ABC(Advanced Block Cipher) 알고리즘 설계

이 병 관*, 정 은 희**, 윤 동 식***

A design of ABC(Advanced Block Cipher) Algorithm

Byung-Kwan Lee*, Eun-Hee Jeong**, Dong-Sic Yun***

요 약

본 논문에서는 EC-DH를 이용한 안전한 키 분배와 처리속도가 개선된 64byte 블록 암호화 알고리즘인 ABC(Advanced Block Cipher) 알고리즘을 설계하였다. ABC 알고리즘은 별도의 S-Box, IP-Box 등을 사용하지 않고 데이터 교환키를 이용해 원본 데이터의 위치를 교환하는 방식을 사용함으로써 기본적인 메모리 점유율을 줄였다. 또한, 고정된 암·복호화 키가 아닌 유동적인 암·복호화 키를 사용해 대칭키의 유출에 대비하였다. 따라서, 본 논문에서 제안한 ABC 알고리즘은 모바일 뱅킹 및 낮은 메모리 환경에 적합한 암호화 알고리즘이라 할 수 있다.

ABSTRACT

This paper designs the ABC(Advanced Block Cipher) algorithm which is a 64byte block encryption algorithm, improves the performance of encryption process time, and makes an key exchange using EC-DH. The ABC algorithm reduces basic memory occupation rates using the original data position exchange method which is a data swap key without S-Box, IP-Box and etc. Also, it prepares the exposure of symmetric key using the unfixed encryption(decryption) key excepting the fixed encryption(decryption) key. Therefore, the proposed ABC algorithm in this paper is a proper encryption algorithm in lower memory environment and mobile banking.

KeyWords : ABC, AES, DES, ECDH, Swap Key

Ⅰ. 서 론

현대 정보화 시대에서 정보 보호의 중요성은 아무리 강조해도 지나치지 않으며, 인터넷 뱅킹, 온라인 주식 거래, 각종 전자 상거래 등의 사용으로 정보 보호는 선택이 아니라 필수적인 사항이라 할 수 있다. 정보 보호 기술의 핵심은 암호 기술이고, 공개키 알고리즘인 RSA, ECC 등과 대칭키 알고리즘인 DES, AES, SEED 등으로 분류한다. 공개키 알고리즘은 키 관리가 용이하지만 처리 속도가 느린 단점이 있어 주로 인증이나 전자서명에 사용되며, 키 관리의 어려움은 있지만 암호화 속도가 빠른

* 관동대학교(bklee@kwandong.ac.kr)
** 교신저자 강원대학교(jeongeh@kangwon.ac.kr)
*** 안동과학대학(yundos@asc.ac.kr)
접수일자 : 2010년 6월 4일, 수정일자 : 2010년 6월 17일, 심사완료일자 : 2010년 6월 18일

대칭키 알고리즘은 정보 암호화에 선호하며 그 대표적인 알고리즘이 DES(Data Encryption Standard)이다.

현재 모바일 뱅킹의 암호 알고리즘은 대칭키 알고리즘을 사용하고 있다. 즉 휴대폰에 들어 있는 키와 ATM에 들어 있는 키가 같아야 하므로, ATM은 모바일 뱅킹 서비스가 가능한 모든 휴대폰의 개인키를 관리해야한다. 따라서 ATM이 도난당하거나 해킹되었을 때 모든 모바일 금융을 위한 전체키가 노출될 수 있으므로, 대형 금융사고가 일어날 수 있다[1].

본 논문에서는 EC-DH를 이용한 안전한 키 분배와 처리속도가 개선된 블록 암호화 알고리즘인 ABC(Advanced Block Cipher) 알고리즘을 설계한다. ABC 알고리즘은 별도의 S-Box, IP-Box 등을 사용하지 않으므로 메모리 점유율을 줄이고 고정된 암·복호화 키가 아닌 유동적인 암·복호화 키를 사용해 대칭키의 유출에 대비하고, 모바일 뱅킹 및 낮은 메모리 환경에 적합한 암호화 알고리즘으로 설계하고자 한다.

