오클: 완전동형암호화(FHE)와 신뢰실행환경(TEE) 기반의 다자연산(Multi-party Computation) 프로토콜

고하준, 이수민, 오재기
주식회사 LG 전자

hajoon.ko@lge.com, sumin.lee@lge.com, jaeky.lee@lge.com

OKL: Efficient Multi-party Data Computation Protocol based on Fully Homomorphic Encryption and Trusted Execution Environment

Hajoon Ko, Sumin Lee, Jaeky Lee
LG Electronics Inc.

요 약

본 논문은 다자 TEE 통신을 기반으로 동형암호키를 생성하고 관리하는 OKL 프로토콜을 제시한다. 본 프로토콜은 TEE, 동형암호화, 다자연산 기술을 복합적으로 사용하는 것을 특징으로 하며, 기존의 다자연산에만 기반한 기술들보다 더욱 통신 효율적이면서도 동등한 보안성을 유지하는 것을 특징으로 한다.

Ⅰ. 서 론

다자연산(Multi-party Computation) 기술은 서로 다른 데이터 소유 주체들이 서로에게 데이터 공개를 하지 않으면서 서로의 데이터들을 입력값으로 필요로 하는 공통된 연산을 협력하여 연산함으로써 결과값을 도출하는 보안 프로토콜이다. 다자연산은 통계, 머신러닝 학습, 추론 등의 다양한 응용분야에서 사용되고 있다. 한편, 다자연산 기술의 실사용에 있어서 가장 큰 난관은 통신과부하이다. 다자연산에서는 모든 연산을 덧셈/곱셈의 형태로 변환해야 하며, 각 곱셈마다 프로토콜 참여자들간의 RTT 를 필요로 하기 때문이다. 다자연산의 통신과부하 문제에 대한 대체기술로서 완전동형암호화 기술이 대두되는데, 이는 데이터가 암호화된 상태에서 덧셈, 곱셈 연산을 무제한으로 가능하게 해주는 암호기법이다. 하지만 동형암호 기술의 문제 중 하나는 동형연산에 사용되는 데이터들이 동일한 동형암호키로 암호되어야 한다는 것인데, 따라서 데이터 주체가 다른 경우, 동형연산을 위하여 키전환키(Key-switching key)를 사용하여 서로 다른 키들을 동일하게 일치시켜주어야 하는데, 이러한 키전환키를 생성하는 주체가 단일실패점(single-point failure)이 될 수 있다는 보안성 문제가 있다. 키전환키를 신뢰실행환경(Trusted Execution Environment)에서 관리할 수 있지만, TEE 는 다양한 곁채널공격(side-channel attack)들에 취약하다.

위와 같은 문제들을 해결하기 위하여 본 논문에서는 다자 TEE 기반의 동형암호키 생성 및 관리를 통하여 안전하고 통신 효율적인 OKL 프로토콜을 제안한다. 본 프로토콜은 기존의 다자연산 기반의 프로토콜들과 다르게 통신량이 목표 연산식의 복잡도에 영향을 받지 않으며, 따라서 연산의 통신효율성이 높으면서도 연산의 결과값 이외에 어떠한 중간값도 연산 참여자들에게 직접 노출하지 않는다는 동등한 보안 목표를 달성한다.

Ⅱ. 배경

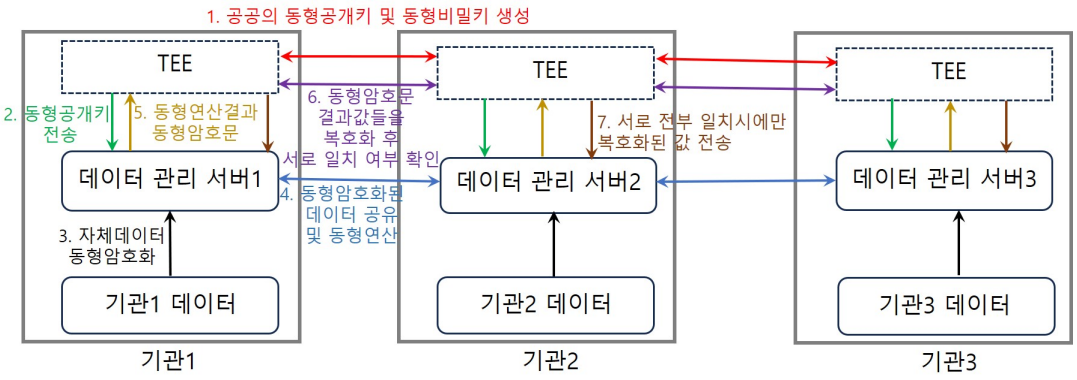
TEE[1]는 프로세서가 민감한 데이터와 연산에 대하여 접근하지 못하도록 격리하는 안전한 연산 영역이다. 보안에 핵심적인 연산을 외부와 차단된 모듈 안에서 수행함으로써, 운영체제가 전복되더라도 데이터의 무결성과 기밀성을 유지할 수 있다.

