특 집

암호 기술의 국내·외 개발 동향

서 창 호*, 이 옥 연**, 류 희 수***, 정 교 일***

*공주대학교 응용수학과, **국민대학교 수학과, ***한국전자통신연구원 정보보호기반연구팀

요 약

시스템의 고속화와 정보통신망의 대용량화 추세에 적극 대응하기 위한 암호 알고리즘(대칭키, 공개키, 전자서명) 및 고속 암호 프로세서 등에 관한 국내외 표준 암호 기술 개발 동향을 살펴본다.

I. 서 론

디지털 정보사회가 고도화되고, 전자거래가 활성화됨에 따라 암호 기술의 사회·경제적 활용은 특정분야에서 이용되는 특수기술에서 차세대 사회 경제의 기반기술로 크게 변화하고 있으며, 정보보호 역기능에 대비하기 위한 암호기술의 필요성이 증대하고 있다. 암호정책에 관한 국제적인 권고사항을 경제개발협력기구(OECD)를 통하여 제정하여 Security 산업의 활성화를 꾀하거나, 암호에 관한 각종 학술활동이 세계 곳곳에서 붐을 이루고 있는 외국의 흐름에 맞추어 우리나라에서도 한국정보보호학회가 설립되고 정보보호에 관한 각종 학술 행사가 개최되는 등 활발한 활동이 전개되고 있는 실정이다.

관심이 고조되고 있는 정보보호는 1970년대부터 국방, 외교 분야만이 아니라 민간, 상업용 분야로 전환되기 시작하여 DES[1], RSA[3], ECC 등의 암호 알고리즘의 연구와 개발 및 응용 제품의 보급이 활발해졌으며, 1990년대에 냉전 체제의 붕괴로 인한 군용기술의 민간 이전과 인터넷의 보급으로 인하여 각종 해킹사고나 도청 등의 발생으로 인하여 Security의 관심과 중요성이 확대일로에 있다.

암호기술은 합법적인 참여자들 간에 메시지를 암호화/복호화 하기 위한 규칙에 대한 약속을 정하고 이 규칙에 따라 보내고자 하는 메시지를 암호화시켜 전달, 혹은 보관하고 메시지를 수신하거나 접근 권한이 있는 사람이 필요에 따라 이를 복호화하도록 하는 기술이다. 일반적으로 암호기술의 기본 기능은 기밀성 기능(암호 알고리즘)과 인증 기능으로 나눌 수 있다. 기밀성 기능이란 정보통신망에서 전송되는 중요 데이터의 불법적인 노출을 방지하는 기능으로, 메시지를 제3자가 해독 불가능한 형태로 변형하거나 또는 암호화된 통신문을 해독 가능한 형태로 변환하기 위한 원리, 수단, 방법 등을 취급하는 기술을 말한다.

암호시스템은 키관리 측면에서 대칭키(관용키, 비밀키) 암호 시스템(symmetric key cryptosystem)과 공개키 암호 시스템(public key cryptosystem)으로 분류된다. 관용 암호 시스템은 송·수신자가 동일한 키에 의하여 암호화 및 복호화 과정을 수행하므로 키를 안전하게 전송하고 보관함에 어려움이 있다. 실제로 어떤 통신망은 너무 복잡하여 키 관리가 곤란할 수도 있다. 이러한 키 관리의 어려움을 해결하기 위하여 제시된 개념이 공개키 암호시스템이다.

공개키 암호시스템은 암호화와 복호화 과정에서 서로 다른 키를 사용하고, 암호화키를 공개하여 키의 전송 및 비밀보관 등이 필요없게 만든 시스템이다. 1976년 W. Diffie와 M. E. Hellman은 논문 "New Directions in Crypto-

graphy"에서 공개키 암호시스템이란 개념을 최초로 제시하였다. 그 후 공개키 개념을 실현하기 위하여 여러 알고리즘들이 발표되었지만 현재 안전성과 효율성을 인정받고 있는 공개키 시스템은 RSA 공개키 암호시스템, ElGamal 공개키 암호시스템, 타원곡선 암호시스템(Elliptic Curve Cryptosystem) 등이 있다.

기밀성 기능을 지원하기 위한 기술은 대칭키 암호알고리즘과 공개키 암호알고리즘으로 나누어지며, 대칭키 암호알고리즘으로 키 길이가 56비트인 DES(Data Encryption Standard)와 키 길이가 128비트인 AES(Advanced Encryption Standard) 등이 있으며, 공캐키 암호알고리즘으로 RSA가 전세계적으로 표준으로 인정받아 사용되고 있고, 국내에서는 대칭키 암호알고리즘으로 128비트 SEED가 국내 표준 암호기술로 사용되고 있다.

암호의 인증 기능이란 기밀성 기능과는 달리 현대 사회의 업무가 고도의 지식 정보사회로 변형되는 과정에서 새로이 야기되는 정보보호 문제를 해결하는 기능으로, 정보화 사회가 활성화 될수록 매우 중요한 역할을 담당하게 된다. 인증 기능을 지원하기 위한 기술로서는 전자서명 알고리즘, 해시 알고리즘, 부인방지 프로토콜, 개인식별 프로토콜 등이 있으며, 전자서명 알고리즘으로 RSA, DSA, ECDSA와 해시 알고리즘으로 SHA-1 등이 전세계적으로 사용되고 있고, 국내에서는 전자서명 알고리즘으로 KCDSA와 해시 알고리즘으로 HAS-160 등이 사용되고 있다.

