활용성 강화 데이터 프라이버시 보호 기술 동향

Trends in Data Privacy Protection Technologies with Enhanced Utilization

김주영 (J.Y. Kim, ap424@etri.re.kr) 미래암호공학연구실 선임연구원
조남수 (N.S. Jho, nsjho@etri.re.kr) 미래암호공학연구실 책임연구원
장구영 (K.Y. Chang, jang1090@etri.re.kr) 미래암호공학연구실 책임연구원

ABSTRACT

As the usability and value of personal information increase, the importance of privacy protection has increased. In Korea, the scope of the use of pseudonymized personal information has increased because of revisions to the law. In the past, security technologies were used to safely store and manage personal information, but now, security technologies focused on usability are needed to safely use personal information. In this paper, we look at issues related to the de-identification and re-identification of personal information. Moreover, we examine the standards and techniques related to the de-identification of personal information.

KEYWORDS 데이터 3법, 비식별화

Ⅰ. 서론

최근 개인정보 활용을 통한 데이터 경제활성화를 위해 데이터 3법이라고 불리는「개인정보보호법」,「정보통신망법」,「신용정보보호법」이 개정되었다. 이에 따라 개인정보의 비식별화를 통해 가명정보를 생성하고 이를 상업적 용도로 활용하는 것이 가능해졌다. 그러나 비식별화 조치를 미흡하게 하여 특정 개인을 식별하게 되는 등의 안전 의무를 위반한 경우 5년 이하의 징역 또는 5,000만 원 이하의 벌금 및 전체 매출액의 3%에 해당하는 과징금을 부여하는 만큼 개인정보를 비식별화하는 프라이버시 보호 기술에 대한 중요성이 매우 높아졌다.

데이터 3법 개정 이전에도 개인정보 프라이버시 보호를 위해 정부에서는 개인정보 비식별 조치 가이드라인을 통해 프라이버시 유출을 최소화할 수 있는 가이드라인을 제시하였다[1]. 하지만 비식별화된 정보도 다른 비식별화된 데이터 간의 결합과 추론을 통해 재식별의 위험성을 가지고 있다. 데이터 3법에서도 이러한 부분을 고려하여 데이터 결합은 정부가 지정한 기관에서만 시행할 수 있도록

* DOI: https://doi.org/10.22648/ETRI.2020.J.350609
* 본 연구는 한국전자통신연구원 연구운영비지원사업의 일환으로 수행되었음[20ZR1320, TDC 원천기술개발 데이터 생성 기술 연구].

하였지만 가명정보 간의 재결합을 통한 재식별 공격(Re-identification Attack)과 같은 프라이버시 유출의 위험성은 여전히 존재한다. 따라서 재식별 공격에도 취약하지 않은 프라이버시 보호 기술이 필요하나 기존의 프라이버시 보호 기술은 안전성에 중점을 두었기 때문에 데이터를 실질적으로 활용하는 데 어려움이 많았다. 예를 들어, 기존의 암호 기반의 프라이버시 보호기술들은 데이터 암복화에 과도하게 소요되는 리소스 및 복호화 단계에서의 데이터 유출 등의 문제로 인해 데이터 활용에 어려움이 있었다.

본 고에서는 현재 개인정보 활용을 위한 비식별화에 대한 이슈 및 표준 동향을 살펴보고, 표준 동향에 맞춰서 활용성이 강화된 데이터 프라이버시 기술 동향에 대해 알아본다.

Ⅱ. 개인정보 비식별화

이 장에서는 개인정보 비식별화와 관련된 이슈와 관련 표준화 동향을 살펴본다.

1. 비식별화 관련 이슈

가. Netflix Prize

Netflix Prize는 Netflix가 제공하는 데이터 셋을 이용해서 개인에게 영화를 추천하는 알고리즘을 공모하는 대회로 2007년부터 2009년까지 진행되었다. 2008년 텍스사 대학교 연구진[2]은 NetflixPrize를 위해 개인정보가 비식별화된 데이터 셋 50만 건과 영화 리뷰 사이트인 IMDb의 리뷰 데이터를 결합하여 사용자를 식별화 시도를 진행하였다. 그 결과 IMDb에서 실명으로 공개된 리뷰들과 Netflix에서 제공한 데이터를 결합하여 Netflix에서 제공한 정보가 누구의 데이터인지 유추할 수 있었으며, 이로 인해 공개하지 않은 자신의 관람 영화정보까지 모두 공개될 수 있음을 보여주었다. 해당 사례를 통해 비식별화된 데이터도 다른 데이터와 결합할 경우 충분히 식별화될 수 있음을 확인하였고, 현재 공개되지 않은 미래에 공개될 데이터와 결합하면 식별 가능할 수 있다는 잠재적 위험성을 확인하였다.

