동형암호를 적용한 보안 제어 기술 동향 분석

이윤지[1], 백윤흥[1]
[1]서울대학교 전기정보공학부, 서울대학교 반도체 공동연구소
yjlee@sor.snu.ac.kr, ypaek@snu.ac.kr

Homomorphic Encryption for Securing Cyber Physical Systems: A Survey

Yunji Lee[1], Yunheung Paek[1]
[1]Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center(ISRC), Seoul National University

요 약

동형암호는 암호화된 상태에서도 연산을 수행할 수 있는 암호이다. 양자컴퓨터 시대가 눈앞에 도래한 지금 양자컴퓨터에도 안전한 격자 문제에 기반을 둔 동형암호가 적용될 수 있는 분야는 무궁무진하다. 하지만 동형암호만으로는 프라이버시 즉 기밀성은 보장하지만 무결성이 보장되지 않는다. 따라서 기밀성과 무결성 모두를 보장하라는 요구를 만족시킬 수 있는 개념의 암호체계가 등장했는데 바로 동형 인증 암호이다. 이 논문에서는 동형 인증 암호와 이를 적용할 수 있는 응용 분야 중 하나인 동형 제어 기술에 대해 소개하고, 무선통신을 사용하는 사이버 물리 시스템을 안전하게 제어하기 위해 기존에 적용된 보안 기술과 비교하여 동형 인증 암호를 적용한 사례는 어떤 기대효과를 누릴 수 있는지 살펴본다. 이를 통해 제어기가 해킹되지 않도록 하는 안전성에 중점을 둔 '보안 비용'과 하드웨어 가속, 알고리즘 최적화로 '실시간 제어'가 가능하게 하는 기술의 최적화가 적절한 조화를 이룰 수 있도록 설계하는 연구의 상업적 효과에 대해 탐구한다.

1. 서론

암호(Cryptography)란 송신자와 수신자 간 통신과정에서 인가되지 않은 제 3 자가 대화의 내용을 알아내지 못하도록 수학적 기법을 사용하여 원문을 변형시키는 것을 말한다. 일반적인 암호체계는 송신자가 원문 메시지(평문)를 암호화 키를 통해 암호화시킨 후 이를 전송, 수신자는 전송 받은 암호문을 다시 복호화 키를 통해 복호화 한 평문, 즉 원문 메시지를 획득하게 되고, 필요시 이를 검증할 수 있도록 서명을 삽입하거나, 비밀키(암호화 키 등)를 교환하는 절차로 이루어져 있다.

이 원리를 이용하는 우리가 친숙한 DES, AES 등의 기존 암호체계가 꾸준히 발전해온 한편, 이를 대체할 수 있는 4 세대 암호에 대한 소요도 끊임없이 제기되어 왔는데 그 중 가장 대표적인 것이 Gentry[1]에 의해 2009 년 처음 제안된 '동형암호(HE, Homomorphic Encryption)'라는 최신의 암호체계이다. 동형암호는 우리가 일반적으로 알고 있던 기존의 암호체계와 가장 결정적인 차이가 있다. 그것은 바로 암호문 상태로 연산을 수행한다는 것인데, 이는 아주 명백한 장단점을 가지고 있다. 장점은 물론 우리의 비밀키를 상대방과 공유할 필요가 없어 프라이버시 측면에서는 수요자의 요구를 완벽히 충족할 수 있으나, 암호문의 연산이라는 평문의 연산과는 비교할 수 없는 연산량의 증가를 보여준다는 단점이 있다.

하지만 양자컴퓨터의 개발이 현실화되면서 더 이상 기존의 AES, RSA 등의 암호체계로는 충분히 빠른 것과는 별개로 양자컴퓨터에 대한 안전을 보장할 수 없게 되었다. 따라서 양자컴퓨터에 대해 내성이 있다고 알려진 격자 문제(RLWE 등)에 기반을 둔 동형암호를 표준화하고 성능을 개선하기 위해 많은 후속 연구들이 이루어졌다. 여러 갈래가 있지만 크게 두 갈래로 나눈다면 수학적 알고리즘의 개선을 통해 더 많은 연산을 가능하게 하는 연구와 실시간으로 더 많은 연산을 가능하게 만드는 소프트웨어 최적화 및 하드웨어 가속기 개발 관련 연구이다. 그 중 가장 대표적인 것이 HEAAN[2]이라는 근사계산 동형암호 체계를 소개한 것으로 현재는 개발자의 이름을 따 CKKS 라고 대중적으로 명명되었다. 이를 이용해 Machine Learning 등 근사연산을 사용해 데이터 분석을 수행하는 분야에 동형암호의 적용이 가능해졌다.

