Reliable, Highly Secure, Low Power Hardware based passcode generator using Memristor

G. Saranya devi\textsuperscript{1}, Aishwarya Singh\textsuperscript{2}, Akanksha Singh\textsuperscript{3}, R.Priyanka\textsuperscript{4}, P.Simran Khan\textsuperscript{5}, N.Ramya\textsuperscript{6}

Assistant professor\textsuperscript{1}, Student\textsuperscript{2,3,4,5,6}, Electronics and Communication, SRM institute of science and technology, Tamil nadu, India

Abstract-- Secret sharing schemes can be useful in creating and distributing authentication secrets over multiple servers for resisting dictionary attacks at the server side. Design of lightweight cryptography is evaluated in the model. The main advantage of this approach is that it does not need the computational expensive cryptographic techniques. Lightweight encoding algorithms such as LDPC is used to increase the entropy and remove erasures. In the proposed system, Design of CPLD based RTL memristor is developed in which N number of Memristor values are stacked inside the Memory of CPLD, which acts as a Digital Memristor. Random numbers generated through memristor are used as a key for Lightweight cryptography in this model.

1. INTRODUCTION

The requirement of information security within an organization has undergone major changes in the last several years. The security of information felt to be valuable to an organization was provided primarily by physical and administrative documents, before the widespread of data processing equipment. Another major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer. Network security is required to protect data while in transit.

Secret sharing plans are perfect for putting away data that is very sensitive and exceptionally essential. Models include: encryption keys, rocket dispatch codes, and numbered ledgers. Every one of these snippets of data must be kept profoundly classified; in any case, it is additionally important that they be lost. Conventional strategies for encryption are ill suited for at the same time accomplishing large amounts of privacy and unwavering quality. This is because while putting away the encryption key, one must pick between keeping a solitary duplicate of the key in one area for extreme secret, and keeping numerous duplicates of the key in various areas for more noteworthy unwavering quality.

Secret sharing plans are likewise fascinating from an execution perspective, as they regularly depend on an absolute minimum of cryptographic suppositions. Specifically, by not making any suspicions about the hardness of specific issues, for example, figuring numbers, processing discrete logarithms, or discovering short vectors, secret sharing plans can give a computational preferred standpoint contrasted with other cryptographic instruments, for example, homomorphic encryption. The plans are critical in distributed computing conditions. Consequently, a key can be dispersed over numerous servers by an edge secret sharing component. The key is then remade when required. It has additionally been recommended for sensor systems where the connections are at risk to be tapped by sending the information. [9]

2. LITERATURE SURVEY

Access to a particular data is given to a party or a claimant depending on the key or password they have. The access is either granted or denied. In this section we will review the different existing hardware and software based authentication systems.
A. Basic access authentication

There are different methods to access a classified document, the simplest one being password based authentication, where a user can gain access to an information on having the knowledge of password protecting that information. There are different methods of doing so, first being information being known to both sides, second being the key possessed by the claimant and lastly different inherent methods like biometric, signatures or face recognition techniques.

Out of these, passwords are used more commonly where a hashed table is used to store this data in pairs of username and password and the server matches this pair to validate the user. The protection provided has low entropy and can be improved by introducing different rules that need to be followed while forming a password. Mapping of the password can be slowed down which will increase the number of trials for the hacker. There are different attacks such as dictionary password search and replay attack that can pose a threat on the user data. Moreover, the hacker can directly hack into the data base thus causing threat to the data.

Due to the above discussed threats, there are different challenge response identification and strong authentication methods that can be used to increase the entropy of the password. Here the entropy refers to the level of security of data.

B. Secret sharing and multiple user authentication.

Secret sharing is a well-known problem and solution which refers to dividing a piece of data or the message among different parties. This means the data can be only accessed when there is a sufficiently good number of parties willing to reveal their shares.

Shamir’s secret sharing algorithm follows a similar concept and introduces the concept of threshold scheme. It has two variables where K is the threshold value and N is the total number of parties (K<=N).

![Fig. 1: Shamir’s Key Sharing Mechanism](image)

Now if there is piece of information S, it can be divided among N parties such that the knowledge is equally known to all of them, now if one has to access the data at least K number of shares will be needed to access. Even one less than he threshold value will not be able to restore the data S. One such application of this technology is used in wars or nuclear transmission so that the authority of transmission does not lie with one individual.

