International Journal of Engineering & Technology, 7 (3.33) (2018) 90-93

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Design of Power Monitoring Security Module for Embedded Device with Elliptic Curve Algorithm

***Angyoon Jeon[1] and Youngho Ko[2]**

,Chonbuk National University, Jeonbuk, Korea*
**Corresponding author E-mail: jeonak@jbnu.ac.kr, koyh@jbnu.ac.kr*

Abstract

Currently, we are pursuing smart home construction, intelligent living environment, environment-friendly residential living and quality of life. However, power monitoring terminals using various wired and wireless networks and protocols in home networks are very vulnerable to security. In this study, we design and develop security system for smart meter terminal which can analyze the cryptographic technology of smart meter, which is vulnerable to physical attack, and exposes personal information from the outside, and maximize the efficiency of terminal.

Keywords: *SPA, Scalar multiplication, Elliptic Curve Discrete Logarithm Problem, sub channel attacks.*

1. Introduction

Since the public-key cryptosystem was first proposed by Diffie-Hellman in 1976, information confidentiality, integrity, Party authentication, and non-repudiation [1]. Elliptic curve cryptographic schemes were proposed independently in 1985 by Neal Koblitz [2] and Victor Miller [3]. The Elliptic Curve Cryptosystem (ECC) is an elliptic curve. The elliptic curve cryptosystem has attracted considerable attention in obtaining public and private keys because it provides the same level of security as other cryptosystems currently in use, 1/4. When the key size is reduced, it implies that it consumes less computation and less energy in encrypting and decrypting data. For digital signatures currently being discussed, public key cryptography is essential, for the most widely used RSA now, Key sizes must be 1024 bits to be considered safe, because it has the disadvantage of being too long. On the other hand, ECC guarantees the same level of security with a key size of about 160 bits, which can be used for smart cards and electronic money for e-commerce transactions. Further, the present invention can be applied to encryption of a mobile communication device having a limited power source capacity. For this reason, ECC is attracting attention as a next generation public key cryptography. However, the practical implementation of elliptic curve cryptography is the most problematic implementation of finite field arithmetic based on elliptic curve arithmetic, because it is a matter that must be solved.

Therefore, this study aims at developing an efficient computation method for finite elements, and analyzing elliptic curve cryptosystem which can be applied effectively and its implementation.

Also, in this paper, we propose a protocol such as ISO / IEC, JTC1, SC25, which is in the process of international standardization of protocols and interconnection technologies required for home electronic devices. Designing a hardware device, for authentication and service of packet data of electronic devices, public key-based encryption, Elliptic curve, hardware design using encryption algorithm.

2. Development Contents of Elliptic Curve Cryptosystem Module

In order for an elliptic curve to be considered to be at least safe, it should at least be robust against attacks against known elliptic curves. Apart from the theoretical safety of the cryptosystem, a so-called side channel attack (SCA), in which a secret key is found by using / analyzing additional information such as power consumption, difference in execution time or power consumption of an algorithm, , Mobile phones, PDAs, and the like.

2.1 Elliptic Curve Algorithm

The elliptic curve standards used for hardware implementation are IEEE P1363, ANSI X9.62 (Elliptic Curve Digital Signature Algorithm), ANSI X 9.63 (Elliptic Curve Key Agreement and Transmission Protocol), ISO / IEC Based on the Elliptic curve cryptography standard), SEC 2 (Elliptic curve cryptography is the standard), ATM Forum (proposed as a system that provides confidentiality, authentication, data integrity and access control), PKCS 313). The elliptic curve theory used in this paper is a field of logarithmic geometry that has been studied over the past 100 years, and it is easy to implement cryptographic applications because it has an efficient algorithm that performs natural group operation and its operation. The elliptic curve cryptosystem is a cryptographic system that replaces multiplicative groups of finite fields used in discrete algebra by elliptic curve groups. The efficiency of an elliptic curve cryptosystem can be seen from the following three perspectives.