나. 유전자 재식별화

최근 DNA 분석 기술에 발달에 따라 유전자 정보를 이용하여 신원을 유추하는 기술은 점점 더 진화하였다. Whitehead 연구소는 1000 Genome Project를 통해 익명의 백인 남자의 염색체 정보를 수집하고 이를 인터넷에서 수집한 DNA 정보와 가계도 검색엔진인 Ysearch, SMGF를 통해 익명의 백인 남자를 추론하였다[3]. 그 결과 가계분석 등을 통해 약 12% 정도 신원을 확인할 수 있었고, 5%는 잘못된 신원으로 확인되었으며, 83%는 신원을 확인할 수 없었다. 이는 특정인의 유전자 정보의 일부가 친족의 유전자 정보와 결합하여 개인을 식별할 수 있다는 것을 보여준 사례로, 본인이 등록하지 않은 정보에 의해서도 개인이 식별될 수 있음을 보여주는 사례이다. 유전자 정보는 개인의 식별할 수 있는 많은 양의 데이터를 포함하기 때문에 민감도가 매우 높다. 일례로 Parabon Nanolabs는 DNA를 이용한 제약 및 분석 서비스 회사로써 2015년 담배꽁초에서 추출한 DNA 정보를 이용하여 몽타주를 생성, 이를 담배꽁초 투기를 막는 공익광고에 사용하였다.

이는 DNA 정보가 결합을 통해 개인을 유출할 수 있을 뿐만 아니라 개인의 외모 또한 유추할 수 있음을 보여준다. 따라서 유전자 정보를 이용하여 데이터를 가공하거나 연구를 진행할 경우 데이터의 프라이버시 보호는 매우 중요하다.

표 1 재식별화 기술[4]

기술	설명
Prosecutor Attack	기존 지식을 사용하여 특정 데이터 주체에 속하는 레코드를 다시 식별
Journalist Attack	기존 지식을 사용하여 특정 레코드의 데이터 주체를 다시 식별
Marketer Attack	기존 지식을 사용하여 해당 데이터 주체로 가능한 한 많은 레코드를 재식별
(In–) distinguishability Attack	데이터 집합에 특정 데이터 주체의 존재를 확인
Inference Attack	다른 속성 그룹과 관련된 민감한 속성을 추론

표 2 ISO/IEC 20889 비식별화 기술[4]

기술	설명
통계도구	데이터의 전체적인 구조를 바꾸는 통계적 성질의 방법으로 데이터 집합을 비식별화하거나 비식별화 효율을 높이기 위해 사용
암호화 도구	비식별화 기법의 효과를 높이거나 비식별화 기술의 일부로서 작용함. 형태보존암호, 순서보존암호, 동형암호 등이 포함됨
억제기술	범주형 데이터에 적용되는 기술로 마스킹이나 데이터 속성을 삭제하는 기술로 구현이 용이
가명화 기술	데이터의 고유식별자를 해시 등을 이용하여 간접식별자로 치환하는 기술
원자화	데이터 집합을 식별자와 나머지 속성으로 분리화하는 기술. 원자화 된 데이터는 서로 다른 접근 권한을 가져야 함
일반화 기술	데이터의 세분화를 감소시키는 기술로 라운딩, 랜덤 라운딩 등 특정한 값을 상위 속성으로 대체하는 기술
무작위 기술	데이터의 노이즈를 삽입하는 등 속성값을 수정하여 추론의 효율을 낮추는 비식별화 기술
재현 데이터	기존 데이터로부터 인위적으로 새로운 데이터를 재현하는 기술. 원본 데이터와 너무 가깝게 재현될 경우 원본 데이터의 유출 위험이 있음

2. 비식별화 관련 표준

가. ISO/IEC 20889

ISO/IEC 20889는 2018년에 제정된 표준으로 해당 표준은 비식별화 기법을 분류하고 재식별화의 위험을 낮추기 위한 기술 및 기술의 적용 가능성을 포함한 특성을 설명하는 것을 목적으로 한다[4]. 해당 표준에서 비식별화된 데이터를 재식별화하는 공격기법에 대해 표 1과 같이 정의한다.

