2020 vol.6

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

KISA REPORT

CONTENTS

주제 제안 및 정기 메일 신청 | kisareport@kisa.or.kr

인터넷 정보보호 관련 이슈, 현안 등 궁금한 내용을 보내주시면 선별 후 보고서 주제로 선정됩니다.

또한, KISA Report 온라인 서비스 제공을 원하실 경우 신청해주시면 매월 받아보실 수 있습니다.

차세대 암호기술 '양자내성암호'와 '동형암호'

김도원 (dowonkim@kisa.or.kr)

한국인터넷진흥원 선임연구원

1. 개요

암호기술은 수학적인 원리에 안전성을 기반하며, 보안에 있어 중요한 정보를 직접적으로 보호하는 원천 기술이다. 지금의 IT환경에서는 AES나 RSA 같은 현대 암호들로 충분히 필요한 기능들이 제공되고 있지만, 4차 산업혁명 시대를 맞이하면서 사회적으로 문제가 될 수 있는 새로운 보안 이슈들이 발생하고 있다.

양자컴퓨터가 개발된다면 양자 기반 알고리즘인 Shor 알고리즘에 의해 기존의 공개키 암호알고리즘을 더 이상 사용할 수 없게 된다. 또한, Grover알고리즘으로 인해 대칭키 암호의 키 사이즈를 2배, 해시 함수의 출력 길이를 3배 증가시켜야 기존의 안전성을 가질 수 있다. 이러한 양자컴퓨팅 환경이 다가옴에 따라 '양자내성암호'가 주목을 받고 있다.

또한, 올해 초 데이터 3법이 개정되면서 개인정보 활용과 관련된 데이터 산업이 주목받고 있다. 데이터를 활용하는 과정에서 개인의 프라이버시는 보호되어야 하며, 이러한 프라이버시 보호기술로는 동형암호, 차분 프라이버시, 다자간계산 등이 있다. 동형암호는 데이터를 복호화 없이 연산할 수 있는 기술로, 데이터 처리 속도가 느리지만 다른 제약 없이 모든 분야에 활용할 수 있는 암호기술이다.

본고에서는 양자컴퓨팅 환경에서 활용될 수 있는 '양자내성암호'와 프라이버시 보호 기술인 '동형암호'에 대하여 소개하고자 한다.

2. 양자내성암호(Post-Quantum Cryptography, PQC)

2-1. 양자내성암호 소개

암호 원천기술 중 하나인 공개키암호는 인터넷 뱅킹, 전자 주식 거래, 인터넷 쇼핑 등 전자 거래 보안의 핵심이 되는 기술이다. 전 세계적으로 사용되고 있는 공개키암호로는 RSA, Diffie-Hellman 키교환, 타원

곡선 암호 등이 있으며, 이들은 인수분해나 이산대수 문제와 같은 수학적인 원리를 이용하여 설계되었다. 1994년 Shor는 양자 알고리즘을 이용하여 인수분해나 이산대수 문제를 모두 짧은 시간 내에 풀 수 있는 것을 증명하여 대부분의 공개키 암호들이 해독될 수 있다는 것이 밝혀졌으나, 이전까지는 양자 컴퓨터가 실용화되기에는 기술적인 어려움이 있어 큰 문제로 인식되지는 않았다.

하지만, 최근 양자 컴퓨팅 기술이 발달하여 양자 컴퓨터의 실현 가능성이 높아지면서, 이러한 문제를 해결할 수 있는 양자내성암호에 대한 연구가 활발히 진행되고 있다. 양자내성암호는 기존 공개키암호를 대체할 수 있는 기술로 인수분해나 이산대수 문제가 아닌 새로운 문제에 안전성을 기반하고 있으며, 기반을 두는 문제에 따라 격자 기반, 코드 기반, 다변수 기반, 해시 기반, 아이소제니 기반으로 구분할 수 있다. 또한, 알고리즘 기능에 따라 암호화/키교환 알고리즘과 전자서명 알고리즘으로도 구분할 수 있다.

