서울대학교	보 도 자 료			
	배 포 일	2014. 11. 10.	매 수	6
연구처 연구지원과	담당과장	이 선 희	배포부서	기획처 홍보팀
	자료문의	서울대학교 수리과학부 천정희 교수(jhcheon@snu.ac.kr 880-1443) 명지대학교 수학과 서재홍 교수 (jaehongseo@mju.ac.kr 031-330-6157)		

사물인터넷에 활용가능한 고속 공개키 암호 개발
- RSA보다 수백배 빠른 복호화 가능 -

논문명: A New Additive Homomorphic Encryption based on the co-ACD Problem

□ 연구진 :

서울대학교 수리과학부 천정희 교수
싱가폴 난양공대 수학과 이형태 박사
명지대학교 수학과 서재홍 교수

□ 내용 및 의의 :

대형 인터넷 기업 및 은행의 사용자 정보 유출, 해킹에 의한 유명인의 클라우드 및 소셜 네트워크 서비스에 저장되어 사생활 정보 유출 등에 관한 사건들을 통해 인터넷 환경에서의 개인정보보호 침해 대응에 대한 요구가 높아지고 있다.

특히, 스마트기기를 비롯한 다양한 소형전자기기의 활용이 높아짐에 따라 **사물인터넷에서의 개인정보보호는 ICT분야에서 중요한 현안들 중의 하나이다.** 이론적으로는 개인정보 데이터의 암호화가 중요한 대안이 될 수 있지만, 암호화 및 복호화에 필요한 계산량이 커서 실제 사용되기에는 문제가 있었다.

본 연구팀은 사물인터넷에서 활용이 가능한 고속 공개키 암호를 개발에 성공하였다. 이번 결과는 현재 가장 널리 활용되고 있는 RSA 암호 시스템과 유사한 암호화 속도를 갖는 반면 복호화 과정은 수백배 빠른 성능을 기록하며, 사물인터넷 환경에서 활용이 되는 작은 전자기기들에 활용이 될 수 있을 것으로 기대된다. 또한, 기존의 RSA, 타원곡선암호가 양자컴퓨터에 의해 다항식시간에 해독되는 알고리즘이 있는 반면, **새로운 공개키암호가 기반하는 격자문제는 양자컴퓨터에 강한 것**으로 여겨지고 있다.

개발한 암호 시스템은 암호문 간의 덧셈을 지원하는 덧셈 동형 암호의 성질을 지니는데, 이는 데이터베이스, 클라우드 서비스 등 암호화된 상태로 개인정보 활용을 필요로 하는 서비스에 다양하게 활용될 수 있을 것으로 기대된다.

이번 연구 결과는 정보보호분야 세계 최고 학회인 ACMCCS (ACM Conference on Computer and Communications Security) 2014 에 채택되어, 11월 초 미국 애리조나에서 발표될 예정이다. http://www.sigsac.org/ccs/CCS2014

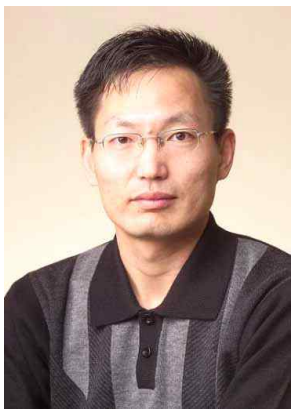
□ 연구진 소개

서울대학교 수리과학부 천정희(45) 교수 (email: jhcheon@snu.ac.kr)
싱가폴 난양공대 수학과 이형태(32) 박사 (email: hyungtaelee@ntu.edu.sg)
명지대학교 수학과 서재홍(33) 교수 (email: jaehongseo@mju.ac.kr)

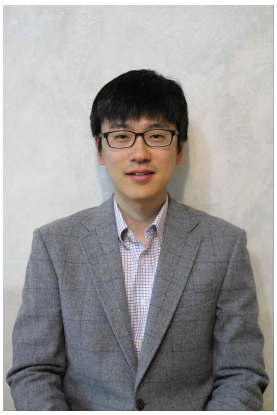
□ 연구비 지원 프로그램

미래창조과학부(산업융합원천기술개발사업)

□ 관련사진(연구책임자 및 연구관련 사진)


천정희 교수 (서울대)


이형태 박사 (난양공대)


서재홍 교수 (명지대)

관련 자료

사물인터넷에 활용가능한 고속 공개키 암호 개발

2014. 11. 10.

