Journal of the Korea Academia-Industrial cooperation Society
Vol. 12, No. 5 pp. 2322-2326, 2011

DOI: 10.5762/KAIS.2011.12.5.2322

스마트카드용 Hybrid 암호시스템 설계

송제호[1], 이우춘[1*]
[1]전북대학교 IT응용시스템공학과

The Design of Hybrid Cryptosystem for Smart Card

Je-Ho Song[1] and Woochoun Lee[1*]
[1]**Dept. of IT Applied System Eng. Chonbuk National University**

요 약 기존 암호시스템은 비도를 증가시키기 위하여 데이터와 키 값을 별도로 사용하고 일정 횟수의 반복성을 수행하며 무한수열에 가까운 LFSR의 주기특성을 증가시키므로 암호시스템의 효율이 저하되는 문제점이 있다. 본 논문에서 제안된 알고리즘은 대칭형 암호방식에 비대칭형 암호개념을 적용한 새로운 기능의 데이터 재배열, 치환, 데이터 암호블록, 키 스케쥴러로 구성하였다. 본 논문에서 제안된 암호알고리즘은 범용 SYNOPSYS를 이용하여 스마트 카드의 암호시스템을 설계하였고 40MHz의 시스템 속도로 ALTERA MAX+PlUSⅡ 툴의 모의실험한 결과 단일 라운드로 16 라운드의 비도와 640Mbps의 데이터 처리율로 AES보다 52% 향상됨 확인하였다.

Abstract General cryptosystem uses differently the data and key value for the increment of security level, processes the repetition of limited number and increases the periodic feature of LFSR similar infinite series. So, it cause the efficiency of the cryptosystem. In this thesis, proposed algorithm is composed of reformat, permutation, data cipher block and key scheduler which is applied the new function by mixed symmetric cryptography and asymmetric cryptography. We design the cryptosystem of smart card using the common Synopsys and simulate by ALTERA MAX+PLUSⅡ at 40MHz. Consequently, we confirm the 52% increment of processing rate and the security level of 16 rounds.

Key Words : Cryptosystem, Cryptography, Security level, Processing rate, Smart card

1. 서론

사회에서 정보의 가치는 개인이나 기업체의 중요한 자산으로 인식되어질 수 있을 뿐만 아니라 국가의 안보와도 밀접한 관계를 맺고 있다. 정보의 중요성에 대한 비중이 커짐에 따라 정부 차원에서는 초고속 정보 통신망, 무궁화호 위성 통신망 및 5대 기간 전산망(교육 연구망, 국방망, 공안망, 행정망, 금융망)의 구축으로인한 통신의 보안성(security)이 다각도로 요구되며 기업이나 민간에서도 정보의 처리 및 교환이 활발해짐에 따라 정보보호가 심각한 문제로 대두되고 있다. 이러한 정보를 보호하기 위해서 실질적으로 필요한 것이 암호기법(cryptography)이다[1,2].

최근에는 전자상거래 환경이 구축되면서 실물경제가 사이버 세계에서 이루어지고 있다. 이러한 시점에서 가치변환 및 이동의 수단으로 스마트 카드(smart card)의 중요성이 부각되고 있다. 가치이동의 수단뿐만 아니라 활용분야가 다양하기 때문에 정보 통신망 환경에서 스마트 카드가 중요한 보안장치로 수요나 활용면에서 급격한 증가율을 보이고 있다.

본 논문에서는 스마트 카드의 암호시스템에 적합하도록 블록 및 스트림 암호알고리즘에 기반을 둔 혼합형 암호알고리즘을 제안하였다. 제안된 혼합형 암호알고리즘은 스마트 카드에 대한 구조, 특성, 안전성, 관련 표준, 기술 및 다양한 응용부분을 고려하여 국가간 스마트 카드 표준화 기구인 ISO /IEC JTC1 SC17의 기준을 적용하였다[4,5,6].

대칭형 암호방식에(symmetric cryptography) 비대칭형

*교신저자 : 이우춘 (wclee@jbnu.ac.kr)
접수일 11년 03월 20일 수정일 (1차 11년 04월 25일, 2차 11년 05월 10일) 게재확정일 11년 05월 12일

암호방식(asymmetric cryptography)개념을 적용한 새로운 혼합형 암호알고리즘은 데이터 재배열, 치환, 데이터 암호블록, 키 스케쥴러로 구성되어 있고, 데이터 암호화 과정은 128 비트 평문 블록을 64 비트씩 2개의 블록으로 분할하고 확장을 거친 후 80 비트 크기를 가지는 혼합형 키를 사용하여 암호화하였다[6,7]. 또한, 단일 라운드(round)만을 사용하고도 기존 16 라운드에 해당하는 비도(security level)를 얻도록 혼합형 키(hybrid key)와 블록 암호시스템의 비선형 부분인 F 암호함수부분을 더욱 더 비선형화 시켰다. 입력 신호를 평문 및 키 데이터로 사용할 수 있고 암호문은 비인가자에게 인증용으로 적용되며 기존 시스템과 호환성이 용이하도록 하였다[8,9].

