Regular paper http://dx.doi.org/10.13067/JKIECS.2013.8.10.1485

임베디드 전력 모니터링 보안 모듈 설계

윤찬호* · 김광준** · 장창수***

Embedded-based Power Monitoring Security Module Design

Chan-Ho Yoon* · Gwang-Jun Kim** · Chang-Soo Jang***

요 약

스마트 그리드용 전력망이 구축시범사업이 진행됨에 따라 스마트 디지털가전 AV기술, 냉난방 습도 공기 자동관리를 위한 복합에너지 관리기능을 담당하는 스마트 홈 에너지관리기술, 노약자와 장애인을 위한 주거설계와 가족 구성원에 대한 개인별 바이오정보 측정을 담당하게 될 헬스케어 기술, 생체인식 보안과 동작감지센서 등을 다루는 스마트 홈 시큐리티 기술 등 연구가 진행되고 있다. 본 논문에서는 물리적 공격에 취약한 외부에 노출되는 문제점이 발생하게 되는 스마트미터기에 대응되는 암호기술을 분석하고 단말기의 효율성을 극대화 할수 있는 스마트 미터기 단말기용 보안시스템 설계를 제안하였다.

ABSTRACT

The demonstration project of the electrical grid for Smart grid is progressed, the smart digital appliances AV technology, Smart home energy management technology charging the management function of complex energy for the automation management of air conditioning and heating, humidity and air, the health care technology charging the design of housing for the elderly and disabled and the measurement of individual bio information, and the Smart home security technology dealing with the biometric security and motion sensors, etc. have been studied. The power monitoring terminal which uses a variety of wired and wireless networks and protocol is the target additionally to be considered in addition to the security vulnerabilities that was occurred in the existing terminal. In this research paper, the author analyzes the cryptographic techniques corresponding to the smart meter occurred by the problems that are exposed on the outside which are vulnerable to physical attacks, and intends to propose the design of the security systems for the Smart meter terminal being able to maximize the efficiency of the terminal.

키워드

Embedded System, Smart Grid, Security Module, Cryptography
임베디드 시스템, 스마트 그리드, 보안 모듈, 암호기법

Ⅰ. Introduction

Smart grid is the next generation intelligent electrical grid which IT technology is fused into the electrical grid, and the cyber security threat of this grid is greatly increased in comparison with the existing electrical grid, and the security efforts of Smart grid is constantly being researched. The

* 전남대학교 컴퓨터공학과(yoonchanho@hotmail.com)
** 교신저자(corresponding author) : 전남대학교 전기전자통신컴퓨터공학부(kgj@jnu.ac.kr)
*** 전남대학교 전기전자통신컴퓨터공학부(csjang@jnu.ac.kr)
접수일자 : 2013. 08. 23 심사(수정)일자 : 2013. 09. 23 게재확정일자 : 2013. 10. 21

development of terminal and various contents for the resulting energy savings and energy reduction is being achieved. Especially, if the device which sensors are built-in it can be directly connected to an external network, measured data is delivered directly to the service provide[1],[2],[3]. On the other hand, if LAN is equipped to appliances, the measured information through the gateway is sent to the external network and then is delivered to the service provider. For example, in the case of monitoring using the environment sensors, the measured data is passed to the gateway in the home using a short-range communication such as ZigBee, Bluetooth, and is sent to external network. At this time, the gateway should be prepared for the security vulnerabilities in addition to the ability to simply transfer data[4],[5],[6].

In this research paper, the hardware device by analyzing ongoing ISO/IEC JTC1 SC25 protocol as international standards for the protocol and interconnection technology associated with electronic equipment and systems in the home related to data interchange/operation through FPGA platform, was designed, and also the hardware applying an elliptic curve cryptographic algorithm corresponding to simple power attack method that is one of the sub-channel the public key-based password in order to obtain the authentication and service for packet data of electronic devices was designed.

II. Power Monitoring Security Module

IEEE P1363, ANSI X9.62(elliptic curve electronic signature algorithm), ANSI X 9.63(elliptic curve key agreement and transport protocol), ISO/IEC(1488 additional type electronic signature-part 3 E1GAMAL type signature algorithm in the certificate-based mechanism), ATM Forum(Proposed as a system that provides confidentiality, authentication, data integrity and access control), PKCS 313(during standard working by Elliptic curve cryptography standard), SEC 2(Elliptic curve cryptography come up as a standard), SEC 2(Elliptic curve cryptography comes up as a standard), etc. that are the standard of the elliptic curve used to the hardware implementation, can be seen[7],[8],[9].

