DESIGN OF A LOW COST DIGITAL LOCK

**Liakot Ali, Haslina Jaafar, Nurul Amziah Md.Yunus
and Wan Zuha Wan Hasan**

Dept. of Electrical and Electronic Engineering
Universiti Putra Malaysia (UPM)
43400 Serdang, Selangor Darul Ehsan
Malaysia
(liakot@eng.upm.edu.my)

RINGKASAN: *Kertas kerja ini mengemukakan reka bentuk sebuah kunci digit berkos rendah menggunakan perisian EDA. Sistem kunci konvensional yang sedia ada kini boleh diganti dengan kunci digit yang dicadangkan. Data yang dikodkan disimpan ke dalam ingatan kunci sebagai kunci utama. Apabila pengguna memasukkan kata laluan ke dalam sistem, kata laluan tersebut akan dibandingkan dengan kata laluan pada kunci utama dan seterusnya isyarat keluaran untuk mengaktifkan kunci dijana jika kata laluan tersebut betul. Kod boleh diprogram oleh pengguna untuk memantapkan lagi sistem keselamatan kunci ini. Sistem kunci yang dicadangkan ini mempunyai kos yang rendah dan mampu dimiliki oleh pengguna berpendapatan rendah.*

ABSTRACT: This paper presents the design of a low cost digital lock using EDA (Electronic design automation) software. The conventional lock and key system can be replaced using the proposed digital lock. A coded data word is stored in the memory of the lock as a master key. When user inserts his password in the lock, it is compared with the master key and an output signal for the actuation of the lock is generated if the password is correct. The code word is user programmable, which enhances the security of the lock. The proposed lock is low cost and affordable for the low budget people.

KEYWORDS: Digital Lock, ASIC, PLD, FPGA

INTRODUCTION

Digital technology has been improved dramatically during the last fifty years. Electronic products and equipment have become a part and parcel of our daily life (Liakot *et. al.,* 2004). Digital lock is a demand of this electronic era. The important features of the digital lock are keyless, flexible and reliable. For many applications such as maintaining entry only to authorised person into a large building, the digital lock eliminates the problem associated with duplication, distribution and loss of the key. Traditional locks are hardwired and are therefore inflexible.

The use of electronic locks has spread rapidly in recent years. Security code using push button, electromagnetic, smart card, wireless, voice tone, fingerprint and eye retina recognition system have replaced the conventional lock and key system. The security code door opening system offers a convenient way of opening and closing a door by entering a personal identification number (PIN) via a keypad. This is the most popular and affordable system in the market. Electronic card access is now the best technology for opening locked common area doors and gates. The card is software programmed and can be used to monitor employee attendance time. In wireless door opening system, which consists of transmitter and receiver, user can open the door remotely. Consequently, this system is commonly used for car, gate and garage opening system. Biometric is the statistical use of variations in the elements of living organisms such as fingerprint, voice and eye retina. This method is extremely accurate. Design of a micro-processor based electronic lock has been proposed (Poirier and Vishnubhotla, 1990). The system uses discrete electronic components, which are to be assembled on a printed circuit board (PCB). Hence the system is still costly. Due to high cost of the door opening system described in this paragraph, only selective customers use the electronic lock till now and get benefit of the modern technology.

To break the red brick of the price-wall, this paper presents the design of low cost digital lock using EDA software. The following sections of this paper describe the features, architecture and simulation result of the proposed digital lock.

FEATURES OF THE DIGITAL LOCK

The digital lock has the following features:

- 3-bit key for the input
- Require 3 bit-combination for pass-code
- Reprogrammable pass-code
- Alarm would active after detection of errors of the pass-code entered. The alarm is activated when the 3rd error pass-code is entered since the last correct pass-code.
- The activated alarm can only be deactivated when the correct pass-code is entered.

ARCHITECTURE OF THE DIGITAL LOCK

Figure 1 shows the block diagram of the digital lock. It consists of several modules such as decoder, counter, multiplexer and comparator.
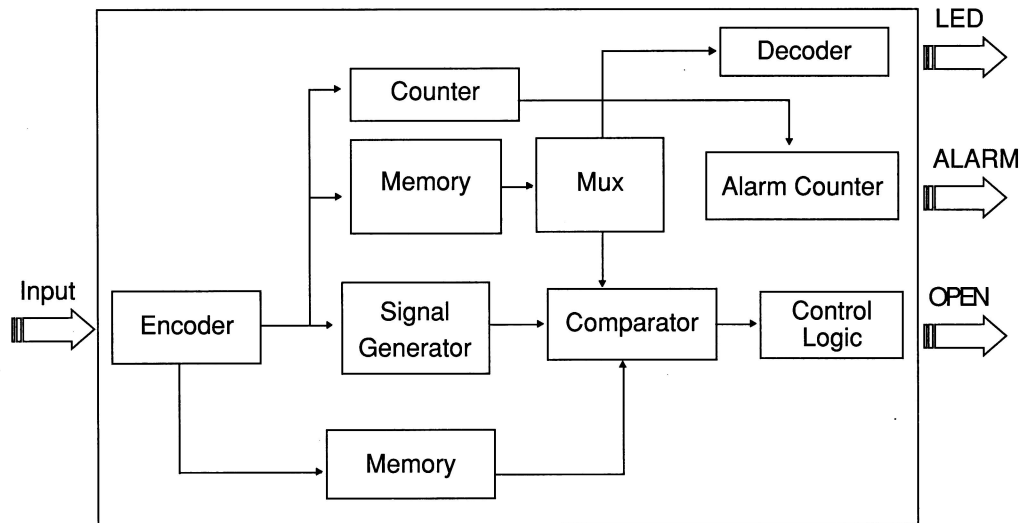