2. 기존 암호알고리즘

데이터의 암호화・복호화, 인증, 부인봉쇄 등에 사용되는 알고리즘으로 암호화・복호화의 키가 서로 다르다. 공개키 암호화 방식은 비대칭키 암호화(asym -metric-key cryptography) 방식 또는 양방향 암호화(two-key cryptography) 방식이라고 한다.[10,11] 공개키 암호알고리즘은 소인수분해(factorization) 기법에 근거를 둔 RSA와 이산대수(discrete logarithm) 문제에 근거한 Diffie-Hellmam, DSA(Digital Signa -ture Algorithm), ElGamal, ECC(Elliptic Curve Cryptograph)등이 있다.[12,13]

공개키 암호시스템의 주요기능은 다음과 같다.

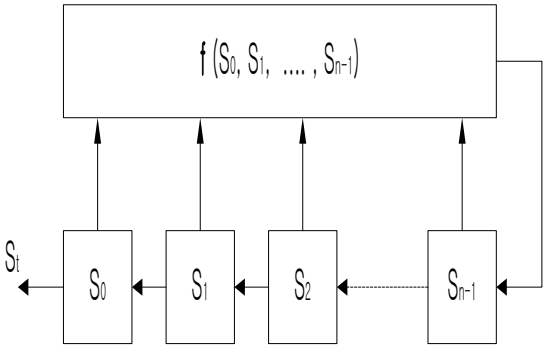
첫째 인증은 수신된 메시지가 정당한 송신자로부터 전송된 것인지를 확인할 수 있게 하고 송・수신자간의 실제 신원을 확인하는 것을 가능하게 한다. 둘째 기밀성은 수동적인 공격으로부터 데이터를 보호하는 것으로서 정당한 권 한이 부여된 사용자만이 데이터의 내용을 파악할 수 있다. 셋째 무결성은 수신된 메시지가 불법적으로 재생된 것인지 또는 전송과정 에서 변조되었거나 재구성되었는지에 대한 확인을 보장한다. 넷째 부인봉쇄는 송・수신자간에 전송된 메시지에 대한 분쟁을 해결해 준다. 다섯째 전달방지는 기밀성을 가진 정보를 받은 인증된 사용자가 다른 사용자에게 전달할 수 없도록 한다.

여섯째 접근제어는 정보에 대한 접근이 차별화 되어 있을 때 권한 자만이 재원의 접근을 허가한다. 일곱째 유용성은 정보가 필요할 때마다 인가된 범위안에서 접근을 허용한다.

Diffie와 Hellman은 기존 암호 방식의 단점을 보안하기 새로운 개념으로 공개키 암호방식을 소개했다. 이후, 연구가 활발히 진행되어 MIT의 Ron Rivest, Adi Shamir, Len Aaleman에 의해 1977년에 RSA라는 공개키 기반의 암호알고리즘이 발표되어 현재에도 여러분야에서 이용된다.

