

DESIGN AND IMPLEMENTATION OF DIGITAL CODE LOCK SYSTEM USING VHDL

A.Lakshman¹, CH.Ramanjaneyulu², B.Nagi Reddy³, B.Brahma Sai⁴

¹UG Student, Department of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

²UG Student, Department of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

³UG Student, Department of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

⁴UG Student, Department of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India

ABSTRACT

Security is the main problem facing now a days. Everyone thinks that they want security for their effects. So, in this design, we described a cinch which will ameliorate the security for their effects. By this design we can give security for effects like buses, banks, sale operations like ATM. At present also there were number cinches but they didn't give important security for our effects because if we take a three number law cinch also, the maximum chances needed to break the cinch is thousand. So, in order to break the cinch it'll take lower span of time. thus security is less in similar systems. Technological advancement has been constantly and constantly made on colorful electronic bias with little or no emphasis on locking systems. Unlimited access and absolutely no interference to data, train operation, machine auto, and bank strongboxes by interferers, needed the need for a programmable electronic code lock system. This programmable electronic law cinch system is an intertwined combination cinch which is programmed and responds only to the right sequences of number that's reconciled in. In certain situations we need to tell the password to others, in that time we loss security for our effects and if the word is known to someone also also we loss security for our effects because there's no chance to change the code as it's formerly fixed. A key defended access control module is an abecedarian part of all security systems. It allows only the sanctioned people to enter into a defined zone. A VHDL law of the lock system had been designed and scripted in Xilinx Vivado Software.

Keywords: Security, Data, Digital, Password

1. INTRODUCTION

Electronical or Digital locks are electronic or battery-operated cinches that don't bear the use of physical keys for access. They're used as an volition to the conventional mechanical locks, with the automated features giving a more creative security result depending on its intended use. Like any other door cinch, digital cinches also use a latch or a bolt that can run across the door and the doorframe to help access. What differs is the way latch or bolt is controlled. Digital locks work by the use of any of the following RFIDs, Leg canons, fingerprints, smartphones, and more. Digital cinches are generally set up on buses and doors, but they can also be used for lockers, cabinetwork and closets. Reviews of these cinches for buses and doors are occasionally mixed, but for businesses who use lockers and closets, the benefits of digital cinches are lesser compared to the traditional key locks.

1.1 Why Code Locks

The design and construction of a programmable electronic digital code cinch system provides a sure way of icing this security and safety for data. Programmable digital law cinch system is a high security law cinch system that can be used to lock electronic bias similar as TV set, computer system and other electrical appliances. They're generally used in public structures similar as hospitals, services and seminaries, which can have a number of digital cinches located throughout the structure to secure different areas, or for domestic parcels where multitudinous caregivers or nursers need independent access. Fast access – some use remote controls, so you can snappily pierce the property when if its raining. There's little that can go wrong and accordingly, digital door cinches can last for numerous years. As their operation is so straightforward compared to ‘high tech’ electronic access control options similar as biometric point compendiums. The fact that digital door cinches can fluently and snappily be reprogrammed means that security can be incontinently reinstated if compromised or if there's a transfiguration in staff. The most robust digital door cinches will be able of opposing all but the most violent attacks and will give numerous times ‘dependable service, indeed when installed on external doors and when subordinated to heavy business or extreme use..

2. EXISTING METHOD

Technology has made it easier for humans to live comfortably in the ultramodern world due to a growing number of installations. As a result of the preface of a number of technologies, people are now suitable to negotiate numerous effects more fluently in their day- to- day lives. still, it can lead to security enterprises as well. thus, we must insure he security of our lives and our particular things. It's imperative that experimenters continue to pay further attention to widgets and cinches in order to guard our lives and parcels are defended in the long run. The problem with conventionally installed door cinches is that nearly anyone can break them and gain access to the home. With only a essence cinch that can be disfigured or melted can not neglect security issues.