본 고에서는 II장에서는 대칭키 암호알고리즘, III장에서는 공개키 암호알고리즘, IV장에서는 전자서명 알고리즘에 살펴본다. 그리고 V장에서는 전자공학분야에서 관심을 두고 있는 암호프로세서 개발현황에 대하여 살펴본다.

II. 대칭키 암호알고리즘

암호 시스템은 키 관리 형태에 따라 크게 대칭키 암호알고리즘과 공개키 암호알고리즘으로 나뉘어질 수 있다. 관용키 암호알고리즘은 송·수신자 간에 미리 약속된 동일한 키를 가지고 있어야 하기 때문에 키 분배의 어려움이 있지만 빠른 속도와 비교적 높은 안전성 및 키의 사이즈가 작다는 장점이 있다. 대칭키 암호알고리즘은 다시 데이터 처리형식에 따라 블록 암호알고리즘과 스트림 암호알고리즘으로 나누어진다. 블록암호방식은 평문을 정해진 사이즈의 불록단위로 암·복호화를 수행하는 방식이다.

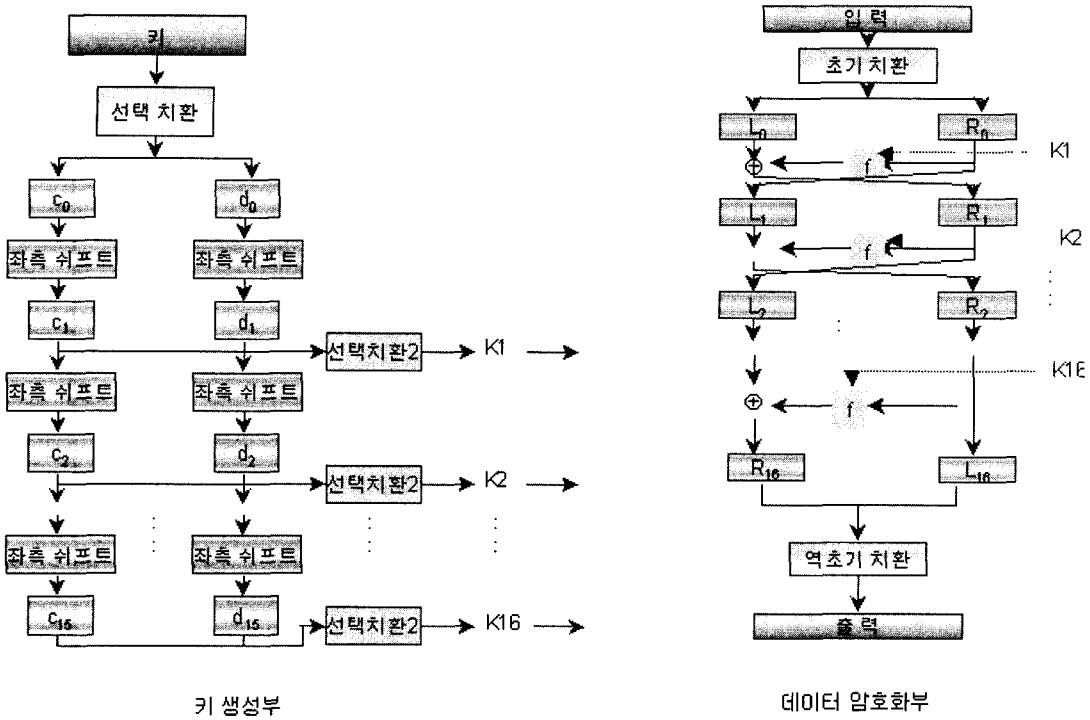
우리에게 가장 널리 알려진 블록 암호 알고리즘은 1977년 미국 NIST에서 표준으로 정한 DES이며 1990년대에 유럽의 Lai와 Massey가 제안한 IDEA, AES, Skipjack 등이 있으며, 국내에서는 1999년 한국정보보호센터(KISA, 현 한국정보보호진흥원)가 주관이 되어 국내 전문가들과 공동으로 블록 암호알고리즘인 SEED를 개발하였다. 스트림 암호 방식은 평문을 하나의 비트열로 취급하여 한 번에 1비트씩 또는 바이트 단위로 암호화시키는 알고리즘이다. 에러 전파 현상이 없으며 블록 암호 알고리즘에 비해 빠르고 용이하게 구현할 수 있다.

본 절에서는 근래까지 국제표준으로 사용되는 DES, 국내표준으로 사용되는 SEED, 새로운 표준으로 제정된 AES 알고리즘에 대하여 살펴본다.