II. 관련연구

2-1 대칭키 알고리즘

대표적인 대칭키 알고리즘인 DES는 56Bit 키를 이용하여 64bit 평문 블록을 64bit의 암호문 블록으로 만드는 미국표준 블록 암호방식이다. DES는 통계적 암호 해독에 견딜 수 있도록 충분히 견고하게 제작되었지만, 최근 기술의 발달로 DES 알고리즘은 쉽게 해독이 가능하므로 DES는 더 이상 안전한 암호가 아니다. 이에 DES의 한계점을 개선한 새로운 대칭키 알고리즘으로 AES가 미국 표준안으로 채택되었지만, 여전히 DES가 많은 곳에서 사용되고 있다.

AES는 전체적인 설계논리는 DES와 마찬가지로 대치와 치환으로 구성되어 있다. 하지만 DES보다는 수학적으로 안전한 암호 논리 기반으로 설계되어 알려진 보안 공격이 없고, 비선형 구조인 S-Box를 사용하므로 안전한 암·복호화 알고리즘이다. 또한, AES는 간결한 구조로 안전성 분석이 용이하며, 특히 임의로 키 길이를 128, 192, 256비트 중 선택할 수 있으며, 그 중 128비트만 미국 표준안으로 선택되었다.

SEED는 한국 정보보호센터가 1998년 개발한 한국형 표준 대칭키 128비트 블록 암호 알고리즘으로 2005년 ISO/IEC 국제표준으로 등록하였다. SEED는 안정성, 신뢰성이 우수하고 SW구현 시 3중 DES보다 처리속도가 빠른 특징을 갖는다[2].

2.2 EC-DH

EC-DH는 Diffie-Hellman 알고리즘을 타원곡선 위로 옮긴 것으로 X9.63으로 표준화 되어 있다. X9.63에서 사용하는 도메인 파라미터는 ECDSA에서의 도메인 파라미터와 같고, X9.62에서 선택 파라미터로 사용하는 cofactor $h = |E|/n$는 small subgroup 공격을 막기 위해 필수적으로 사용된다. 그리고, 각 사용자는 파라미터 n, G,$E(F_p)$, h를 모두 알고 있다고 가정한다.

ECC는 유한체(finite field) 상의 타원곡선 점들 간의 연산에서 정의되는 이산대수 문제의 어려움을 이용하는 것으로 전자서명 과 키 교환 알고리즘에 주로 이용된다[2,3].

그림 1은 EC-DH를 이용한 키 교환 과정을 설명한 것이다[3].

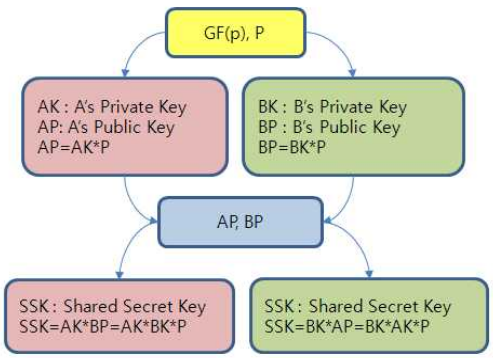

그림 1. EC-DH 키 교환 흐름도
Fig. 1 EC-DH Key exchange Flowchart

Ⅲ. ABC 알고리즘 설계

본 논문에서 제안한 ABC 알고리즘은 DES나 AES와 같이 S-Box를 사용하지 않고, 데이터 블록 간의 데이터 교환 및 비트 연산으로 암호화 하는 알고리즘이다. 따라서 ABC 알고리즘은 기존의 대칭키 알고리즘에 비해 메모리 공간을 적게 사용 한다. 또한, 고정된 대칭키가 아닌 유동적인 대칭키를 사용하므로 암호화가 한층 강화되었다고 볼 수 있다.

그림 2는 ABC 알고리즘의 전반적인 흐름을 설명한 것이다.