People are vulnerable to security pitfalls due to the ease with which conventional door cinches can be broken. Crime rates have increased in numerous countries that use mechanical cinches due to the ease with which they can be broken. It isn't indeed possible to identify who has immorally entered a house or apartment where mechanical cinches are used. therefore, prostrating these obstacles is a veritably grueling task. People generally use CCTV to secure their homes. Any suspicious incident can be delved using the images stored in the database. This type of approach is unresistant, but an active approach is demanded then. When a security trouble occurs, this type of approach allows immediate action to be taken. It's clear from this that most security systems presently available in homes and businesses are deficiently suited to cover the inhabitants of these structures. By applying new technology- grounded control systems and other styles that allow for effective access control, these security breaches can be addressed.

2.1 Simple Door Locks

The existing cinches are called simplex code locks. Combination numbers in simplex cinches are related to Stirling figures of the appendages that reduce the cost of the system, but control it within the Bluetooth range. There are smart door cinch systems that let you know when doors open and near, and some systems allow you to set individual passcodes for different people so you know who's entering. The cinch can also be combined with a smart doorbell camera, allowing you to see exactly who is at your door with just a click of the button.



Fig-1: Simple Door lock

When a security word is used for security door cinch systems, the person is only allowed to pierce the security area if the word is correct. But watchwords and canons can be fluently stolen or lost. Biometrics can be suggested as an ideal result to this. It seems that there aren't only advantages but also disadvantages to using watchwords. Using point recognition technology for security doors is a veritably accurate result, but in an epidemic situation like COVID 19, this isn't a veritably good system. Compared to this, facial recognition can be considered as a good system. The five- button door cinch is a traditional system that can be seen from the early times and can be installed at an affordable cost. There are also door cinch systems that ameliorate this technology with further number of buttons. While considering the ATM operations, the problems associated with simple cinches is data inconsistency between multiple deals. impasse, a situation where the deals try to pierce cinch on formerly locked data particulars.

2.2 Three Switch Code Lock

In the being system if consider a three switch law also, in order to break the cinch, the number of chances to unleash the system is thousand. So, for an unknown stoner it's veritably easy to break the cinch with in a short time. So, there's lower security for a system.



Fig-2: Three Switch Code Lock

3. PROPOSED METHOD

The main ideal of the design proposed then's to design and develop an digital law cinch system in order to ameliorate the security features of the effects like houses, buses and bank sale operations. currently, with the urbanization and eclectic felonious types, the effectiveness of the crucial- and- cinch has been challenged. Communication network substantially use digital data to be transferred because digital data will give further delicacy than analog data. Digital data is transmitted in form of bits at high speed. The transmitting bits is called as sluice of bits. The end stoner can admit only the needed information.

Table 1: Truth table for FLIP-FLOPS

D1	D2	D3	D4	Q1	Q1BAR	Q2	Q2BAR	Q3	Q3BAR	Q4	QBAR4
1	2	3	3	1	0	1	0	1	0	1	0
1	2	X	X	1	0	1	0	0	1	0	1
1	X	X	X	1	0	0	1	0	1	0	1
2	X	X	X	0	1	1	0	0	1	0	1
3	X	X	X	0	1	0	1	1	0	0	1
3	X	X	X	0	1	0	1	0	1	1	0