First, computational aspect: Here, the amount of computation is the amount of computation required to perform the public key and private key transmission, and the elliptic curve cryptosystem has a very small amount of computation compared to the existing public key cryptosystem

Second, key size aspect: elliptic curve cryptosystem has very small key size, so there is little storage space required to store any key.
Third, in terms of communication bandwidth: elliptic curve cryptosystems require very little communication bandwidth to encrypt messages or transmit signatures. Figure 1 shows an overall block diagram of what we are going to develop.

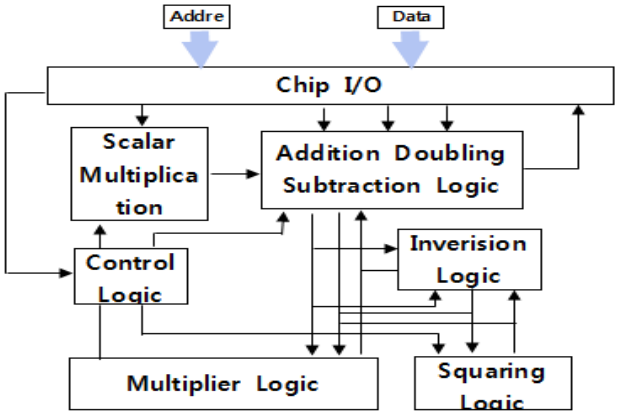

Fig. 1: overall block diagram.

2.2 Elliptic Curve Scalar Multiplication Algorithm Corresponding to SPA

For the two points P= (x_1, y_1) and Q= (x_2, y_2) of the elliptic curve GF (p) elliptic curve *E:* $y^2 = x^3 + ax + b$.

- $P+Q=(x_3,y_3), x_3=(\frac{y_2-y_1}{x_2-x_1})^2-x_1-x_2, y_3=(\frac{y_2-y_1}{x_2-x_1})(x_1-x_3)-y_1$
- $2P=(x_3,y_3), x_3=(\frac{3x_1^2+a}{2y_1})^2-2x_1, y_3=(\frac{3x_1^2+a}{2y_1})(x_1-x_3)-y_1$

Addition of two points on the elliptic curve and doubling of one element can be obtained by subtracting two finite elements, the inverse of one finite element, the multiplication of two finite elements, and the square of one finite element. It can be obtained by repeating double operation and addition" with scalar multiplication $dP = (d_{n-1}, d_{n-2}, \ldots d_0)P=(d_0P+d_12P+ d_22(2P)+\ldots)$ of elliptic curve.

2.3. Multiplier Structure

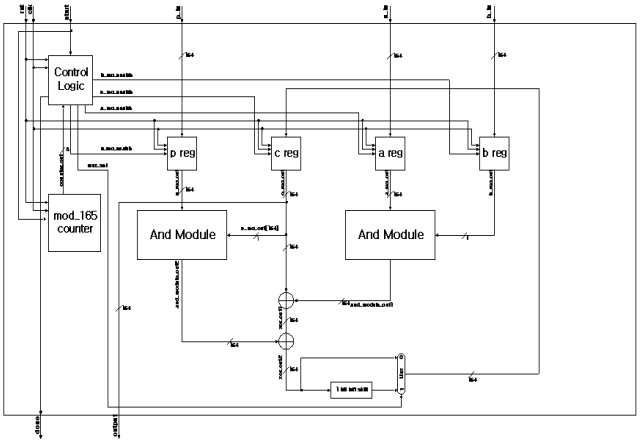

Fig. 2: Multiplier's architecture.

