초경량 공개키 암호 설계에 관한연구

이경효° , 박익수, 오병균
목포대학교 정보공학부
{mediakh°, upark, obk}@mokpo.ac.kr

The study of lightweight public key cryptosystem design

Kyoung-Hyo Lee°, Ik-Su Park, Byeong-Kyun Oh
Department of Information Security Mokpo National University

요 약

유비쿼터스 기술을 실용화함에 있어 가장 요구되는 기술 요소 중의 하나는 유비쿼터스 네트워킹상의 보안 및 암호기술이다. 유비쿼터스 장치들의 제약된 계산능력과 허용되는 네트워킹 대역폭의 한계로 인해 기존 공개키 암호 시스템을 적용하기에 특성화된 암호기술인 초경량 암호시스템이 필요하게 된다. 본 연구에서는 기존의 공개키 시스템의 특징을 분석하여 유비쿼터스 환경에 적용가능성을 살펴보았고 새롭게 제시된 공개키 시스템들의 특징을 비교하여 경량화에 적합한 암호시스템의 요구조건과 활용 가능성을 예측해보았다.

1. 서 론

유비쿼터스 기술을 실용화함에 있어서 가장 요구되는 기술 요소 중의 하나가 유비쿼터스 장치들의 제약된 계산 능력과 허용되는 네트워킹 대역폭의 한계로 인해 유비쿼터스 상의 보안 및 네트워크 상의 보안 및 암호기술이다. 보안기술의 핵심 부분 중 하나인 공개키 암호기술의 경우, 현재 널리 사용되고 있는 시스템들인 RSA, 타원곡선 암호 시스템 등은 그 여러 가지 특성 분석과 구현, 그리고 안정성 분석 등이 널리 이루어져 있다. 실용적인 활용과 이론적인 이해 양쪽 모두의 결과로 기존 시스템을 수정하여 필요한 정보량과 계산량을 효율적으로 개선해야 한다. 예를 들어 128비트 대칭키 수준의 보안을 유지하기위해 RSA의 경우 3072비트, 그리고 보다 효율적이라고 알려져 있는 타원곡선 암호의 경우에도 GF(2283)의 정보량이 요구되는데 이와 같은 크기의 정보를 소형 경량의 유비쿼터스 장비들에 필요한 양만큼 저장하기에는 어려운 경우가 발생되고 암호시스템의 암호화 및 복호화와 같은 기본 작용의 처리속도 역시 실용적으로 이용하기에는 많은 개선이 필요하다. 본 논문에서는 유비쿼터스 환경에 적용될 RFID나 USN센서노드들에 대한 개발환경과 여기에 접목할 기존 공개키 암호시스템들의 특징을 알아보고 분석하여 유비쿼터스 환경에 적용가능성을 살펴보고 새롭게 제시되고 있는 공개키 시스템의 적용가능성을 예측해본다.

2.기존 공개키 경량화를 위한 특성분석

초경량 공개키 설계를 위해서 이미 검증된 기존의 공개키들의 장단점과 문제점을 살펴보고 이들 공개키 들은 기반문제가 어렵다는 가정과 거기서 상응하는 보안 모델에서 충분히 안전하다고 증명된 것들이다. 기존의 암호시스템의 종류를 살펴보면 Knapsack 공개키 암호 시스템, RSA암호시스템, Rabin암호시스템, ElGamal암호시스템, 타원곡선 암호시스템 등이 있다.

