A Dynamic Cryptography Door Lock System Based on Visible Light Communication

Shuyan Chen[1], Jianhua Shen[2,*], Xiaodi You[2], Jian Chen[2], Changyuan Yu[3]
[1] Jinling College, Nanjing University, Nanjing, China; [2] School of Telecommunications & Information Engineering, Nanjing University of Posts & Telecommunications, Nanjing, China; [3] Department of Electronic & Information Engineering, The Hong Kong Polytechnic University, Hong Kong.
*Contact email: shenjh@njupt.edu.cn.

***Abstract*—A visible light based door identification system without auxiliary access unit is proposed. Based on a prove-of-concept implementation with CPLD/FPGA devices, dynamic cryptography door lock scheme has been verified. By updating the sequential half-duplex random passcode after every door-key match, higher security can be ensured compared with conventional schemes.**

Index Terms—Visible light communication, Security, CPLD, FPGA.

I. INTRODUCTION

Due to the advantages of low cost, energy efficiency, etc., visible light communication (VLC) techniques has been widely investigated [1]. In particular, visible light cannot penetrate through walls, therefore VLC inherently features high data security. On the other hand, electronic controlled door lock systems have been widely deployed in areas where safety and convenience are in demand. Typical electronic door lock systems use techniques such as keypads, NFC [2] and Wi-Fi [3]. These door lock systems are expensive and not fully secure.

In order to overcome the problem, in [4], the authors build a door lock system using visible light technique. However, the system still needs to use Bluetooth to update passcode. Besides, the system cannot produce quasi-random passcode. The employment of Bluetooth and Pseudorandomness will also severely limit the high security and cost effectiveness.

In this paper, we propose a novel door lock system, where bidirectional data links are based on visible light. The prove-of-concept implementation is based on a complex programmable logic device (CPLD) board and a field programmable gate array (FPGA). By using FPGA in our system, the quasi-random passcode can be generated [5].

II. PROPOSED VLC DOOR LOCK SYSTEM

A. System Structure

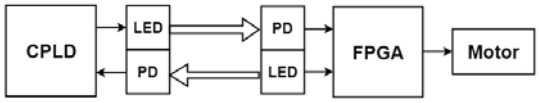

Figure 1. System structure

The work was supported by National Natural Science Foundation of China (No. 61271239).

Fig. 1 shows the block diagram of the door lock controlling system. This whole system can be assorted into two separate systems, i.e., the "Key system" and the "Lock system". The "Key system" mainly contains a light emitting diode(LED), a photodiode(PD) and a CPLD. The "Lock system" mainly contains a LED, a PD, an FPGA and a motor.

B. Working Procedure

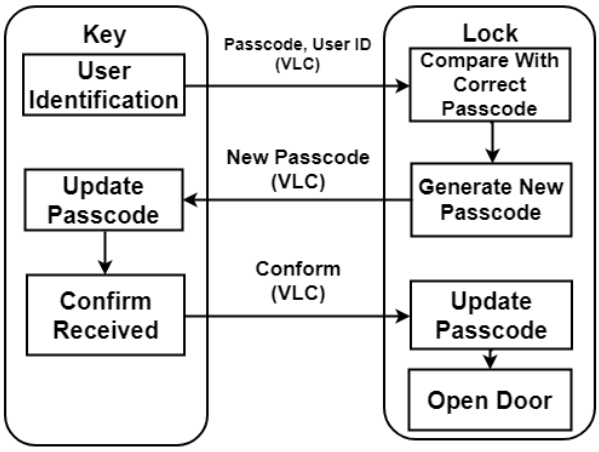

Figure 2.The door opening procedure

Fig. 2 shows the block diagram of the door opening procedure. Note that in this case all data links are setup via VLC. The procedure mainly includes three steps:

(a) When a user places the Key on a door lock and presses the button, the Key will transmit its passcode and user identification (ID) to the Lock.

(b) After the Lock receives the data, it will compare the received passcode with the ID's corresponding passcode. If they are matched, the Lock will generate a new quasi-random passcode and feed it back to update the Key for the door opening in the next time.

(c) If the Key receives the new passcode correctly, it will response by sending a confirm message to the Lock. When there is a passcode updating and a confirm message received, the new passcode will be stored and the motor will be activated to open the door.

C. Transmitter and Receiver

Based on IEEE standard 802.15.7[6], On-Off Keying (OOK) modulation is applied to transmit data between the Key and the Lock. When receiving data, bit synchronization will be performed on CPLD/FPGA with a Verilog developed digital phase lock loop (DPLL).