서 울 대 학 교

Title: 사물인터넷에 활용가능한 고속 공개키 암호 개발

1.연구배경및현황

인터넷의 보급은 트위터, 카카오톡 등과 같은 SNS 서비스 등을 통한 급속한 정보의 전달이 가능하게 하였으며, amazon, 애플스토어 등의 인터넷 쇼핑몰을 통해 거리의 제약에 구애 받지 않고 공급자와 구매자를 손쉽게 연결해주는 것이 가능하게 하는 등 현대인의 문화생활의 편의성을 크게 향상시켰다. 하지만, 서비스 공급자가 확보한 사용자의 개인정보, 휴대용 전자 단말기나 클라우드 서버에 저장한 사생활 정보가 해킹 등의 악의적인 공격을 통해 외부에 유출된 일련의 사례들을 통해 부주의한 인터넷의 활용이 심각한 개인정보보호의 침해를 야기할 수 있다는 사실은 이미 널리 알려진 사실이다. 최근에는 이러한 인터넷 환경에서의 개인정보보호 달성을 위한 대안으로서 데이터의 암호화 기술 및 암호화된 데이터의 효과적인 조작기술의 중요성이 커지고 있다.

사물인터넷이란 전자기기와 전자기기를 연결하는 네트워크로 스마트폰, 스마트워치, 구글 글래스 등으로 대표되는 스마트 기기 및 센서, 드론, CCTV 등 다양한 전자기기들이 연결된 인터넷을 의미한다. 스마트 기기 등을 통해 개인의 신상, 위치, 대화내용 등의 정보가 공개 네트워크인 인터넷을 통해 빈번하게 전달이 되는 상황에서 이를 보호하기 위한 데이터의 암호화는 필수이다. 하지만, 사물인터넷의 특성상 활용이 되는 전자기기들은 기존의 사람들 간의 인터넷에 주로 활용이 되던 PC보다 제한된 성능 (제한된 배터리 및 메모리)을 가지는 경우가 일반적이기 때문에 기존의 인터넷 환경에서 사용이 되어온 암호화 방식을 그대로 적용하기에는 무리가 있다. 이러한 현실적인 요구에 따라 AES로 대표되는 기존의 비밀키 암호를 대체하기 위한 여러 가지 경량 비밀키 암호가 제안된 바 있다.

비밀키 암호화 방식과 달리, 키 교환 및 인증 등에서 널리 활용이 되고 있는 공개키 암호화 방식의 경우 아직까지 1970년대에 발표된 첫 번째 공개키 암호인 RSA 암호가 공인인증서, Open SSL 등 현재 인터넷 환경에서 가장 보편적으로 사용이 되고 있다. RSA 암호는 수학계에서 오랜 기간 동안 난제로 여겨져 온 큰 수의 소인수분해 문제에 안전성을 기반하여 강력한 안전성을 제공함에도 불구하고 서버나 PC 이 외의 작은 전자기기에서 활용하기에 상대적으로 효율성이 나쁘다는 단점이 있다. 그 동안 RSA를 대체할 다양한 시도들이 있었으며 그 중에서 대표적인 것이 타원곡선 암호이다. 타원곡선 암호는 RSA 암호와 비교할 때 메모리 측면에서 향상을 이루어 무선 인터넷 환경에 적합하지만, 암호화 및 복호화 시에 요구되는 계산량이 많아 전력소모가 크기 때문에 사물인터넷에서 요구하는 수준의 경량화/고속화를 달성하기에는 무리가 있다.