Figure 2 shows the architecture of Multiplier.
When the prime number is $P= 2^{n-t} A = a_{n-1}2^{n-1}+a_{n-2}2^{n-1}+\ldots+a_12+a_0 = (a_{n-1}, a_{n-2}, \ldots a_0)$ with $B = b_{n-1}2^{n-1}+b_{n-2}2^{n-1}+\ldots+b_12+b_0 = (b_{n-1}, b_{n-2}, \ldots b_0)$ of product.
AB mod P = $A(b_{n-1}, b_{n-2}, \ldots, b_1,b_2)$ mod P
$= bn\text{-}1(A2^{n-1})+bn\text{-}2(A2^{n-1})+ \ldots +b1\ (A2)+b_0A$ mod P
$= (\ldots((b_{n-1}A2 \text{ mod } P)+b_{n-2}A \text{mod } P)2 \text{ mod } P+\ldots+b_1A \text{ mod } P)2 \text{ mod } P+b_0A \text{ mod } P$
Can be obtained by repeatedly applying mod P and mod P of two finite elements. Figure 3 shows the hardware architecture.

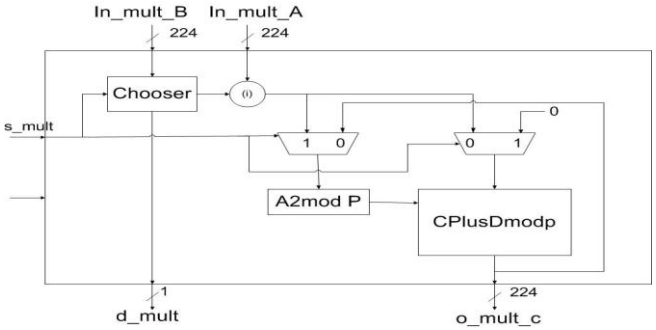

Fig. 3: Hardware architecture.

Table 1 and Figure 4 show the result of simulation and simulation result of UmodP performed on the result using the integer adder obtained by A2modP and CPlusDmodP of the multiplier.

Table 1: Synthetic result performed by UmodP

Device utilization summary: Selected Device : 6vlx760ff1760-2 Slice Logic Utilization: Number of Slice Registers: 240 out of 948480 0% Number of Slice LUTs: 2945 out of 474240 0% Number used as Logic: 2945 out of 474240 0% Slice Logic Distribution: Number of LUT Flip Flop pairs used: 2951 Number with an unused Flip Flop: 2711 out of 2951 91% Number with an unused LUT: 6 out of 2951 0% Number of fully used LUT-FF pairs: 234 out of 2951 7% Number of unique control sets: 3 IO Utilization: Number of IOs: 1124 Number of bonded IOBs: 1124 out of 1200 93% Specific Feature Utilization: Number of BUFG/BUFGCTRLs: 1 out of 32 3%
Timing Summary: ---------- Speed Grade: -2 Minimum period: 22.751ns (Maximum Frequency: 43.954MHz) Minimum input arrival time before clock: 11.977ns Maximum output required time after clock: 6.438ns Maximum combinational path delay: 6.540ns

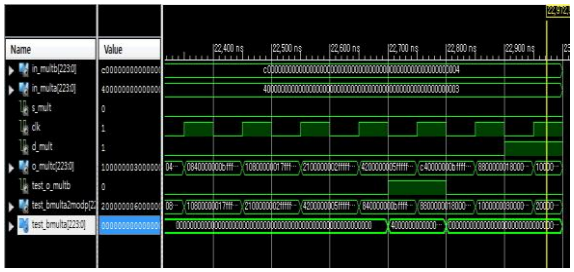

Fig. 4: Simulation result

Figure 5 shows the experimental setup for measuring the amount of power consumed by the security module during cryptographic operation. Figure 6 shows the amount of power consumed by the internal basic operations used in the cryptographic algorithms through the experimental apparatus shown in Fig. Figure 7 shows the modular exponentiation algorithm in the cryptographic module. When the implementation of the if () statement is determined according to the format in which the bits of the key are divided into 0 and 1 as shown in the left figure 5 is a diagram showing that the secret key can be easily found by collecting the electric power waveform consumed by the user.