[표1] 공개키 암호시스템의 성능비교

	RSA 1024	ElGamal 1024	ECC 168
암호화속도(ms)	0.73	31	31
복호화속도(ms)	27	16	15

[표1]은 셀룰론 450MHz 머신에서 Microsoft Visual C^{++} 6.0SP2로 컴파일한 결과이다. Crypto^{++}3.1을 사용하였고 현재 Crypto^{++}는 5.2.1버전까지 나와 있다. 이전 버전의 결과를 사용하는 이유는 원하는 공개키 시스템을 동일 조건으로 실험한 구 버전의 자료뿐이었고 버전이 바뀌었어도 ECC의 코드 최적화에는 큰 변화가 없기 때문이다. RSA의 복호화보다 ECC의 암호화가 더 느린 성능을 보이는데 코드의 최적화가 덜되어있다. 가장 대표적인 공개키이자 많이 사용되는 공개키인 RSA는 개발된 이후 끊임없이 연구가 이어져왔고 그로인해 다른 시스템보다 더 좋은 효율성을 보인다. 위의 표는 동일한 환경에서 실험한 결과이고 기존의 공개키 들도 그 특징을 살려 잘 사용한다면 유비쿼터스 환경에 적용할 수 있을 것이다.

일반적인 RSA는 큰정수의 모듈러를 구현해야 하기 때문에 PDA, 모바일 폰, 스마트 카드, RFID와 같은 제한된 환경에 적합하지 않다. 그리고 다른 공개키 암호 시스템과 비교해보았을 때 키 생성에 요구되는 시간이 더 길고 같은 안전도를 구현하기 위해서 더 큰 크기의 키가 요구된다. 이것은 더 많은 메모리를 요구하는 것과도 일맥상통한다. 그러므로 RSA를 유비쿼터스 환경에 적용하기 위해서는 암호화지수가 작은 수이거나 2진 표현시 적은 1을 가지는 특별한 지수를 사용함으로서 계산상의 효

「본 논문은 2005년도 지역IT협동연구센터 디지털 콘텐츠 저작권 관리기술 연구비 지원에 의하여 연구되었음」

율성을 꾀할 수 있다. 유비쿼터스 환경에 기존의 공개키 암호 시스템을 그대로 적용하기란 사실상 불가능하다. 그러나 약간의 변형이나 수의 특성을 이용한다면 기존의 공개키 들도 변형 사용할 수 있을 것으로 보인다. RSA 복호화보다 ECC암호화가 더 느린 성능을 보이는 것은 코드의 최적화가 덜 된 것으로 보인다. 가장 대표적인 공개키인 RSA는 개발되 이후에 끊임없는 연구가 있었다. 그로 인해 다른 시스템보다 더 좋은 효율성을 보이는 것으로 추측된다. 암호시스템의 안전도, 효율성, 특징 등을 잘살려 사용한다면 유비쿼터스 환경에 적용할 수 있을 것으로 보인다.

3.최근 공개키 경량화를 위한 특성분석

기존의 공개키들은 제안된 이후로 안전성에 대한 증명이 오랜 기간 동안 이루어져 충분히 검증된 것들이다. 그에 비해 안전도는 명확히 증명되지 않았지만 경량화가 가능할 만한 새로운 공개키들을 살펴보기로 한다.

3.1 겹선형쌍 기반 암호시스템

겹선형쌍 기반 암호시스템의 안전도는 어떤 군에서 GDHP와 BDHP의 풀기 어려움에 기초를 두고 있다. 또는 유사하게 군G1과 G2쌍에서 거기에 상응하는 co-problem의 풀기 어려움에 근거를 둔다. 가장 대표적인 쌍인 Weil과 Tate paring 모두 Miller의 알고리즘으로 계산 가능하나 Tate paring이 Weil paring보다 일반적으로 더 효율적으로 구현이 가능하다.

ID기반 4개의 암호기법은 4개의 알고리즘으로 구체화 할 수 있다. 시스템 파라미터와 마스터키를 생성하는 Setup, 마스터키를 사용해 거기에 상응하는 임의의 비트열인 개인키를 생성하는Extract, 공개키를 사용해 평문을 암호화 하는 Encrypt, 맞는 개인키를 이용해 원문으로 복원하는 Decrypt알고리즘이다. Setup과 Extra가 일반적인 암호시스템에서 키 설정단계에 해당하지만 여기서는 Setup, Extract, Encrypt, Decrypt용어를 그대로 사용하였다.

