정 보 보 호 학 회 지
제 31 권 제4호, 2021. 8

동형(Homomorphic)암호 표준동향

나 재 훈*

요 약

암호학을 세대로 구분하면 단순 패스워드 인증을 1 세대, 송수신 및 데이터 저장 암호를 2 세대, 서명 및 키 공유에 활용하는 암호를 3세대, 키를 사용하지 않는 암호를 4 세대라고 분류 할 수 있다. 현재 암호는 3 세대에 있으며, 암호키를 많이 사용함으로 인하여, 키의 노출로 인한 안전성의 문제를 해결하고자 연구가 있었으며, 4세대 암호로 동형암호가 제시되고 있다. 동형암호는 종대종(End-to-End) 암호의 신뢰성을 보장하며, 중간 과정에서 데이터 처리를 위하여 복호하지 않고서도 가공이 가능하도록 가단성(Malleability)을 제공한다. 이러한 속성을 기반으로 비식별화 처리하지 않고서 원데이터를 처리할 수 있어서, 데이터의 가치가 보존되고, 신뢰성 있는 데이터를 체득할 수 있다. 더욱이 중간단계에서 복호하지 않고서 데이터를 처리는 개인정보보호를 원천적으로 제공할 수 있는 메커니즘으로 파악된다. 본 고에서 동형암호 관련 산업동향 및 국제표준화 동향을 살펴본다.

Ⅰ. 서 론

ICT(Information and Communication Technology) 기술의 발전은 인간의 문화에 많은 영향을 미치고 있다. 그 기술의 발전 속도는 매우 빨라서 이론에서 기술로 기술이 산업 응용의 전환 단계가 융합되어 이론이 구상되는 시점에서 응용을 고려하는 개발과정이 발생하고 있다.

이러한 변화는 디지털의 전환(Digital Transfomration)의 한 면이라고 생각이 된다. ICT 기술의 발전으로 실생활의 편리성을 추구하다 보니 데이터가 사이버 공간(Cyber Space)에 집중되고, 그 양이 방대하게 되면서, 단순 통계적 처리만 하여도 가치 있는 정보를 획득하기에 이르렀다. 그러나 이러한 처리 과정에서 개인 정보의 유출이 발생하고, 또 역공학(Reverse Engineering)를 통하여 개인에게 민감한 정보를 채굴하고, 비즈니스에 악용하는 사례가 발생되고 있어서, 유럽에서는 GDPR을 한국에서는 데이터 3법을 시행을 하게되었다. 이러한 비즈니스의 추세에 따라 데이터의 저장 뿐만 아니라 처리에 있어서 안전하게 데이터를 획득, 처리, 파기하는 메커니즘과 제도가 필요하다. 본 고에서는 암호학적 관점에서 데이터(정보)의 처리과정에서 안전성과 협업성을 제공하는 완전동형암호(FHE, Fully Homomorphic Encryption)에 대하여 살펴본다.

Ⅱ. 동형 암호 (Homomorphic Encryption)

암호학에서도 디지털 전환으로의 환경변화에 따른 요구사항에 부응하는 메커니즘 연구가 오래전부터 진행되고 있었다. 사실 디지털 전환으로 암호학에 연구가 추진된 것이 아니고, 공개키 메커니즘으로 해결하지 못하는 데이터의 안전성을 개선하고자 하는 연구가 지속적으로 있어 왔다. 단순 사용자 인증에 해당하는 패스워드 사용을 1세대라고 한다면, 송수신 및 저장 데이터 암호를 2세대, 서명 및 키 공유에 활용하는 암호를 3세대라 구분할 수 있으며, 3세대 암호가 네트워크상의 데이터 안전성을 충족하지 않게 되는 상황이 발생 되어 4세대 암호, 즉 키를 사용하지 않는 암호화가 필요하게 되었다고 볼 수 있다. 이는 3세대에서 키를 많이 사용하다 보니 키의 장소를 알게 되고, 이어서 키를 해킹하여 암호문을 해독할 수 있게 되는, 또 네트워크 상에서 전달되는 암호화된 데이터 일지라도 반복 출현하는 데이터를 기반으로 원본을 판독하는 데이터의 안전성 문제가 발생하게 되었으며, 이와 같은 문제를 개선하기 위하여, 즉 정보의 공개 없이, 또는 유출 없이 전산적 처리를 하고 최종 사용자만이 그 내용을 복호화 할 수 있도록 하며, 그리고 데이터에 대