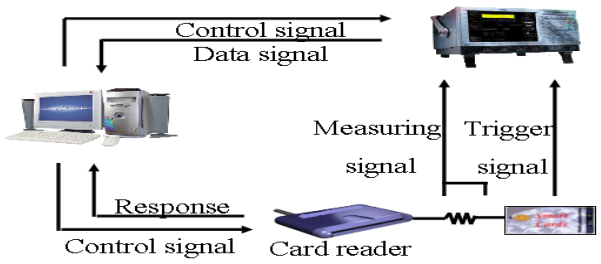

Fig. 5: Power equipment configuration diagram of power analysis.

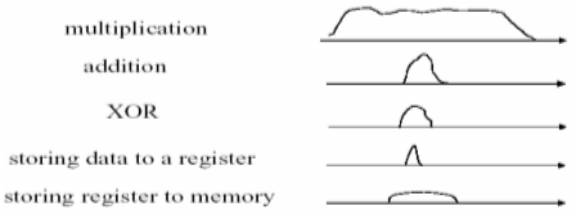

Fig. 6: Comparison of Power Consumption by Operation.

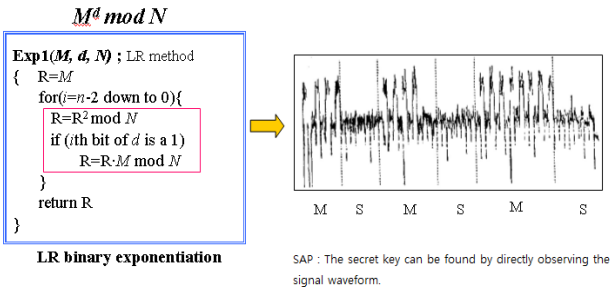

Fig. 7: SPA to analyze the power waveform generated by the modular exponentiation algorithm. (Example)

Therefore, in this study, we propose an elliptic curve scalar multiplication algorithm corresponding to simple power consumption analysis (SPA) technique per bit of secret key without speed reduction.

2.4. Inverted Structure

The method of obtaining the inverse of the finite element is obtained by using Equation $AR \equiv 2^k U \bmod P$, $AS \equiv 2^k V \bmod P$.
If the initial value is $V \leftarrow P$, $U \leftarrow A$, $R \leftarrow 1$, $S \leftarrow 0$, then k = 0, then both equations are satisfied.

2.5. Finite Field Operation Verification Method

A random integer X satisfying 0 <X <q is selected for the base point G on the elliptic curve in accordance with the generation method of the key pair described in the ECDSA verification system of the encryption algorithm verification standard (ECDSAVS) = Find the point of the only elliptic curve calculated by XG. During the process of calculating Y = XG, the verification of the finite field operation is performed through the intermediate value of the finite field operation result.

3. Cryptographic Module Interface Design

There is a need for a step-up of security, adding an information appliance authentication function, enabling services to be delivered only through valid devices.
It is necessary to provide data encryption and integrity to prevent spoofing of personal information and unauthorized use of information devices, data tampering or tampering by malicious hackers.
In this paper, we try to provide confidentiality and integrity of data generated from information devices with hardware module to protect data of information devices in smart home. As smart-armed devices such as smart phones and smart TVs continue to emerge, observations are being made that household appliances have entered the era of smart appliances. N-screen services are becoming more widespread than traditional analogue appliances, simply replacing them with digital smart appliances and sharing and viewing content between smartphones, smart TVs and PCs.
We have proposed an embedded-based cryptographic module interface design that can connect and interoperate with a home network system that remotely controls electricity, gas, water use, meter reading, crime prevention, and disaster prevention while remotely controlling smart home appliances with smartphones.

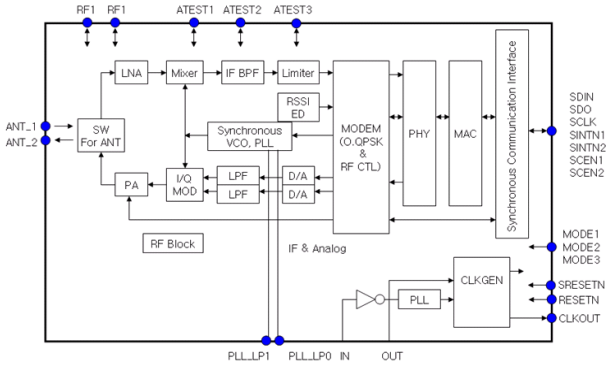

Fig. 8: Control board.