1. DES

DES는 1977년 컴퓨터 보안의 필요성에 의해 제안된 미 연방 정보처리 표준 46(FIPS PUB 46)으로 채택된 대칭키 암호 알고리즘이다. 현재 ISO의 표준(DEA-1)으로 제정되어 있으며, 지난 20년 동안 세계적인 표준으로 사용되어 왔다. DES는 56비트의 키를 사용하며, 16단계의 단일 반복 과정을 거쳐 64비트의 암호문 출력을 내는 Feistel 구조를 갖는다. 복호화시에는 동일한 키를 사용하여 암호화의 역순으로 수행된다. 〈그림 1〉은 DES 기본 구조를 나타낸다.

초기에 128비트의 키 길이로 설계되었던 DES는 NSA에 의해 56비트로 키 길이가 줄어든 이후 꾸준히 키 길이에 대한 논쟁이 있어 왔으며



〈그림 1〉 DES 기본 구조

컴퓨팅 파워가 증가하고 네트워크 기술이 발달하면서 DES에 대한 다양한 공격이 시도되어 왔다. 이에 DES의 대안으로서 안전성이 향상된 3중 DES(Triple DES)가 나오게 되었다. 이 알고리즘은 2개의 키를 사용함으로서 키 길이가 112비트로 늘어나게 되었으며, 이에 따른 안전성의 증가로 인해 키 관리 표준 ANS X9.17과 ISO 8732, 그리고 PEN(Privacy Enhanced Mail) 등에서 채택되어 사용되고 있다. 현재 3중 DES에 대한 실용적인 암호분석 공격법은 없는 것으로 알려져 있다.

2. SEED

SEED는 1999년에 한국정보보호센터에서 개발한 대칭키 암호알고리즘이다. SEED는 Feistel 구조로 이루어져 있으며, 128비트의 평문 블록단위당 128비트 키로부터 생성된 16개의 64비트 라운드 키를 입력으로 사용하여 총 16라운드를 거쳐 128비트 암호문 블록을 출력한다.

SEED는 DES 등의 외산 암호알고리즘이 보안성에 문제가 있다고 판단하여 개발되었으며, 국내 전자상거래(EC)·전자우편·전자문서교환(EDI)·위성방송시스템 등의 분야에서 데이터 송수신 및 저장시 암·복호화 기능을 제공한다.

3. AES

DES는 1977년 미국 연방 표준으로 공표된 후 매 5년마다 안정성 평가를 통하여 1998년까지 안전성을 인정받아 왔다. 그러나 컴퓨터 처리 속도의 비약적 발전으로 56비트 키에 대한 안전성을 보장할 수 없게 됨에 따라, 1998년 NIST에서는 DES를 대신할 새로운 128비트 블록 알고리즘 표준으로 AES를 공모하였다.

이 결과 1998년에 15개의 알고리즘을 후보로서 선택하였으며 평가 기준에 의거하여 1999년 8월 9일에 5개의 최종 후보 알고리즘을 채택하였다. 그리고 2001년에 미국의 차세대 표준으로 RIJNDAEL[8]을 선정하였다. AES선정에 필요

〈표 1〉 AES 후보 알고리즘

알고리즘 (국가)	제안자	형 태
RIJNDAEL (벨)	Daemen, Rijmen	SPN
MARS(미)	IBM	Modified Feistel
RC6(미)	RSA Lab.	Modified Feistel
SERPENT (영, 이, 노)	R. Anderson, E. Bihan, L. Knudsen	SPN
TWOFISH (미)	B. Scneicr, J. Kelscy, D. Whiting, D. Wagner, C. Hall, N. Fersuson	Feistel

한 안전성 평가에 있어 다음과 같은 사항에 대해 주안점을 두었다.

- 구현 측면 : KAT(Known Answer Test)와 MCT(Monte carlo Test)를 이용해 테스트
- 효율성 측면 : 메모리 및 계산상 효율성 비교 (펜티엄 프로-200, Smart Card, 64M-RAM, Windows 이외의 다양한 플랫폼)
- 안전도 : 암호학적 분석보다는 수학적으로 최적인지에 중점
- 알고리즘 구현 특성 : 유연성→다양한 키 및 블록 크기 제공, 응용 환경 적합 여부와 S/W 및 H/W 적합성 및 설계의 단순성

Ⅲ. 공개키 암호알고리즘

공개키 암호알고리즘은 비대칭 암호 알고리즘이라고도 불려지며, 수학적 함수를 기반으로 한다. 이 시스템은 대칭키 암호알고리즘과는 달리 공개키와 개인키 쌍이 존재하며, 공개키는 누구나 사용 가능하고 개인키는 비밀리에 보관하는 방식을 의미한다. 이방식의 배경에는 비밀키 암호시스템의 키 관리 및 분배의 문제점을 해결하는 데 중점을 두고 있으며, 동시에 디지털 서명에도 사용 가능하다는 측면에서 그 응용 범위가 매우 넓다.

1. RSA

1978년에 R. Rivest, A. Shamir, L. Adleman이 제안한 RSA 암호는 수년 동안에 제안된 모든 공개키 알고리즘 중에서 이해 및 구현이 가장 용이한 알고리즘으로 평가받고 있다. 또한 이 알고리즘은 가장 대중적으로 알려졌다. RSA 암호는 큰 수의 인수분해의 어려움에서 안전성을 얻고 있으며, 비밀키로 큰 소수를 사용한다. 다음은 메시지 암호화 및 복호화를 위한 키 생성 단계를 나타낸 것이다.