표 1의 공격기법과 함께 공격자는 다음과 같이 상황에 따라 재식별 접근방식을 조합하여 사용한다.

- singling out: 데이터 주체에서 특성 집합을 관찰하여 데이터 주체에 속하는 일부 또는 모든 레코드를 식별
- linking: 동일한 데이터 주체 또는 데이터 주체 그룹에 관한 레코드를 개별 데이터 세트에 연결
- inference: 다른 속성 집합의 값을 이용하여 특정 정보의 속성을 추론

이러한 재식별 공격을 막기 위해 ISO/IEC 20889는 비식별화 기술, 정형화된 프라이버시 측정 모델, 비식별화 기술을 적용하기 위한 원칙 등을 다룬다. 그 중 비식별화 기술 분류는 8개로 표 2와 같다.

ISO/IEC 20889는 구조화된 데이터 집합을 식별을 위해 일반적으로 사용되는 기법에 초점이 맞추어져 있다. 따라서 자유형 텍스트, 이미지, 오디오나 비디오를 포함하는 복잡한 데이터 집합에서는 적용이 어려울 수 있다.

나. NISTIR 8053

NISTIR 8053은 NIST에서 발간한 보고서로 구조화된 정보의 비식별처리 및 재식별 접근법과 구조화되지 않은 정보의 비식별처리에 관한 챌린지를 다루고 있다[5]. 해당 보고서에서 다루고 있는 구조화되지 않은 정보는 의료 문서, 사진과 비디오, 의료 영상, 유전정보, 지리정보 및 지도정보에 대

해 설명한다.

의료 문서에는 구조화되지 않은 정보들이 다수 포함되어 있다. 주로 평서문으로 이루어진 데이터들이 포함되는데, 성명과 주소 등의 식별자를 모호하게 표현하거나 에디슨 병, 벨 마비, 라이터 증후근 등 병명을 개인정보로 오인하여 삭제할 가능성이 있다. 또한, HIPAA(Health Insurance Portability and Accountability Act) 세이프하버 요소를 제거한 후에도 의료 주체를 식별할 가능성이 있다. HIPAA 세이프하버 요소는 개인을 식별할 수 있는 18가지 요소로 성명, 주소, 전화번호, 계좌번호, 생체인증 식별자, 증명사진 등을 포함한다. 의료 문서의 비식별화는 주로 HIPAA 세이프하버 요소를 제거하는 방식으로 진행되었는데, Meystre 등이 수행한 연구에서 2013년 솔트레이크시티 VHA 의료 센터의 퇴원 정보를 비식별화를 수행한 결과 주치의나 치료 전문가를 식별할 수 없었다. 해당 연구에서 사용된 비식별화 방법은 가명화 기법으로 환자명이나 주소를 유명인이나 유명장소로 치환하여 사용하였다. 이러한 방법은 재식별화의 위험성을 경감시킬 수는 있으나 다른 정보와 연결하여 재식별화 가능성은 여전히 존재한다.

사진과 비디오 정보는 GPS, 촬영정보와 같은 정보들이 데이터 헤더에 메타데이터 형태로 존재할 수 있다. 그러나 이러한 메타데이터가 아닌 바이너리 형태로도 식별데이터가 존재할 수 있으며, 콘텐츠 자체에도 개인을 식별할 수 있는 정보들이 많이 포함될 수 있다. 따라서 사진과 영상 데이터를 비식별화하기 위해 식별자 분류체계를 다음과 같이 정의한다.

- 생체인식: 얼굴, 홍채, 지문과 같이 영구적이고 개인을 식별하는 데 사용할 수 있는 생리학적 식별자와 음성, 걸음과 같은 행동학적 생체인증 식별자
- 소프트 생체인식: 점, 연령, 성별, 인종과 같은 개인의 식별하진 않지만, 부수적인 생체인증 식별자
- 비생체인식: 문체, 어조, 복장, 머리 모양 등

콘텐츠의 비식별화는 음성 변조나 사진을 흐리게 하는 형태로 진행되었다. 대규모 콘텐츠 데이터를 이러한 방식으로 비식별화했을 때 식별 정밀도와 정확성에 문제가 여전히 남아 있다. 또한 모자이크 및 블러 이미지 복구, 얼굴 이외에 정보(복장, 자세 등)를 이용한 개인식별 등의 재식별 위험성이 있으며 비식별화된 콘텐츠 데이터의 사실 왜곡 등의 문제점이 있을 수 있다.