* 한국전자통신연구원 정보보호연구본부 (전문위원/책임연구원, jhnah@etri.re.kr)

한 이론적 안전성을 넘어 시스템의 구조적 측면에서의 안전성을 보장하여 개인정보를 보호하는 동형암호 알고리즘이 고안되었다. 일반적으로 암호화는 데이터의 기밀성과 무결성을 제공한다. 그러나 동형암호는 데이터의 무결성을 보장하지 않으며, 가단성(Malleability)을 제공하여, 암호화된 데이터를 연산처리가 가능하다.

동형암호 스킴은 오랜기간 동안 연구 되었으나, 크게 관심을 받지는 못 하였다. 완전동형암호 스킴에 대한 문제는 1978년에 제기되었으며, 그리고 30년 동안 해결방안이 없었다. RSA, ElGamal, Pailier 등의 부분동형암호 스킴들이 개발되었으며, Pre-FHE(Pre-Fully homomorphic encryption) 시대를 거쳐 향후 1~4세대를 구분한다.

2.1. 동형암호의 유형

동형암호의 뜻은 비밀 키에 액세스하지 않고 암호화된 데이터를 연산처리가 가능 하도록 한 암호화의 한 형태이다. 이러한 연산의 결과는 암호화된 상태로 유지되며, 대칭 키 또는 공개 키 암호화의 확장으로 볼 수 있다. 동형의 의미는 대수학에서 동형(Homomorphism)을 나타내며, 암호화 및 복호화 기능이 일반 텍스트와 암호문 사이에서 동형으로 처리되는 것이다.[1] 즉 암호화된 데이터를 복호하지 않고, 암호화된 상태에서 직접 연산처리를 하여도 그 결과가 원문 처리 결과와 동일한 암호화 방법을 의미하며, 아래와 같이 유형을 분류한다.

- Partially Homomorphic Encryption (PHE): 주어진 데이터 셋에 대해 무제한의 시간 동안 한 가지 유형의 수학 연산(예를 들어 곱셈)만 허용한다.
- Somewhat Homomorphic Encryption (SHE): PHE 에 비해 허용 범위가 넓지만 여전히 제한적이어서, 주어진 데이터 집합에 대해 덧셈과 곱셈을 몇 차례만 허용한다.
- Fully Homomorphic Encryption (FHE): 최선의 방법으로, 데이터에 대해 횟수에 제한없이 다양한 유형의 연산을 허용하지만 대신 성능 측면에서 현저히 불리하다.

Ⅲ. 유스케이스

3.1. 스토리지 아웃소싱

데이터 스토리지 아웃소싱은 자사내에 스토리지 운영에 따른 공간, 운영, 기술 및 인력등을 줄이고 유지보수 및 업그레이드에 따른 문제를 해결 할 수 있는 효율적인 방안이 된다. 속지의 법과 규제가 상충되는 경우에도 이를 해결하기 위하여 스토리지를 해외로 아웃소싱 할 수 있다.

일반적 암호화는 데이터 저장과 통신상의 비밀 문제를 해결 하지만 암호화된 데이터에 추가하거나 수정하는 것은 동형암호가 해결할 수 있다. 이러한 동형암호는 플랫폼 엔지니어가 권한을 악용해 사용자를 스토킹하는 것과 같은 사고 발생을 미연에 차단할 수 있다. 또한 동형암호를 사용하면 데이터를 클라우드에 안전하게 저장할 수 있으면서, 동시에 암호화된 데이터를 연산하고 검색에 사용할 수 있다.