Though this method address a lot of issues, it has its own drawbacks in terms of complexity, scalability and privacy of the parties. Firstly, expensive formulas need to be applied in order to generate the original data and secondly this system reveals the III. MEMRISTORS

In the passive circuit network there are three existing electrical circuits, namely the resistor, the capacitor and the inductor. A hypothetical element which is known as the fourth class of electrical circuit is known as the memristor, it is a combination of memory and resistor. It is mostly like an identity of each party, which also means user duplicity can occur.
inactive component of the circuit that is used to relate the integrals of current and voltage for a two terminal component. Thus the resistance of this memristor varies in accordance with the memristance function allowing access to the previous states of the applied voltage. [3]

![Memristor relations](image)

**Fig. 2: Memristor relations**

The resistance increases or decreases in a memristor with respect to the direction of current flow. Irrespective if the direction the resistance must always remain positive.[7] If the current is stopped the memristor retains the value of the last resistance that it had. In the above figure the relation between the flux and voltage and the relation between voltage and charge, and the relation between charge and current is shown. The only relation missing is the relation between the charge and flux. This can be derived by the memristor relation which gave birth to memristor.[5]

A. **Memristors in security**

The hardware security memristors have more advantages compared to CMOS designs. Properties like non volatility, bias dependant write time, fabrication variations in a filament and non linearity in current voltage relations are provided by analog memristors. These properties are investigated for a better hardware security systems.[1]

B. **Features of memristors**

Non volatility: Because memristors act non volatile in nature, non volatility has been included as a standard feature. Low resistive state (LRS) and high resistive state (HRS) are associated with every memristor. A continuous spectrum between LRS and HRS is observed in an analog operation. These are used for safeguarding the resistance value. The memristor population at initial state are randomly distributed and secure random keys are generated using memory as a seed.

Bias dependant write time: The time required to switch from one resistive state to another is bias dependant write time. This is mostly used in PUF approached memristors. Required write time can be manipulated by adjusting the bias voltage.

Fabrication variation in filament thickness: Filament thickness varies with physical properties of memristors. A large variation in the resistance of the device is due to a small change in the film thickness. Design security features and fabrication variations results in random variability. Large filament thickness makes the write time of HRS to LRS transition an unused memristor. The resistive switching devices are highly non-linear. It is a property needed for
secure hardware design and therefore using its property will implement better usage of the meristor in secret authentication system.[8]

3. PROPOSED MODEL

A. Block Diagram ENCRYPTION

The encryption block diagram for this system can be explained as follows. The input to the system is given in terms of voltage. The voltage is finely tuned with the help of a voltage tuner. This is done because even the slightest change in the voltage value refers to different resistance values. After the voltage is finely tuned, it is given to the memristor. As memristor is a non-volatile device, it stores its past values also. Here ohm’s law is applied and the resistance is calculated with the help of a constant value. This resistance is stored in the resistance LUT memory and is given as the seed to pseudo random number generation algorithm. Different methods are used to generate a sequence of random numbers with a fixed period. After the sequence is generated, with a pre set scheme, certain numbers are picked from the sequence which form the pseudocode or the key. Then the data that has to be transmitted is taken as input and is encoded using LDPC which is a lightweight encryption algorithm. Here a parity set is added to the message set which helps to encode the message as well as to overcome erasures if any, during data transmission. Then this encrypted data is transmitted along the channel.

DECRIPTION: The encrypted data is received at the receiving end and then the LDPC decryption scheme is applied on the received data.

If there is data loss, then again the subsets are formed and the subsets with single erasures are used first to retrieve the missing data. Using the same process, the entire message is retrieved and then the message set is separated from the parity set. The user at this end enters the voltage as the input. If this matches the input at transmitting end, then the same key is generated and access is granted else the granted is denied to the user. The system already has a knowledge of the key that has to be verified hence even the numbers to be picked from the sequence should match the algorithm. This makes it very hard to hack into thus increasing the security of the system.
B. **Key Generation**

In any cryptographic system, key is one of the most essential elements. It is the passcode to access the data on both sides of the channel. There are different forms of keys used for data transmission which includes single access and multiple share. There are different means of key sharing such as symmetric and asymmetric key. In symmetric there is only one key that is used for both encryption of plain text and decryption of cipher text. The keys might be identical or go through a simple transformation.