그 외에도 검색 가능한 공개키 암호화기법인 겹선형맵에 기반을 둔 (Searchable Public Key Encryption: SPKE)과 계층적인 기반 암호화 기법인 HIDE과 이중 계층적 ID기반 암호화기법인 이중 HIDE과 랜덤 오라클이 아닌 상황에서 ID기반 암호화 기법 등이 있다. 이 기법들은 공개된 e-mail과 같은 ID정보를 이용해 공개키를 생성하므로 따로 공개키 디렉토리를 유지할 필요가 없다는 장점이 있지만 RSA암호시스템과 비교를 했을 때 겹선형쌍 암호 시스템은 암호화 속도는 76배, 복호화 속도는 4배 느렸지만 안전성에 대한 증명은 거의 이루어진 상태이다.

3.2 NTRU 알고리즘

NTRU암호시스템 구현은 다항식의 산술적인 구현과 실제 암호시스템의 구현이다. 다항식 연산을 최적화함으로서 속도를 향상시킬 수 있고 가장 많은 시간이 소요되는 연산이 환(ring)에서 키생성 부분에서 역을 구하는 것이지만 암호화나 복호화 성능에 영향을 미치지 않는다. 곱셈 연산은 암호, 복호화 속도를 향상시키기 위해서는 다항식 곱셈 알고리즘의 구현과 그것의 최적화에 중점을 두어야한다.

[표2]NTRU 키 크기에 따른 속도

(ms)	NTRU 167	NTRU 167	NTRU 167
키생성속도	8.3	19.8	71.2
암호화속도	0.8	1.9	6.6
복호화속도	1.4	3.5	12.7

[표2]는 키생성, 암호화, 복호화 시에 걸리는 시간을 나타낸다. 일반적으로 NTRU 167은 RSA 512,NTRU 263은 RSA 1024,그리고 NTRU 503은 RSA 2048 정도의 안전도를 가진다고 할 수 있다. NTRU 263의 공개키는 1842비트의 정수로 코딩되고 개인키는 다항식 f의 역 f^{-1}이 저장되므로 공개키보다 두 배가 더 크다. NTRU암호시스템은 비록 Lattic축소 공격을 피할 수 있도록 개발되었음에 틀림이 없지만 복호화 방법은 GGH암호 시스템과는 매우 다른 짧은 lattic기저를 알고 있음에 근거한다. 이런 면에서 G호는 사실 McEiece암호 시스템과 유사하다. 왜냐하면 모두 작은 랜덤 기여를 인지하고 줄여나감으로서 복호화가 수행되기 때문이지만 NTRU암호시스템은 가분성을 고려함으로서 훨씬 큰 랜덤수를 줄인다. NTRU는 일반적으로 가장 많이 사용되는 RSA나 ECC보다 훨씬 더 빠른 성능을 나타내는 것은 분명하다. 즉 같은 안전도에서 ECC보다는 대략 두배 이상의 나은 성능을 보인다. 그러나 NTRU의 키 크기는 ECC보다 크고 NTRU의 메시지 확장은 ElGamal ECC보다 두 배나 더 크다는 것을 고려해야한다.

3.3 딸임군 암호시스템

딸임군 암호시스템은 CRYPTO2000에서 Diffie-Hellman 형태의 문제에 기반을 두어 처음 소개되었고ASIACRYPT 2001에서 C코드를 이용해 구현한 논문이 발표되었고 현재도 구현상의 효율성이나 기반 문제의 난해도에 관해 암호학 분야에서 활발한 연구가 진행 중이다.