- 키 생성 단계

1) 두 개의 큰 소수 p와 q를 선정하여 합성수 $n=pq$를 법으로 한다.
2) n을 공개하고 $\phi(n)$과 서로소인 임의의 정수를 e를 선택, 공개키로 한다.
3) $cd\equiv 1 \pmod{\phi(n)}$이 되는 d를 구해 비밀키로 한다.

이러한 절차를 거쳐 공개키와 유클리드 알고리즘을 이용한 비밀키가 생성되고 다음과 같이 암호화 및 복호화가 수행된다.

- 공개키 : n, e
- 비밀키 : p, q, d
- 암호화 : $C\equiv M^e \pmod{n}$ (공개키로 암호화)
- 복호화 : $M\equiv C^d \pmod{n}$ (비밀키로 복호화)

여기서, 만약 공개키 n과 e로부터 비밀키 d를 구할 수 있다면 RSA 암호는 해독되게 된다. 이렇게 되기 위해서는 공개키 n으로부터 $\phi(n)=(p-1)(q-1)$을 구해내야 한다. $\phi(n)$을 구하게 되면 유클리드 알고리즘을 이용하여 쉽게 d를 구할 수가 있게 되므로 RSA 암호 알고리즘의 안전성은 n의 소인수 분해, 즉 p와 q를 구해내는 것에 달려 있다.

RSA 공개키 암호알고리즘을 이동통신 및 무선 PKI 환경에서 빠른 속도로 동작할 수 있게

하기 위한 기술로는 RSA사의 "멀티프라임(multi-prime) 기법" 등이 있다.

2. 최근의 공개키 암호 시스템

이제까지 제안된 공개키 암호 중 RSA, ElGamal, 타원곡선 암호(ECC) 등이 대표적으로 많이 사용되고 있고, 이들은 모두 가환군 내에서의 이산대수나 소인수분해 문제에 기반하고 있는데 가환군의 구조는 잘 알려져 있으며, 위 문제들에 대한 효과적인 알고리즘도 계속 연구되고 있다.

가장 널리 알려져 있는 RSA 공개키 암호 방식은 안전성을 위하여 키의 길이가 상당한 길이가 요구되어 연산능력이 제한된 이동 통신 단말기에는 사용이 제한될 수 있다. 이에 1995년 Koblitz와 Miller는 타원곡선을 이용한 공개키 암호시스템을 구성할 수 있다고 제안하였다. 그 후 비트당 안전도가 타 공개키 시스템보다 효율적이라는 것이 알려졌고, 최근 높은 속도의 구현이 가능하게 되었다.

타원곡선 암호시스템(ECC)은 유한체의 덧셈군에 근거한 시스템으로써 다음과 같은 장점을 가진다.

① 군(Group)을 제공할 수 있는 다양한 타원곡선을 활용할 수 있다. 즉, 다양한 암호시스템 설계가 용이하다.
② 초특이 타원곡선을 피하면 이 군에서의 준지수 시간 알고리즘이 존재하지 않는다. 즉 안전한 암호시스템을 설계하는 것이 용이하다.
③ 타원곡선 암호시스템은 기존의 공개키 암호와 같은 안전도를 제공하는 데에 더 작은 키 길이를 가지고 가능하다.
④ 타원곡선에서의 더하기 연산은 유한체의 연산을 포함하므로, H/W와 S/W로 구현하기가 용이하다. 더욱이 이 군에서의 이산대수 문제는 특히, 같은 크기의 유한체 K에서의 이산대수 문제보다 훨씬 어렵다고 알려져 있다.

유한체 위에서의 타원곡선(ECC)은 DH 공개키 암호 방식, DSA 같은 서명 기법을 구현하는 데에 사용될 수 있고, 이러한 시스템들은 짧은 키 길이를 가지고도 다른 공개키 암호 시스템과 동등한 안전도를 제공할 수 있다. 또한 짧은 키 길이를 갖는다는 것은 대역폭과 메모리가 작아짐을 의미하는데, 이로 인해 메모리와 처리능력이 제한된 스마트카드, 이동통신에서의 보안성 제공 같은 응용에서 중요한 기반 암호 기술이 될 수 있다. 또한 공개키 암호의 사용 범위가 계속 넓어지고 있으며, 시장 규모도 커지고 있어 세계 각국은 자국의 고유의 공개키 암호를 확보하려하고 있다. 위의 암호들이 기반하고 있는 난제를 찾아 암호를 구성하려는 시도들이 이루어지고 있는데, 최근 Silverman 등이 제안한 격자문제에 기반을 둔 NTRU, 모든 유한 비가환군에 적용되며 비가환군의 특징을 바탕으로 난수를 매번 발생시키지 않고 고정하여 사용할 수 있는 XOR 등이 있다.