[표 1] 기반 문제에 따른 양자내성암호 유형

종류	내용
격자 기반 (Lattice-based)	격자(Lattice) 위에서 계산하는 문제의 어려움에 기반하는 암호 시스템
코드 기반 (Code-based)	일반적인 선형 코드(Linear Code)를 디코딩 하는 어려움에 기반하는 암호 시스템
다변수 기반 (Multi-variate)	유한체(Finite Field) 위에서 계산하는 다변수함수 문제의 어려움에 기반하는 암호 시스템
해시 기반 (Hash-based)	해시 함수의 안전성을 기반으로 한 전자 서명 시스템
아이소제니 기반 (Isogeny-based)	순서(Order)가 같은 두 타원곡선 사이에 존재하는 아이소제니(Isogeny)를 구하는 문제의 어려움에 기반을 두는 암호 시스템

2-2. 양자내성암호 동향

양자내성암호는 2006년 PQCrypto 학회 때부터 본격적인 논의가 시작되었고, 2016년 NIST에서 Post-Quantum Cryptography Standardization(PQC 표준) 공모를 시작하면서 전 세계적으로 양자내성암호에 대한 연구/개발이 진행되고 있다.

NIST PQC 표준 공모는 양자내성암호 표준 알고리즘을 선정하기 위해 시작되었다. 2017년도 12월, 1라운드에 제출된 총 69개의 알고리즘이 공개되었으며, 국내에서 제안한 알고리즘은 5개가 포함되었다. 1라운드에서는 알고리즘의 안전성을 위주로 평가되었고, 2019년 1월에 2라운드에 제출된 26개의 알고리즘이 공개되었다. 대부분의 알고리즘은 미국이나 유럽에서 제안한 알고리즘이며, 아시아에서는 중국에서 제안한 1개의 알고리즘만이 2라운드에 포함되었다. 2라운드에서는 안전성과 함께 성능도 본격적으로 평가되며, 2024년 이전까지 드래프트 표준이 완료될 예정이다.

[표 2] NIST PQC 표준 공모 - 2라운드 선정 알고리즘

대표 국가	기능	알고리즘
미국(8)	암호화/키교환(6)	BIKE, Classic McEliece, FrodoKEM, NTRU, NTRU Prime, Three Bears
	전자서명(2)	Picnic, Ranbow
프랑스(5)	암호화/키교환(3)	HQC, ROLLO, RQC
	전자서명(2)	FALCON, GeMSS
네덜란드(4)	암호화/키교환(2)	CRYSTALS-KYBER, Round5
	전자서명(2)	MQDSS, SPHINCS+
벨기에(2)	암호화/키교환(1)	SABER
	전자서명(1)	LUOV
독일(2)	암호화/키교환(1)	NewHope
	전자서명(1)	qTESLA
영국(1)	암호화/키교환(1)	NTS-KEM
이탈리아(1)	암호화/키교환(1)	LEDAcrypt
스위스(1)	전자서명(1)	CRYSTALS-DILITHIUM
캐나다(1)	암호화/키교환(1)	SIKE
중국(1)	암호화/키교환(1)	LAC

국제표준화기구 ISO/IEC에서도 양자내성암호 표준화가 진행 중에 있다. JTC 1/SC 27/WG 2에서 진행 중이며, 격자 기반, 코드 기반 등 기반을 두는 문제에 따라 표준 파트가 구분되고 많은 검증이 이루어진 해시 기반 전자서명이 우선적으로 표준화될 예정이다.

비록 NIST PQC 표준 공모에서 2라운드에 진출하지는 못했지만, 국내에서는 NIMS에서 개발한 HIMQ와 서울대에서 개발한 격자 기반 양자내성 암호 링-리자드(Ring-Lizard)가 TTA표준 TTAK.KO-12.0348, TTAK.KO-12.0349으로 등록되어 있다.

