정 보 보 호 학 회 지
제 33 권 제5호, 2023. 10

# 동형암호 기술과 활용 동향

손 민 아*, 신 성 철**

요 약

4차 산업혁명과 더불어 빅데이터의 활용이 보편화되었고, 최근 생성형 AI를 기점으로 인류의 정보 활용은 매년 그 최대치를 갱신하고 있다. 이 과정에서 의도치 않은 개인정보 노출 및 프라이버시 침해 사례들이 발생하고 있다. 동형암호는 정보 활용과 보호가 동시에 필요한 이 시점에서 주목할만한 기술이다. 최근에는 국내·외 다양한 분야에서 동형암호 기술의 적용사례가 등장하고 있으며, 이는 동형암호 기술이 상용화 단계에 이르렀음을 보여 준다. 본 고에서는 동형암호 활용사례를 중심으로 동형암호 기술 동향을 살펴보고자 한다.

## Ⅰ. 서 론

데이터 보안의 핵심은 세 가지로 데이터 저장, 데이터 전송 및 데이터 이용 중 보호로 정의한다[1]. 기존 암호화 기술의 경우, 데이터 이용 시 복호화가 필요하므로, 이 과정에서 데이터 유출 및 침해 위험이 존재한다. 반면, 동형암호는 일반 암호화 기술과 달리 데이터 저장 및 전송 중의 보호뿐 아니라 데이터 이용 중에도 보호할 수 있는 특징을 갖고 있다.

개인정보를 보호하는 동시에 분석이 가능한 동형암호는 “암호화의 성배” (the holy grail of cryptography) 라고 불리며[2], 정보기술 분야의 전문 연구 그룹 가트너(Gartner)는 동형암호를 기업들이 경쟁 우위를 확보하기 위해 눈여겨봐야 할 신기술 중 하나로 선정한 바 있다[3].

최근 데이터 보호를 강화하면서 활용할 수 있는 데이터 프라이버시 강화 기술[1]들이 연구되고 있고, 그 중 동형암호에 대한 연구도 국내·외에서 활발히 이뤄지고 있다. 암호화된 상태에서 복호화 없이 데이터 처리가 가능함으로써, 금융, 국방, 의료 등 민감정보를 다루는 영역은 물론 마케팅에서도 기대와 활용사례들이 등장하고 있다.

본 논문에서는 동형암호 기술 및 활용사례에 관해 연구해보고자 한다. 2장에서는 동형암호의 개념에 관해 설명하고, 3장에서는 동형암호 활용 동향에 대해 살펴보고 4장에서 본 논문의 결론을 맺는다.

## Ⅱ. 동형암호 (Homomorphic Encryption)

### 2.1. 개요

동형암호는 암호화된 데이터에 대해 복호화 과정 없이 연산을 수행할 수 있는 기술로서, 제 3자에게 암호화된 데이터를 전달하여 데이터를 보호하면서 데이터 분석을 수행할 수 있다[4].

수학적 관점에서 동형사상이란 두 대상 간의 변환·사상·함수에서 대수적 구조를 보존하는 형태의 하나이다. 따라서, 동형암호는 동형연산 후 그 결과가 평문의 연산 결과와 동일함을 의미한다[5].

평문 $m_1, m_2$의 암호문 $c_1 = Enc(m_1), c_2 = Enc(m_2)$가 주어졌을 때, 동형암호로 암호화하여 복호화하지 않은 상태에서도 연산구조를 그대로 가져간다[6]. 아래 수식은 동형암호 개념의 간단한 예시이다.

$$Dec(Enc(m_1) + Enc(m_2)) = m_1 + m_2 \quad (1)$$

$$Dec(Enc(m_1) * Enc(m_2)) = m_1 * m_2 \quad (2)$$

1) 프라이버시 강화 기술(Privacy Enhancing Technology, PET), 개인정보 위험관리 기술. 프라이버시 침해 위험을 관리하기 위해 핵심 기술로 암호화, 익명화 등의 개인정보 보호 기술에서 사용자가 직접 개인정보를 통제하기 위한 기술을 포함함.

* ㈜크립토랩 (연구원, ari95@cryptolab.co.kr)
** ㈜크립토랩 (실장, scshin73@cryptolab.co.kr)

동형암호 개념은 1978년 처음 소개되었고, 2009년 크레이그 젠트리 (Craig Gentry)가 암호화한 상태에서 임의의 연산을 무한 반복할 수 있는 부트스트래핑(Bootstrapping) 기법을 활용하여 완전동형암호(Fully Homomorphic Encryption)를 제안했다[5]. 현재 완전동형암호는 젠트리의 1세대 스킴(scheme)을 시작으로, 최초의 사용 가능한 2세대 BGV, BFV, 작은 데이터 처리에 효과적인 3세대 CGGI, 실수 연산이 가능한 4세대 CKKS[2]까지 개발되었다[7].