Ⅳ. 디지털 서명

보통의 경우 암호라 하면 비밀통신을 연상한다. 물론 정보화 사회에서도 비밀통신은 중요하다. 그러나 일상업무 중에서는 비밀문서의 취급보다는 일반문서에 대한 서명이나 인증이 훨씬 빈번하게 있을 것이다. 정보화 사회에서는 종이로 작성된 문서 대신에 컴퓨터나 네트워크 내에서 위·변조나 복사가 용이한 바이너리 파일로 작성된 문서를 취급하게 될 것이므로 전자서명이나 인증은 비밀통신 이상으로 아주 중요한 기능이다. 일반적으로 서명이나 인감은 개인의 필요성에 의하여 언제든지 생성할 수 있고, 이 서명 또는 인감을 수신한 사람은 누구든지 수신된 서명이나 인감의 정당성을 쉽게 확인할 수 있으며, 서명의 생성자나 인감의 소유자 이외에는 이 서명이나 인감을 위조할 수 없어야 한다.

다음에서는 이들 전자 서명 방식들에 대해 살펴보기로 한다.

1. DSS

DSS(Digital Signature Standard)는 미국의 NIST에서 1991년 8월 30일 발표한 디지털 서명안이다. 핵심 알고리즘은 DSA(Digital Signature Algorithm)으로서 약 6개월의 공개 검토를 거친 결과, 검토자의 90% 정도가 문제점이 있다는 답을 한 것으로 알려졌다. 이러한 우려들은 여러 분야에서 일고 있는데, 트랩도어가 존재할 가능성과 기존 512비트의 법의 값을 1024비트로 늘여야 한다는 주장이 나오고 있으며, 특허권에 있어 Schnorr의 특허에 걸려 있어 문제점으로 지적되고 있다.

또한 미국의 NIST는 2000년 2월 15일자로 디지털 서명 표준안 (DSA)의 개정안을 발표했다. 1998년 DSA에 RSA를 추가한 FIPS 186-1에 이어서, FIPS 186-2로 명명된 이 개정안은 1999년 1월에 승인된 ANSI X9.62에 명시되어 있는 ECDSA의 내용을 담고 있다. 이 개정안으로 미국 정부는 일반인으로 하여금 서명 알고리즘을 선택할 때 DSA, RSA, ECDSA 중에서 자유롭게 선택할 수 있게 하였다.

2. KCDSA

디지털 서명에 대한 중요성이 날로 증가하면서 국내에서는 1994년부터 디지털 서명 표준화에 대한 연구가 시작되었다. KCDSA(Korean Certificated Digital Signature Algorithm)는 국내 디지털 서명 표준화의 일환으로 개발된 서명 방식으로 1998년에 한국정보통신기술협회(TTA)에서 그 표준을 규정하고 있으며, 여기서는 임의의 길이를 갖는 메시지 정보에 대해 부가형 전자서명을 생성 및 검증할 수 있게 해주는 확인서를 이용한 부가형 전자서명 알고리즘을 규정하고 있다. 공개 검증키는 CA라 불리는 모든 사람이 인정하는 제3자가 공개 검증키 정보를 CA의 비밀키로 서명한 확인서를 배포함으로써 공개 검증키의 소유자를 보증한다.

이미 살펴보았던 DSS와 KCDSA를 비교해 보도록 한다. 이들 두 방식은 모두 이산 대수 문제를 푸는 어려움에 근거하고 있다. 오직 비밀키에 의해서만 서명이 생성되고 있으며, 공개키를 통해서는 비밀키를 유출해 낼 수 없다는 특징을 가지고 있다. 이는 디지털 서명을 수행하는데 있어 안전성에 중요한 요소가 된다.

국외로 수출하는 부분에 있어 DSA와 Schnorr 방식은 특허가 걸려 있는 관계로 제약이 있으며, 수출을 위해 그만큼 기능면에서 우수해야 할 것이라는 지적이 나오고 있다. 현재, 위의 두 가지 방식은 어떤 해시 함수를 사용할 것인가에 대한 아무 정보도 없는 것이 특징이며, 아직은 고려 사항이다.

이상에서 살펴본 것 외에도 많은 디지털 서명 방식들이 존재하고 있으며, 이들 응용 분야 또한 다양하다. 이러한 디지털 서명은 사소하게는 개인간의 안전한 통신에서부터 크게는 국가기간 전산망을 위하여 꼭 필요한 요소이며, 그러기에 외국 기술의 의존보다는 국내 고유의 기술이 필요한 부분이라 하겠다.

V. 암호 프로세서 개발 및 동향

암호 프로세서는 각종 보안 서비스를 위해 고속 처리가 필요하거나, 경박단소화를 위하여 암호 알고리즘을 구현한 칩으로 그 종류로는 CPU의 연산동작을 보조하기 위한 보조 프로세서 형태의 칩과 CPU코어를 내장하여 범용 CPU 기능을 수용한 SoC(System on a chip) 형태의 칩이 있다.