3. 동형암호(Homomorphic Encryption, HE)

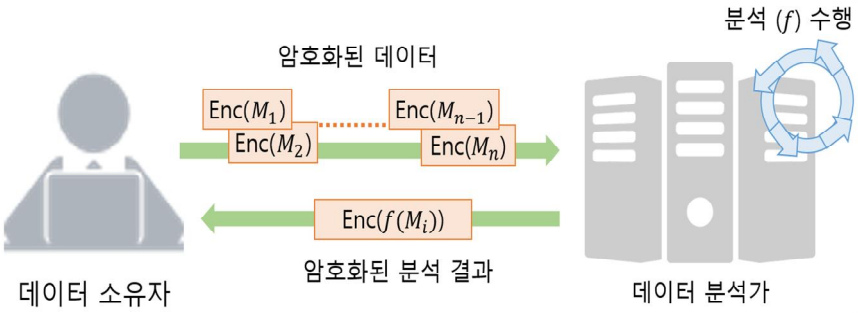
3-1. 동형암호 소개

2020년 초, 개인정보 보호법, 신용정보의 이용 및 보호에 관한 법률, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 소위 말하는 '데이터 3법'이 개정되면서, 국내 데이터 산업이 발전하기 위한 법적 기반이 마련되었다. 이에 따라 개인정보를 통한 가치 창출이 방대해지겠지만, 그만큼 개인정보보호의 중요성이 강화되고 있다.

개인 프라이버시 침해를 방지하기 위해 개인정보 보호를 강화할 수 있지만, 데이터 종류를 강력히 제한하여 데이터의 활용도가 현저히 떨어지게 된다. 해결책으로 차분 프라이버시(Differential Privacy) 등

데이터 비식별화 기술이 제시되고 있지만, 비식별화 과정에서 손실이 발생할 수 있고 다른 정보와 결합 시 재식별의 위험성도 존재한다. 이와 같은 데이터 활용과 개인정보 유출의 딜레마를 해결할 수 있는 것이 바로 동형암호이다.

동형암호는 암호화된 데이터를 복호화하지 않더라도 평문처럼 데이터 처리가 가능한 암호기술이다. 데이터의 소유자는 동형암호로 암호화한 데이터를 분석자에게 전달하면, 분석자는 암호화된 상태로 데이터를 분석하고 분석된 결과를 다시 소유자에게 전달한다. 즉, 암호화된 데이터가 복호화 되지 않은 상태에서 모든 처리가 이루어져, 데이터의 소유자와 분석자가 다르더라도 데이터의 원본이 노출되지 않는다.



동형암호 사용 예시

동형암호는 데이터 유출을 원천적으로 차단할 수 있지만, 속도가 느리고 암호문이 10배에서 100배 정도 커지는 단점이 있다. 동형암호는 2009년 IBM에서 '완전동형암호'를 제안하면서 주목받기 시작하였고, 당시 동형암호는 1bit를 처리하는 데에 수십 분이 걸렸다. 하지만, 매년 평균적으로 약 8배의 속도 발전이 있어 현재는 평문 처리속도에 비해 약 1,000배정도로 볼 수 있으며, 미 국방부 DARPA 과제에서는 하드웨어 가속화를 통해 2024년까지 평문 처리속도의 약 10배 이내의 수준으로 줄이는 것을 목표로 하고 있다.

3-2. 동형암호 동향

동형암호 국제표준은 2019년에 ISO/IEC 18033-6이 제정되었다. 해당 표준에는 ElGamal 암호화를 토대로 한 동형암호 표준이며, 덧셈 동형연산만 지원한다. 국내 표준으로는 서울대에서 개발한 근사연산 동형암호 알고리즘이 TTA표준(TTAK.KO-12.0347)으로 등록되어 있다.

2017년 7월에 MS 주관으로 시작된 Homomorphic Encryption Standardization(HES)에서는, 널리 사용되고 있는 격자 기반 동형암호 스킴과 라이브러리들의 표준화를 목표로 하고 있다. 대학(서울대, MIT 등)과 정부기관(NIH, NIST 등), 그리고 기업(Intel, MS, IBM, Google 등) 등 다양한 기관에서 참여하고 있으며, 현재까지 총 4번의 회의가 열렸다.