![Symmetric Encryption Diagram](image1)

**Fig. 5: Symmetric encryption**

The other form is asymmetric key which uses two different type of keys for encryption and decryption, it is also known as public key cryptography. The keys are nothing but large numbers paired together and are not identical. Out of the pair one key is shared to the public hence the name public key while the other key is kept as a secret. Out of the two keys any one can be used to encrypt a message and the other is used for decrypting it.

![Asymmetric Encryption Diagram](image2)

**Fig. 6: Asymmetric encryption**

There are certain disadvantages to this system regarding the security of the public key. While the two parties are sharing the key there might be a hacker trying to hack in and get access to the key.

In our system we use pseudo random numbers as key for data transmission. This number can be generated using pseudo random number generation that follow different methods to generate a sequence of random numbers. This sequence has a period depending upon the input bit size of the seed. The seed is nothing but the resistance value calculated from the input voltage by Ohm’s law. The sequence repeats itself after its period. Once the sequence is generated for the particular value of resistance we apply different algorithms using shift registers and xor gate to select particular random values from the sequence. This finally forms the key for the secret sharing of the system. This key is transmitted along with the encrypted data to the channel and is used at the receiving end to validate the user and give the access.[10]

![Pseudo Random Number Generation Diagram](image3)

**Fig. 7: Pseudo random Number Generation**
C. LDPC Algorithm

A parity check code is a block of code which has fixed length binary vectors. A codeword containing \( n \) bits can process: \( n-r=k \) information digits, \( r \) = checked digit. Construction of parity check matrix can be understood by constructing a matrix of ‘\( r \)’ row and ‘\( n \)’ columns. Equations are represented by the rows and digit are represented by the columns. If an \((i,j)\) element is ‘1’, it shows that \( j \)-th equations contains \( i \)-th code digit.

\[
\begin{align*}
C_3 \oplus C_6 \oplus C_7 \oplus C_8 &= 0 \\
C_1 \oplus C_2 \oplus C_5 \oplus C_{12} &= 0 \\
C_4 \oplus C_9 \oplus C_{10} \oplus C_{11} &= 0 \\
C_2 \oplus C_6 \oplus C_7 \oplus C_{10} &= 0 \\
C_1 \oplus C_3 \oplus C_6 \oplus C_{11} &= 0 \\
C_4 \oplus C_5 \oplus C_9 \oplus C_{12} &= 0 \\
C_1 \oplus C_4 \oplus C_5 \oplus C_7 &= 0 \\
C_6 \oplus C_8 \oplus C_{11} \oplus C_{12} &= 0 \\
C_2 \oplus C_3 \oplus C_9 \oplus C_{10} &= 0.
\end{align*}
\]

Fig. 8: LDPC code for \( n=12 \)

Fig. 9: Parity check matrix for simple LDPC code

A low density parity check code is a linear error correcting code that can be used for correcting erasures across a noisy transmission channel. A major property of LDPC code is, compared to percentage of 0’s in parity check matrix, percentage of 1’s is very low, hence decreasing the overall density of the parity check matrix. Every equation in LDPC codes have equal number of codes associated with them and ever code bit is encapsulated in the same number of equation.[6]

They have a threshold in which the upper limit defines the upper bound for the channel noise upto which the lost information can be made as small as desired. They are used in application that require reliable and highly efficient information transfer over the constraint channel. Initially hamming codes were used for data correctio across the channel but with large data it became difficult to retrieve multiple erasures. This happened because the subsets of the message signal were huge and overlapping hence the density became high.

To overcome this problem LDPC was introduced which makes use of smaller and random subsets. Hence the density of the subsets is reduced. Here the parity set is also involved in the subsets hence even if an erasure occurs in the parity set,LDPC will be able to retrieve it. Firstly the parity set is formed using the bits of message sets. Then random subsets including both message and parity sets are formed.
This encodes the original message signal and is transmitted across the channel. At the receiving end LDPC decryption algorithm is applied which performs two tasks, firstly it retrieves the original data and then separates the message signal from the entire set.