이런 동형암호를 산업분야에 응용하기 위한 다양한 노력도 이루어졌다. 앞서 말한 머신 러닝 분야를 포함해 개인정보보호, 동형 제어 기술 등이다. 이 논문에서는 동형암호의 다양한 응용 분야 중 동형 제어 기술에 초점을 맞출 생각이다. 동형 제어 기술이란 동형암호의 원리를 드론, 자율주행 자동차 등 최근 실생활에서 주목받고 있는 실시간 제어 기술의 해킹을 막고 안전하게 무선 통신 시스템을 통제하는 기술을 말한다. 이를 위해서는 동형암호에서 제공하는 기밀성뿐만 아니라 무결성도 충족시켜야 하는데, 이를 가능하게 하기 위한 '동형 인증 암호(HAE, Homomorphic Authenticated Encryption)'를 소개한다. 동형 인증 암호를 통해 제어기(controller)의 해킹 시 발생할 수 있는 원격조종, 정보조작, 위치정보 공개 등의 보안 위협을 막고 시스템 전체를 안전하게 제어할 수 있다.

따라서 본 논문에서는 먼저 동형암호 기술과 동형 인증 암호에 대해 소개하고, 동형암호 기술을 적용할 수 있는 한가지 상용화 사례인 사이버 물리 시스템과 보안 제어 기술 동향에 대해 살펴보겠다. 이를 통해 사이버 물리 시스템에 동형암호 기술이 적용되기 위해 선형 동형 인증 암호를 중심으로 어떻게 기존 연구들이 진행되어 왔는지 소개하고, 향후 동형암호에 대한 활발한 연구가 안전한 실시간 제어 기술에 어떤 반향을 가져올 수 있을지 분석하고자 하였다.

2. 동형암호(HE)와 동형 인증 암호(HAE)

실제로 동형암호 개념에 대한 첫 제안은 1978 년으로 거슬러 올라간다. 하지만 당시에는 평문이 아닌 암호문의 연산도 동형성을 가졌으면 좋겠다는 제안에 그쳤다면, 2009 년 Gentry[1]에 의해 발표된 최초의 동형암호 스킴(scheme)은 암호문의 동형 연산도 충분히 안전(secure)할 수 있다는 것을 처음 보여주었다. 또한 Gentry 는 재부팅(bootstrapping)이라는 기법을 통해 암호문 연산을 무한히 할 수 있게 하는 완전동형암호(FHE, Fully Homomorphic Encryption)를 처음으로 제안하기도 했다. 동형암호의 종류에는 부분동형암호(PHE, Partial Homomorphic Encryption), 제한동형암호(SHE, Somewhat Homomorphic Encryption), 그리고 완전동형암호(FHE)가 있는데 PHE 가 덧셈, 곱셈 연산 중 하나만을 지원한다면 SHE 는 덧셈, 곱셈 모두를 지원하나 제한된 수의 연산만 가능하고, FHE 여야만 재부팅을 통해 연산의 수를 무제한으로 확장할 수 있어 최근 개발되는 대부분의 라이브러리는 FHE 를 지원하는 것을 목표로 한다.

대표적인 FHE 스킴에는 각각의 지원 데이터와 연산에 따라 아래 표와 같이 세 가지로 구분할 수 있다.

[표 1] 대표적인 완전 동형 암호 스킴 종류

	동형암호	평문 데이터	지원 연산	비고
[3] [4]	2012 BGV 2012 B/FV	int 정수	모듈러 연산	패킹 재부팅(선택시)
[5]	2016 TFHE	Boolean data {0, 1}	단일 비트 연산 (XOR)	재부팅(항상)
[2]	2017 CKKS	double 실수(복소수)	근사 연산 (approximate)	패킹 재부팅(선택시)

동형암호, 특히 완전동형암호는 아직 상용화하기에는 기존의 암호체계에 비해 느리지만 효율성을 개선하기 위한 연구(알고리즘 최적화, 하드웨어 가속 등)가 활발하며 최근에는 상업화에 앞서 표준화(standardization) 작업도 진행 중이다.