Because the elliptic curve theory used in this paper has a natural group operation and an efficient algorithm that perform the operations as one field of the algebraic geometry that have been studied over the past 100 years, cryptographic applications is easy. Elliptic Curve Crypto system is the crypto system that the multiplication group of the finite field that use in discrete logarithm, is replaced to the elliptic curve group. Efficiency of elliptic curve cryptography system can be seen from the following three viewpoints. Figure 1 shows the entire block diagram of elliptic curve algorithm that is composed of several circuit.

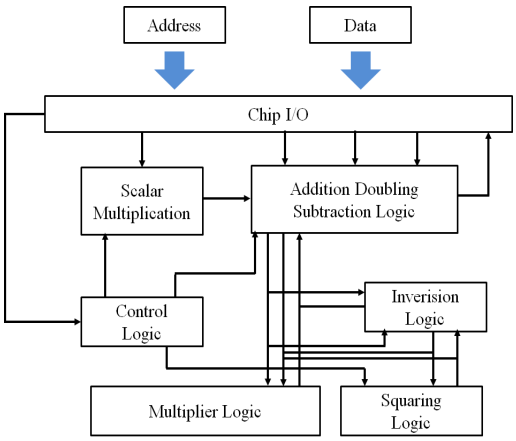

Fig. 1 Entire block diagram

First, the computational complexity side. Where the computation is required in order to perform a public key and a private key transport, and the elliptic curve crypto system has very small computation compared to the existing public-key cryptography.

Second, the size side of key. The elliptic curve cryptography system is very small size of the key, so the less space is required to store arbitrary key.

Third, aspects of the communication bandwidth. In the elliptic curve cryptography system, the communication bandwidth required to encrypt a message or to send signatures is very small.

- The design of Loop structure for the efficiency of optimal resource

- Designing the shortening method of multiplication time improving by transforming Coron's algorithm as an inversion device and a multiplication device to minimize the performance degradation by SPA correspondence like Figure. 2.

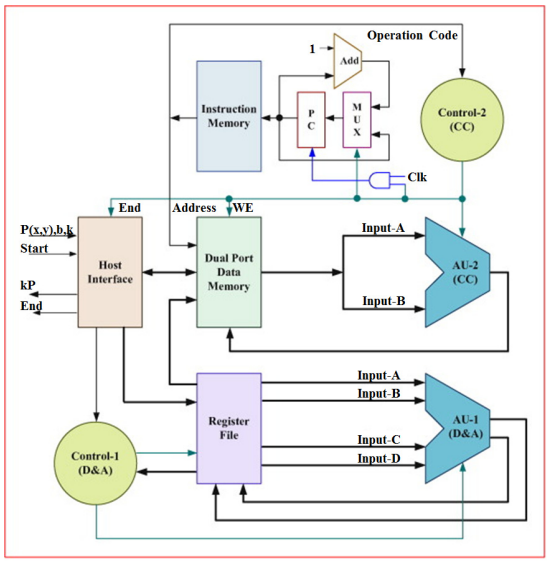

Fig. 2 Scalar multiplication architecture

- Appropriate algorithm design in VHDL for FPGA implementation
- FPGA implementation of elliptic curve algorithm and producing of test board for measurement of simple power consumption
- Commands, Internal operations, internal I/O module design and FPGA Implementation
- Memory control design for key management
- External interface design

Figure 3 is the experimental setup diagram measuring the amount of electric power consumed while the security module performs cryptological operation.

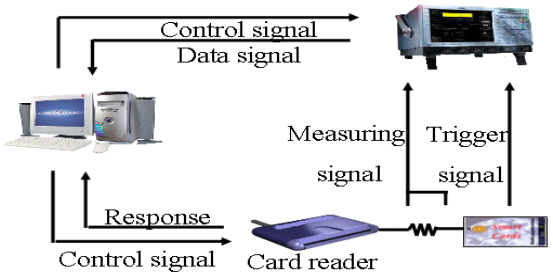

Fig. 3 Experimental equipment diagram of power analysis

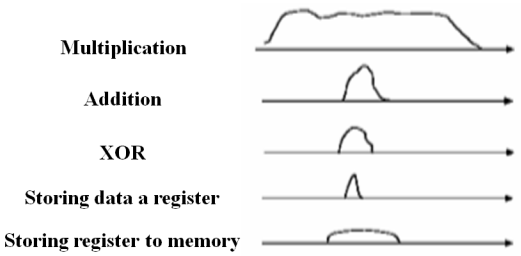

Fig. 4 Comparison of power consumption according to operation

Figure 4 shows that the amount of power being consumed by internal basic operations used in cryptographic algorithm through the experiment device such as shown in Figure 3 is different.