[표3] 딸임군 암호시스템과 암호시스템의 성능비교

PKC	Security Parameter	암호화		복호화	
		ms/op	Kbyte/sec	ms/op	Kbyte/sec
RSA	1024	0.32	396	10.23	12.52
ECC	163	14.27	1.472	25.72	0.817
NTRU	n=263	0.27	996.79	0.64	425.80
Braid	n=100,l=15	13.4	146.53	10.4	188.13

[표3]은 여러 시스템과의 비교를 통해 객관적인 성능에 대한 평가를 해보았다. RSA와 ECC는 셀룰론 850MHz에서, NTRU는 PentiumIII800MHz에서, Braid는 PentiumIII 860MHz머신에서 실행되었다. 딸임군 암호시스템은 NTRU보다는 좀 미약하지만 ECC와 비슷한 정도의 효율성을 가진다. RSA1024와 ECC163, NTRU263의 안전도는 10^{12}정도이고 Braid n=100, l=15의 안전도는 2^{85}인 점까지 감안하면 비교적 좋은 성능을 나타내는 것으로 보인다. 딸임군 암호시스템은 제안된 지 몇 년 되지 않아 정확한 안전도나 키 생성에 관한 분야 등 앞으로 연구할 가치가 많은 분야이고 많은 가능성을 내포하고 있는 것으로 보인다. 유비쿼터스 환경에 적용할 기반 문제를 제공하는 스킴으로 보인다.

3.4 Lucas 수열기반 암호시스템

LUC공개키 알고리즘은 대부분의 알고리즘에서 사용하

는 지수처리 과정을 사용하지 않고 Lucas수열로 이를 대치하였다는 점에서 주목을 받고 있다.

처음엔 같은 키 크기의 RSA와 안전도도 비슷하지만 성능이 두 배 정도 느렸으나 Luc, 체인을 계산하는 효율적인 알고리즘들이 개발되어 유비쿼터스 환경에 적용해 볼 수 있을 정도로 향상 되었다.

[표4] RSA와 LUC비교

	LUC	RSA
키생성	n=p*q를 만족하는 소수 p와 q를 생성	n=p*q를 만족하는 소수p와 q를 생성
	e를 생성하고 $de\equiv1 \mod(p^2-1)(q^2-1)$을 만족하는 d를 생성	e를 생성하고 de=1 mod n을 만족하는 d를 생성
암호화	$E=V_e(M,1) \mod n$	$E=M^e(M,1) \mod n$
복호화	$M=V_d(E,1) \mod n$	$M=V_d(E,1) \mod n$
상재속도	4	3

RSA암호시스템을 해독하기위하여 메시지M에 대한 암호문 $E=M^e(M,1) \mod n$이 주어졌을 때 LUC시스템에서 주어진 e와 d를 사용하여 $E^d \mod n$을 계산하는 것으로 충분하다. 왜냐하면 $de\equiv1 \mod(p^2-1)(q^2-1)$이 $de\equiv1 \mod n$에 대하여 해독된다면 RSA시스템은 해독될 수 있음을 의미한다. 겹선형쌍 암호시스템은 군에서 Diffie-Hellman 문제의 어려움에 기초하고 NTRU는 두개의 서로 다른 모듈러에 의한 다항식 연산을 적용하여 안전성을 보장하였고, 땋임군 암호시스템은 땋임군위의 공액문제의 어려움에 기반 하였고, Lucas수열기반암호시스템은 지수연산을 대신하여 Lucas수열을 사용하였다.

[표5] 새로운 공개키 암호 시스템 성능비교

(ms)	겹선형쌍 기반	NTRU	땋임군기반	IUCAS 수열기반
암호화속도	48	0.34	15.47	0.1
복호화속도	30	0.8	12.01	3.76

[표5]의 결과만 보면 각셀의 값이 연산당 처리속도를 의미하므로 그 값이 가장 작은 NTRU의 성능이 다른 암호 시스템보다 월등하게 좋은 것을 알 수 있다. 실제로 NTRU Cryptosystems, Inc는 RFID와 같은 비접촉식 카드를 위한 알고리즘을 구현하였고 8비트, 16비트, 32비트, 프로세서용 소프트웨어와 스마트카드용 하드웨어를 갖춘 패키지(GenuID)를 제공하고 있다.