의료 영상은 DICOM(Digital Imaging and Communication in Medicine) 양식으로 헤더에 메타정보와 픽셀 형태로 저장된다. 따라서 메타정보는 직접적으로 환자의 이름과 같은 식별자 혹은 준식별자가 포함될 수 있으며, 픽셀에는 시각적으로 개인을 식별할 수 있는 생체인식정보가 포함될 수 있다. DICOM 표준안에는 비식별처리에 관한 사항이 포함되지 않지만 활용가치가 없는 MRI 데이터를 삭제하는 연구가 진행 중이며, DICOM을 비식별화하기 위한 오픈소스 프로젝트가 진행되었었다.

유전정보는 본인의 정보뿐만 아니라 유전이 되는 대상의 모든 정보도 식별이 가능하기 때문에 민감도가 높은 정보이다. 유전자 정보의 효율적인 비식별화 처리는 뚜렷한 성과가 없는 실정이다.

지리정보와 지도정보는 일반화와 Perturbation을 이용한다. Perturbation은 실제 거리에 오차를 둠으로써 위치 정보를 비식별화하는 방법이다. Perturbation은 실제로 물체가 존재하면 되지 않는 위치로 움직일 수 있다. 예를 들어, 식당이 물속에 위치하게 되는 상식 범위 밖에 결과가 발생할 수 있다. 일반화의 경우도 관측정보와 다른 일반화 영역에

서 사용되거나 여러 관측지가 연관되어 있을 때 재식별화의 위험성이 커질 수 있다.

III. 프라이버시 보호 기술 동향

1. 프라이버시 모델

프라이버시 모델은 비암호화 기반 비식별화 기술로 데이터의 프라이버시를 보호하기 위해 사용하는 대표적인 모델이다. k-익명성, l-다양성, t-근접성 모델이 있다.

k-익명성은 식별자 및 준식별자를 일반화했을 때 동일한 레코드가 k개 이상 존재하게 하여 프라이버시를 보호하는 방식이다. 예를 들어, 표 3과 같이 k=3이 적용된 비식별화된 데이터 집합에서 식별자 정보를 사전에 알고 있으면 3명 중 1명으로 유추할 수 있지만, 특정인을 정확히 유추할 수는 없다. 하지만 표 3의 여성의 경우 식별자 정보를 알고 있으면 모든 등급이 B이므로 해당 식별자를 가지고 있는 사람이 B 등급을 가진 것을 유추해낼 수 있다. 이처럼 k-익명성은 한 속성값이 모두 동일할 경우 재식별의 위험이 커진다.

이를 보완하기 위해 l-다양성이 사용된다. l-다양성은 유일한 속성을 제거하거나 세분화하는 등의 조치를 통하여 l개의 민감 정보를 가지도록 한다. 예를 들어 표 3의 점수값을 A, B와 같은 등급이 아닌 점수 형태로 세분화하여 동일 속성값을 없애거나 아예 해당 속성을 없애는 조치를 할 수 있다.

표 3 k=3이 적용된 비식별화 데이터

구분	성별	이름	연령	점수	학과
1	남	김##	〈30	A	국문
2	남	김##	〈30	B	체육
3	남	김##	〈30	A	물리
4	여	나##	〈25	B	기계
5	여	나##	〈25	B	컴퓨터
6	여	나##	〈25	B	전자

표 4 l-다양성이 적용된 비식별화 데이터

구분	성별	이름	연령	점수	학과
1	남	김##	〈30	92.1	국문
2	남	김##	〈30	87.2	체육
3	남	김##	〈30	91.1	물리
4	여	나##	〈25	86.2	기계
5	여	나##	〈25	85.3	컴퓨터
6	여	나##	〈25	86.6	전자

l-다양성을 충족하더라도 민감한 정보가 몰려 있을 경우 프라이버시 유출의 위험이 있을 수 있다. 표 4의 경우 l-다양성을 충족하지만 4, 5, 6번 레코드를 보면 학과는 다르지만, 공과대학 소속이란 것을 확인할 수 있다. 또 한 나이가 25세 이하인 경우 점수가 30세 이하보다 낮다는 것을 유추할 수 있다. 따라서 표 5와 같이 수정하여 데이터 분포를 높여 쏠림 및 유사성 공격을 방지한다.

k-익명성과 l-다양성 모델만으로는 민감 속성 기반의 공격에 여전히 취약하다. k-익명성을 더 강화하기 위한 모델로 m-유일성 모델이 제시되어 있다[6].

