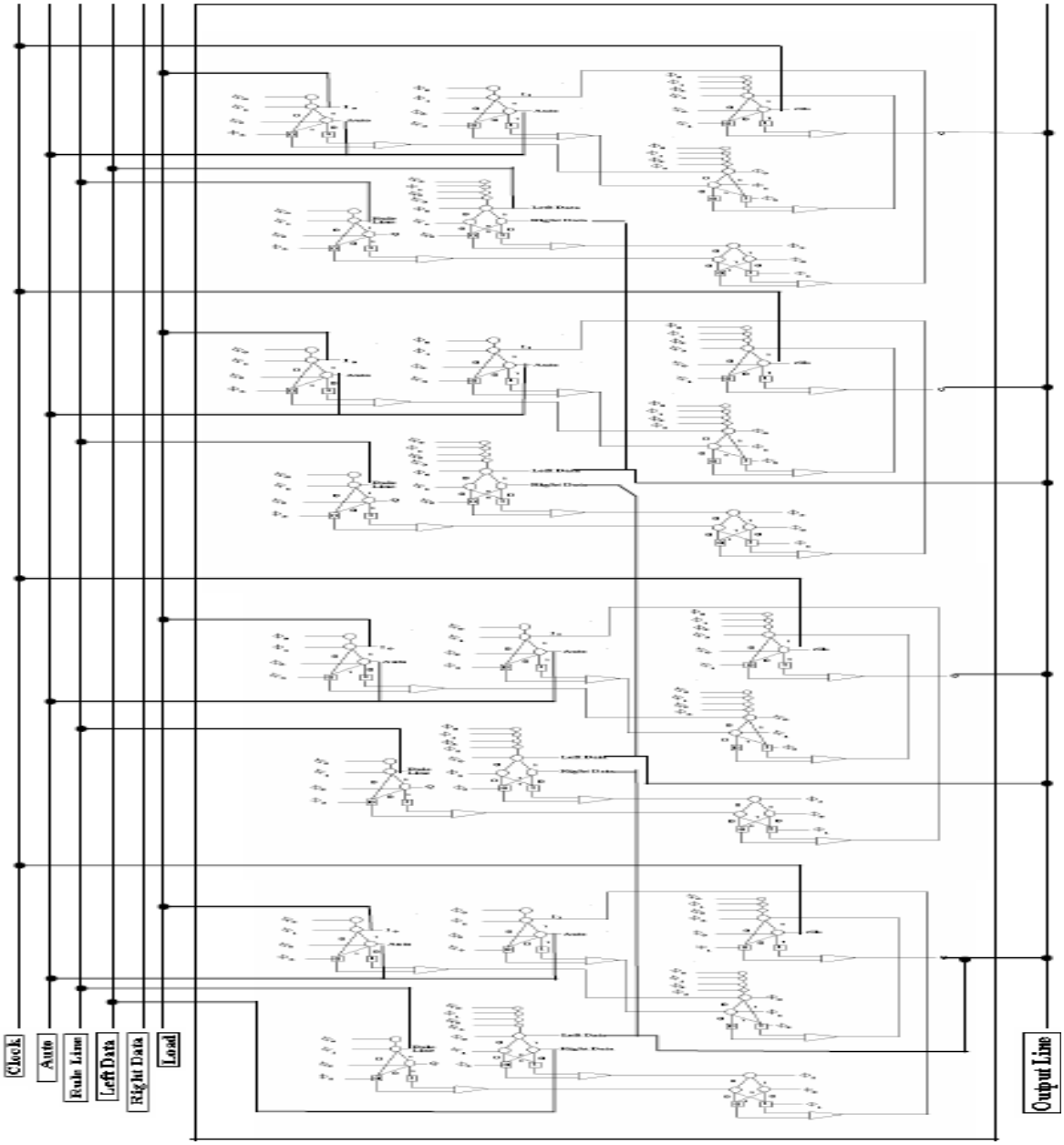

Fig. 3 SED based 4 bit PCA

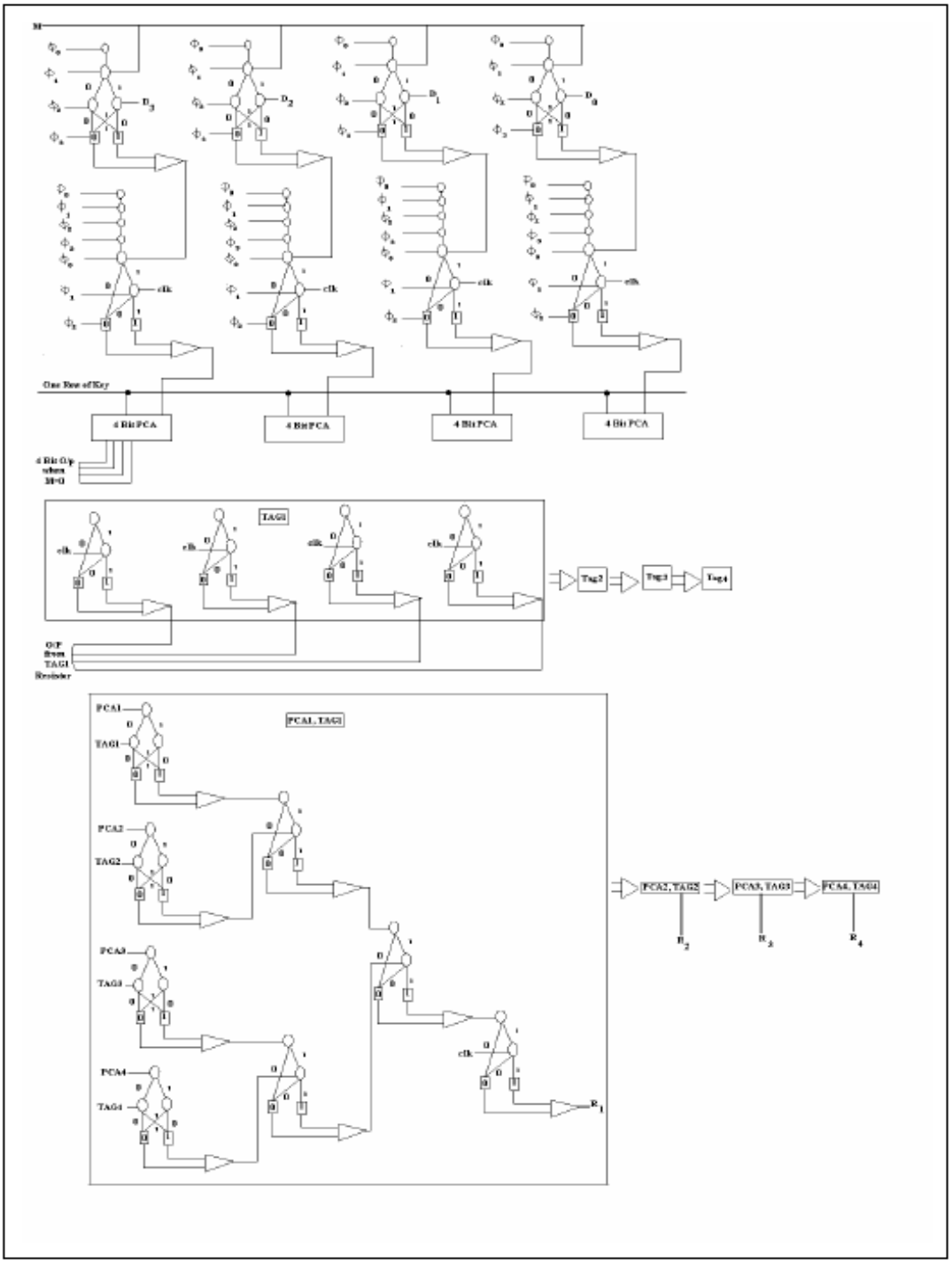