Consider that the password of the circuit is 1233. These particular switches are connected as the inputs of the D flip flops respectively. On pressing the above switches in sequence will lead to a high output, else the output is low. Let us assume that a person who is trying to break the lock presses 3321. In this case the output of the fourth flip flop is high since fourth switch is connected to the corresponding fourth flip flop. The output of this D flip flop is AND'ed with negated output of third flip flop which is high due to default settings. Hence the output of AND gate is high which leads to a high output at the OR gate and this signal is given as feedback which resets all the flip flops. The major advantage of the proposed system is that it provides high security by misleading a person who's trying to hack the lock by the number of input bits to be entered. Then a person who knows the word will only enter the law, which is he'll press only four bits of law and will have access. But a person who's trying to break the lock will no way know that the figures of bits in the word are 4, because the figures of inputs to be entered are 10. The circuit will only work when 4 bits of the word are pressed, but when further than 4 bits are pressed, it'll beget the affair of the OR gate to be high and this high signal is given to the flip flops in the feed reverse and will reset them. So, there's high probability that the hacker will always enter further than 4 bits (since he doesn't know that there are 4 wise duds corresponding to 4 bits of law) and every time the circuit is reset. The word of the circuit can be changed by connecting the needed switches of the new word to the separate flip flops as asked. piecemeal from figures, letter and alphanumeric characters can also be used to set the word.

4.SIMULATION RESULTS

Initially all the inputs are at undefined state. Now, Initialize the corresponding values to the respective inputs i.e., trailing edge as '1' and leading edge value as '0' to clock and for enter inputs using force clock command and for reset set force value as '0'.

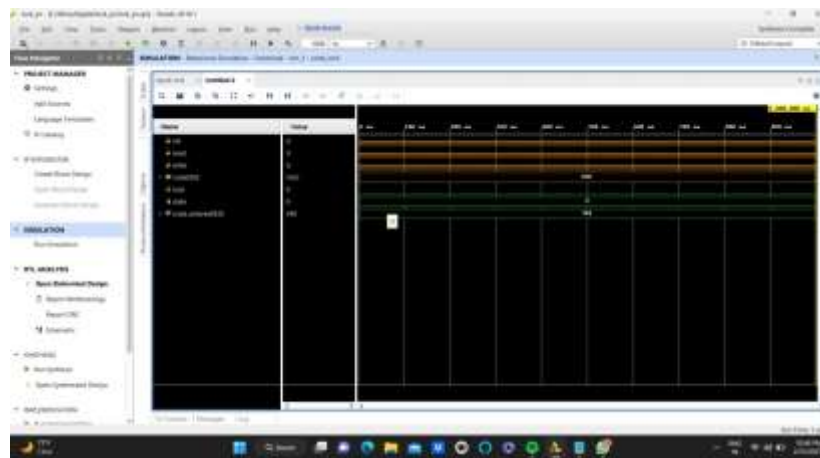


Fig-3: Initializing the inputs

- Here in the code, We initialize the default password, at the stage of value initializing, we should enter the password for checking. Here system checks the password that we have initialized defaultly and with the password that we have given at running state. So if the password was matched then the lock will open. In our output view, the lock state will be '1' which indicates the lock is opened and the state goes to second state. As shown in the below resultant the lock timing state goes up.
- Here we initialize a variable called state, For this state goes into different cases i.e., if we consider initial case that if passwords are matched the state will move to second state in the second state our lock will be initialized to '1'. Remember that the inputs entered here is of ten bits.
- If we want to make password for more than ten bits it would be no restriction for the user. On selecting the force clock it lets you assign a signal a value that toggles at a specified rate between two states, in the manner of a clock signal, for a specified length of time. Here we are assigning the values in binary form. In practical we can assign password in any types such as binary form, digits form, alphanumeric also.