한편 암호체계가 가장 중요하게 제공하는 기능은 보안의 3 요소 중 기밀성, 무결성과 인증 등을 충족시키는 것이다. 동형암호 자체만으로는 프라이버시, 즉 기밀성만 보장하지만 동형 메시지 인증 코드(MAC), 동형 서명 등의 인증 기술을 결합한 동형 인증 암호를 사용하면 나머지 무결성과 진정성(Authenticity)까지 보장할 수 있다. 즉, 동형암호를 적용한 사이버 물리 시스템(CPS) 모델은 제어 신호 내용의 유출에 대해서는 안전하지만 유출된 신호의 위조 공격에 대해서는 안전성을 보장받지 못하기 때문에 동형 인증 암호를 사용해야 안전한 제어 기술이라는 것이다.

동형 인증 암호(HAE, Homomorphic Authentication Encryption)는 2014 년 [6]에서 처음 제안되었다. 이 이전에도 동형 메시지 인증 코드를 사용한 스킴들이 제안되었으나, 선택 암호문 공격(CCA, Chosen Ciphertext Attack)에 대한 안전성이 입증되지 않은 낮은 보안 수준이었으며, [6]에서 비로소 IND-CPA 와 SUF-CPA(선택 평문 공격에 대한 기밀성과 위조 불가능성), 그리고 IND-CPA 와 SUF-CPA(선택 암호문 공격에 대한 기밀성과 위조 불가능성), 즉 프라이버시와 무결성을 모두 만족하는 HAE 스킴을 제안하였다.

그러나 HAE 는 암호문 크기와 연산의 복잡성에 기반한 비효율성 때문에 실제 사용하기에는 많은 제한이 있었다. 따라서 실제 사이버 물리 시스템에 적용하기 위한 선형 동형 인증 암호(LinHAE, Linear Homomorphic Authenticated Encryption)가 [7]에서 소개되었는데, 암호화 및 평가 절차가 빠른 선형 연산을 지원하는 선형 동형 인증 암호를 제어기에 적용하여 서명과 메시지의 동형 성질을 유지하면서 데이터의 기밀성(프라이버시)와 무결성(위조 불가능성)을 만족하고 동시에 사이버 물리 시스템(드론 등)의 실시간 제어가 가능하도록 설계하는 데 성공하였다.

3. 사이버 물리 시스템과 보안

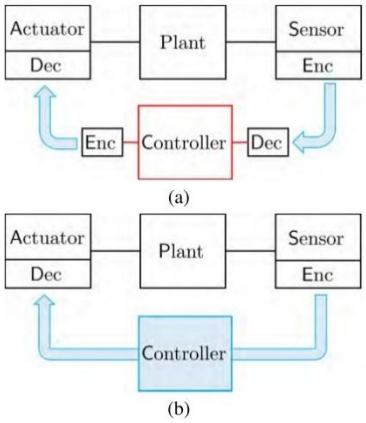
사이버 물리 시스템(CPS, Cyber Physical System)이란 물리적(Physical) 구성요소와 네트워크적 구성요소가 제어기(controller)와 작동기(actuator)를 통해 상호작용하는 시스템을 말한다. 간단하게 생각할 수 있는 드론부터 커넥티드 카(자율주행 자동차), 원전 시스템 그리고 가상 세계에서의 시뮬레이션을 통해 실제 세계에 적용하기 위해 최근에 학계 뿐만 아니라 산업계에서도 많이 사용하고 있는 디지털 트윈(DT, Digital Twin) 등이 모두 넓게는 사이버 물리 시스템에 속한다.

사이버 물리 시스템은 센서, 제어기, 작동기 등 여러 요소들로 구성된 복잡한 특성과 구성요소 간의 유기적인 결합과 소통을 통해 작동하기 때문에 보안을 위협하는 다양한 수준에서의 네트워크 공격이 예상된다. 무엇보다 기존의 사이버 공간이 해킹되거나 보안 위협을 받는다면 이 네트워크를 통해 연결되어 있는 현실의 물리 시스템(스마트폰, 자동차 등의 개인적이고 일상적인 장치부터 원전, 항공 등의 산업 기반 시설에 이르기까지)으로도 확대될 수 있다는 점에서 매우 위협적이다. 이를 방지하기 위해서는 사이버 물리 시스템에 보안 요소가 필수적으로 포함되어야 하는데 일반적으로 보안의 3요소인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)이 해당되며, 각 요소를 기준으로 시스템의 안전성을 침해하는 다양한 사이버 위협이 존재하는데 아래 표에서 자세히 살펴볼 수 있다.