최근 동형암호는 연산시간을 빠르게 단축하고, 정확도를 높이면서 저장공간을 차지하는 비율을 줄이는 등 상용화를 위한 기능들이 개선되고 있다[8,9,10].

## Ⅲ. 동형암호 활용 동향

최근 국내·외에서 동형암호 관련 활발한 연구가 진행되고 있고, 이러한 연구는 금융, 공공기관, 의료 등 다양한 분야에 영향을 미치고 있다. 본 장에서는 동형암호 기술을 적용한 활용사례를 알아본다.

### 3.1. 위치정보 보호

위치정보는 개인의 행동 패턴, 선호도, 생활 습관 등을 직접적으로 반영하는 매우 민감한 개인정보이다. 위치정보의 무분별한 공유나 유출은 사용자 추적 및 프로파일링과 같은 프라이버시 침해 위험을 포함하며, 이는 정치, 종교, 성적 학대, 차별 등 다양한 형태로 나타날 수 있다. 따라서, 위치정보는 우리의 개인정보 보호와 자유를 지키기 위한 중요한 보호 대상이다.

우리는 일상에서 다양한 위치기반 서비스를 사용하고 있다. 그러나, 이런 서비스를 이용하는 과정에서 위치정보가 무심코 제 3자에게 유출되거나 남용될 우려가 있다. 이때 동형암호 기술을 적용한 위치기반 서비스를 사용한다면, 자신의 위치정보를 안전하게 보호하면서 안심하고 서비스를 사용할 수 있다.

#### 3.1.1. 코동이(코로나 동선 안심이)

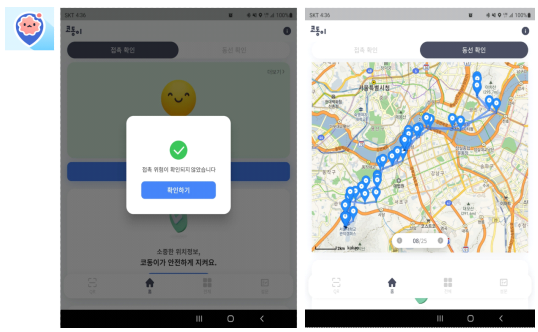
COVID-19 초기에는 접촉에 의한 감염 가능성이


〔그림 1〕 위치정보 애플리케이션

높아 확진자와의 접촉을 식별하는 것이 중요하였다. 하지만 이 과정에서 확진자 및 밀접 접촉자들의 동선 공개로 프라이버시 침해에 대한 이슈가 제기되었다. 이 문제를 해결하고자 크립토랩은 사용자의 위치정보를 보호하면서 확진자와의 접촉 여부를 알 수 있는 동선추적 앱을 개발하였고, 시민들의 자발적 참여를 통한 디지털 역학조사 서비스를 구현하였다.

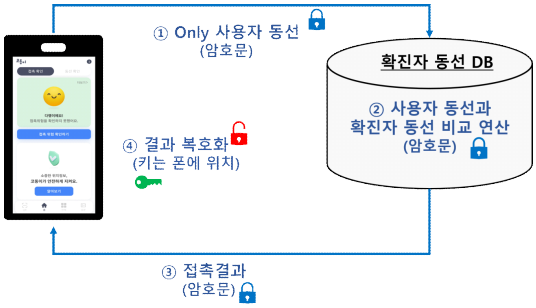
코동이 앱은 동형암호 기술이 적용된 최초의 상용 서비스로, 앱 이용자는 동형암호를 통해 프라이버시를 보호하면서 확진자와의 접촉 여부를 알 수 있다. 코동이 앱에 저장된 사용자 동선을 동형암호화하여 확진자 방문 QR 정보가 있는 서버로 전송하여 같은 장소에 있었는지를 비교 연산하고, 암호화된 결과를 이용자 앱에서 확인한다[11].

코동이는 출시 이후 약 20만 건의 누적 다운로드를 달성하였으며, 2021년, 경기도/통계청(`21.02)과 서울대(`21.07)/인하대(`21.10)가 코동이를 공식으로 채택한 바 있다[12]. 한국 질병관리청의 시범사업을 통해

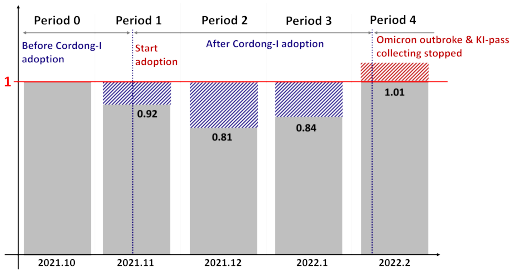


〔그림 2〕 코로나 동선 안심이 화면 예시

2) CKKS(Cheon-Kim-Kim-Song)은 2016년에 개발된 실수 연산이 가능한 4세대 완전동형암호 알고리즘이다.