4. 맺음말

올해 6월에는 코리아크레딧뷰로(KCB)에서 세미나를 통해 국내에서 개발한 동형암호 혜안(HEaaN)을 활용하여 국민연금공단 데이터와 KCB 신용데이터를 결합·분석하는데 성공하였고, 세계 최초로 상용화하였다고 밝혔다. 양자내성암호의 경우에도, 다가오고 있는 양자컴퓨팅 시대를 대비하여 공인인증서 등 기존 공개키암호로 구성되어 있는 기반들을 빠른 시일 내로 양자내성암호로 대체할 방안을 마련해야 한다.

차세대 암호기술로 간주되던 암호기술들은 더 이상 차세대가 아닌 현재에 적용되고 있다. 새로운 암호기술들이 국내 암호산업에 안전하게 활용될 수 있도록, 우리나라도 국제적인 이슈에 지속적으로 대응하면서 그에 맞는 연구개발 및 안전성 검증 기준 마련이 필요하다.

〈 KISA 주요 활동 안내 〉

사이버 위협 동향보고서 발간 (분기별)

□ 개요

o KISA는 분기별 발생했던 사이버 위협(취약점, 주요 공격사례) 정보제공과 국내 전문가 기고문을 읽기 쉬운 보고서로 제작하여 공개 중(16년~)

- 주요 독자층을 대상으로 수록 내용을 내실화하여 금년도 변화 도모

※ (기존) 다양한 독자층을 고려하여 일반인편-전문가편의 내용을 분리했으나 내용의 통일성이 없는 의견에 따라 (개선) 보안 전문가층을 대상으로 심도 깊은 정보 제공

o "사이버위협 동향 보고서"는 매년 분기 말 제작되어 KISA 보호나라와 KISA SNS를 통해 공개

- 별도 책자를 만들어 이를 기관·기업에서 신청 시 최대 3부까지 제공(무료)

□ 주요내용

o 사이버 공격 예방 및 피해 최소화, 민간 기업의 보안수준 강화 및 임직원 보안 인식 제고를 위한 다양한 위협정보 수록

① 사이버 위협 트렌드(언론동향, 취약점 및 해외 사이버 위협 동향)

② 보안지식 및 사이버 위협 통계

③ 전문가 칼럼 ▸ 해당 부분은 별도로 발췌하여 영문화 및 해외CERT 공유

④ 최근 이슈 분석 수록

o 또한, KISA 내 주요 행사, 사업의 이슈를 수록하여 독자로 하여금 예정된 KISA의 주요사안 확인 및 필요 시 연락할 수 있는 채널로 활용

- 보고서를 읽는 독자 중 스스로 분석한 내용 또는 하고 있는 보안관련 업무를 알리기 위해 전문가 컬럼 등을 통해 외부로 확산 가능

□ 향후계획

o 매년 정기적으로 제작되며 분기별 마지막 달 3번째 금요일 게시

□ 보고서 문의

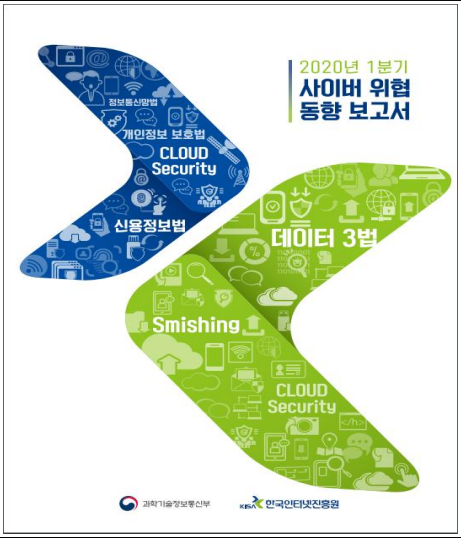
o 한국인터넷진흥원 침해사고분석단 종합분석팀 배한철 책임 연구원 (☏ 02-405-4795)