2. 암호 기반 프라이버시 보호 기술

프라이버시 모델을 통한 데이터 비식별화는 비식별화 조치 이후에 새롭게 생성된 데이터와의 결

표 5 t-근접성이 적용된 비식별화 데이터

구분	성별	이름	연령	점수	학과
6	여	나##	〈25	86.6	전자
1	남	김##	〈30	92.1	국문
5	여	나##	〈25	85.3	컴퓨터
2	남	김##	〈30	87.2	체육
4	여	나##	〈25	86.2	기계
3	남	김##	〈30	91.1	물리

합으로 식별이 될 수 있는 위험이 여전히 존재한다. 따라서 더 강력한 비식별화를 위해 앞서 언급한 ISO/IEC 20889의 암호화 도구들이 필요하다. 이 절에서는 데이터 비식별화에 활용 가능한 암호 기술들에 대해 알아본다.

가. 형태보존암호

형태보존암호(FPE: Format-Preserving Encryption)는 경량암호의 일종으로 입력과 출력이 동일한 형태로 나오는 암호알고리즘이다. 그림 1과 같이 카드 번호를 AES와 같은 블록 암호로 암호화할 경우 입력값의 길이와 형태가 다르다. 하지만 형태보존암호의 경우 입력값과 길이와 형태가 동일하게 보존된다.

블록기반의 암호 알고리즘은 지정된 블록 사이즈만큼 출력 결과가 생성된다. 즉, 그림 1과 같이 AES로 암호화할 경우 원래 평문 크기보다 암호문의 크기가 커질 수 있다. 반면 형태보존 암호는 평문과 암호문의 길이와 속성이 동일하므로 데이터베이스에 저장된 데이터를 암호화해도 저장공간이 늘어나지 않으며 데이터 레코드의 속성을 변경할 필요가 없다. 하지만 형태보존암호는 평문의 길이가 짧으면 안전성에 문제가 있을 수 있다. 이를 보완하기 위해 형태보존암호는 Tweak을 사용한다. Tweak은 비밀정보가 아닌 일종의 부가 정보로 Tweak을 조절함으로써 동일한 평문에 다른 암호문 생성하게 하여 평문을 유추하는 것을 어렵게 한다.

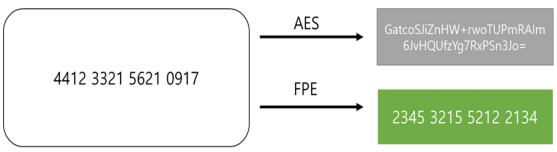
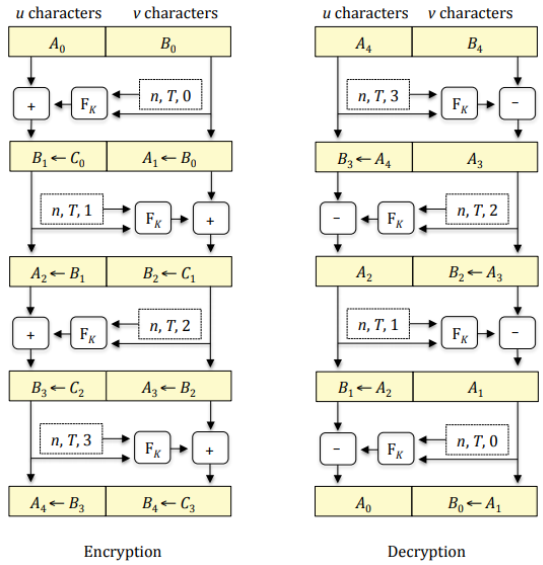


그림 1 **형태보존 암호의 예**

형태보존암호는 NIST에서는 형태보존암호에 대한 표준을 진행하였다. 그 결과 M. Bellare 등이 제안한 FFX[Radix]와 E. Brier등이 제안한 BPS-BC가 FF1, FF3으로 선정되었다[7].