![Graph for LDPC algorithm](image)

**Fig. 10: Graph for LDPC algorithm**

The above graph contains two types of nodes, bit and parity nodes. A code symbol is represented by a bit node and parity equation is represented by a parity node. A parity node is connected to a bit node only when that particular bit is involved in that respective parity equation. Each parity node is connected to bit node by 4 connections and each bit node is also connected to parity node by 3 connections. Hence bit node and parity node are encoded with respect to eachother. This makes it easier to decode erasures in a fast cascading manner.[2]

![LDPC bit node and parity node connection](image)

**Fig. 11: LDPC bit node and parity node connection**

Errasures in a channel occur when the message arriving at the reciever end contains missing bits, which causes loss in data in channel. LDPC fixes these erasures and retrieve the original message. It adds additional level of security, since it is a low density parity check coder, the overall system remains computationally inexpensive. Both data and parity are encoded in low density parity set, low density of parity set helps in fixing the erasures occurring in the channel.

Messages are passed along the lines of the graph for decoding purpose. The messages along the i-th bit node, $c_i$ are estimated. All the estimates are combined at the node in a structured way. Initial estimate of each bit node is taken and the probability of the node corresponding to ‘1’ is taken from the channel output. This estimate is sent across to all the parity nodes along that line. New estimate is taken by each parity node involving the bit node connected to it and this estimate is then again sent to all the bit nodes connected to that parity node. Each parity node is aware of the fact that there are even number of ‘1’s in the bits connected to it. But the estimate received by the parity node gives information that each bit connected to it is a ‘1’. In this case parity node forms a new estimate and broadcasts it along the i-th line along with all the probability information supplied to it.

The data and key are decoded in cascading manner in the decoder. Since each parity set has lesser number of bits associated with it, the decoding process is faster as compared to hamming codes. The parity sets are formed in a random number, this removes the problem of constructing a structure for the algorithm.

### 4. HARDWARE IMPLEMENTATION

To extract the current state of the device a memristor based secret reconstruction and authentication circuit is developed. To access the read operation the memristor should have a high biased voltage. To determine the output resistance a simple amplifier is used. To perform N number of function like speed, voltage, capacity programmable logic devices (PLDs) are used.
Introduction to CPLD device: On a single device it has few PLD blocks or macro cells that are interconnected. To make these connections we use multiple blocks and general purpose interconnect with more sophisticated logic. Blistering speeds and complex gating are widely maintained by CPLDs. It can calculate the output speeds before designing CPLDs. CPLDs timing model is easy to design with low development cost at high speed.

Features and specifications of CPLDs:
- Logic delay on all pins
- 1600 usable gates with 72 macrocells
- 72 I/O pins
- In system programmable voltage -5V
- Controlled commercial voltage and temperature range

![CPLD](image)

Fig. 12: CPLD

Components of CPLD kit:
POWER SUPPLY: Universal switch mode power supply (SMPS) is used as input power supply. It has an operating voltage of 3.3V DC and a constant power of 0.4 A. SMPS has a supply voltage of 100V to 240V.

OSCILLATOR: It uses a crystal oscillator of 40 MHz and an input frequency of 40MHz. This oscillator can be implemented through a shift register.

DISPLAY: To display the data CPLD uses two seven segment displays. It is connected through wires by proper allotment of pins that are used in programme.

JUMPER SETTINGS: General purpose fixed I/O pins can be selected by proper jumper settings. Jumpers are provided at the sides of CPLD chip. For selecting the CPLD pin with allotted applications the jumpers at sides are used. [4]

5. ADVANTAGES
SYSTEM MODEL: The system used is a hardware dependant system that has most of it’s components readily available. This thus makes the system inexpensive. Moreover the controls present in the system are tunable and reconfigurable. Also the entire model is lightweight.

POWER CONSUMPTION: In general the power consumed by cryptography based systems are very high however, in this system the overall power used up remains very less which thus makes the system reliable.

COMPLEXITY: Most of the models are very complex due to the various inputs and the complexity of the process happening between the various components. However, this system is less complex as it requires only a voltage value to be given as an input into the device, thus making the computation process easier.

SECURITY: The basis of cryptography is security and there is major issue of security in other models proposed due to hacking. However, in this particular system, since the value of the voltage that is given as input is known only to the user, the security of this system is guaranteed as the
remaining process is carried within the devices thus keeping all the essential information non accessible.