[붙임] 사이버위협 동향 보고서 소개

1분기 위협동향 보고서 주요 내용 예시

구 분 (타겟)	주 제	내 용
Trend (CISO)	국내 사이버 위협 동향	· 국내 주요 사이버 위협동향 조사, 분석 및 설명 - 데이터3법, 클라우드 보안, 코로나19 스미싱/악성코드 관련 언론보도
	취약점 동향	· 고위험 취약점 정보 요약 및 소개 - NVD* 발표 취약점 중 CVSS 7점 이상 취약점의 정보 소개 * NVD(National Vulnerability Database): 美국립표준기술연구소, NIST에서 공유하는 소프트웨어 취약점 데이터베이스
	해외 사이버 위협 동향	· 해외 주요 정보보호 기업 발표 보고서(3건) 소개 ※ 소개 대상: M-Trends 2020(FireEye), Mobile malware evolution 2019(Kaspersky), Ransomware against the Machine(FireEye)
Guide (국민·기업)	이슈 Q&A	· 신규 보안이슈를 Q&A 형태로 설명 - 데이터 3법 주요 내용 및 관련 보안 이슈
	설문조사	· 사이버위협 이슈 키워드에 대한 대국민 인식도 조사 - 스마트폰 보안 인식도 설문조사 결과
	KISA 사용설명서	· KISA에서 제공하는 대국민 서비스 소개 및 사용 안내 - 중소기업 정보보안 지원 서비스
How To (실무자)	Case Study	· 기업의 주요 정보보호 이슈 해결사례 소개 - 엔씨소프트, 보안관리자의 크리덴셜 스터핑 공격 대응 방안 - 안랩, 코로나19 확산 상황을 악용한 사이버 보안 위협들
	Spotlight	· 신규 보안기술에 대한 소개 - 카카오, 데이터 3법의 보안 활용 방안
Special Issue (CISO)	특별호	· 언택트(untact: 비대면) 업무환경에서의 보안 대응방안 - SKT, 넥슨, 티몬 등 3개 기업의 재택근무 환경, 보안대응 소개 - 코로나19 안심정보 및 코로나19 정보보호 6대 실천 수칙 소개

사이버위협 동향보고서 표지 (국문 · 영문)



제1회 2020 AI보안 기술개발 교육 안내

AI(인공지능)와 보안기술이 융합된, 지능화된 보안기술 개발 역량을 갖춘 전문인력 양성 프로그램 운영 (www.kisaaisec.or.kr)

□ 교육 개요

o **(목적)** 사이버 보안분야 인공지능(AI), 빅데이터 분석 등을 활용하여 지능형 사이버 위협에 대응하기 위한 최정예 AI보안 기술개발 인력 양성

o **(교육 대상)** 대학(원)생 및 재직자 등 누구나 신청 가능
※ 선발평가를 통해 AI와 정보보호에 관심이 있고 기초 지식을 갖춘 교육 대상자 50명 선발

o **(교육 기간)** 공통/전문 교육 120시간 포함 총 5개월 교육(6~10월)

o **(수료 혜택)** 교육생 전원 수료증 발급, 우수 교육생 5명 대상 인증서* 수여
* KISA 원장 명의의 'K-Shield AI Security' 인증서 발급

□ 교육 일정 및 내용

교육생 모집	교육생 선발평가	공통/전문 교육	부트캠프	팀프로젝트	챌린지 참가
· '20.5.11~ 6.4	· 필기평가: '20.6.9 · 실기평가 '20.6.12	· 평일반: '20.7.20~9.2 · 주말반: '20.6.20~8.29	· '20.9.11~ 9.13 (2박3일 예정)	· 9월~10월 (4주)	· 11월

o **(선발평가)** 1차 필기(정보보안 + AI기본), 2차 심층면접을 통해 50명 선발

o **(공통/전문 교육)** 이론중심의 공통 교육(48h)과 실습중심의 전문 교육(72h) 운영
※ 공통/전문 교육기간 내에 AI 기술개발에 필요한 수리·통계·데이터 과학 특강 4회 운영

①공통 교육과정	②전문 교육과정	③특강
정보보호	악성코드 자동분류	수리
데이터	취약점 자동탐지	통계
인공지능	빅데이터 분석	데이터 과학

o **(부트캠프)** 산업계 멘토와 함께하는 AI 알고리즘 활용 실습 집중 교육 워크숍

o **(팀프로젝트)** 실제 기업의 침해사고 사례 및 정보보호 이슈와 연계한 멘토링 형태의 AI보안 기술개발 프로젝트 수행

□ 관련 문의

o 정보보호R&D기술공유센터 보안기술확산팀 손경아 주임연구원(☎1256)