Figure 1. *Block diagram of the digital lock*

The digital lock runs on asynchronous mode. Due to its asynchronous operation, it can operate much faster because the user will not be bounded and constrained to any clock transitions. To open the lock, the correct combination of 3-bit input is to be keyed in using the buttons of a keypad. A signal generator is used to produce the pulse needed for its asynchronous operation when the key is pressed. An encoder has been designed to convert the input signal into useful signal before flowing into the internal circuitry of the digital lock. A counter is used in the design to keep track of the current bit of the input of the digital lock while it is processing. This counter plays an important role in the digital lock which allows only the wanted memory data to flow to the comparator and also inform the other part of the circuit of the current state of the digital lock. A memory circuit is designed to store the correct pass-code to open the digital lock. When the user keys-in the pass-code, the input signal is then compared with the memory data; if data input is correct, the open signal would be generated. If any of the pass-code is wrong, the digital lock would only respond after the user has pressed three buttons. As this digital lock is made programmable, a special memory counter has been designed to activate the specific memory circuit when the user wants to alter the pass-code to open the digital lock. The

comparator is used to compare the signals from the input and the signals from the memory. If the signals are identical, it will produce a signal which goes to the control logic circuit. The control logic circuit is designed to control all the actions of the digital lock such as comparison of the pass-code, to produce the open signal etc. The alarm counter is designed to activate the alarm when attempts to open the lock have failed. It increases the security of the digital lock and also avoids someone from tempting with the pass-code by trial- and error. When the alarm is activated, the user has to key in the correct pass-code to deactivate it. The decoder is designed to activate the LEDs. There are three LEDs, only one would light up at a time, each LED indicates the current bit of input.

SIMULATION RESULTS

The proposed digital lock has been designed using Max + plus II EDA software (Altera, 1998). Block by block design technique has been used in the proposed design. Every micro-functional block is designed and simulated in this approach and once its functionality is verified then another block is designed using the same approach (Floyd, 2002, Rabaev *et. al.* 2002, Mano, 2002, Nelson *et. al.* 1995). Finally, all the blocks are integrated and the whole system is verified again. Figure 2 shows the software generated symbolic diagram of the digital lock.
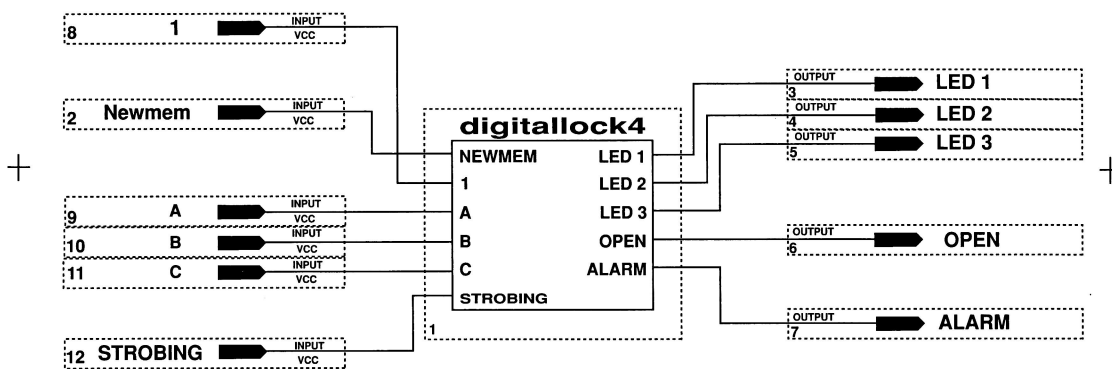

Figure 2. *Symbolic diagram of the Digital Lock*

Table 1 describes the input/output signals as shown in the symbolic diagram.