FF1과 FF3는 Feistel 구조를 기반으로 하고 있다. Feistel 구조는 그림 2와 같이 암복화가 진행된다. 먼저 메시지를 A_0와 B_0로 분할한다. 키가 K인 라운드 함수 F_K 함수에 B_0와 전체 비트 길이 n, Teakw 값 T, 라운드값 0을 입력으로 하여 생성된 출력값을 A_0와 모듈러 덧셈을 진행하여 C_0을 생성한다. 다음 라운드에서 C_0를 B_1으로 정의하고 B_0를 A_1으로 정의하여 앞서 진행했던 연산을 반복한다. 복호화도 비슷하게 진행되나 라운드 지수가 역전되고 모듈러 덧셈이 뺄셈으로 대체되며 B_n가 아닌 A_n부터 라운드 함수에 입력값으로 넣는다. FF1는 10개의 라운드를 반복하고 FF3는 8개의 라운드를 반복한다. 형태보존암호의 블록 사이즈가 작을 경우



출처 NIST, "Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption," 2019.

그림 2 **Feistel 구조[7]**

코드북 공격에 취약하다. 코드북 공격은 평문을 미리 암호화하여 암호문을 대응시키는 표를 이용하여 평문을 찾는 공격이다. FF3의 경우 코드북 공격에 취약한 것이 알려져[8] 이를 개정한 FF3-1이 NIST800-38G Rev.1을 통해 표준화가 진행되고 있다.

나. 순서보존암호

기존 블록암호 알고리즘으로 암호문을 생성할 경우 평문대비 암호문의 크기와 형태가 달라지기 때문에 크기 비교를 위해서는 반드시 복호화가 필요하다. 또한 운용 중인 데이터베이스에 있는 데이터를 암호화할 경우 기존의 생성한 인덱스를 사용할 수 없기 때문에 인덱스 생성에 대한 비용이 발생한다. 따라서 암호문 상태에서 크기를 비교하거나 암호화 생성 이후에도 기존의 데이터베이스에서 생성한 인덱스를 활용할 수 있는 암호 알고리즘이 필요성이 대두되었다. 순서보존암호(OPE: Order Preserving Encryption)는 이러한 요구사항을 충족하기 위해 제안되었다. 대표적인 순서보존암호 알고리즘으론 Programmable Order-Preserving secure Index Scheme(POPIS)가 있다. POSIS는 단조증가 함수 기반의 암호 알고리즘으로 다음과 같은 수식으로 이루어져 있다[9].

$$E(x) = a * x + b + noise$$

noise는 순서를 유지하면서 암호문을 유추할 수 없도록 하기 위해 0에서 a까지 범위에서 추출된 임의의 값을 사용한다. 예를 들어 a와 b가 각각 2와 7이고 x가 1, 2일 때, $E(1) = 2*1 + 7 + noise$ 와 $E(2) = 2*2 + 7 + noise$가 되며 $E(1)$의 값의 범위는 9부터 11, $E(2)$ 값의 범위는 11부터 13이기 때문에 $E(2) > E(1)$ 이 성립하게 된다. 이러한 특성으로 인해 순서보존암호를 이용하여 암호화된 데이터베이스에서는 평문상태에서의 인덱스를 그대로 사용하거나 복호화 없이 매칭이나 질의가 가능하다. 그러나 암호문으로부터 순서 정보를 알아낼 수 있기 때문에 평문을 알 경우 1:1로 암호문과 매치되므로 원본 데이터의 유출 위험이 발생하게 된다. 또한 공격자가 평문과 평문의 빈도수를 알게 되면 평문과 매칭되는 테이블을 유추할 수 있다. 따라서 순서보존암호 알고리즘도 단독으로 사용되는 것보다는 취약점을 보완해 주는 다른 보안장치와 함께 사용되어야 한다.

다. 동형암호

기존 암호 알고리즘은 적용한 데이터에서 암호문 간에 연산을 진행하기 위해서는 반드시 복호화를 진행한 뒤에 연산을 진행해야 한다. 따라서 개인정보와 같은 민감한 데이터를 다룰 때는 복호화로 인한 데이터 유출의 위험성이 발생하게 된다. 이러한 위험성을 줄이기 위해 복호화 키 없이도 암호문 간에 연산, 탐색, 분석 등의 작업을 수행할 수 있는 암호 알고리즘의 필요성이 발생하였다. 4세대 암호 기술인 동형암호(HE: Homomorphic Encryption) 알고리즘은 이러한 요구사항을 충족시키기 위해 설계되었다. 동형암호는 복호화한 뒤에 연산하여 암호화한 결과물과 암호화된 상태에서 연산한 결과물의 형태가 동일하다는 의미로 동형이라 명명한다.