III. Cryptographic Module Interface Design

The need for security one-step enhanced that allow to be provided through only valid devices by

adding the authentication function of information appliances has been raised, and toprovide data encryption and integrity to prevent the leakage of individual sensitive information by malicious hackers, and unauthorized use of information appliances, or to prevent the forgery of data became necessary. In this paper, the author intends toprovide the confidentiality and integrity of data occurring from information appliances as a hardware module to protect the data of information appliances in the smart home. As the devices armed with 'smart' such as smartphone and smart TV have been continually come pouring out, it is the situation that the observation that life appliances rushed to the era of smart appliances is coming out.

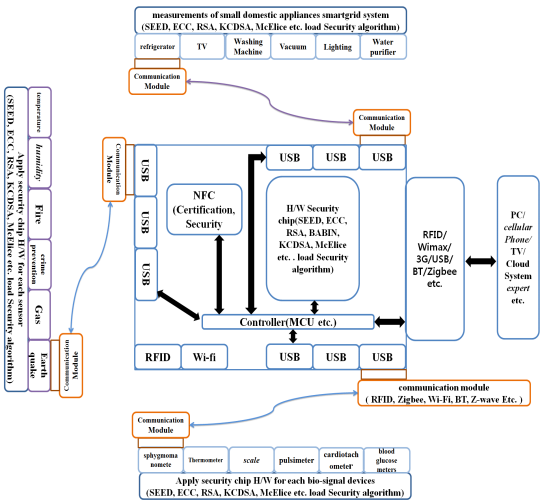

Fig. 5 Cryptographic module interface design for home devices

Figure 5 shows that N screen service interlocked so that existing analog household appliances can be shared and appreciated the contents between smartphone and smart TV, PC beyond dimension to be replaced by simply digital smart appliances is widely spread, and while being reached the time that the household smart appliances are remote controlled by a smartphone, that the design of embedded-based cryptographic module interface coupled and interoperable with the home network system remotely controlling the use and metering of electricity, gas and tap water, and crime prevention and disaster prevention are proposed.

Figure 6 shows the main board which can monitor and control the amount of power between household appliances and meter to confirm the power transmission of the appliances to the smart grid meter. Figure 6 shows that the communication of transmitting and receiving of terminals (transmission module of household appliances) was designed by applying Bluetooth (Stollmann) 2.0.

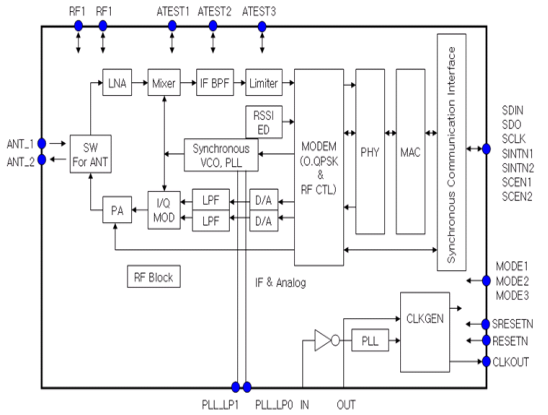

Fig. 6 Monitoring of electric power amount and control board

Figure 7 shows that the communication of transmitting and receiving of terminals (transmission module of household appliances) was designed by applying Bluetooth (Stollmann) 2.0. Figure 6 is the photograph showing integrated monitoring experiment by collecting the amount of power of the household appliances, and this was designed based on Android, and the wireless transmission of the appliances was designed with Stollman Bluetooth 2.0.

Fig. 7 Electric power amount monitoring of household appliances

Ⅳ. Conclusions

In this paper, the embedded-based electric power monitoring security module which could lead safe energization of Smart home because it is easy to apply to smart appliances due to the authentication or key management and data protection between smart household appliances, and low-area and low-power, and the application of the algorithm corresponds to SPA was designed, and in order to experiment it, Android-based embedded boards have been designed and implemented. Smart grid, as well as u-Health transferring personal biometric information, etc. will be applicable.