3.2. 헬스케어

의료정보가 ICT 기술과 접목하여 의료기관에서 일어나는 제반 업무를 정보통신기술(ICT)을 이용하여 의사나 간호사의 일상적인 기록 작업이나 계산업무로부터 의사 및 간호사의 업무현황, 작업지시, 내원하는 고객(외래, 입원환자 등)의 건강정보, 과거 병명에서 현재 병의 진행과정, 치료 방법 등과 의료기관의 관리정보, 경영정보, 원무관리시스템 등의 병원 전체 운영을 위한 시스템을 포함하여 제반적인 모든 정보를 다루는 시스템이 헬스케어 시스템이다. 헬스케어 산업이 많은 관심을 받고 있지만 기대에 부응하여 크게 성장하지 못하는 이유중 하나는 개인정보보호 규제이다. 치료중 발견되는 환자의 병명 및 병력은 민감한 정보이며, 이러한 정보의 통계적 결과물도 어느 지역성과 문화적 정보가 포함되어 있어서 정보의 활용에 규제가 따르는 문제가 발생되는 경우가 빈번하게 발생한다.

동형암호는 이러한 데이터에 대한 전처리를 하여서 암호화된 형태로 저장이 가능하며, 필요에 따라 암호화된 데이터의 내용을 알지 않아도 안전하게 연산처리 하가 가능하다.

3.3. DNA 분석

개인의 유전정보를 이용하여 개인 맞춤형 정밀치료에 활용할 수 있는 기술 개발이 각광을 받고 있지만 반면 공공장소에서 주운 머리카락에서 DNA를 분석하여 얼굴을 만드는 소프트웨어를 이용하여 3D 프린팅을 하면 매우 유사한 모형을 작성할 수 있다. 그러므로 DNA는 매우 민감한 정보로서 프라이버시 문제를 발생한다. 동형암호는 이러한 이슈를 해결하는 대안으로 제시된다. DNA 정보를 동형암호화하여 저장 및 처리하면, DNA 정보의 유출을 방지하는 효과가 있다.

3.4. 가상물리시스템 (Cyber physical system)

원자력의 SCADA (Supervisory control and data acquisition) 네트워크나 ITS (Intelligent transportation system)의 자율주행 인프라는 인간사회에 매우 중요한 시스템이다. 이러한 인프라가 중요하게 여겨지고 또 관리가 필요하다고 피력이 되고 있으며, 가상물리시스템의 기본 개념이 스마트 팩토리, 스마트 시티, 디지털 트윈과 같은 인프라에 반영되고 있다. 이러한 인프라는 센서, 제어기와 엑츄레이터라는 구조를 갖는데, 현재 센서 데이터를 임의조작하는 일이 가능한데, 동형암호를 이용하면 센서 데이터를 암호화하여 제어기에서 복호화하지 않은 상태에서 연상처리가 가능하여 가상물리시스템의 안전성을 제고하는 핵심 기술로 활용이 가능하다.

3.5. 기계학습 (Machine learning)

머신러닝의 용어적 의미는 방대한 데이터를 분석해 미래를 예측하는 기술이다. 즉 컴퓨터가 스스로 학습과정을 거치면서 입력되지 않은 정보를 습득, 문제를 새로운 분류체계를 만들면서 데이터를 분석해 문제를 해결한다. 그러나 개인정보보호가 적용되는 환경에서 취득하는 데이터의 정확성이 이슈가 되는데, 즉 비식별화 처리가된 데이터의 개인정보의 결합도가 낮아 데이터의 가치가 떨어지는 문제가 제기되고 있다. 이러한 상황을 극복하고자 하는 방법으로 순수 데이터를 그대도 암호화 하고, 암호화된 데이터를 개인정보 유출 없이 기계학습 처리를 하여 관련 패턴을 찾아, 산업에 적용할 수 있다.