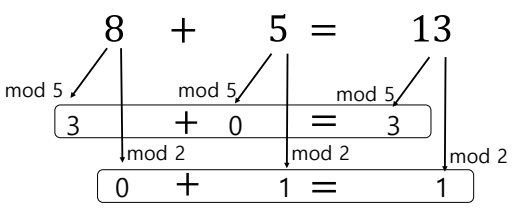


그림 3 동형암호 덧셈의 예

동형암호의 덧셈은 다음 식과 같이 암호화된 m_1, m_2를 더한 값이 $m_1 + m_2$을 암호화한 값과 동일하며, 이 과정에서 암호화 키가 사용되지 않는다.

$$E(m_1 + m_2) = E(m_1) + E(m_2)$$

동형암호 덧셈이 진행되는 과정의 예를 살펴보면 그림 3과 같이 진행된다. 8을 5,2로 mod 연산하여 (3,0)과 5를 5,2로 mod 연산한 (0,1)을 구한다. 결과값 중 첫 번째 값 3과 0을 더하고 두 번째 값 0과 1을 더해서 (3,1)를 얻는다. 8과 5를 더한 13의 5,2 mod 한 값이 (3,1) 이므로 mod를 이용하여 암호화한 값을 더한 값이 평문을 연산한 값을 암호화한 결과와 동일하다는 것을 확인할 수 있다. 예시로 든 덧셈뿐만 아니라 곱셈, AND, XOR 등의 모든 논리 연산을 지원하는 동형암호를 완전동형암호라고 한다.

현재 알려진 동형암호 알고리즘으로는 IBM에서 개발하고 있는 HELib, 마이크로소프트의 SEAL, 서울대학교의 HEAAN이 있다.

HELib는 IBM에서 개발하고 있는 동형암호 라이브러리이다. 오픈소스이며 C++ 기반으로 구현되어 있다. HELib는 멀티 쓰레딩을 지원하고 있으며 비트 shift, 덧셈, 곱셈 등의 저수준의 연산 기능을 지원하며 Smart–Vercauteren 기반의 암호문 압축 기능을 지원한다.

SEAL는 마이크로소프트에서 개발한 동형암호 라이브러리로 오픈소스이며 C++기반으로 구현되어 있다. SEAL 비주얼스튜디오에서 사용 가능한 라이브러리 형태로 제공되며 소스코드가 모두 공개되어 있다. 마이크로소프트는 클라우드 환경 및 딥러닝 환경에서 활용할 수 있도록 SEAL을 지원하고 있으며, 실제로 2016년 CryptoNet이라 불리는 신경망 네트워크에 MNIST 데이터셋을 SEAL로 암호화한 데이터를 학습시켜 정확도를 99%까지 달성하였다[10]. SEAL은 가장 널리 활용되고 있는 기계학습 라이브러리인 텐서플로우에서도 활용이 가능하고 현재 CPU만 지원하며 GPU 지원도 예정되어 있다.

HEAAN은 서울대학교 천정희 교수팀이 개발한 동형암호 오픈소스 라이브러리이다. 앞서 언급한 다른 동형암호 라이브러리와 동일하게 C++로 구현되어 있다. HEAAN은 근사연산 동형암호로 계산결과에 영향을 미치지 않는 소수점 아래값을 버리는 근산 연산을 통해 동형암호의 연산속도를 개선한 알고리즘이다[11]. 따라서 모든 연산을 지원하는 완전동형암호와는 달리 준동형암호 알고리즘에 속한다. 완전동형암호는 암호문 연산의 효율이 평문 연산의 효율보다 많이 떨어진다. HEAAN은 특정 연산에만 효율을 최적화하여 활용성을 높였다.