Note that the LED needs a constant current source and the PD needs an amplification circuit, which can only be actualized outside the CPLD/FPGA chip.

At the Key side, CPLD/FPGA I/O uses 0 V and 3.3 V to represent digital "0" and "1", respectively. The LED is attached directly to the CPLD/FPGA I/O port as in Fig. 3. LED will flash to transmit data at a flickerless rate of 10kb/s to avoid possible harm to human eyes.

At the Lock side, the PD is attached to a differential amplification circuit as in Fig. 3. It will output 0 V and 3.3 V to represent digital "0"and "1", respectively, according to the received visible light state. As a result, VLC signal can be converted into binary data for further processing in the electrical domain.

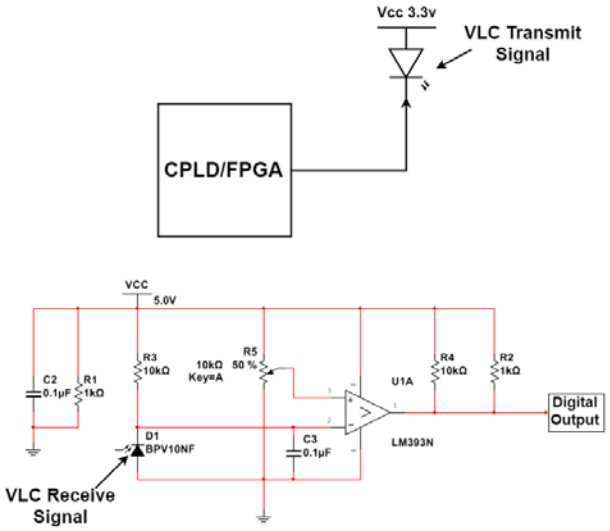

Figure 3.Transmitter and Receiver Circuit

D. Quasi-Random Number Generating

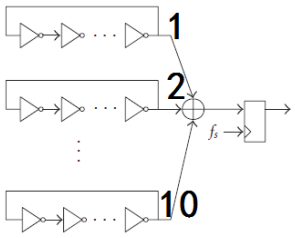

Figure 4. Quasi-random Number Generator

In order to ensure data security, we adopt a quasi-random number generator. It contains ten equal length oscillator rings which serve as noise sources. The rings are connected to an exclusive OR (XOR) tree. The output from the XOR tree is sampled by one D flip-flop. The generator can be developed by Verilog and actualized on FPGA. Based on the difference of the sampling time, the system can output quasi-random digital "0" and "1" sequence [5].

E. Data Transfer

In Fig. 5 we provide the waveforms of OOK at the transmitter and receiver side, respectively. A binary data sequcence of "110000000101" is transmitted and received. The upper waveform is the modulated pattern while the lower waveform is the demodulated version. Apparently, the two waveforms are identical, thus the data is deemed to be transferred properly.

Figure 5. Transmitted and Received waveform

F. Door Demo

Figure 6. Door closed (left) and opened (right)

In Fig. 6, we use lego blocks to demo a door. The circled part is the motor attached to the FPGA. The motor will drive the door to rotate, which represents door opening actuation. We repeatedly tested the door opening operation for thousands of times and no false door opening action is caught.

III. CONCLUSIONS

We have demonstrated a visible light identification system without auxiliary access unit for a door lock application. By using bidirectional VLC, the installation cost is much lower compared to other conventional schemes. In addition, data security is high by updating the passcode with quasi-random numbers. The prototype is beneficial to future commercialization of VLC.

REFERENCES

[1] L.U.Khan, Visible light communication: *Applications, architecture,standardization and research challenges, Digital Communications and networks* .Feb 2016.

[2] C.-H. Hung, Y.-W. Bai, and J.-H. Ren,*IEEE 5th ICCE-Berlin*, pp. 260-261,2015.

[3] N. Hashim, N. F.A.M.Azmi, F.Idris and N.Rahim, *ARPN Journal of Engineering and Applied Sciences*,vol. 11,no. 5, March 2016.

[4] Seok-Jeong Song and Hyoungsik Nam,*Current Optics and Photonics*,vol. 1, no. 2, pp. 90-94,April 2017.

[5] KnutWold and Chik How Tan,*International Journal of Reconfigurable Computing*,June 2009, Article ID 501672.

[6] IEEE 802.15.7 Visible Light Communication: Modulation Schemes and Dimming Support.