1985년에 만들어진 ElGamel 알고리즘은 이산대수 문제에 기반을 두고 있는 것으로 이산대수를 계산하는 것이 어려워 해독하기 힘들다는 가정 하에서 제안된 공개키 암호화 알고리즘이다. 이러한 알고리즘은 공개키 암호화시스템으로서 암호화와 서명 알고리즘(signature algorithm)으로 구성되어 있다. 비밀키 암호화(private key cryptography) 방식은 대칭키 암호화(symmetric key cryptography) 방식 또는 단일키 암호화(one-key cryptography) 방식이라고 한다. 비밀키 암호방식은 송・수신자가 안전한 통신로를 사용하여 사전에 공유한 키를 사용하는 방식으로 공개키 암호방식에 비하여 속도가 빠르고 구현이 용이하므로 기밀성을 보장하기 위한 암호의 용도로 많이 쓰인다.[14] 비밀키 암호시스템은 변환하는 방법에 따라 데이터를 블록 단위로 처리하는 블록 암호알고리즘(block cryptoalgorithm)과 평문의 작은 단위인 비트단위로 처리하는 스트림 암호알고리즘(stream cryptoalgorithm)으로 나눈다.[15,16] 블록암호는 1977년 미국의 DES알고리즘이 제안되어 많은 발전이 있었는데 설계 사상이 공개되지 않아 암호학자들로 하여금 오늘날 블록암호를 발전시킨 계기가 되었다. 그 이후 일본의 FRAL, 호주의 LOKI 유럽의 IDEA, DAFER, 미국의 CR5 등이 제안되어 현재까지 사용되고 있다.[17,18] 블록 암호알고리즘은 DES와 같은 형태인 Feistel 구조와 치환(substitution)과 재배열(permutation)을 반복하여 사용하는 S-P 네트웍 구조등으로 구성된다. Feistel 방식은 한 라운드에 평문의 일부만 처리하여 병렬처리 효율이 낮은 반면 라운드 함수 설계의 융통성과 암・복호화 과정이 동일하다는 장점을 가진다. S-P 네트웍 방식은 한 라운드에서 전체 평문을 암호화하므로 병렬처리가 가능하여 속도가 빠르지만 복호화를 고려하여 암호화 과정을 설계하므로 설계의 폭이 좁다라는 단점을 가진다. 스트림 암호방식은 데이터를 비트 단위로 처리하는 암호방식으로서 블록암호에 비하여 암호화의 속도는 빠르고 암호문을 해독하기 힘든 장점이 있다. 그리고 스트림 암호방식은 하드웨어로 구현되어 군용통신과 같이 데이터 통신 내용이 매우 민감한 부분에 적용되며 보통 긴 주기를 가지는 수열을 발생하여 문자열과 비트별 논리합을 하여 암호문을 발생하는 방법을 사용한다. 따라서, 암호의 안전성은 전적으로 키 수열의 안전성에 기인한다. LFSR은 스트림암호에서 의사난수발생기(PRG : pseudo random generator)를 이용하여 수학적으로 분석이 가능한 이진수열을 효율적으로 발생할 수 있는 장치로 유한체 위에 정의된 선형

점화식 수열로 모델링할 수 있으며 수열의 특성은 점화식에 의해 유도되는 특성다항식에 의하여 결정된다. LFSR은 암호뿐아니라 대역확산통신 등에도 많이 활용되고 구현 복잡도가 작아 빠른 속도가 요구되는 곳에 적용되며 생성과정은 그림 1과 같다[3,6].



[그림 1] LFSR 구조

유한체 GF(2)={0,1}위에 다음과 같이 정의된 수열을 식 (1)로 나타낸다.

$$S_{j+n} = (C_0 S_{j+n-1} + C_1 S_{j+n-2} + \cdots + C_{n-1} S_j) \mod 2, \quad j \geq 0 \quad (1)$$

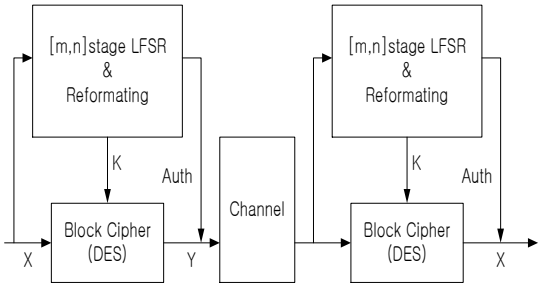
여기서, $S_0, S_1, \cdots, S_{n-1}$은 초기치로 정의 된다. 이때 식 (1)의 특성다항식(characteristic polynomial) $f(x)$는 식 (2)와 같다.

$$f(x) = s^n + C_0 x^{n-1} + C_1 x^{n-2} + \cdots + C_{n-2} x + C_{n-1} \quad (2)$$

이때 C_{n-1}은 반드시 1이어야 하며 초기 값이 모두 0인 경우는 배제한다. LFSR에서는 초기 값으로부터 나머지 수열을 모두 생성할 수 있기 때문에 특성다항식 $f(x)$의 특성이 중요하다. 따라서, n개 단을 갖는 LFSR에 의하여 생성되는 수열의 특성은 n차 특성다항식에 의하여 결정된다.

3. 제안된 Hybrid 암호알고리즘

현재의 암호알고리즘 개발이 활발하고 구현의 방법론이 다양화되고 있지만 비인가자들은 계속적인 정보유출을 원하며 이로 인한 정보유출 피해는 정보화 사회로의 발전과 더불어 계속될 전망이며 막대한 피해를 주고있다. 또한 암호알고리즘의 구현론적에서 소프트웨어 방식은 융통성이 크며 업데이트가 용이하지만 크랙 및 해킹에 취약성을 보인다. 그러므로 본 논문에서는 정보누출 및 변조를 막고 정보보호 차원에서 하드웨어에 의한 구현을 선택하여 플랫폼의 유·출입부분에서 동작하도록 Hybrid 암호알고리즘을 제안하였으며 설계된 암호시스템은 대칭형 암호시스템을 기본으로 비대칭형 암호시스템 특징을 가질 수 있도록 설계하였다.