표 6은 공개키 알고리즘과 동형암호의 성능을 비교한 것이다[12]. 공개키 알고리즘은 암호화 성능이 동형암호 성능보다 뛰어나지만 복호화 성능

표 6 공개키 암호와 동형암호의 성능 비교[12]

	공개키 크기	암호문 크기	평문 크기	암호화 시간	복호화 시간	덧셈 시간	곱셈 시간	허용 Depth	안전성
RSA	2,048bit	2,048bit	–	6.1ms	205.5ms	–	–	–	–
ECC	193bit	80B	–	8.7ms	18.1ms	–	–	–	–
Helib	343KB	105KB	≤ 1KB	17ms	6ms	0.6ms	54.3ms	6	128bit
SEAL 2.4V	2,000KB	224KB	≤ 1KB	5.9ms	1.6ms	0.2ms	24ms	9	128bit
HEAAN	80KB	96KB	16KB	43ms	12ms	5ms	100ms	6	128bit

은 동형암호가 공개키 알고리즘보다 약간 빠르다. 동형암호의 성능 개선을 위해 많은 연구들이 진행되고 있다. 실제로 동형암호의 부트스트랩에 걸리는 시간이 2011년에는 1bit에 1,800초가 걸렸지만 HEAAN의 경우 현재 0.05초로 개선되었다.

Ⅳ. 결론

본 고에서는 활용성 강화 데이터 프라이버시 보호 기술과 관련된 표준화 동향과 비암호화 기반의 데이터 비식별화 기술 및 암호화 기반의 데이터 비식별화에 대해 알아보았다. 비암호화 기반 데이터 비식별화 기술은 암호화 기반의 비식별화 기술보다 활용성이 높지만, 비식별화된 데이터에 대한 식별화의 위험이 암호화 기반의 비식별화 기술을 적용한 데이터들보다 높은 편이다. 반면 암호화 기반의 비식별화 기술은 높은 안전성을 가지고 있지만, 비암호화 기반의 비식별화 기술들보다 현재는 효율성 및 활용성이 낮다.

개인정보는 경제성이 높아지고 활용범위가 넓어질 것으로 예상되는 만큼 개인정보 유출에 따른 위험성과 피해가 커질 가능성이 높다. 따라서 과거에는 개인정보를 안전하게 보관 및 관리하는 형태로 연구가 진행된다면 향후에는 개인정보의 활용성이 커지면서 안전뿐만 아니라 활용성을 높이기 위한 연구들이 진행되어야 한다. 비암호화 기반 및 암호화 기반 비식별화 기술들의 현재 해결해야 하는 과제가 많이 남아 있는 만큼 꾸준한 연구가 필요하다.

용어해설

DICOM 의료용 디지털 영상 및 통신 표준

Re-identification Attack 비식별화된 정보를 재식별화하는 공격 기법

약어 정리

DICOM	Digital Imaging and Communication in Medicine
FPE	Format-Preserving Encryption
HE	Homomorphic Encryption
HEAAN	Homomorphic Encryption for Arithmetic of Approximate Numbers
HIPAA	Health Insurance Portability and Accountability Act
OPE	Order Preserving Encryption
POPIS	Programmable Order-Preserving secure Index Scheme
SEAL	Simple Encrypted Arithmetic Library

참고문헌

[1] 국무조정실 외, "개인정보 비식별 조치 가이드라인," 2018.

[2] A. Naranyanan et al., "Robust De-anonymization of Large Datasets," arXiv preprint, CoRR, 2016, arXiv: cs/0610105.

[3] M. Gymrek et al., "Identifying Personal Genomes by Surname Inference," Science, vol. 339, Issue 6117, 2013, pp. 321-324.

[4] ISO/IEC 20889:2018, "Privacy enhancing data de-identification terminology and classification of technique," 2018.

[5] NIST, "De-Identification of Personal Information," 2015.

[6] 이원석, "익명화 데이터의 익명 결합 방법," 전자금융과 금융보호 제15호, 2019, pp. 86-102.

[7] NIST, "Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption," 2019.

[8] 송정환, "형태보존암호는 필요한가?" ICT Standard Weekly 제929호, 2019.

[9] 이현조, 장재우, "암호화 데이터상에서 효율적인 질의처리를 위한 주기함수 기반 그룹순서 보존 암호화 기법," 정보과학회논문지, 데이터베이스, 제41호 제3권, 2014. 6, pp. 145-154.

[10] N. Dowlin et al., "CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy," Microsoft Research, 2016.

[11] J. H. Cheon et al., "Homomorphic Encryption for Arithmetic of Approximate Numbers," ASIACRYPT, 2017.

[12] 천정희, 어윤희, 김재윤, "개인정보가 보호되는 동형암호기반 금융데이터분석," 금융정보연구 제7권 제1호, 2018, pp. 33-60.