〔그림 3〕 코동이 동형암호 연산



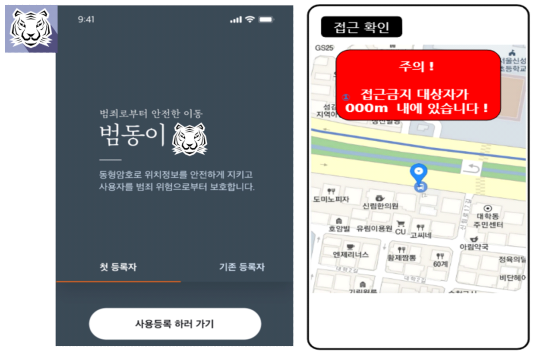

〔그림 4〕 수원시와 타 경기지역 코동이 효용성 비교 결과

코동이는 전국적으로 알려졌으며, 수원시에서의 시범 사업을 통해 경기 타지역에 비해 방역 성과가 유의미하게 높아 코동이의 효용성을 입증하였다.

동형암호 적용을 통해 위치정보 유출로 인한 사생활 침해 우려를 해소한 코동이 앱은 디지털 방역에 대한 시민들의 적극적인 참여를 끌어냈다는 점에서 의미가 있다.

### 3.1.2. 범동이(범죄위험 동선 안심이)

스토킹 범죄, 데이트 폭력, 가정 폭력 및 성폭력 등의 발생 증가와 함께 최근에는 묻지마 폭행·살인이라는 사회적 이슈도 확산되고 있다. 이 중에서도 피해자와 피의자가 특정되는 스토킹 범죄의 경우 재범률이 높고 강력범죄로 번질 가능성이 크다. 경찰은 이런 문제에 대응하기 위해 신변 보호용 스마트워치를 활용하고 있지만, 이는 피의자의 접근을 확인하고 신고하는 사후 개입 방식으로 피해자 중심의 선제적 보호에는 한계가 있고 가해자 위치가 아닌 피해자의 위치만을 수집한다. 법원에서 내리는 접근금지 명령 역시 피의자가 접근 시 사전 대처나 예방에 한계가 있고 피해자의 집이나 직장 등을 가해자에게 알려 특정 범위 내에서 접근하지 못하도록 하는 것이기에 피해자의




〔그림 5〕 범동이 화면

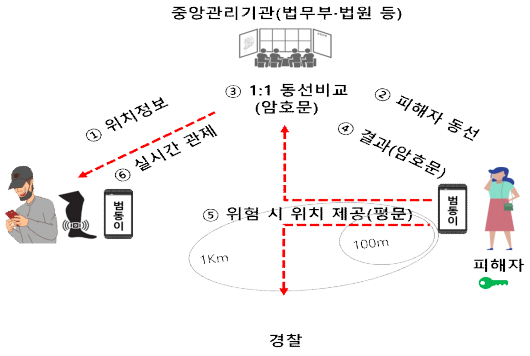
사생활 침해가 우려된다.

전자발찌도 동일하게 피해자 중심의 사전적 보호에는 한계가 있어, 동형암호를 활용하여 사용자의 프라이버시 침해를 방지하고 피해자 중심의 적극적인 보호가 가능한 서비스가 개발되었다.

범동이 서비스는 동형암호 기술을 활용하여 신변 보호 대상자의 위치정보를 암호화한 뒤, 가해자와의 거리를 실시간으로 계산하여 위험성을 알려주는 서비스이다. 피의자가 일정 거리 이내로 접근하면 피해자 혹은 경찰에게 알림을 보내어 범죄를 예방한다[13].

이 서비스에서 또 하나 주목할만한 점은 범죄 발생 직전까지 잠재적인 사생활 침해를 방지하기 위해 범죄자의 위치정보도 보호한다는 것이다. 법적 위반 상황일 경우에만 피해자와 경찰에 알려 사전 조치를 한다.

해당 서비스는 동형암호를 통해 안전하게 위치정보를 보호하면서 스토킹, 성범죄 등의 범죄를 예방하고 피해자의 불안감 감소와 함께 범죄 발생 전까진 범죄자의 위치정보도 동형암호화하여 프라이버시를




〔그림 6〕 범동이 개념도

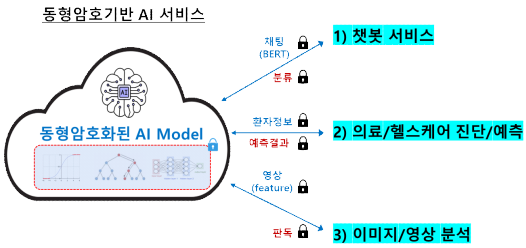
보호할 수 있다는 점에서 가치가 있다.