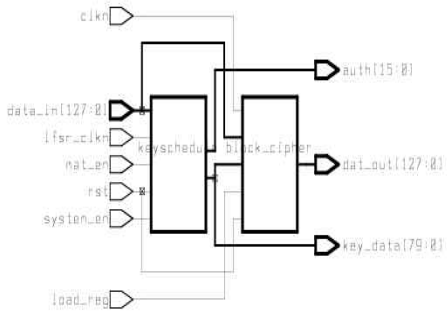


[그림 2] 제안된 Hybrid 암호시스템

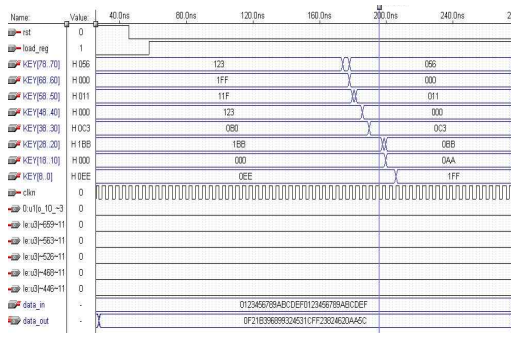
그림 2는 입력 데이터 X에 대하여 키 스케줄러에서 X에 의한 키 값 K를 생성하고 생성된 키값 K와 입력데이터 X를 이용하여 암호화된 출력값 Y를 생성하는 메카니즘으로 구성되어 있다. 또한 키 스케줄러에서는 암호화용 키값과 인증용 수열을 동시에 생성하며 이 두값은 전송로(channel)를 통하여 수신자에게 전송된다.

제안된 Hybrid 암호시스템은 기존 혼합형 암호시스템과는 매우 큰 차이를 가진다. 기존 혼합형 암호시스템은 비도를 증가시키기 위해서는 LFSR의 주기를 길게하기 때문에 블록 데이터 값도 증가되는 단점을 가지고 있다. 또한 데이터와 키값을 별도로 사용함으로써 암호화에 필요한 자원관리를 항상 염두에 두고 있어야 한다. 특히 키값은 고정된 값으로 존재하게 되므로 비인가자의 키값 획득은 암호화의 필요성을 무력화시키는 중요한 요인으로 작용된다. 그러나 본 논문에서 제안된 그림 3과 같은 새로운 스마트 카드용 Hybrid 암호시스템은 유입되는 정보데이터를 기반으로 암호화에 사용되는 키 값을 생성하므로 데이터에 따라서 암호화 패턴이 변화되는 장점을 가지고 있다. 대칭형 암호방식에 비대칭형 암호개념을 적용한 새로운 혼합형 암호알고리즘은 입력신호를 평문과 키 데이터로 동시에 사용하고 생성된 암호문은 인증용 정보를 산출하며 단일 라운드로 비도와 F 암호 함수부분을 더욱더 비선형화 시켰다. 제안된 Hybrid 암호시스템의 전체 블록도는 Synopsys ver 1999.10으로 설계하였고 128비트 테이터 길이, 80비트 키 길이, 40MHz의 시스템

속도를 Altera MAX+PlusⅡ툴로 모의실험한 결과 데이터 처리율이 640Mbps로서 그림 4에서 확인하였다. 입력 데이터는 “0123456789ABCD EF0123456789ABCDEF"이며 출력 데이터는 “0F21 B396899324531 CF23824620AA5C" 이다.



[그림 3] 제안된 Hybrid 암호시스템의 전체 블록도



[그림 4] 제안된 Hybrid 암호시스템의 모의실험 결과

본 논문에서 제안된 새로운 Hybrid 암호알고리즘을 이용하여 스마트 카드의 암호시스템에 적용한 결과를 표 1로 나타내었다. 제안된 알고리즘과 기존의 알고리즘을 6개의 파라미터(parameter)로 비교해 보면 다음과 같이 성능이 향상됨을 확인하였다.