Table 1. Input/Output signals of the digital lock

Name	Type (Input / Output)	Description
1	Input	Always 'high'
NewMem	Input	'High' when reprogramming new pass-code into digital lock
A , B , C	Input	Keypad to receive input signal from the user
STROBING	Input	Signal used by internal circuitry to eliminate glitches
LED1	Output	To indicate the digital lock is currently waiting for bit 1 of pass-code.
LED2	Output	To indicate the digital lock is currently waiting for bit 2 of pass-code
LED3	Output	To indicate the digital lock is currently waiting for bit 3 of pass-code.
OPEN	Output	Signal to mechanical devices to open the lock
ALARM	Output	Signal to alarm, when error has occurred 3 times consecutively

Figure 3 shows the simulation results of the digital lock. Part I as indicated in Figure 3 shows the digital is being programmed into having the pass-code as A-B-A. While programming, NewMem input is at logic high. While the NewMem input is activated, the digital lock would stop all the signaling process and proceed to receive data only. After the digital lock is programmed, the NewMem input is deactivated. In part II, III and IV, the digital lock is tested by three wrong pass-codes. In part II, the digital lock is tested by the input A-B-C. As a result, the digital lock did not respond to open the lock because of the wrong pass-code. In part III, the digital lock is tested by the input B-C-B as this is the second error since the last time a correct pass-code is entered. The digital lock did not respond to open the lock and the LEDs return indicating the digital lock is waiting for the first bit of the combinational input. In part IV, the digital lock is tested by the input C-B-B, which is also the wrong pass-code. As the 3rd error of pass-code entered into the digital lock, the alarm is activated. As shown in the simulation the alarm remains aloud. In part V, the correct pass-code is entered which is A-B-A. When the correct pass-code is entered, the alarm is deactivated and at the same time the digital lock would send a signal to open the lock.

Simulation results as shown in different parts of Figure 3 prove the proper functionality of the lock when it is realised into physical hardware. Hardware realisation of the design can be performed using a single chip field programmable gate array (FPGA) or programmable logic device (PLD) circuit. It can also be fabricated as an application specific integrated circuit (ASIC) for improved performance.
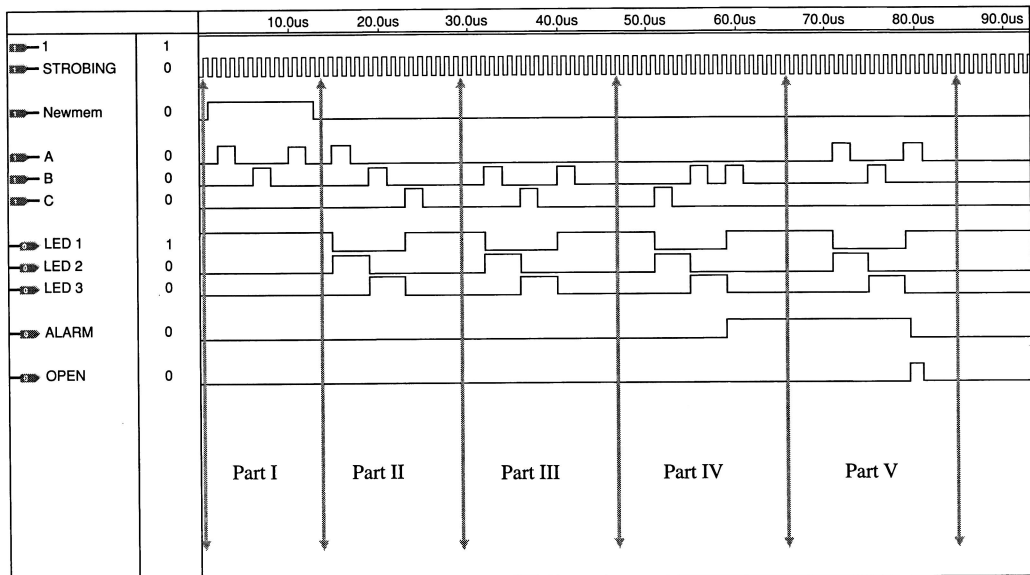

Figure 3. *Simulation results of the digital lock*

CONCLUSION

Design of a digital lock using EDA software has been presented in this paper. Its simulation results ensure the proper functionality of the lock in its different mode of operation. Since the design of the digital lock can be realised into single chip hardware, it will be low cost with improved performance. The design concept proposed in this paper can be further extended to a more complex circuit, which may have larger word for pass-code and also more input keys, to enhance the security as well as performance of the lock.

REFERENCES

Altera (1998). Data Book, Altera Corporation, **37(1)** pp: 17-28 San Jose, USA.

Floyd, T. L. (2002). Digital fundamentals, Prentice Hall, USA

Liakot, A., Roslina, S., Ishak, A., Alauddin M. A. and Bambang S. S. (2004). Challenges and directions for IC testing, integration. *VLSI Journal,* Elsevier Science, Netherland.

Mano, M. M. (2002). Digital design, Prentice-Hall International Inc., New Jersey, USA.

Nelson, V. P., Nagle, H. T. and Irwin, J. D. (1995). Digital logic circuit analysis, Prentice-Hall International Inc., New Jersey, USA.

Poirier, D. C. and Vishnubhotla, S. R (1990). A microprocessor-controlled door lock system. *Consumer Electronics, IEEE Transactions*, **36(2)**: pp 129-136.

Rabaev, J. M., Anantha C. and Borivoje N. (2002). Digital integrated circuits, Prentice Hall, UK.