3.6. 양자컴퓨팅 내성 암호

인터넷뱅킹, 전자상거래와 통신 등의 암호체계는 풀기가 거의 불가능한 수학 문제에 기반으로 한 국제 표준 공개키 암호인 ‘RSA(Rivest Shamir Adleman)’와 ‘ECDSA(Elliptic Curve Digital Signature Algorithm)’를 대표적으로 사용하고 있다. RSA는 소인수분해 대상 숫자 단위가 무한히 커지면 이를 풀 수 없다는 수학적 난제로 잠금장치를 걸어놓은 것이다. 즉 공개키로 암호화하고 개인키로 복호화하는 방식으로 정보를 잠근다. 그런데 이들 암호는 ‘꿈의 컴퓨터’ 양자컴퓨터가 출현 되면 폐기될 전망이다. 양자컴퓨터가 사용하는 ‘쇼어 알고리즘’으로 실시간 해독이 가능하기 때문에, 인터넷뱅킹, 쇼핑 등 전자상거래와 현재 암호화 통신이 무용지물이 되는 것을 의미한다. 양자컴퓨터 기술 이후의 공격에 대응할 수 있는 암호로서 동형암호가 제시되고 있다. 동형암호를 포함한 격자기반암호는 양자컴퓨터가 도입되어도 깨지지 않는 차세대 암호체계라는 것이 암호학계의 중론이다. 격자 문제는 “현재로서는 풀 수 있음이 증명되지 않은 문제”인 NP 완전 문제(NP complete problem)로 분류 되어 있다.

3.7. 금융 협업

금융분야에서 개인정보보호가 필요하면서도 정확한 분석 결과가 필요한 카드, 보험사등에서 활용이 기대되고 있다. 이상거래 탐지(Fraud detection)나 개인신용평가(Credit scoring) 뿐만 아니라 고객의 프라이버시를 보호하면서 맞춤 서비스에 동형암호를 적용하면, 데이터 기밀성을 보장하면서 다자간 협업 서비스가 가능하다. 국외의 활용 예로서 알리바바의 자회사 앤트파이내셜 (ANT financial)은 신용분석, 마케팅 분석 및 은행데이터 결합분석 등을 위해 동형암호기술을 적용하고 있으며, SAP는 2018년 “SAP’s Guiding Principles for AI”를 발표할 때 동형암호를 핵심 요소기술로 소개한 후, “SAP 이노베이션 센터 네트워크(Innovation Center Network)” 전담조직을 통해 사업적 활용 방안 모색 및 블록체인, 벤치마킹 및 마케팅 서비스에 기술 적용을 진행하고 있다.

Ⅳ. 산업 및 표준 동향

4.1. 산업 동향

동형암호 개념은 Rivest, Adleman, and Dertouzos에 의하여 1978년 제시되고, IBM의 연구원인 Craig Gentry에 의하여 2009년 격자 기반 암호화를 사용하는 완전한 동형암호(Fully FHE)를 위한 구조가 최초로 제시되었다. 동형암호 스킴 관련하여 여러가지 오픈소스 구현물들이 존재하며, 다음과 같은 목록을 참조할 수 있다.[2]

- Microsoft SEAL: BFV 및 CKKS 스킴을 지원하는 마이크로소프트의 오픈소스 라이브러리.
- ALISADE: BGV, BFV, CKKS, TFHE 및 FHEW와 같은 여러 동형 암호화 체계를 지원하며 다자간 지원을 제공하는 방위 계약 업체 컨소시엄(DARPA 자금을 지원받는)의 오픈소스 라이브러리.
- HELib: CKKS 및 BGV 체계와 부트스트랩을 지원하는 IBM의 초기에 널리 사용되는 라이브러리.
- FHEW/TFHE: TFHE 스킴을 지원하며, TFHE는 FHEW에서 설계되었지만, FHEW는 더 이상 활발하게 개발되지는 않는다.
- HeaAn: 고정 소수점 근사 산술을 기본적으로 지원하는 CKKS 스킴을 구현한 라이브러리.
- ΛOλ(“LOL”이라고 발음): FHE를 지원하는 링 기반 격자 암호화를 위한 Haskell 라이브러리.
- NFLlib: 저수준 프로세서 프리미티브를 사용하여 고성능 동형 암호화를 탐색하기 위한 유럽 HEAT 프로젝트의 파생 결과인 라이브러리.
- cuHE: 이 라이브러리는 동형 암호화를 가속화 하기 위한 GPGPU 사용에 관한 연구.
- Lattigo: Go로 작성된 격자 기반 암호화 라이브러리.
- Concrete: TFHE 스킴의 사용자 맞춤을 지원하는 라이브러리.