범동이는 개인정보보호위원회, 한국인터넷진흥원에서 주최한 '22년 개인정보 보호·활용 기술개발 스타트업 챌린지에서 우수상을 받았다.

### 3.2. Private AI

Private AI는 사용자의 개인 데이터를 보호함과 동시에 개인화된 서비스를 제공하는 인공지능을 의미한다. 인공지능의 활발한 활용과 인기 상승에 따라 개인정보와 기밀정보에 대한 보호가 중요한 화두로 떠오르고 있다. GDPR[3] 및 CCPA[4] 같은 규정들은 개인정보 보호를 설계 초기부터 요구하고[14], 특히 기업들은 최근 생성형 인공지능 도구의 사용으로 발생하는 기밀정보 유출의 위험성을 우려하고 있다. 실제로 생성형 인공지능 서비스 출시 후, 국내 대기업 직원이 서비스 이용 중 사내 기밀정보 등을 입력하여 총 3건의 데이터가 유출되는 사고가 발생했다. 계속되는 해당 서비스 사용으로 인한 기밀정보 유출 우려에, 몇몇 기업들은 생성 모델 기반 인공지능 도구의 사내 사용을 직원들에게 제한하는 조치를 했다[15, 16].

생성형 AI 등의 인공지능 서비스 활용 중 정보 유출 발생 문제와 우려가 제기되는 가운데, 정보 활용과 보호를 동시에 가능하게 하는 동형암호 기술은 이러한 고민을 해결할 수 있는 탁월한 솔루션이다. 현재 동형암호 기반의 챗봇, 의료·헬스케어 진단 예측, 이미지·영상 분석 등의 기능을 제공하는 다양한 서비스가 개발되고 있다.




〔그림 7〕 동형암호 기반 인공지능 활용 예시

3) GDPR(General Data Protection Regulation, 유럽 일반 개인정보 보호법), 기업 및 조직이 EU 회원국 내에서 이루어지는 거래와 관련하여 EU 시민의 데이터와 개인정보를 보호하도록 규정하는 데이터 보호법.

4) CCPA(California Consumer Privacy Act, 캘리포니아 소비자 개인정보 보호법), 미국 최초의 포괄적인 개인정보 보호법.

#### 3.2.1. 동형암호 마이데이터 기반 백신 부작용 알림 서비스

보건의료 데이터 시장의 매년 성장률 37.6% 예상[17] 등 의료 산업은 민감한 의료정보에 대한 수요가 점점 늘어나고 있지만, 데이터의 유출은 상당한 위험을 초래할 수 있으며 예측할 수 없는 피해를 초래할 수 있다. IBM 발간 데이터 유출 비용 보고서에 따르면, 의료분야의 데이터 유출 비용은 2020년대 대비 41.6% 증가한 120억 원으로 역대 최고치이고 12년 연속 유출 비용이 가장 높다[18]. 의료 데이터는 환자의 개인정보뿐 아니라 질병 및 유전정보 등 프라이버시와 밀접한 정보를 담고 있기에 더욱 민감하다.

안전한 의료 데이터 활용이 가능한 동형암호 기반의 '나의 건강기록(PHR)[5]'을 활용한 백신 부작용 알림 서비스는 동형암호화된 의료 마이데이터를 활용하여 개인별 백신 부작용을 예측하고 사후관리를 통해 추가적인 부작용을 예방하는 시스템이다[19].

팬데믹 동안 백신 부작용 사례의 증가로 인해, 사람들은 백신 접종 전 부작용 발생에 대한 사전 대비에 큰 관심을 보였다. 그러나, 현실적으로 백신 부작용 사전진단 등의 서비스는 의료행위에 해당하므로, 이 백신 부작용 알림 서비스는 백신 접종 후의 부작용 예측 및 사후관리에 초점을 맞추어 개발되었다. 사후관리를 위해 백신 정보, 건강보험공단 진료 및 검진 데이터는 물론 국세청의 소득 데이터 등을 종합적으로 활용하여 정밀한 개인 맞춤형 사후관리 서비스를 제공한다. 특히 백신 부작용 취약계층 및 고위험군 분류에 따른 효율적인 대상자 사후관리 지원 예정이다.