현재 암호화/복호화, 해시, 메시지 인증, 공개키 연산 등의 기능이 하나의 칩으로 구현되는 추세로 공정 기술의 발전으로 인한 집적도의 증가로 칩에서 수용 가능한 로직의 크기가 증가함으로서 가능하다. 그리고 DES, 3-DES, AES 등 암호 알고리즘과 SHA-1, MD-5 등 상용으로 나와 있는 다양한 암호 알고리즘을 지원한다. 또한 PCI, PCMCIA, USB, IEEE1394 등 표준 정합 기능을 칩에 내장하여 지원한다. 시스템 설계기술이 SLI(system level integration) 형

〈표 2〉 암호 프로세서의 개발 현황

업체명	제품명	기능/특징
Hi/F	6565 Public Key Processo	-RSA 연산 기능 -난수 발생 기능 -PCI-2.1 정합 기능
	7811 Security Processor	-DES, 3-DES, RC4 알고리즘 지원 -SHA, MD5 알고리즘 지원 -MIPS uProcessor 정합 기능 -PCI 정합 기능
Analog Devices	ADSP2141	-DES, 3DES 지원 -SHA1, MD5 지원-공개키 연산기 내장 -ADSP218X 코어 내장 -PCI/CardBus 정합 기능
필립스	VMS747	-DES, 3DES 지원 -MD5, SHA1 지원 -1024 비트 지수승 연산 -난수 발생 기능 -암호/해시 동시 처리기능 지원 -HMAC 기능 지원 -ARM7 CPU 코어 내장 -템퍼 방지 회로 내장 -PCI 2. 2 정합 기능
모토로라	MPC190	-RSA,, EC 연산 기능 지원 -DES, 3DES 지원 -SHA1, MD4/MD5 지원 -HMAC 기능 지원 -PCI-2.2 정합 기능 내장
Rainbow Myktronx	MYK-82A	-미정부 type-2 알고리즘 (skipjack, KEA) 지원 -1024 지수승 연산기능지원 -DES, SHA 지원 -난수 발생 기능 지원 -ARM7TDMI 코어 내장 -PCMCIA 정합기능 내장 -32 비트 RISC CPU 정합 기능
	MYK-85A	-미정부의 type-1 암호 알고리즘(Baton) 지원 -미 정부의 type-1 해시 알고리즘 지원 -DES, 3DES 지원 -SHA-1 지원 -1024 지수승 연산 기능 지원 -난수 발생 기능(type-1) 지원 -ARM7TDMI 코어 내장 -DS01/DS102 정합 기능 -32 비트 RISC CPU 정합 기능

태로 빠르게 변화함에 따른 현상으로 이미 설계/검증된 로직이 반도체 IP형태로 표준화 됨에 따라 다양한 종류의 기능 블록들도 하나의 칩으로 구현되고 있다. 과거 보드 수준에서 구현되던 기능들이 하나의 칩으로 구현되는 형태로 암호 프로세서 안에 알고리즘 처리용 블록뿐만 아니라 CPU코어, 메모리, 각종 I/O 및 표준 정합용 블록들을 내장하고 있다. 반도체 공정 기술이 CBIC (Cell Based ICs)가 주류를 이루가 선폭 또한 작아짐에 (0.35u→0.25u→0.18u) 따라 고속으로 동작하는 칩이 제작되고 있으며, 알고리즘 구현을 위한 칩의 구조 설계 시에도 고속 병렬 처리가 가능한 파이프라인 구조를 사용하고 있다. 최근에는 OCB(Offset CodeBook) 모드와 같이 병렬 처리가 용이하면서도 고비도의 안전성을 제공할 수 있는 운용 모드가 표준으로 채택되고 있으며 미국의 Hi/Fn사에서 최근에 개발된 제품의 경우 Gbps 단위의 속도로 데이터 처리를 해주는 암호 프로세서도 있으며 이러한 성능의 암호 칩은 조만간 일반화 될 전망된다.

세계 각국의 암호 프로세서 개발 현황은 왼쪽의 〈표 2〉와 같다.

VI. 각국의 최근 동향

미국의 AES에 자극을 받아 유럽 NESSIE 연합과 일본 CRYPTREC은 각자 전자정부를 구축 및 암호 산업의 육성을 위하여 독자적인 암호 기술을 확보하고자 각국의 사정에 따른 AES와 유사한 별도의 계획을 수립하여 추진하고 있다.

1. 유럽

유럽은 정보 사회 기술 내에 NESSIE(New European Schemes for Signature, Integnty, and Encryption) 프로젝트를 2000년 1월부터 시작하였고, 공개적인 모집과 평가를 통하여 강한 암호방식을 만들려는 계획으로 블록 암호, 스트림 암호, 공개키 암호, 전자 서명, 난수 발생기,

메시지 인증 부호, 해시 함수 등 암호를 위한 기본 함수들을 공모하고 있다. 각 함수의 응모 기준은 공개 규격에 맞도록 발표하여 놓고 있으며 벨기에 암호 학자 Bart Preneel이 주도적으로 추진하고 있다.

이 계획은 3년간 선정 작업을 계획하고 있으며, 방식은 Gigabit 네트워크, 스마트 카드, 무선 통신용으로 이용하려고 하고 있으며, 유럽의 암호 산업의 발전에 기여하고자 이스라엘, 덴마크, 프랑스, 독일, 스위스, 스웨덴, 영국, 벨기에, 노르웨이, 핀란드 기업이 참여하고 있으며, 최종 유럽의 암호 프리미티브 표준 제정 프로젝트인 NESSIE에 후보로 등록된 알고리즘 목록을 발표하였다. 등록된 알고리즘으로 블록 암호는 64비트 입출력 크기 6개, 129비트 크기 7개, 160 비트 크기 1개, 가변 입출력 크기 3개가 등록되어 있고, 스트림 알고리즘 6개, 공개키 알고리즘 5개, 서명 알고리즘 7개, MAC, 인증 알고리즘 등이 있다.