2.연구내용및결과

기존의 RSA암호와 타원곡선 암호의 암호화 및 복호화 연산은 지수승 연산을 필요로 한다. 지수승 연산은 기본적으로 덧셈, 뺄셈, 곱셈, 나눗셈 등의 기본적인 사칙연산에 비해 비용이 훨씬 비싼 연산으로 암호 알고리즘의 고속화에 가장 큰 걸림돌이다.

본 연구진는 기존 암호 알고리즘들이 활용하고 있는 정수나 타원곡선 대신 격자구조를 활용하여 공개키 암호 설계를 시도하였다. 사실, 이전에도 격자기반 암호는 존재하였으나 주로 양자컴퓨터를 이용한 공격에 안전한 암호 설계 및 암호화된 데이터의 조작이 가능한 완비동형암호 설계 등에 활용이 되었다. 본 연구진은 기존에 활용이 되어온 격자구조를 변형하여 새로운 형태의 격자구조 (co-ACD)에 기반한 고속 공개키 암호 알고리즘을 개발하였다. 개발된 공개키 암호의 가장 큰 특징은 RSA 암호 등의 단점으로 지적이 되었던 지수승 연산이 없이 사칙연산 등의 간단한 연산만으로 암호화 및 복호화를 수행한다는 것이다. 이를 통하여, 알고리즘들의 고속화에 성공하였으며, 특히 동일한 안전성을 가지는 RSA 암호 시스템에 비해 복호화 속도가 수백배 빠르다. 80비트 안전성을 갖는 파라미터 하에서 1.3 GHz PC에서 측정한 본 연구진이 개발한 암호 시스템의 성능을 다음과 같다.

알고리즘	시간	클락수
키생성	32.44 ms	42170 kilocycle
암호화	0.621 ms	140 kilocycle
복호화	2.37 μs	3 kilocycle

표 개발한 알고리즘의 성능 (80비트 안전성)

아울러, 본 연구진이 개발한 암호 시스템은 암호화된 상태로 평문의 덧셈 연산을 지원하는 덧셈 동형 성질을 갖는다. 이는 헬스케어, SNS 등 개인정보를 활용하는 서비스에서 암호화된 상태로 데이터 처리를 가능하게 해준다. 이번 결과는 기존의 덧셈 동형 암호들과 비교하여 복호화 속도가 1000배 이상 빨라지는 등 효율성이 월등히 향상되었기 때문에, 이를 필요로 하는 다양한 서비스에서 유용하게 활용될 수 있을 것으로 기대한다.

	암호화	복호화
RSA[1)]	140	2680
본 연구 결과	780	3

표 RSA 암호 시스템과 본 연구진의 결과의 연산 속도 비교 (80비트 안전성)

(단위:kilocycle/operation[2)])

1) http://cryptopp.com/benchmarks.html 자료 참조

3.연구성과및향후계획

이번 연구 결과는 11월 초 미국 애리조나에서 개최될 예정인 정보보호 분야 세계 최고 학회, “ACM Conference on Computer and Communications Security 2014” (ACM CCS 2014, http://www.sigsac.org/ccs/CCS2014/)에서 발표될 예정이다. (Microsoft Academics 기준. 보안분야 최고학회)

논문명: A New Additive Homomorphic Encryption based on the co-ACD Problem

본 연구진은 후속 연구로 현재 개발된 고속 공개키 암호의 효율성을 더욱 향상시켜 사물인터넷 보안에 활용할 수 있도록 노력하는 한편, 암호화된 데이터들 간의 덧셈과 곱셈을 모두 지원하는 경량 동형 암호의 개발에 매진할 계획이다.

자연과학대학장 ㊞

수리과학부장 ㊞

추천교수 (강명주) ㊞

추천교수 (이기암) ㊞

2) cycle/operation: 1회 연산 수행에 필요한 cpu 클락 사이클