4.2. 표준 동향

개인정보보호가 규제화 되면서, 전통적 암호 스킴은 데이터의 저장, 처리 과정에서 어려움이 발생되어, 동형암호가 대안으로 대두되고 있다. 2009년 IBM에서 제안하여 연구가 가속되고 있는 동형암호는 산업계에서 자발적으로 표준화의 필요성을 인식하여 컨소시엄 형태의 표준화가 진행되고 있으며,[2] 이를 글로벌 환경으로 보급을 목표로 공적표준화 기구에서도 표준화 작업을 2020년에 시작하여 적극적으로 활동이 이루어지고 있는 상황이다. 관련 표준화 기구로 Homomorphic Encryption Standardization 컨소시엄, ITU-T, ISO/IEC JTC 1 있으며, 관련 표준화 활동을 소개한다.

가. Homomorphic Encryption Standardization[2]

많은 기업과 개인이 클라우드 스토리지 및 컴퓨팅으로 전환함에 따라 쉽게 사용을 위한 기준의 요구가 발생 되고 있다. 현재의 구현은 비전문가가 사용하기에 쉽지 않아서, API를 균일화 및 단순화하고 애플리케이션 개발자에게 API를 사용하도록 표준화 필요성이 구성원 간에 공감대를 형성 하고 있는 상황이다. 참여자로 산업계에서는 Microsoft, Samsung SDS, Intel, Duality Technologies, IBM, Google, SAP 등이, 기관으로는 NIH, NIST, NSF, UN/ITU 등, 학계는 서울대, Boston Univ., Columbia, EPFL, MIT, UCSD 등이 참여하고 있다.

본 콘소시엄은 동형암호의 보안, API 및 애플리케이션등 세 가지 백서를 기반으로 동형암호에 대한 표준을 개발하고 있다. 커뮤니티의 주요 구성원의 검토를 거쳐 공개 의견 수렴 기간이 지난 후 보안 백서는 두 번째 표준화 워크숍(March 15-16 2018, MIT, Cambridge MA, USA) 에서 공개적으로 승인하여 동형암호 표준의 첫 번째 버전을 제정하였다. 이 표준은 스킴 설명, 보안 속성에 대한 설명 및 보안 매개 변수에 대한 표를 제공한다. 표준의 향후 버전에서는 동형암호를 위한 표준 API 및 프로그래밍 모델을 기술 할 예정이다.

나. ITU-T SG17[3]

ITU-T SG17 에서는 동형암호를 이용하여 산업에 적용할 수 있는 분야중 하나로 기계학습 분야를 정하고 동형암호의 이해와 데이터 분석에 있어서 개인정보보호를 위한 처리구조, 절차와 특성들에 대한 지침을 개발중에 있다. 삼성SDS, 서울대, ETRI가 에디터로 참여하여 활동을 하고 있으며, 2020년 3월에 신규아이템(TR.sgfdm, FHE-based data collaboration in machine learning) 채택이 승인되어 개발에 착수하였다.

주요 내용은 완전동형암호 기술을 사용하여, 기계학

습의 보안 추론 서비스 및 데이터 집계에 대한 보안 지침을 제공하며, 데이터 소유자가 기계학습 모델 공급자의 추론 서비스를 사용하는 반면 각 당사자는 자신의 데이터를 공개하지 않는 구조와 절차를 제공한다.