또한 벨기에의 COSIC, 스위스의 ETH, 프랑스의 GRECC 등 순수 암호 이론 연구기관이 구축되어, 자국의 암호 연구 역량을 집중하고 있다.

2. 일본

일본 정부는 2003년 까지는 전자 정부를 구축하는 데 안전한 암호 기술이 필수불가결한 주요 요소임을 파악하고, 개인의 기밀성 확보와 전자문서의 인증 제공 수단이 필요하다고 인식하였다. 이에 일본 정부는 국제적으로는 표준 기구인 ISO/IED JTC1 활동에 노력을 다하고 있다.

공모하는 알고리즘으로는 공개키 암호, 비밀키 암호, 해시 함수, 난수 발생기 등이며 2000년 7월 21일에 1차 공모가 완료되어 48종이 신청되었다. 이 계획에는 기술 검토 결과를 제공하여 일정 수준 이상이 되는 암호 기술은 평가하여 합격되는 방식을 하고 있으며 이 계획을 위하여 일본의 정보처리 진흥 사업 협회인 IPA가 CRYPTREC를 구성한 바가 있다.

국제 표준화 기구인 ISO/IEC 내의 JYC/SC 27에 제출되어 있는 일본의 암호 알고리즘은 MARS(일본 IBM), CIPHERUNICORN-A (NEC), MISTY1(미쯔비시), Hierocrypt(도시바), MULT1-SO1(히다치), Camellia(NTT, 미쯔비시) 등 비밀키 알고리즘 6종, NTT의 EPOC, PSEC 등 공개키 알고리즘 2종으로 총 8개이다.

이 중 비밀키 알고리즘은 대부분이 블록 암호이며, MULT1-SO1 만이 스트림 암호이다. EPOC은 NTT의 OKAMOTO를 중심으로 개발된 확률 공개키 암호로 ElGamal 방식의 변형으로 볼 수 있으며, PSEC은 타원 곡선 암호 일종의 소프트웨어 구현 시 효율성이 높은 OEF(Optimal Extension Field)를 이용한 연산 방법을 사용하였다.

3. 국내 동향

과거에는 정부주도의 암호기술을 개발하고 이용하여 왔으나, 최근에는 전 세계적으로 민간주도의 개발 패러다임으로 변화하고 있다. 국내에서는 근간이 되는 암호 원천 기술이 다른 선진국에 비해 뒤쳐져 있었으나 근래 점차 선진국 대열로 발돋움하고 있는 단계이다. 이에 따라 정부에서의 정책 주도로 1999년 블록 암호 알고리즘인 SEED가 TTA 표준으로 제정되었으며 인증서 기반 표준 전자서명 알고리즘인 KCDSA가 1997년 개발되었고 1998년 해시 함수인 HAS-160이 개발되었다. 또한 2001년 한국정보통신기술협회(TTA)의 정보통신 표준 활용실태 조사 결과, SEED는 14개 분야, 1,894건의 정보통신표준 중 활용도가 1위로 조사되었으며, 2002년 5월 현재, 총 414개 산업체 및 학계에 배포되었다고 한다. 최근에는 KCDSA를 ECC에 적용한 ECKCDSA가 2001년 TTA 표준으로 제정되었다. 이런 기술 발전의 추이뿐만 아니라 민간의 암호 이용이 증대되고 국가의 지배에서 벗어나려는 움직임이 팽배하여 민간이 중심이 되고 주도하는 우리나라의 암호 알고리즘 공모도 생각하여 볼 수가 있는데 실제 이러한 암호 알고리즘 공모 사업이 우리나라에서도 추진이 되고 있다. 이에 따르면 차세대 암호 기술 공모 대상으로는 블록 암호와 스트림 암호, 가변길이의 해시 함수, 의사 난수생성기

등이 될 것으로 보이며 기술 백서 대상 암호 기술로는 여러 가지 공개키 파라미터, 키 분배, 키 유도 함수 등과 사용자 인증 관련한 기술, 공모 대상 알고리즘 이외의 국외 표준 암호 알고리즘 등과 함께 고속화 기술이나 구현 기술 등도 다루어질 예정이다. 위의 공모 대상 알고리즘 중 블록 암호 알고리즘은 이미 우리나라에서 개발된 SEED가 있지만 산업체에서 실제 구현하여 사용하는 데에 따른 속도의 문제점을 지적하고 있어 보완이 필요하며 가변 길이의 출력을 갖는 해시 함수의 경우 KCDSA나 ECKCDSA가 가변 길이의 해시 출력을 요구하므로 이를 뒷받침하기 위해 필요한 것이다.