[표 2] [8]에 소개된 사이버 물리 시스템 위협 종류

보안 요소	공격 유형	세부 공격 종류	대표 위협 설명
기밀성	Disclosure 도청 공격	Replay attack Eavesdropping attack Bias injection attack	이전에 정상적으로 전송된 제어명령을 재전송해 시스템이 올바른 명령으로 인식하게 함
무결성	Deception 기만 공격	Covert attack Zero dynamics attack Robust zero dynamics attack	시스템이 공격받고 있는지 알지 못하도록 데이터가 유출되는 동안 시스템의 출력을 정상적으로 보이게 함
가용성	Disruption 중단 공격	Denial-of-service (Dos) Distributed Dos attack	비정상적 접속시도 등으로 시스템의 리소스를 부족하게 하여 원래 의도대로 사용하지 못하게 함

앞서 소개한 암호화 기술을 통해서 우리는 통신 채널을 암호화함으로써 표에 소개된 다양한 공격을 효과적으로 방어하고 공격자가 시스템을 악용하거나 손상시키는 것을 방지할 수 있다. 아래 그림(a)과 같이 제어기는 내부에 비밀 키를 가지고 있으며 센서를 통해 수신한 암호화된 데이터를 비밀 키를 통해 복호화 후 데이터를 처리, 작동기에 전송하기 전에는 다시 암호화하여 전송하는 것이 기본 동작 원리이다.



[그림 1] 제어기 기존 암호기술(a) 동형암호 적용(b) 비교[7]

하지만 이렇게 제어기 내부에 비밀 키를 사용하여 암호화할 경우 제어기가 외부 위협에 노출되는 취약점에 대한 방어가 불가능하다. 따라서 대응 방안으로 동형암호를 사용하여 위의 그림(b)과 같이 센서에서 제어기를 통해 작동기까지 가는 모든 과정을 암호화한다면 공격자의 제어 신호 도청을 방지할 수 있다.

4. 상용화를 위한 동형 인증 암호 최적화 기술

실시간 제어 시스템에 적용하기 위해서는 연산량이 많아 상대적으로 느리다고 평가받는 동형암호(그리고 동형 인증 암호)의 상용화를 위한 최적화 기술이 필요한데, 다시 말해 빠른 연산을 가능하게 하는 연구들이 다각도로 진행되고 있다. 그 대표적인 예로는 [7]에서 소개된 선형 동형 인증 암호(LinHAE)를 포함해서 기존 동형암호에 대한 스케줄링 등 알고리즘 최적화, 동형암호 하드웨어 가속 등이 대표적이다.

먼저 [7]에서 드론 제어기(controller)에 실제로 적용한 LinHAE는 HAE의 서명 및 메시지에 대한 동형 속성은 유지하면서 실시간 제어를 위해 암호문 간의 선형 연산을 지원함으로써 충분히 빠른 암호화, 평가 및 검증 절차를 수행한다. 예를 들어 드론이 특정한 비행 경로를 따라 자율 비행을 실시한다고 가정할 때 공격자는 제어기를 해킹하여 경로 조작 공격을 시도할 수 있다. 이를 막을 수 있는 방법은 LinHAE를 사용해 제어기로 통하는 모든 정보를 암호화하는 것이다. 계획된 비행 경로 정보를 암호화된 상태에서 산술 연산을 수행하게 함으로써 제어기가 암호화된 변

수만으로 동작하게 하고 임의의 공격 신호가 주입될 때 복호화 알고리즘을 통해 명령의 진위를 학인하고 공격이라고 간주 시 임의의 비행 경로로 비행하지 않도록 실험하는 데 성공하였다.

한편 동형암호 연산의 비효율성을 극복하기 위해 제도적 측면에서 기술의 표준화 외에도 기술적 연구를 통해 효율적인 동형 계산 알고리즘(스케줄링 최적화 등) 및 라이브러리 개발과 하드웨어를 통한 가속 구현을 위한 연구가 계속되고 있는데, 이는 사용자의 데이터를 안전하게 보호함은 물론 최신 AI 모델과 결합하여 기계학습 등의 과정에 걸쳐 데이터의 활용 과정도 안전하게 보호할 수 있다는 획기적인 솔루션을 제공한다는 점에서 많은 소요와 관심이 집중되고 있다. 특히 근사 연산을 지원하는 CKKS 스킴의 경우 통계 분석을 위한 데이터 정규화 및 학습(training)과 추론(inference)에도 사용될 수 있으며, CPU 및 GPU 리소스를 동시에 활용할 수 있는 클라우드 환경에서 연산의 종류에 따라 특정 리소스를 선택함으로써 연산의 효율성을 증대할 수 있다는 점에서 효과적인 최적화 방안이다.