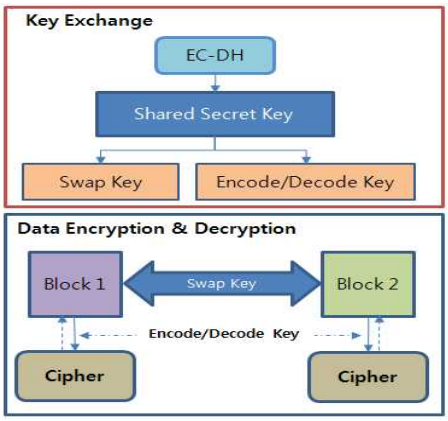

그림 2. ABC 알고리즘
Fig. 2 ABC Algorithm

3-1. 키 생성

본 논문에서 제안한 ABC 알고리즘은 EC-DH 알고리즘으로 공유 비밀키 생성으로 키 교환을 한 후, ABC 알고리즘에 사용될 데이터 교환키와 암·복호화키를 생성하게 된다. 이때, 공유 비밀키의 X, Y의 좌표값 중 각각 4자리만 선택한 후 연접하는데, X와 Y의 값이 4자리 보다 작을 경우에는 4자리까지 0으로 패딩 한다. 그림 3은 키 생성 과정을 설명한 것이다.

이때, 공유 비밀키의 X, Y의 좌표값 중 각각 4자리만 선택한 후 연접하는데, X와 Y의 값이 4자리 보다 작을 경우에는 4자리까지 0으로 패딩 한다. 그림 3은 키 생성 과정을 설명한 것이다.

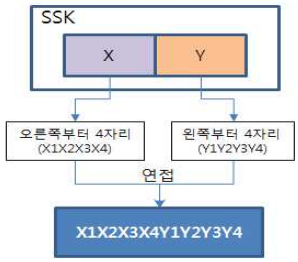

그림 3. 키 생성
Fig. 3 Key generation

이때, 공유 비밀키의 X, Y의 좌표값 중 각각 4자리만 선택한 후 연접하는데, X와 Y의 값이 4자리 보다 작을 경우에는 4자리까지 0으로 패딩 한다.

그림 3은 키 생성 과정을 설명한 것이다.

```
Swap_Key(K, n){
  K : Shared Secret Key;
  n : Block number;
  K=(K0, K1, K2, K3, K4, K5, K6, K7)
  n=n+1
  for(i=0 ; i<=7 ; i++){
    for(j=0; j<=7 ; j++){
      r_j = K_j × n mod 8;
      c_j = K_j × n + i mod 8;

Block_A(i,j) = (r_j − i mod 8, c_j + i mod 8);
    }
  }
 for(i=0 ; i<=7 ; i++){
    for(j=0; j<=7 ; j++){
      r_i = K_j × 3n mod 8;
      c_i = K_j × 7n + i mod 8;

Block_B(i,j) = (r_i − i mod 8, c_i + i mod 8);
    }
  }
  return(Block_A(i,j), Block_B(i,j));
}
```

그림 4. 데이터 교환키
Fig. 4 Swap Key of Data

예를 들어, Swak Key인 $Block_{A(1,0)}$=(6,1)이고, $Block_{B(1,0)}$=(1,4)이면 블록 1의 6행 1열과 블록 2의 1행 4열을 교환한다.

(2) 암·복호화 키

암·복호화 키는 실질적으로 데이터를 암·복호화할 때 사용되는 암·복호화 키로 생성 단계는 다음과 같다.

단계 1. 공유 비밀키를 아스키코드로 변환한다(ASC_Key).

단계 2. 변환된 ASC_Key 값을 블록 데이터와 순환 shift XOR 연산을 한다.

이때, 암호화할 때에는 왼쪽으로 순환 쉬프트하고 복호화할 때에는 오른쪽으로 순환 쉬프트 한다.

그림 5는 실질적으로 데이터를 암호화하고 복호화 시키는데 필요한 암·복호화 키 생성과정을 설명한 것이다.

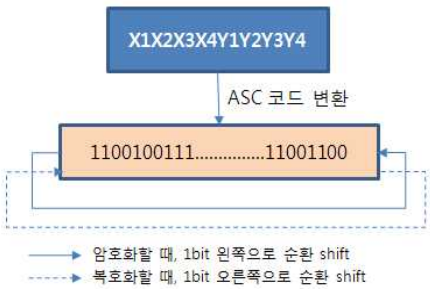

그림 5. 암·복호화 키
Fig. 5 Encode·Decode Key

3-2. 데이터 암호화

ABC 알고리즘의 데이터 암호화 과정은 다음과 같다.

단계 1. 데이터를 블록 단위로 나눈다. ABC 알고리즘은 8×8 byte 블록 단위로 암·복호화를 수행하는 블록암호화 알고리즘으로 데이터 블록의 구조는 그림 6과 같다. 데이터 블록은 64byte 길이 중에서 데이터의 길이를 기록하는 4byte와 블록 번호를 기록하는 4byte로 구성된다.