2020 Vol.1

이슈&트렌드

CES 2020 - 인공지능과 로봇의 만남: 더 많은 시간이 필요
CES 2020 행사에서 가장 핫(hot)했던 제품
CES 2020 서비스화 되는 모빌리티
CES 2020 뷰티테크(Beauty Tech) 화두는 인공지능과 개인화
CES 2020에서 PC의 변화
CES 2020에서 살펴보는 슬립테크 동향
온라인 데이터에서 나타난 “CES 2020” 관심도와 그 내용들
CES 2020 스케치: 모든 것에 테크를 붙인 CES의 뒷담화
미국의 의료분야 데이터사이언스 및 인공지능 정책 동향
개인정보 유출 통지·신고 제도의 개선 검토

2020 Vol.2

이슈&트렌드

인공지능과 데이터 분석으로 질병 확산을 예측할 수 있는가?
코로나 바이러스와 개인정보 활용에 대한 소고
데이터와 헬스케어의 진화
EU의 5G 네트워크의 위험 완화를 위한 조치 방안
데이터 3법 개정의 주요 내용과 전망
국내외 중소기업 정보보호 지원 정책 분석 및 개선 검토
일본 IoT 보안정책 동향 분석 및 시사점

2020 Vol.3

이슈&트렌드

사회적/물리적 거리두기가 IT산업과 사회에 미치는 영향과 주요 이슈
감염병예방법의 정보공개 규정 살펴보기 - 공공의 건강 및 안전, 그리고 프라이버시의 균형
원격근무, 회사를 떠나 일한다는 것
코로나19 확산에 따른 비대면 원격수업에 대한 단상
비대면 협업툴의 미디어적 필수 요건에 대하여
코로나19가 앞당긴 원격 사회 이후 사이버 대피 공간을 위한 가상현실의 역할
RSAC 2020 - 보안 트렌드 살펴보기
연합학습으로 AI 빅브라더 문제 해소
미국과 영국의 드론 대응(Ant-drone) 정책 및 전략 추진동향
중국“네트워크 안전등급 보호 제도” 개요 및 관련 국가표준 제정 동향
광주의 미래 - 인공지능 기반 산업융합 집적단지 조성사업
미래인터넷 기술 성공의 핵심 포인트, 보안

2020 Vol.4

이슈&트렌드

코로나19 팬데믹 시대에 새롭게 주목받는 스타트업
텔레컨퍼런스 도구로 인한 프라이버시 침해 가능성
초·중·고 원격개학, 혼란과 기회 사이
코로나19 사태로 살펴보는 5G 서비스 전망
오프라인 못지않은 온라인 컨퍼런스, GTC 디지털을 가다
초연결로 취약해진 OT보안, 가시성으로 강화
미국 정부의 양자정보통신 및 보안 정책 추진동향
민간 웹사이트 플러그인 개선 실적 및 정책 방향
N번방이 남긴 숙제와 문제, 그리고 개인정보보호

2020 Vol.5

이슈&트렌드

코로나19 이후 구글 빅브러더 등장
코로나19 접촉자 추적 기술의 방향은 공동체의 참여를 끌어내는 것
빅 테크 기업의 1/4분기 실적이 주는 의미
코로나19를 이용한 사이버공격 및 대응 동향
개인정보처리 권한을 남용한 개인정보 무단 조회 및 유출에 대한 조치의 검토
데이터경제 시대의 개인정보 자기결정권 강화 방안
가명정보에 있어서 ‘다른 정보’와 ‘추가 정보’의 차이 및 가명처리의 대상과 범위
팬데믹 시대의 개인정보보호
마이크로소프트 개발자 컨퍼런스 ‘빌드2020’, 비대면 시대 개발을 담다
대구 전략산업 육성은 스마트공장 구축으로

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

발 행 일	2020년 6월
발 행 처	한국인터넷진흥원 (전라남도 나주시 진흥길 9)
기 획	한국인터넷진흥원 ICT미래연구소
편 집	㈜ 해리