〔그림 8〕 인공지능 모델 동형암호화 예시

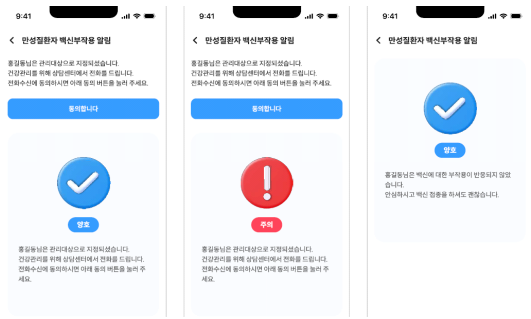
5) 나의 건강기록(Personal Health Record, PHR), 개인이 주도적으로 본인의 의료 데이터를 통합 및 관리하고, 자신이 원하는 대상에 한하여 제공 및 활용하는 기술 및 서비스

이 서비스는 의료기관에서 개발된 예측모형(XGBoost)을 민간기업에서 활용하여 서비스한다. 민간기업에서 개인의 개인정보 및 의료정보를 안전하게 활용하여 백신부작용 예측값을 계산하고자 동형암호를 활용한다. 이 과정에서 데이터를 암·복호화하고 암호화 연산에 필요한 공개키와 비밀키는 사용자의 단말기에 안전하게 저장되어 관리된다.

개인 데이터 저장소(PDS[6])에 통합된 의료 마이데이터는 동형암호화 후 동형연산 서버에 전달되며, 해당 서버에서 암호화된 데이터가 예측모형을 통해 추론(inference)되어 부작용 확률값을 얻게 된다.

동형암호 기술을 적용한 Private AI 서비스는 사용자의 데이터를 암호화하여 안전하게 분석하는 것은 물론, 예측모형을 동형암호화함으로써 예측모형의 파라미터를 보호하여 지적재산권도 보호할 수 있다.


〔그림 9〕 백신 부작용 알림 서비스 화면




〔그림 10〕 백신 부작용 알림 화면

6) 개인 데이터 저장소(Personal Data Store, PDS), 개인이 데이터를 안전하게 보관할 수 있도록 지원하는 서비스 구조화된 보안체계에 따라 PDS는 개인 데이터를 암호화하여 저장하고 개인에게 통제와 권리 권한을 저장한 개인에게 부여한다.

### 3.2.2. 완전동형암호기반 자동 기계학습 (AutoFHE)

국방 분야나 비밀계약과 같은 기밀정보를 다루는 경우 보안상의 이슈로 데이터 접근과 활용이 제한된다. 이로 인해 해당 분야에서의 인공지능의 도입과 지속 개발에 어려움이 있다. 반면, 동형암호 기술을 적용한다면 기밀정보를 보호하면서 인공지능 모델과 데이터를 안전하고 효율적으로 활용할 수 있게 된다.

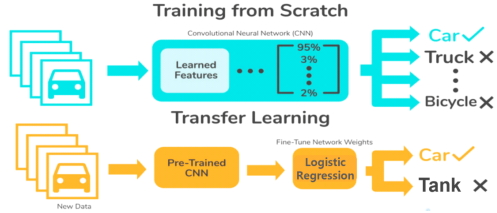
또한, 의료 영상 및 CCTV 등 민감한 개인정보 유출시 프라이버시 침해 위험이 있는 데이터 보호에도 동형암호의 활용은 유용하다.

완전동형암호기반 자동 기계학습 (AutoFHE) 서비스는 개인정보 보호를 위한 클라우드 기반의 자동 기계학습(AutoML) 서비스로, 누구나 데이터 유출에 대한 걱정 없이 자동 기계학습 서비스를 사용할 수 있다.

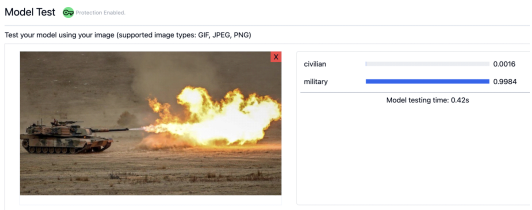
사전 학습된 이미지 분류 인공지능 모델에 사용자가 보유하고 있는 이미지 데이터를 동형암호화해 암호화된 데이터를 보내면 서버에서 추가로 학습 및 추론을 구현하여 사용자에게 분석 결과를 보내준다.

AutoFHE 서비스는 빠른 속도와 우수한 머신러닝 정확도에서 차별화된다. 이 서비스는 올해 머신러닝 학회에서 발표한 동형암호와 전이학습을 결합한 논문[20]을 기반으로 개발되었으며, 다양한 모델을 학습한 후 최적의 모델을 선택할 수 있도록 하였다. 암호화된 데이터를 서버에 전송한 후에 필요한 학습 시간은 학습 데이터양에 따라 다르며, 적게는 4분 정도 소요된다. 이렇게 학습된 모델은 암호화된 상태로 서버에서 사용할 수도 있고, 내려받아서 복호화한 후에 사용할 수도 있다.