데이터의 길이가 필요한 이유는 DES와 달리 ABC 알고리즘은 블록 단위로 데이터 교환을 하기 때문에 적어도 두 개의 블록이 필요하고, 데이터 길이가 128byte 보다 작을 경우 0으로 패딩 되므로 실제 데이터의 길이가 얼마인지 알아야 복호화 되었을 때, 실제 데이터만큼만 추출할 수 있다.

블록 수(n) = 데이터 길이 / 56byte

블록 수(n)은 데이터 교환키 생성에 이용되기도 하지만, 실제로 데이터를 복호화했을 때, 데이터의 순서 정렬로도 이용되기도 한다[5].

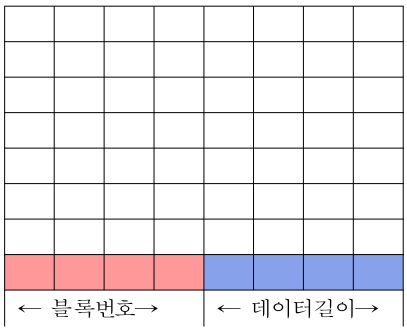

그림 6. 블록 구조
Fig. 6 Block structure

단계 2. 블록에 데이터를 ASC 코드로 변환시켜 저장하는데, 데이터 길이가 블록의 길이보다 작으면 0으로 패딩하고, 데이터와 패딩 데이터를 구분하기 위해 1을 입력한다.

단계 3. 암·복호화 키와 블록의 1행 단위로 XOR 연산으로 암호화 한다.

3-3. 데이터 복호화

ABC 알고리즘의 데이터 암호화의 과정을 역순으로 수행하면 데이터의 복호화가 된다. 복호화 과정은 다음과 같다.

단계 1. 암·복호화 키와 암호문의 블록의 맨 마지막 행부터 1행 단위로 XOR연산을 수행해 복호화 시킨다. 이때, 암·복호화 키는 암호화시킬 때와 반대로 오른쪽으로 1bit 순환 쉬프트 한다.

단계 2. 복호화한 블록 데이터를 데이터 교환키를 이용해 블록간에 데이터를 교환하여 초기의 데이터 블록 형태를 생성한다.

단계 3. 데이터 길이만큼 추출한다.

Ⅳ. 성능분석

본 논문에서 제안한 ABC 알고리즘은 기존의 대칭키 알고리즘은 DES, AES와 암·복호화 수행시간을 비교 분석하였으며, 실험환경은 Windows XP 운영체제에 RAM 2GB, CPU 2.20GH이고 언어는 Visual C++를 사용하였다.

ABC와 DES, AES를 비교할 때, ABC는 데이터 교환을 위해 반드시 2개의 블록이 필요하므로 데이터 128byte를 기준으로 비교하였다.

그림 7, 8은 ABC와 DES의 암·복호화의 수행시간을 비교 분석한 것을 설명한 것이다. 그림에서 알 수 있듯이 ABC가 DES와 AES에 비해 암·복호화 시간을 단축시킨 것을 알 수 있다.

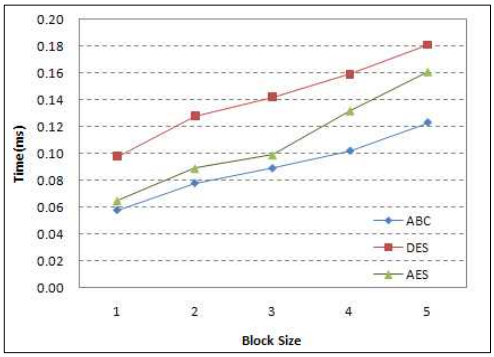

그림 7. ABC, DES, AES 암호화 성능 분석
Fig. 7 Encryption performance analysis of ABC, DES and AES