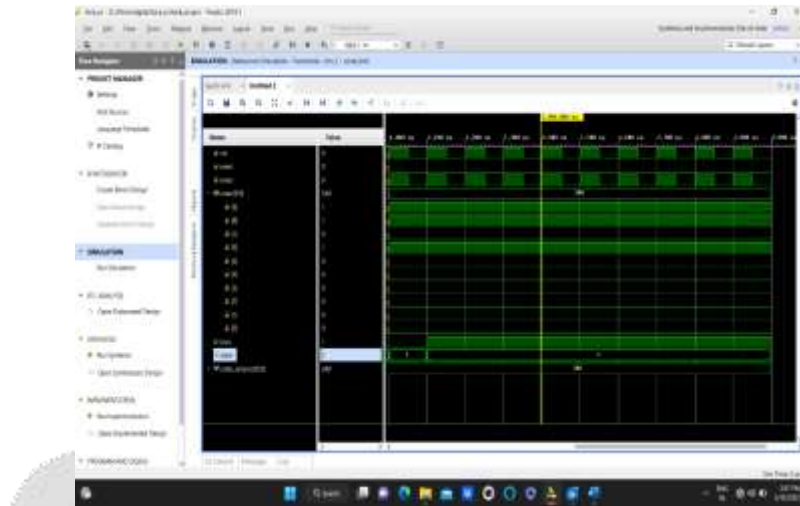


Fig-4:Result for Correct Password

- As shown in the Above resultant waveforms, internally in the assigned program we are fixing the password, after this the system checks the password with the fixed one and the password that we have entered at simulation process.
- If the password entered at the time of simulation process matches with the password that is fixed as password, then the lock variable be '1'.Which indicates the door is unlocked.

5. CONCLUSIONS AND FUTURE WORK

When we Completed this project, We had learned and understand the process of implementing digital code lock. When security is considered in the modern social system, it is more desirable if it can be enhanced and stabilized with technology. Digital code lock technology contributes greatly to satisfying one of society's needs which is security. It must be admitted that the projects and research shown here have been a great help in advancing this digital code lock technology.

It is not a new concept for science society to use a smart door lock, as it has existed for decades. With technological advancements, the field of home security automation is growing rapidly. When security is considered in the modern social system, it is more desirable if it can be enhanced and stabilized with technology. Smart door lock technology contributes greatly to satisfying one of society's needs which is security. It must be admitted that the projects and research shown here have been a great help in advancing this smart door lock technology. It is important to ensure security through various technical strategies such as fingerprint recognition, facial recognition, knocking patterns etc., and to be able to handle keys through remote access. Although hacking and disruptions that may occur in the event of a power outage can be seen here, it should be believed that the remedies for that will come soon.

6. APPLICATIONS OF DIGITAL CODE LOCK

- Access control systems
- Ease of entry. With a smart lock, you won't have to fumble for your keys or jiggle the key in the lock to get it to open.
- More secure places and Transaction processing system, ATM.
- Personal computers and Workstations.
- Medical electronic systems, etc.

7. REFERENCES

- [1]. R. C. Gonzalez and R. E. Woods, digital code lock. Reading, MA: Addison-Wesley, 2011.
- [2]. W. K. Pratt, Digital code lock. New York: Wiley-Inter- Science, 2013.
- [3]. T. M. Lehmann, C. Gonner, and K. Spitzer, "Survey: Methods ," IEEE Trans. Med. , vol. 18, no. 11, pp. 1049–1075, Nov. 2007.
- [4]. C. Weerasnghe, M. Nilsson, S. Lichman, and I. Kharitonenko, IEEE Trans. Consumer Electron., v ol. 50, no. 3, pp. 777–786, Aug. 2004.
- [5]. S. Fifman, "Digital code lock of ERTS multispectral imagery," in Proc. Significant Results Obtained from Earth Resources Technology Satellite-1, 2014.
- [6]. Yang, L-H "Digital code lock design using VHDL with top-down method" 2000/01/01
- [7]. Alice Oke "Development of programmable electronic digital lock system" 2013/02/01.
- [8]. E.Supraja, Dr.H.S.k.Prasad, Wireless security system with digital code lock, July 2014.
- [9]. IEEE, Second international conference on signal and processing(ICISP), 30 November 2017
- [10]. Annie P. Oommen, Rahul, Pranav ,Ponni , Renjith Nadeshn, "Design and Implementation of a Digital Code " , February 2014.
- [11]. A.Adibisi ,"Programmable digital lock system", 2013/02/01.
- [12] Atif Afroz "digital smart door locking system", July 2022.