[그림 12]은 AutoFHE 서비스의 사용 예를 보여 준다. 서버에는 학습된 암호화된 모델이 있고, 사용자가 추론을 위해 선택한 이미지는 암호화된 상태로 서버에 전송된다. 서버에서는 암호화된 데이터와 모델을 사용해서 추론을 진행하고 결과를 사용자에게 전송하




〔그림 11〕 이미지 전이학습 예시




〔그림 12〕 완전동형암호 자동 인공지능 (AutoFHE)

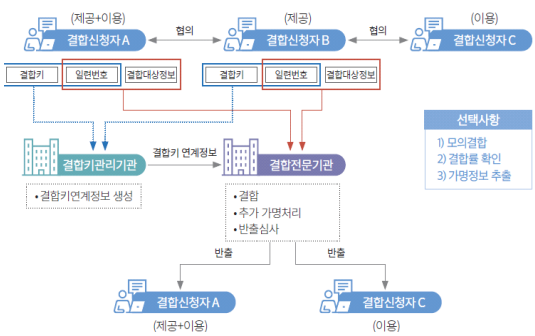
면, 사용자는 이 값을 복호화해서 최종 결과를 볼 수 있다. 이때 암호화 연산에 필요한 시간은 0.42초 정도이고, 결과로부터 선택된 탱크 이미지가 잘 분류됨을 확인할 수 있다.

완전동형암호 자동 인공지능 서비스는 기밀한 정보를 보호하면서 프라이버시 침해 없이 인공지능 도입이 어려운 분야에 유의미한 분석 결과를 빠른 속도로 도출할 수 있다는 것을 보여 준다.

### 3.3. 데이터 결합

2020년 1월 빅데이터 3법(개인정보 보호법, 정보통신망법, 신용정보법)이 개정되면서 개인을 식별할 수 없는 가명정보의 개념이 도입되었다. 가명정보는 통계작성, 과학적 연구, 공익적 기록 보존의 목적이라면 사용자 동의 없이도 데이터 결합 및 분석을 할 수 있다는 점이 데이터 활용관점에서 의미가 크다. 또한, 정부는 세금, 교육, 교통 등 다양한 종류의 공공 데이터를 개방하고 있다[21]. 다만, 가명정보는 개인정보에 준하는 정보보호의 의무가 있고, 무분별한 데이터 결합을 방지하고자 정부는 결합 전문기관을 지정하여 이곳을 통해서만 결합을 할 수 있도록 정하였다.

가명정보 결합을 위해서는 각 결합 신청기관은 데이터를 가명처리 하고 가명처리 적정성 평가를 받아야 한다. 또한, 결합키 관리 기관에서 사전 결합키를 생성하고, 결합 전문기관을 통해 데이터를 결합해야 한다. 가명정보 결합은 데이터 활용관점에서 많은 기회를 열어주었으나, 과정이 복잡하고 시간이 오래 걸리며 결합 분석 중 변수 추가 나 데이터 변경 필요시 결합 프로세스를 다시 해야 하는 번거로움이 있다[22].




〔그림 13〕 가명정보결합 프로세스(가명정보결합가이드라인)

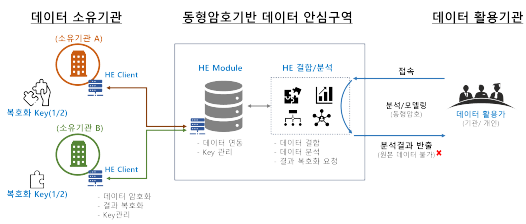
반면, 동형암호를 활용한 데이터 결합은 안전한 데이터 결합 및 분석뿐만 아니라, 데이터 결합 절차의 간소화로 시간과 비용 절감이 가능하다.

#### 3.3.1. 데이터 안심구역

데이터안심구역은 미개방 데이터를 분석·활용할 수 있는 플랫폼으로 공공기관 및 민간기업의 데이터를 무료로 안전한 분석환경에서 활용할 수 있는 플랫폼이다. 데이터산업진흥원에서 최초로 운영하고 있었으나, 2022년 7월 과기부에서는 한국도로공사, 한국전력공사, 국민연금·전라북도, 농림수산식품교육문화원 등 4곳을 추가로 지정하였다. 다만, 기존 안심구역은 가명정보 관리 및 데이터 결합 시 결합전문기관을 이용해야 하는 법적 절차가 필요하여, 현실적으로 익명정보 중심으로 운영되고 있다. 이는 데이터안심구역을 찾는 소비자(분석가) 입장에서는 분석 방법에 제약이 되어 데이터안심구역 활용에 한계가 되고 있다.

만약, 동형암호를 활용한 "데이터안심구역"을 구축한다면, 안전한 데이터 결합 및 분석을 할 수 있다.