Ⅶ. 결 론

암호기술 개발은 전 세계적으로 민간주도의 개발 패러다임으로 변화하고 있다. 암호 기술의 주요연구대상 분야는 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 해시함수 등 각종 암호 알고리즘들을 라이브러리 형태로 구성하여 보안 기능이 요구되는 다른 프로그램 개발 시에 재사용할 수 있도록 하는 고성능 암호 API 기술, 공개키 암호 방식으로 RSA 알고리즘에 비하여 키 길이가 짧아 계산량이 적어 고속의 연산이 요구되는 IC 카드나 USIM 카드 등에 적용되는 타원곡선 알고리즘, 불확정성의 원리를 이용하여 안전한 키 교환이 가능한 차세대 암호 시스템의 대안으로 부각되고 있는 양자암호 기술 등이 있다. 이외에 사용자 인증을 위한 응용계층에서 사용되는 SET (Secure Electronic Transaction), SSL(Secure Socket Layer), 유선상의 네트워크 계층의 보안 프로토콜을 무선환경에 맞게 경량화한 WTLS(Wireless Transport Layer Security), IP 계층의 통신에서 프라이버시 보호기능과 인증 기능을 제공하는 IPsec(Internet Protocol Security)과 키 교환 표준으로 정의한 IKE(Internet Key Exchange), 무선 LAN, IMT-2000 환경에서의 Mobile IPsec 기술, IEEE 802.1x 보안 기술 등이 있다.

시스템의 고속화, 정보통신망의 대용량화 추세에 적극 대응하기 위한 고속·고비도 암호 알고리즘 및 고속 암호 프로세서 등 차세대 표준 암호 기술을 개발 부분, 고속/고비도의 안전한 암호 알고리즘 활용을 위한 기술개발과 암호 프로토콜 적용 기술은 앞으로 연구가 지속되어야 할 분야이다.

참 고 문 헌

〔1〕 ANSI X3.92, "American National standard for Data Encryption Algorithm (DEA)," American national Standards Institute, 1981.

〔2〕 "Advanced Encryption Standard(AES) Development Effort" http://csrc.nist.gov/encryption/aes/, 1999

〔3〕 R.Rivest, A.Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the Association of Computer manufactures. vol.21, no.2, pp.120-126, Feb. 1978.

〔4〕 "Specification for a Digital Signature Standard," NIST, FIPS XX. Draft, August 1991.

〔5〕 정보통신부 "정보보호 기술 개발 5개년 계획," 2001.

〔6〕 Burce Schneier, "Applied Cryptography", John Wiley & Sons, Inc.

〔7〕 Douglas R. Stinson, "Cryptography : Theory and Practice", CRC Press, Inc., 1995.

〔8〕 Daemen and V. Rijmen, "AES proposal : Rijndael, NIST AES proposal" June, 1998.

〔9〕 ANSI X9.63 Public Key Cryptogra-

phy For The Financial Services Industry : Key Agreement and Key Transport Using Elliptic Curve Cryptography.

[10] ISO/IEC JTC 1/SC 27 N 2303 CD 15946-2, Information Technology-Security Techniques-Cryptographic Techniques based on Elliptic Curves: Part 2-Digital Signatures.

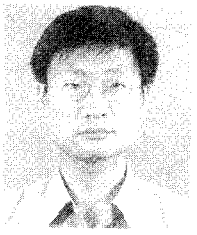
저 자 소 개

서 창 호

1990년 고려대학교 수학과 졸업 (이학사), 1992년 고려대학교 대학원 수학과 (이학석사), 1996년 고려대학교 대학원 수학과 (이학박사), 1996년~1997년 : 국방과학연구소 선임연구원, 1997년~2000년 : 한국전자통신연구원 선임연구원, 팀장, 2000년~현재 : 공주대학교 응용수학과 조교수, 〈주관심 분야 : 암호알고리즘, PKI, 시스템보안〉

이 옥 연

1988년 고려대학교 수학과 졸업 (이학사), 1990년 고려대학교 대학원 수학과(이학석사), 1996년 Univ. of Kentucky(이학박사), 1999년~2001년 : 한국전자통신연구원 선임연구원, 팀장, 2001년~현재 : 국민대학교 수학과 전임강사, 〈주관심 분야 : 이동통신 보안, 암호알고리즘〉



류 희 수

1990년 고려대학교 수학과(이학사), 1992년 고려대학교 대학원 수학과(이학석사), 1999년 Johns Hopkins Univ. 수학과(이학박사), 1999년~2000년 : 홍익대학교 전자과 post-doc, 2000년~현재 : 한국전자통신연구원 정보보호기반연구팀장/선임연구원, 〈주관심 분야 : 암호이론, 통신망 정보보호, 정수론〉

정 교 일

1981년 한양대학교 전자공학과 (공학사), 1983년 한양대학교 산업대학원 전자계산학과 (공학석사), 1997년 한양대학교 대학원 전자공학과 (공학박사), 1981년 엠시스템즈 사원, 1981년 12월~1982연 2월 : 한국전기통신연구소 위촉연구원, 1982년 3월~현재 : 한국전자통신연구원 정보보호기반연구부장/책임연구원, 〈주관심 분야 : IC Card, Security, 국가기반보호, Biometrics, 신호처리〉