다. ISO/IEC JTC 1/SC27[4]

ISO/IEC JTC 1/SC27 WG2에서는 기존에 IS 18033-6, Encryption algorithms – Part 6: Homomorphic encryption 표준이 존재하며, 2019년 개정판을 제정하였으며, 이 표준은 부분 동형 암호를 위한 지수 ElGamal 암호와 Paillier 암호로 두 가지 메커니즘으로 구성되어 있다. 부분 동형 암호는 하나의 유형 연산만, 예 : 덧셈 (Paillier 암호 경우) 또는 곱하기 (지수 ElGamal 암호 경우)의 지원하는 스킴을 기술한다.

반면 완전 동형암호(FHE)는 임의 작업을 지원하고 암호화 데이터에 대한 임의 계산을 허용하는 동형암호 스킴 표준을 위한 작업이 2021년 1월부터 표준아이템 (PWI 15150 – Fully homomorphic encryption) 발굴을 위한 사전 모임을 갖었다. 이 모임에서는 SP Suitability of standardization of fully homomorphic encryption (FHE)에 대한 코멘트 협의 통하여 표준제안 개선 작업과 이를 활용하기 위한 유스케이스 “Approzimate HE in analyzing encrypted data (서울대 천정희 교수)“의 발표가 있었다. 향후 수 차례의 회의를 거쳐, 그 결과를 근거로 WG2 회의에 신규아이템 제안을 계획하고 있으며, 한국에서는 서울대와 삼성SDS에서 참여하고 있다.

Ⅴ. 결 론

유럽의 GDPR과 한국의 데이터 3법에 적절히 대처하고, 4차 산업을 육성하기 위하여 프라이버시 보전형 암호가 필요하며, 완전동형암호가 이 역할을 잘 감당할 것이라고 기대가 된다. 금융권이나 기계학습등과 같은 분야에서 완전 동형암호에 대하여 국제적으로 관심이 고조되고 있는 상황에서 한국(서울대)이 그 핵심 기술 개발에 선두주자로 활동을 하고 있다는 것이 매우 반가운 소식이다.

완전동형암호는 암호학적으로도 발전을 향해 나아가는 진일보한 이론이라고 평가한다. 이론적 검증은 완성되었으나, 시스템 구축과 그 연산처리 성능에 있어서는 아직 개선을 해야 할 숙제가 있으나, 많은 노력을 통하여 진전이 있은 것으로 알려졌으며, 암복호화 과정은 RSA 처리속도에 근사하고 있으며 연산처리 과정에서 속도 개선을 위하여 HW 기반의 연산 가속기를 연구 중에 있다.

완전동형암호 이론이 산업에 효과적으로 적용하기 위하여 표준화가 필연적 단계라 사료된다. 현재 기술과 표준 개발이 병행하여 개발중에 있으므로, 국내와 국제, 사실표준화와 공적표준화, 학계와 산업계, 정책적인 부분에서 개발에 대한 경쟁과 조율이 필요하며 전략적 대응을 기대해 본다.

참 고 문 헌

[1] Homomorphic Encryption, https://en.wikipedia.org/wiki/Homomorphic_encryption

[2] Homomorphic Encryption Standardization, https://homomorphicencryption.org/

[3] ITU-T SG17: Security, https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

[4] ISO/IEC JTC 1/SC 27, https://isotc.iso.org/livelink/livelink?func=ll&objId=8916258&objAction=browse

〈저 자 소 개〉

나 재 훈 (Jae Hoon Nah)

종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 학사

1987년 2월 : 중앙대학교 컴퓨터공학과 석사

2005년 2월 : 한국외국어대학교 정보공학 박사

1987년~현재 : 한국전자통신연구원 정보보호연구본부 전문위원/책임연구원

2019년~현재 : 글로벌ICT표준마에스트로

2009년~현재 : ITU-T SG17 WP4의장, Q7라포처

2018년~현재 : TC307 HoD/대표전문위원

2011년~현재 : 한국정보보호학회 이사

2011년~현재 : 한국정보보호학회 학회지 편집위원장 및 편집위원

<관심분야> 블록체인보안, 핀테크보안, 웹메쉬업보안, 스마트시티보안, 익명인증. 6G보안