In future research directions, the gateways suited for each terminal will be integrated into a gateway for U-healthcare, smart grid and environment sensors and home network configuration, and the author intends to study the security algorithms that can interlock between the heterogeneous devices which the security enhancement function is added, and the integrated system which controls it.

Acknowledgement

This research was financially supported by the Ministry of Education, Science Technology (MEST) and National Research Foundation of Korea(NRF) through the Human Resource Training Project for Regional Innovation

REFERENCES

[1] Don Johnson, The Elliptic Curve Digital Signature Algorithm,certicom.Corporation, 2001.

[2] Davies. John wiley&sonslnc,"Implementing Ssl/ Tls using cryptography and PKi"(2010) Algorithm (ECDSA), ANSI, x9.62-1998, approved Jan.1999.

[3] Sklavos, Nicolas(EDT), Zhang, Xinmiao(EDT), Wireless Security And Cryptography", Taylor &Francis, 2007.

[4] x9.62,Public key Cryptography for the financial services industry, The elliptic curve digital signature

[5] M. Ghorbel, M. Segarra, J. Kerdreux, R. Keryell, A. Thepaut, and M. Mokhtari, Networking and Communication in Smart Home for People with Disabilities, Computers Helping People with Special Needs, Springer Berlin/Heidelberg, 624, 2004.

[6] Kuk-se Kim, Gil-choon Kim and Joon Lee, "Embedded Linux System for Self-Control System of Car", The Journal of The Korea Institute of Electronic Communication Sciences, Vol. 2, No. 1, pp. 62-66, 2007.

[7] Hyun Huh and Jae-hak Lee, "A Study on Development of H8 MCU IDB(Integrated development board) for Embedded Education", The Journal of The Korea Institute of Electronic Communication Sciences, Vol. 4, No. 1, pp. 51-57, 2009.

[8] P. M. L. Chan, R. E. Sheriff, Y. F. Hu, P. Conforto, C. Tocci, and G. Losquadro, Mobility management incorporating fuzzy logic for a heterogeneous IP environment, IEEE Communications Magazine, Vol. 39, No. 12, pp. 42-51 2001.

[9] J. Hou, and D. C. O'Brien, Vertical handover-decision-making algorithm using fuzzy logic for the integrated radio and OW system, IEEE Transactions on Wireless Communications, Vol. 5, No. 1, pp. 176-185, 2006.

저자 소개

윤찬호(Chan-Ho Yoon)

1997년 2월 호남대학교 컴퓨터공학과 졸업(공학사)
2000년 2월 조선대학교 대학원 컴퓨터공학과 졸업(공학석사)
2010년 전남대학교 대학원 컴퓨터공학과(박사과정)
※ 관심분야 : 임베드디 시스템, ATM망, 인터넷 통신, 컴퓨터 네트워크, 실시간 통신 프로그래밍, 영상 처리 및 통신, 프로그래밍 언어(Visual C++, Java, 안드로이드)

김광준(Gwang-Jun Kim)

1993년 2월 조선대학교 컴퓨터공학과 졸업(공학사)
1995년 2월 조선대학교 대학원 컴퓨터공학과 졸업(공학석사)
2000년 2월 조선대학교 대학원 컴퓨터공학과 졸업(공학박사)
2000년~2001년 Dept. of Electrical & Computer Eng. Univ. of California Irvine Postdoc.
2003년~현재 전남대학교 컴퓨터공학과 부교수
※ 관심분야 : 가상화, ATM망, 인터넷 통신, 컴퓨터 네트워크, 실시간 통신 프로그래밍, 영상 처리 및 통신, 프로그래밍 언어(Visual C++, Java, 안드로이드 등), 임베디드 시스템, 의료정보통신 등

장창수(Chang-Soo Jang)

1980년 2월 조선대학교 전자공학과(공학사)
1982년 8월 건국대학교 대학원전자공학과(공학석사)
1997년 2월 서강대학교 컴퓨터공학과(공학박사)
1984년~현재 전남대학교 컴퓨터공학과 교수
※ 관심분야 : 가상화, 컴퓨터구조, 병렬처리 구조, 상호연결망, 마이크로 프로세서, 의료정보 통신 등