첫째, 데이터 소유자는 암호화된 데이터를 제공함으로써 데이터관리 위험을 줄이며, 제 3자가 데이터 활용 시 결과 복호화 소유자가 하여 데이터 소유권을 유지할 수 있다. 둘째, 데이터 활용자는 가명·익명화 과정 없이 원시 데이터(raw data)를 활용할 수 있어, 데이터 손실 없는 고품질의 데이터 분석이 가능하다. 또한, 데이터 결합 시 프로세스가 단순화되어 시간과




〔그림 14〕 동형암호 기반 데이터 안심구역 예시

비용이 절감된다. 셋째, 데이터안심구역을 운영하는 플랫폼 사업자는, 데이터 암호화를 통해 데이터관리 비용이 절감되고, 데이터 소유자와 활용자가 증가하여 플랫폼이 활성화되고 궁극적으로 데이터 유통의 선순환 구조를 만들 수 있다.

### 3.3.2. 다기관 병원 데이터 결합 사례

의료기관에서 데이터 분석 시 질병의 종류와 치료법 등 모든 조합의 데이터들이 존재하지 않는 경우가 많고, 희귀질병의 경우 국내·외에서 사례를 수집하려 해도 그 수가 부족한 경우가 있다. 의료기관에서는 서로 다른 구조로 이루어진 각 기관의 데이터를 통일된 형식으로 변환하여 분석하는 공통데이터모델(Common Data Model, CDM)이 시도되었다. 국내에서도 "의료데이터중심병원"을 허브로 기업·대학·연구기관·병원들이 데이터를 연계·통합하시는 사업을 진행하고 있다.

다만, 질병의 종류가 다양하고 병원별로 의료 데이터의 표준화가 미진하여 그 활용까지는 상당한 시간이 필요할 것으로 보인다.

최근 3개의 의료기관이 비심장수술을 받은 18세 이상의 성인 환자들을 대상으로 동형암호를 활용하여 데이터를 결합하고 사망 여부를 예측하는 연구를 진행하였다. 다기관 병원의 실제 임상 데이터를 동형암호 기술을 적용하여 결합함으로써, 각 기관은 환자의 정보를 타 기관에 공개하지 않고도 충분한 데이터를 확보하여 안정적인 예측모형을 개발하였다.

동형암호를 활용함으로써, 데이터 수가 충분치 않은 중소병원에서도 다기관 결합을 통해 질병 예측모델 성능을 향상시킬 수 있음을 확인하였다.

| Type | Train | Test | | |
|---|---|---|---|---|
| | | A병원 (N=9,392) | B병원 (N=32,437) | C병원 (N=26,373) |
| | | AUROC | | |
| Single | B병원 | 0.915 (0.902-0.928) | 0.939 (0.927-0.950) | 0.890 (0.867-0.912) |
| | A병원 | 0.942 (0.930-0.953) | 0.925 (0.913-0.936) | 0.937 (0.926-0.947) |
| | C병원 | 0.906 (0.890-0.921) | 0.880 (0.853-0.906) | 0.952 (0.943-0.961) |
| Merged | B+C병원 | 0.919 (0.907-0.931) | 0.931 (0.914-0.947) | 0.952 (0.942-0.962) |
| | A+B병원 | 0.927 (0.902-0.952) | 0.940 (0.925-0.955) | 0.934 (0.920-0.947) |
| | A+C병원 | 0.925 (0.903-0.946) | 0.931 (0.916-0.945) | 0.956 (0.950-0.962) |
| | A+B+C병원 | 0.929 (0.905-0.953) | 0.941 (0.927-0.955) | 0.957 (0.951-0.963) |

〔그림 15〕 단일모델과 결합모델의 AUROC 결과

## Ⅳ. 결 론

동형암호는 데이터를 암호화한 상태에서 복호화 없이 연산이 가능하다는 기술의 특성상 데이터 활용 수요가 급증하는 빅데이터, AI 시대에 필수적인 기술이다.

3장에서 살펴보았듯이 동형암호를 통해 일상적으로 노출되는 사용자 위치정보를 보호하면서도 서비스를 이용할 수 있다. 또한, 자신의 민감정보를 보호하면서 최신의 AI 서비스를 이용할 수 있다. 최근 데이터 결합 및 마이데이터 등 빅데이터 플랫폼이 활성화되면서 동형암호를 통해 보다 빠르고 안전한 빅데이터 플랫폼을 구축할 수 있다. 동형암호 기술의 특성상 숫자 형 데이터만 처리 가능할 것이라는 고정관념도 최근 연구를 통해 텍스트는 물론 이미지도 처리할 수 있다는 것이 확인되었다. 동형암호는 원천기술에 관한 연구가 국내·외에서 활발하게 진행되고 있고, 다양한 영역에서 기술의 활용이 구제화되고 있다.

데이터 보호와 활용이라는 두 마리 토끼를 모두 잡을 수 있는 동형암호 기술은 AI 시대에 게임 체인저가 될 것으로 기대한다.