Figure 8 shows a mainboard that monitors and controls the amount of power between home appliances and meters to confirm the transmission of household appliances' power to the smart grid meter.

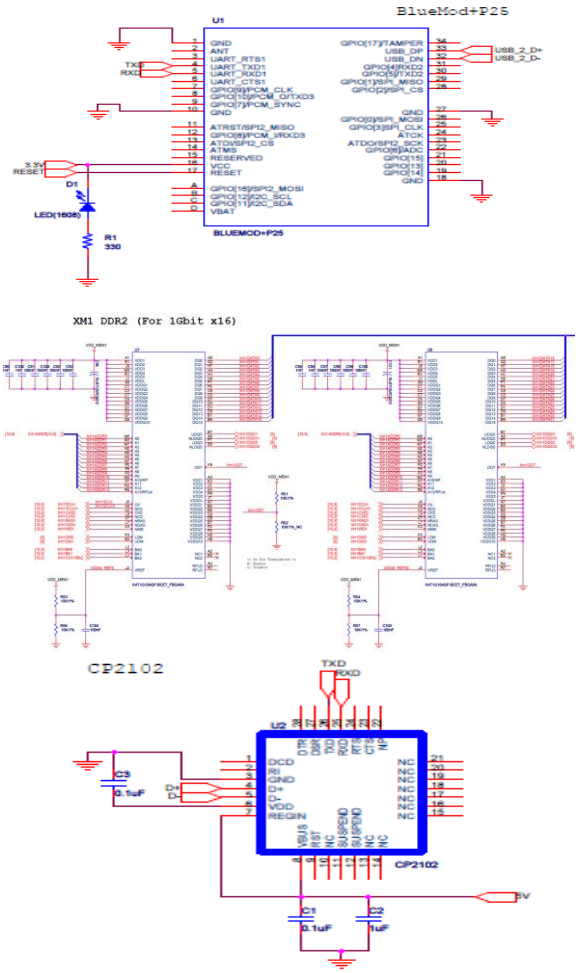

Fig. 9: Receiver module circuit design

Figure 9 shows that the terminal (home appliance transmission module) transmission / reception communication is designed by using Bluetooth (Stollmann) 2.0.

Fig. 10: Electricity Consumption Monitoring System

Figure 10 shows an integrated monitoring experiment image by collecting the electric energy of household appliances. It is designed based on Android. Consumer Electricity The wireless transmission was designed and manufactured with Stollmann Bluetooth 2.0.

4. Conclusion

In a smart home environment, all the information devices in the home are connected organically and exchange data with each other, and the service is provided through such data. In this environment, the diversity of information devices and the sharing of resources among the information devices are becoming more complex and diversified in terms of security considerations.
In this paper, we design and develop a device which is convenient for smart home appliances with smart period authentication, key management, data protection and low area low power.
In addition, an embedded-based power monitoring security module that can lead the secure state of smart home by applying the algorithm corresponding to SPA has been designed.
We designed and implemented an Android - based embedded board to test the developed module. Smart grid as well as u-health that transmits personal biometric information.
Future research directions include integration of one gateway for each terminal application for home network configuration such as U-health care, smart grid, and environmental sensor. In order to develop such devices, we will study security algorithms that can be interworked with security enhancement functions and an integrated system to control them.

References

[1] Diffie W, Hellman ME (1976), “Multiuser cryptographic techniques,” presented at National Computer Conference, New York, and June 7-10, 1976.
[2] Koblitz N (1987), “Elliptic curve cryptosystems”, Math Computer 48, 203–209.
[3] Miller V (1986), “Use of elliptic curves in cryptography”, Advances in Cryptology—CRYPTO ’85, Lecture Notes in Computer Science, 218. Springer, 417–426