ENTROPY: According to the entropy theory in cryptography, a lack of entropy can have a negative impact on the security and performance. However, this system has high entropy making the secret sharing process more reliable and secure. Thus this system stands reliable and economical for other applications as well.

6. OUTPUT RESULT

After performing the necessary simulation, coding and hardware connections, the following observations can be seen.

Firstly, the ModelSim software is simulated to work as a memristor. The same code is dumped into CPLD for the hardware execution. After performing the simulation, a graph is obtained which shows the different values of resistance and voltage. As the voltage varies, the resistance also varies thus following the linear relation of ohm’s law. This is the first part of the execution of this model.

Secondly, a coding for LDPC is dumped into the system and the methods to be followed are specifically chosen. The given message set is encrypted along with the parity set and can be seen in the graph. There are two conditions, firstly the message arrives without any data loss, then the same algorithm is used to decrypt.

If there is any data loss, then shifting the values and using subsets, the original message set is recovered.

For the final output, if the receiver enters the correct voltage value and the system is programmed correctly, then the screen shows access granted or access denied. The same can be shown using green and red LEDs for the hardware implementation.
7. CONCLUSION AND FUTURE SCOPE

Conclusion: Memory devices such as memristors are non-volatile and monotonic. In this paper we have explored these properties of memristor to use it for secured data transmission and passcode generation. In addition to these properties of memristor we have used lightweight encryption algorithms like LDPC that are highly secure and error correcting as well. This is also a robust and hard dependant authentication system that is reliable, lightweight and with very less complexity. We have explained various properties which can be explored further for cryptography applications. This system as such finds many applications without the cost of high complexity. A few of the applications are, hardware based data lock system used in bank lockers and storage vaults. Secure data transfer in online data sharing and confidential data sharing in an organisation.

Future Work: Regarding the temperature and noise control, the operational temperature and noise levels in the system should be maintained and methods for the same should be researched for uninterrupted and reliable mechanism as in cryptography the decryption function doesn’t work if the noise is greater than a certain a maximum value. Even though an aging model is still elusive, certain error correction mechanisms should be implemented. Certain properties of memristors can be further explored to enhance the working of the model.

8. REFERENCE

[1] M. T. Arafin et al., "A survey on memristor modeling and security applications", Quality Electronic Design (ISQED) 2015 16th International Symposium on, 2015.
[2] T. Richardson, R. Urbanke, “Efficient encoding of low density parity check codes”, IEEE Transcations on information theory, vol.47,pp.638656, Feb.2001.
[3] Ascoli, F. Corinto, V. Senger, R. Tetzlaff, "Memristor model comparison", IEEE Circuits and Systems Magazine, vol. 13, no. 2, pp. 89-105, 2013.
[4] Praveen Malav, Bushan Patil, Rabinder Henry, “Compact CPLD board Designing and Implemented for Digital Clock”, International Journal of Computer Applications (0975-8887) Volume 3- No: 11, July 2010.
[5] F. Corinto, A. Ascoli, M. Gilli, "Analysis of current–voltage characteristics for memristive elements in pattern recognition systems", Int. J. Circuit Theory Appl., 2012.
[6] R. G. Gallager, “Low density parity check codes”, IRE Tran. on information theory, IT-8,1962,pp.21 28
[7] L. O. Chua, "Resistance switching memories are memristors", Applied Physics A, vol. 102, no. 4, pp. 765-783, 2011.
[8] D. B. Strukov, G. S. Snider, D. R. Stewart, R. S. Williams, "The missing memristor found", Nature, vol. 453, no. 7191, pp. 80-83, 2008.
[9] Douglas R. Stinson, "An explication of secret sharing schemes", Designs Codes and Cryptography, vol. 2, no. 4, pp. 357-390, 1992
[10] Boaz Barak and Shai Halevi. A model and architecture for pseudo-random generation with applications to /dev/random. In Vijayalakshmi Atluri, Catherine Meadows, and Ari Juels, editors, ACM CCS 05: 12th Conference on Computer and Communications Security, pages 203–212, Alexandria, Virginia, USA, November 7–11, 2005. ACM Press.