## 참 고 문 헌


[1] Fahmida Y. Rashid,"What is confidential computing?", 2020, IEEE Spectrum

[2] 동아사이언스, "뚫리지 않는 방패, 동형암호의 '아버지'",http://m.dongascience.com/news.php?idx=58582, Accessed on September 2023.

[3] CIO Korea, "암호화의 성배, '동형암호'란? 사용사례는?", https://www.ciokorea.com/news/221474, Accessed on September 2023.

[4] Gentry C., "Computing arbitrary functions of encrtypted data", 2010, ACM

[5] Gentry C., "Fully homomorphic encryption using ideal latiices", 2009, ACM

[6] Cheon, J., Euh, Y., J., "Privacy-preserving finance data analysis based on homomorphic encryption", 2018, Review of Financial Information Studies

[7] Cheon, J., Kim, A., Kim, M., Song, Y., "Homomorphic encryption for arithmetic of ap-

proximate numbers”, 2017, Springer International Publishing

[8] Jung, W., Lee, E, Kim, S., Kim, J., Kim, N., Lee K, Min, C., Cheon, J.H. Ahn, J.H., “Accelerating fully homomorphic encryption through architecture-centric analysis and optimization”, 2021, IEEE Access

[9] Youngjin Bae, Jung Hee Cheon, Wonhee Cho, Jaehyung Kim and Taekyung Kim, Meta-BTS: Bootstrapping precision beyond the limit, 2022, CCS

[10] Youngjin Bae, Jung Hee Cheon, Jaehyung Kim, Jai Hyun Park and Damien Stehlé, HERMES: Efficient Ring Packing using MLWE Ciphertexts and Application to Transciphering, 2023, Crypto 2023

[11] 파이낸셜 뉴스, “방역당국, 자가 동선확인 앱 ‘코동이’ 전국 시행 검토”, https://www.fnnews.com/news/202112281530313861, Accessed on September 2023.

[12] 뉴스원, “‘자발적 참여 방역’ 실험 한달, ‘K-방역 2.0’ 가능성 보다”, https://www.news1.kr/articles/?4449870, Accessed on September 2023.

[13] ㈜크립토랩 홈페이지,“유즈케이스-국내사례”, https://www.cryptolab.co.kr/use-cases/domestic/, Accessed on September 2023.

[14] GDPR, “Article 25 GDPR. Data protection by design and by default”, https://gdpr-text.com/ko/read/article-25/, Accessed on September 2023.

[15] 이코노미스트, “[단독] 우려가 현실로,,,삼성전자, 챗GPT 빗장 풀자마자 ‘오남용’ 속출”, https://economist.co.kr/article/view/ecn202303300057?s=31, Accessed on September 2023.

[16] EBN 산업경제, “‘기밀 유출 막아라’, ... 챗GPT 경계 나선 삼성·LG·SK”, https://m.ebn.co.kr/news/view/1577665, Accessed on September 2023.

[17] 메디게이트 뉴스, “‘보건의료 데이터’ 시장 연평균 37% 성장 전망...10년 뒤 최대 9조원 시장 예측”, https://medigatenews.com/news/3217099664, Accessed on September 2023.

[18] IBM, “2022년 데이터 유출 비용 연구 보고서”, 2022, IBM

[19] 이데일리, “차 의과학대, K-DATA 마이데이터 종합기반 조성사업 선정”, https://www.edaily.co.kr/news/read?newsId=01738406635671568&mediaCodeNo=257, Accessed on September 2023.

[20] Seewoo Lee, Garam Lee, Jung Woo Kim, Junbum Shin and Mun-Kyu Lee, HETAL: Efficient Privacy-preserving Transfer Learning with Homomorphic Encryption, 2023, ICML(oral)

[21] ZDNET Korea, “미개방 데이터 안심하고 활용하세요...데이터 안심구역 4곳 지정”, https://zdnet.co.kr/view/?no=20230104100646, Accessed on September 2023.

[22] 컴퓨터월드, “[특집]데이터 결합, 데이터 경제 활성화 이끈다”, https://www.comworld.co.kr/news/articleView.html?idxno=49930, Accessed on September 2023.

## 〈저자소개〉

**손 민 아 (Mina Sohn)**

2018년 7월 : 북경대학교 신문방송학과 졸업

2020년 7월 : 북경대학교 뉴미디어학과 석사

2023년 9월 : 크립토랩 데이터사업개발실 연구원

〈관심분야〉 정보보호, 신문방송학, 빅데이터

**신 성 철 (Sungchul Shin)**

1999년 2월 : 중앙대학교 응용통계학과 졸업

2002년 2월 : 서울대학교 통계학과 석사

2023년 9월 : 크립토랩 데이터사업개발실 실장

〈관심분야〉 정보보호, 통계학, 빅데이터