완전동형암호는 암호화된 데이터를 복호화하지 않고도 직접 연산이 가능하도록 하여, 원본 데이터의 기밀성을 유지한다. 따라서 제 3 자 또는 제 3 서버가 민감한 데이터를 처리하더라도 그 내용이 노출되지 않는다.

Ⅲ. 본론

Ⅲ-가. 위협 모델

OKL 프로토콜은 N 개의 데이터소유 개체들의 통신으로 이루어져 있으며, 각 개체는 데이터관리 서버와 TEE(예: SGX, Trusted Zone) 모듈로 이루어져 있다. TEE 모듈은 신뢰받는 주체들이며, 데이터관리 서버는 신뢰를 받지 못하며 (차후 설명), 그 외부의 모든 개체들은 전혀 신뢰받지 못한다. 외부 개체들간의 통신은 서버들간의 일반통신과 TEE 들간의 TEE 통신으로 구분되며, 두 종류의 통신 모두 종단간 암호화된다. 일반통신은 외부 모든 개체들에 의한 데이터 유출/변조를 막으며, TEE 통신은 외부 개체들 및 데이터 관리 서버들에 대해서도 데이터 유출/변조를 막는다. OKL 프로토콜의 목표는 여러 데이터 소유 서버들이 서로의 데이터들을 모두 합쳐서 공공의 연산을 수행하도록 해주되 (예: 전체 데이터들의 평균값 같은 통계수식 연산 또는 머신러닝 학습/추론과 같은 복잡한 수식 연산), 이 과정에서 각 데이터 소유자가 자신의 소유가 아닌 외부 서버들 소유의 데이터들에 대한 정보를 얻을 수 없도록 막는 것이다. 특히, 각 데이터 소유자가 획득하는 유일한 값은 공공의 연산에 대한 최종 연산 결과값이다. 서버들은 자신이 소유한 데이터에 대해선 위변조 없이 정직하게 동형암호화한 후 다른 서버들에게 공유한다고 가정하며, 한편 다른 서버들로부터 받은 동형암호화된 데이터에 대해선 그것을 자신의 TEE 모듈에게 전달하는 과정에서 모든 종류의 위변조 공격 및 기밀성 유출 공격을 감행할 수 있다. 또한 각 서버는 다른 서버들과 공모할 수 있으며, 단 하나의 서버라도 공모에 참여하지 않으면 본 프로토콜은 데이터의 유출/위변조로부터 안전하다.



Ⅲ-나. OKL 프로토콜

도 1 은 OKL 프로토콜을 도식화하며, 총 7 단계로 구성되어 있다.

(1) 프로토콜에 참여하는 모든 데이터소유자들의 TEE 모듈들이 서로 다자 통신을 하여 합의를 통하여 공통된 동형암호 공개키와 비밀키를 생성한다. 이 합의는 각 TEE 모듈이 생성한 난수들의 도합을 seed 값으로 취급하여 MPC 를 사용하여 동형암호키쌍을 생성한다. 연산의 결과는 동형공개키(암호화키, 부트스트래핑키, 재선형키, Galois 키 포함)와 조각난 동형비밀키 share 들이며, 각 TEE 모듈은 온전한 동형공개키 및 동형비밀키 share(조각) 하나씩을 소유한다.

(2) 각 TEE 모듈은 동형공개키만 자신이 속한 머신의 데이터 관리 서버에게 공유한다. 따라서 각 서버는 동형공개키에만 접근이 가능하며, 동형비밀키 또는 그 share 에는 접근이 불가하다.

(3) 각 서버는 자신이 관리하는 데이터들 중에서 본 프로토콜에서 사용될 데이터들을 동형공개키로 암호화한다.