Fig.4 Complete Design of a 4 Bit PCA

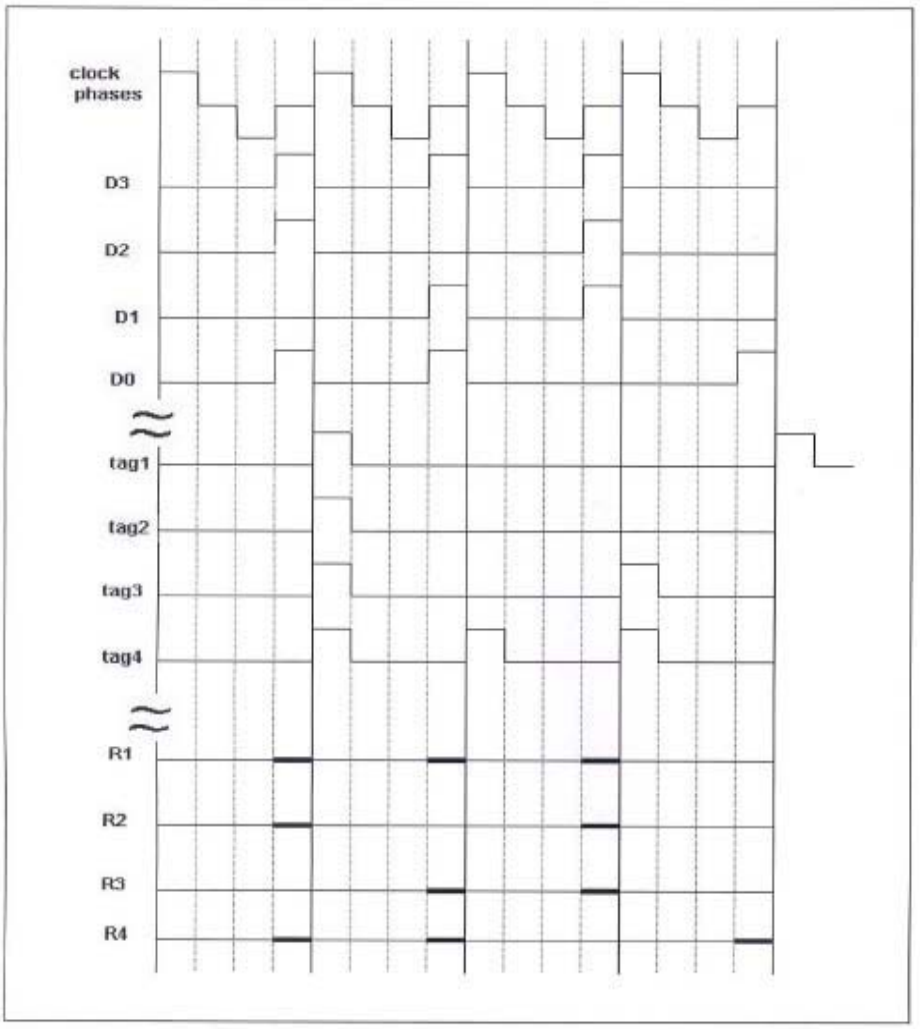

Fig. 5 Generated Data and its Corresponding Timing Diagram