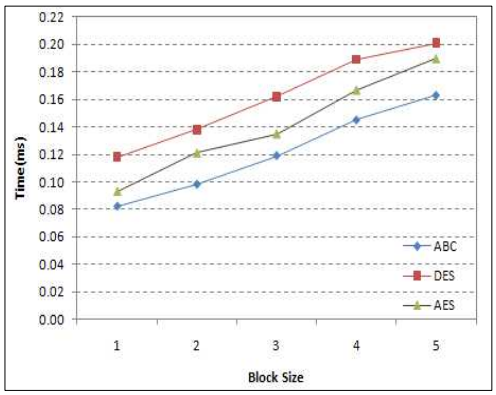

그림 8. ABC, DES, AES 복호화 성능 분석
Fig. 8 Decryption performance analysis of ABC, DES and AES

Ⅴ. 결 론

모바일 네트워크 고도화 및 단말기의 비약적인 발전으로 모바일 뱅킹 등의 개방형 플랫폼을 사용하는 스마트 폰의 보급이 확산되고 있으며, 이에 따른 정보 노출에 따른 개인 사생활 침해 등 여러 문제점이 증가하고 있다.

본 논문에서 제안한 ABC 알고리즘은 기존의 대칭키 알고리즘처럼 별도의 S-Box 등을 사용하지 않고, 원본 데이터를 교환하는 방식을 이용하므로 메모리 점유율이 기존의 대칭키 알고리즘보다 작으며, DES와 AES 보다 빠른 암·복호화 처리속도로 실행되므로 모바일 뱅킹 등 작은 메모리를 사용하는 환경에 적합한 블록암호화 알고리즘이라 할 수 있다. 향후 ABC 블록 알고리즘에 대한 안전성을 검증하고, ABC 블록 암호 알고리즘의 대칭키의 크기를 확장한다면, 암호화의 강도가 좀 더 강화되고, 신뢰성이 향상 될 것으로 기대한다.

참고문헌

[1] 조진만, 김수형, 문기영, 장종수, 손승원, “모바일 지급결제의 시장 현황 및 표준화 동향”, 전자통신동향분석, 제20권, 제1호, pp.35-42, 2005
[2] 이병관, 정은희, 인터넷 보안, 남두도서, 2004
[3] N. Koblitz, "Elliptic Curve Cryptosystems", Mathmatics of Computation, Vol.48, No.177, pp203-209, 1987
[4] 정은희, 김학춘, 이병관, “U-헬스케어 시스템의 보안 기법 설계”, 한국전자정보통신기술학회 학술대회, 제 권, 제1호, 2010
[5] 이병관, 조인석, 정은희, 양승해, “ThreeB 대칭키 알고리즘을 이용한 SET의 성능개선”, TELECOMMUNICATIONS REVIEW, 제13권 제6호, PP. 1009-1026, 2003.
[6] 한정규, 조유근, “모바일 멀티미디어 데이터를 위한 의사난수생성기와 순열기법을 결합한 효율적인 암호화 기법”, 정보과학논문지:시스템 및 이론, 제34권 제11,12호, pp.581-588, 2007.
[7] 조용국, 송정환, 강성우, “AES(Advanced Encryption Standard) 안전성 평가에 대한 고

찰", 정보보호학회논문지, 제11권, 제6호, pp67-76, 2001.

저자약력

이병관(Byung-Kwan Lee) 정회원

1975년 2월 부산대학교 기계설계학과 학사
1986년 2월 중앙대학교 전자계산공학과 공학석사
1990년 2월 중앙대학교 전자계산공학과 공학박사
1988년 ~ 현재 관동대학교 컴퓨터학과 교수

<관심분야> 네트워크 보안, 전자상거래, 컴퓨터 네트워크

정은희(Eun-Hee Jeong) 정회원

1991년 2월 강릉대학교 통계학과 이학사
1998년 2월 관동대학교 전자계산공학과 공학석사
2003년 2월 관동대학교 전자계산공학과 공학박사
2003년 9월 ~ 현재 강원대학교 지역경제학과 부교수

<관심분야> 네트워크 보안, 전자상거래, 웹 프로그래밍

윤동식(Dong-Sic Yun) 정회원

1992년 2월 관동대학교 전자계산공학과 공학사
1994년 2월 관동대학교 전자계산공학과 공학석사
2000년 2월 관동대학교 전자계산공학과 공학박사
1999년 3월 ~ 현재 안동과학대학 정보부사관학과 부교수

<관심분야> 네트워크 보안, 전자상거래, 웹 프로그래밍