[표6] 8비트 프로세서에서 예상성능

(block/sec)	RSA	ECC	NTRU	Pairing	Braid	LUC
암호화	1.9	0.7	33.82	0.02	0.1	1.62
복호화	0.16	1.07	16.17	0.04	0.13	0.1

겹선형쌍 암호시스템은 소형장비에 적용하기엔 무리가 따를 것으로 보이고 각 암호 시스템의 장단점을 잘 파악하여 실제 시스템에 적용하는 것이 중요하다.

이와 같이 현재의 PDA정도의 장치와 유비쿼터스 노드 등에서 쓰이는 5MHz의 peanut프로세서의 성능 차이를 감안한다면 RSA를 적용하는 경우 현재 수준에 비해 40~50배 정도의 경량화가 요구되며 가장 효율성이 좋은 NTRU의 경우도 현재 수준에 비해 2배 정도의 경량화는 되어야 할 것으로 보이고 메모리 관점에서도 최소 3배 이상은 경량화 되어야 실제로 사용이 가능할 것으로 보인다.

4. 결론

최근에 정수론을 기반으로 한 알고리즘 외에 다양한 기반 이론으로 암호화학적 시도가 이루어지고 있다. 그러나 현재의 유비쿼터스 환경에 적용할 만한 좋은 암호시스템은 무엇이냐의 질문에 정확한 답이 될만한 것은 아직 존재하지 않는다. 따라서 본 논문은 현재 존재하는 암호 시스템의 효율성에 대해 객관적으로 비교해보고 작은 장비에서 가상의 효율성을 예측해보았다. 그리고 앞으로 현재의 암호 시스템이 얼마나 더 경량화 되어야 실생활에 응용 가능할지 연구해보았다. RSA나 ECC등과 같이 그간 연구되어온 시스템의 경우 그 효율성 증진에 있어 많은 발전을 기대하기 어려울 수 있는 반면 비교적 최근에 연구되기 시작한 땋임군 등과 같은 새로운 기반 논리의 경우, 보다 효율적 시스템을 구성할 수 있을 것이다. 특히 NTRU의 증명 가능한 안정성 등이 보장될 수 있다면 그 효율성 등을 감안할 때 매우 경량화에 적합한 암호 시스템으로 활용가능하리라 예측된다. 즉 키생성의 효율성과 작은 크기의 키로 보통 수준의 안전도를 유지해야하며 연산 과정이 효율적이어서 연산에 요구되는 메모리나 전력이 적어야하며 암호화 복호화 속도가 빠르면 가장 이상적인 초경량 키가 될 것이다

5. 참고문헌

[1] 센서노드 http://www.cs.berkeley.edu/~pal/pubs/tinyos-nsdi04

[2] UCLA Smart Kindergarten.http://nesl.ee.ucla.edu/projects/ smartkg/

[3] MIT Oxygen project. http://www.media.mit.edu/

[4] RFID,http://reasecurity.com/

[5] M.Bellare, P.Rogaway, "Optimal Asysmetric Encryption -How to Encrypte with RSA", Eurocrypt 94 Proceedings, Lecture Notes in Computer Science Vol.950, A.De Santis ed., Springer-Verlag,(1994).

[7] Certin Kaya Koc,"RSA Hardware Implementation", 1995.

[8] S.E.Eldridge C.D.Walter.HardwareImplementation of Montgomery's Modular Multiplication Algorithm. IEEE Trancations on Computers, June 1993

[9] E.Ozturk, B.Sunar,and E.Sava,"Low Power Elliptic Curve Cryptography Using Scaled Modular Arithmetic,"Proceedings of Cryptographic Hardware and Embedded Systems-CHES 2004:6th International Workshop Cambridge, MA, USA, Springer-Verlag Heidelberg, August, 2004