[표 1] 기존 암호알고리즘과 새로운 Hybrid 암호알고리즘의 비교

내용/알고리즘	DES	SEED	AES	혼합형
구 조	Feistel	Feistel	SPN	Feistel& SPN
라운드 수	16	16	10	1
데이터 길이(bit)	64	128	128/192/ 256	128
키 길이(bit)	56	128	128	80
시스템 속도(MHz)	80	40	33	40
데이터 처리율(Mbps)	50	251	256	640

5. 결론

최근 정보보호 시스템은 비도는 높고 처리속도가 빠른 암호시스템에 기반을 둔다. 비대칭키 암호알고리즘으로는 RSA, ECC등이 있으며 대칭키 암호알고리즘으로는 DES, SEED, AES등이 있다. 기존 블록 암호방식은 16 라운드의 암호화와 복호화를 수행하고 스트림 암호방식은 안전성을 획득하기 위하여 무한수열에 가까운 LFSR의 주기특성을 가지도록 한다. 그러나 반복의 증가 또는 LFSR 주기 길이의 증가는 비밀키 암호시스템의 효율을 저하시키는 요인이 된다. 본 논문에서는 이동성 및 네트워크 환경이 강조되는 스마트 카드의 암호시스템에 적합한 블록 및 스트림 암호알고리즘에 대하여 고찰하였다. 그리고 제안한 Hybrid 암호알고리즘을 스마트 카드에 대한 구조, 특성, 안전성, 관련 표준, 기술 및 다양한 응용부분을 고려하여 국가간 스마트카드 표준화 기구인 ISO/IEC JTC1 SC17의 기준을 적용하였다. 대칭형 암호방식에 비대칭형 암호개념을 적용한 새로운 Hybrid 암호알고리즘은 데이터 재배열, 치환, 데이터 암호블록, 키 스케쥴러로 구성되어 있고, 데이터 암호화 과정은 128 비트 평문 블록을 64 비트씩 2개의 블록으로 분할하고 확장을 거친 후 80 비트 크기의 혼합형 키를 사용하여 암호화하였다. 제안된 Hybrid 암호알고리즘을 이용하여 스마트 카드의 암호시스템을 범용 Synopsys로 설계하였고 40M Hz의 시스템 속도환경에서 640Mbps의 데이터 처리율을 확인하였다. 그러므로 제안된 Hybrid 알고리즘을 스마트 카드의 암호시스템에 적용할 경우 입력 신호를 평문 및 키 데이터로 사용할 수 있고 암호문은 비인가자에게 인증용으로 적용되며 기존시스템과 호환성이 용이하여 하드웨어 설계와 보안기능 및 처리속도를 향상시킬 수 있다고 사료된다.

참고문헌

[1] W.Stallings, Cryptography and Network Security, Prentice Hall, 1998.

[2] B. Schneier, Applied Cryptography : Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., New York, USA, 1994.

[3] D. R. Stinson, Cryptography Theory and Practice, Chapman & Hall/CRC, 2002.

[4] H. Miyano, AMethod to Estimate the Number of Ciphertext Pairs for Differential Cryptanalysis, Abstracts of ASIACRYPT91, 1991.

[5] 서광석, 김창한, 암호학과 대수학, 북스힐, 1999.
[6] T. Siegenthaler, "Decrypting a Class of Stream Ciphers Using Ciphertext Only," IEEE Trans. on Computer, Vol. C-34, No. 1, pp. 81-85, Jan. 1985.
[7] R.Rueppel, "Stream Ciphers," Contemporary Cry ptology: The science of Infor. Integrity, New York, IEEE Pres, pp. 65-134, 1991.
[8] 이병관, 전자상거래 보안, 남두도서, 2002.
[9] VISA Open Platform Overview, 1999.
[10] E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, J. of CRYPTOLOGY Vol. 4 No. 1, 1991.
[11] B. Schneier, Applied Cryptography : Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., New York, USA, 1994.
[12] W. Diffie and M. E. Hellman, "New directions in Cryptography," IEEE Trans. on Infor. Theory, Vol. IT-22, No. 6, pp. 644-654, Nov. 1976.
[13] R. Revest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," CACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978.

송 제 호(Je-Ho Song) [정회원]

- 1991년 2월 : 원광대학교 전자공학과 (공학사)
- 1993년 2월 : 원광대학교 전자공학과 (공학석사)
- 2003년 2월 : 원광대학교 전자공학과 (공학박사)
- 1996년 3월 ~ 현재 : 전북대학교 IT응용시스템공학과 교수

<관심분야>
VLSI, 정보통신, 통신망 네트워크 시스템설계

이 우 춘(Woo-Choun Lee) [정회원]

- 1977년 2월 : 단국대학교 전기공학과 졸업.
- 1986년 2월 : 명지대학교 대학원 전기공학과 졸업(석사).
- 1995년 2월 : 동대학원 전기공학과 졸업(박사).
- 1992년 3월 ~ 현재 : 전북대학교 IT응용시스템공학과 교수

<관심분야>
전기기기, 전력변환