(4) 이전 단계에서 생성된 동형암호화된 데이터들을 본 프로토콜에 참여하는 다른 모든 데이터 서버들과 다자 통신을 기반으로 공유한다. 따라서 각 서버는 본 프로토콜에 참여하는 모든 서버들의 데이터를 동형암호화된 형태로 가지게 되며, 이중에서 서버 자신이 암호화한 데이터 이외의 외부 데이터에 대해선 어떤 값인지 알 수 없다. 한편, 서버들이 서로에게 동형암호화된 데이터를 전송할 때에는 해당 동형암호문을 종단간 암호화 프로토콜(예: TLS)을 사용하여 암호화하는데, 그 이유는 동형암호문은 데이터의 기밀성만 보호할 뿐 위변조성은 검증할 수 있는 방법이 없기 때문이다. 이 문제를 해결하기 위하여 동형암호문을 TLS 로 전송하면 도중에 데이터의 위변조가 일어나더라도 TLS 통신 단계에서 이를 간파함으로써 위변조된 데이터에 대한 당혹스러운 동형연산 프로세싱을 방지할 수 있다.

(5) 각 서버는 자신이 전송받은 모든 서버들의 동형암호화된 데이터들을 기반으로 동형연산을 수행한다. 이 동형연산은 덧셈, 곱셈, 슬롯회전, 부트스트래핑의 연산들로 이루어져 있으며, 전체 동형연산이 끝날 때까지 다른 서버들과의 중간 통신이 필요 없다. 한편, 이 동형연산식은 모든 서버들이 동일하게 수행하는 공통된 연산식이다. 각 서버는 동형연산을 모두 완료한 후, 자신이 도출한 결과값 동형암호문을 자신의 TEE 모듈에게 전송한다.

(6) 각 TEE 모듈은 연산 결과값을 다른 모든 TEE 모듈들과 통신하며 동형비밀키 share 들을 기반으로 MPC 연산으로 복호화를 수행함으로써 동형암호문을 복호화하고, 해당 결과값이 다른 모든 TEE 모듈들의 복호화된 값들과 일치하는지 확인한다.

(7) 각 TEE 모듈은 동형연산의 결과값이 서로 모두 일치함이 확인되는 경우에만 자신의 데이터 관리 서버에게 결과값을 전송한다.

Ⅲ-다. 보안성 분석

우선, 본 프로토콜에 참여하는 개체들을 제외한 외부 개체들에 의한 모든 데이터 위변조는 TEE 모듈들과 서버들의 종단간 암호화 통신(예: TLS)에 의하여 원천 차단된다. 더 나아가서, 만일 특정 서버가 악의적 의도를 가지고 자신이 전송받은 다른 서버의 데이터를 암호화한 동형암호문을 위변조한다면, 해당 위변조된 데이터를 기반한 동형연산 결과값은 6 번 단계에서 TEE 모듈이 복호화하고 검증하는 단계에서 다른 TEE 모듈들의 복호화된 값들과 다름을 간파하게 되므로 동형암호문에 대한 데이터 위변조가 발각된다. 만일 다수의 서버들이 공모하여 동일한 방식으로 동형암호문을 위변조하더라도, 본 프로토콜에 참여하는 모든 서버들 중에서 단 하나의 서버라도 데이터 위변조 공모에 참여하지 않는다면, 해당 서버의 TEE 모듈에 의하여 다른 모든 TEE 모듈들도 데이터 위변조 사실을 간파하게 된다. 또한 각 서버는 연산의 최종결과값만 알 수 있을 뿐, 중간값에 대하여 접근할 수 없으며, 그 이유는 TEE 모듈이 최종 연산 결과값만 복호화하여 전송해주기 때문이다. 또한 한 TEE 모듈이 곁채널공격에 노출되더라도 온전한 동형비밀키를 노출하지 않으며, 왜냐면 동형비밀키는 각 TEE 모듈마다 하나의 share 만을 소유하기 때문이다.

한편, 서버들은 최종 연산 결과값을 기반하여 입력 데이터들에 대한 역 유추 공격은 시도할 수 있는데, 해당 유추는 중간 동형암호 연산에 사용되는 데이터 개수(연산의 변수 개수에 해당) 및 연산의 복잡도에 따라서 유추의 성공 여부가 결정된다. 이러한 데이터 입력값 역 유추는 본 프로토콜의 보안성 보장 범위를 벗어나는 문제로 간주한다.

Ⅳ. 결론

본 논문에서는 다자 TEE 를 기반으로 동형암호키를 생성하고 관리함으로써 기밀 데이터 기반의 연산을 안전하고 통신 효율적으로 수행하는 OKL 프로토콜을 제안한다. 이로써 기존 다자연산 기술들의 통신과부하 문제의 해결책을 제시한다.

참 고 문 헌

[1] Antonio Muñoz, Ruben Ríos, Rodrigo Román, Javier López, A survey on the (in)security of trusted execution environments, Computers & Security, Volume 129, 2023, 103180, ISSN 0167-4048