5. 결론

본 논문에서는 차세대 암호 기술인 동형암호와 이를 사이버 물리 시스템에 적용하기 위해 인증 기술을 결합한 동형 인증 암호에 대해 소개하고, 이를 적용한 동형 제어 기술의 연구 동향에 대해 살펴보았다. 특히 동형 제어 기술은 실시간 제어가 가능해야 하므로, 평문 연산에 비해 느리고 제약이 있는 동형암호를 적용해도 충분히 빠르게 연산이 수행될 수 있도록 구현하는 데 중점을 맞추고 연구가 진행되어야 한다. 이를 위해 선형 연산만 수행하는 동형 인증 암호 구현, 소프트웨어 최적화 및 하드웨어 가속기 등의 연구를 통해 빠르고 메모리 절감을 달성하여 상업성이 보장되는 동형암호를 구현한다면 기존 암호 기술에 충분히 견줄 만한 실시간 제어 기술을 적용할 수 있을 것이라 생각한다.

사이버 물리 시스템에 대한 보안 위협은 더 이상 가상 세계의 단순한 컴퓨터 네트워크 해킹에서 그치는 게 아니라 당장 우리의 생명과 자산을 위협할 수 있는 현실 세계로 확장된다는 점에서 치명적이다. 이는 더 이상 개인의 문제가 아니며 과거 이란의 Stuxnet 바이러스를 통한 원전 위협 사례, 드론이 우크라이나 전쟁 등 최신 전사에서 공격적으로 활용되는 사례에서 볼 수 있듯 국가의 기반을 뒤흔드는 중대한 문제이다. 보안 비용과 성능 향상 사이의 이상적인 trade-off 를 달성하고 양자컴퓨터 시대에도 적용 가능한 최신 암호 기술 개발을 통해 실시간 통신의 안전성이 확보된다면 강력한 보안을 보장하는 것이 무엇보다 중요한 군사적 활용 뿐만 아니라 상업적 활용에도 적극적인 어필을 할 수 있을 것으로 기대된다.

ACKNOWLEDGEMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행되었으며(No.RS-2023-00277326), 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행되었으며(No.RS-2024-00438729, 익명화된 기밀실행을 이용한 전주기적 데이터 프라이버시 보호 기술 개발), 2023 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이며(No.2021-0-00528, 하드웨어 중심 신뢰계산기반과 분산 데이터보호박스를 위한 표준 프로토콜 개발), 2024 년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원되었으며, 본 연구는 반도체 공동연구소 지원의 결과물임을 밝힙니다.

참고문헌

[1] Craig Gentry. “Fully Homomorphic Encryption Using Ideal Lattices.” Proceedings of the forty-first annual ACM symposium on Theory of computing, 2009.

[2] Cheon Jung Hee, Kim Andrey, Kim Miran, Song Yongsoo. “Homomorphic Encryption for Arithmetic of Approximate Numbers.” ASIACRYPT, 2017.

[3] Zvika Brakerski, Craig Gentry, Vinod Vaikuntanathan. “Fully Homomorphic Encryption without Bootstrapping.” ITCS, 2012.

[4] Fan Junfeng, Vercauteren Frederik. “Somewhat Practical Fully Homomorphic Encryption.” Cryptology ePrint Archive, 2012.

[5] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, Malika Izabachene. “Faster Fully Homomorphic Encryption: Bootstrapping in less than 0.1 Seconds.” ASIACRYPT, 2016.

[6] Chihong Joo, Aaram Yun. “Homomorphic Authenticated Encryption Secure Against Chosen-Ciphertext Attack.” ASIACRYPT, 2014.

[7] Cheon Jung Hee, et al. “Toward a Secure Drone System: Flying With Real-Time Homomorphic Authenticated Encryption.” IEEE Access, 2018.

[8] Andre Teixeira, Kin Cheong Sou, Henrik Sandberg, Karl Henrik Johansson. “Secure Control Systems: A Quantitative Risk Management Approach.” IEEE Control Systems Magazine, 2015.