클라우드 서버를 활용한 가블드 회로 위탁 연산에 대한 연구

이동주 [1], 남기빈 [1], 주유연 [1], 백윤흥 [1]
[1] 서울대학교 전기정보공학부, 서울대학교 반도체공동연구소

{djlee, kvnam, yyjoo}@sor.snu.ac.kr, ypaek@snu.ac.kr

A Study on the Outsourced Garbled Circuit Evaluation Using Cloud Server

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

요 약

데이터 프라이버시에 대한 관심이 높아지면서 여러가지 프라이버시 보호 기술에 대한 연구가 활발히 이루어지고 있다. 대표적인 프라이버시 보호 기술로는 동형암호, 다자간연산, 신뢰실행환경, 차등 프라이버시 등이 있다. 본 논문은 다자간 연산의 대표적인 기술인 가블드 회로를 외부 서버에 안전하게 위탁하여 연산할 수 있는 기술에 대해 소개한다.

1. 서론

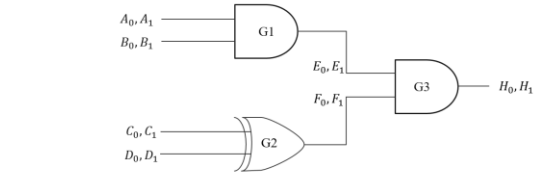
클라우드 컴퓨팅 기술이 널리 활용됨에 따라 데이터 프라이버시에 대한 관심이 점점 높아지고 있다. 데이터 프라이버시 보호를 위한 기술로 다자간 연산(**M**ulti-**P**arty **C**omputation), 동형암호(**H**omomorphic **E**ncryption), 차등 프라이버시(Differential Privacy), 신뢰실행환경(**T**rusted **E**xecution **E**nvironment) 등이 있는데, 이 중 다자간 연산은 연산 참여자의 입력 정보를 공개하지 않으며, 공통된 함수를 안전하게 연산할 수 있는 기술이다. 다자간 연산의 대표적인 기술로 Yao의 가블드 회로(Garbled Circuit)가 있다[1]. 하지만 서로의 프라이버시를 보장하며 안전하게 연산하기 위해선 많은 통신과 부가적인 연산이 필요하다. 이러한 연산 부담을 줄이기 위해 클라우드 서버를 활용하여 기존 가블드 회로의 연산을 위탁하는 방식의 연구가 지속적으로 이루어져 왔다. 본 논문은 이러한 서버 위탁 가블드 회로에 대한 연구들을 소개한다.

2. 배경 지식

2 장에서는 앞으로 설명한 내용의 이해를 돕기 위한 배경 지식 및 개념을 간단히 설명한다.

2-1 가블드 회로(Garbled Circuit)

가블드 회로는 이자간 연산(2-party computation)으로서 두 명의 참여자가 각자의 입력 정보를 숨긴 채 공동의 함수를 안전하게 연산할 수 있는 기술이다. 참여자 두 명은 각각 garbler 와 evaluator 로 역할이 나뉘며, garbler 와 evaluator 는 공동으로 연산할 함수를 회로의 형태로 변환한다. Garbler 는 해당 회로의 진리표를 암호화(garbling) 하여 evaluator 에게 보내며, evaluator 는 oblivious transfer 라는 프로토콜을 통해 연산에 필요한 입력 값을 받아와 그 입력 값을 key 로 하여 암호화된 진리표를 복호화 한다. 그리고 evaluator 와 garbler 는 결과를 공유하여 출력 값을 얻어낸다.



G1(AND)		
Input1	input2	Output
A_0	B_0	$Enc_{A_0,B_0}(E_0)$
A_0	B_1	$Enc_{A_1,B_1}(E_1)$
A_1	B_0	$Enc_{A_0,B_1}(E_0)$
A_1	B_1	$Enc_{A_1,B_0}(E_0)$

G2(XOR)		
Input1	input2	Output
C_0	D_0	$Enc_{C_0,D_1}(F_1)$
C_0	D_1	$Enc_{C_0,D_0}(F_0)$
C_1	D_0	$Enc_{C_1,D_1}(F_0)$
C_1	D_1	$Enc_{C_1,D_0}(F_1)$

G3(AND)		
Input1	input2	Output
E_0	F_0	$Enc_{E_1,F_1}(H_1)$
E_0	F_1	$Enc_{E_0,F_0}(H_0)$
E_1	F_0	$Enc_{E_0,F_1}(H_0)$
E_1	F_1	$Enc_{E_0,F_0}(H_0)$

그림 1 회로 암호화 예시

2-2 보안 수준(Security Definition)

다자간 연산 프로토콜 상, 공격자 모델에 따라 두 가지 보안 수준으로 나뉘어 진다.

Semi-honest security. 공격자는 프로토콜을 벗어나지 않으며 약속된 규약대로 충실히 이행한다. 하지만 프로토콜 상 주고받는 정보를 토대로 상대의 프라이버시를 유추하려고 한다. 상대적으로 약한 보안성을 지니지만 매우 효율적이다. 기본적으로 가블드 회로는 semi-honest secure 한 프로토콜이다.

Malicious security. 공격자는 상대의 프라이버시를 탈취하기 위해 프로토콜을 벗어나 행동할 수 있다. 예를 들어, 약속되지 않은 값을 전송하거나 임의로 통신을 중단할 수 있다. Malicious security 를 유지하기 위해선 보다 많은 부가적인 인증 과정이 필요하다. 기존에는 여러 개의 가블드 회로를 동시에 만들어, 연산할 회로와 검증할 회로를 random coin toss 방식을 통해 고르는 cut-and-choose 방식이 사용되었다[9]. 이후 2017 년에 새롭게 제안된 information theoretic MAC(message authentication code) tag 방식[10]을 통해 좀 더 효율적으로 보안성을 높일 수 있었다.

3. 클라우드 서버를 활용한 가블드 회로 위탁 연산 기술

실제 어플리케이션에서 가블드 회로 기반의 서비스가 수행될 시, 두 명의 참여자는 각각 서비스 제공자와 사용자로 나눌 수 있다. 가블드 회로의 특성상 두 참여자 모두 많은 연산과 통신 부하를 유발한다. 특히 사용자가 모바일 기기와 같은 낮은 컴퓨팅 리소스를 기반으로 서비스를 이용하는 경우 그 단점이 더 크게 부각된다. 이를 해결하기 위하여 사용자의 연산 및 통신을 제 3 의 클라우드 서버에 위탁하여 연산할 수 있게 하는 기술이 지속적으로 연구되어왔다. 구체적으로, 가블드 회로의 역할은 garbler 및 evaluator 로 나뉘며 사용자가 어떤 역할을 수행하는지에 따라 서버 역시 대신 수행해야하는 역할이 달라진다.

3-1 Garbler 위탁 방식

먼저 사용자 및 서버가 garbler 의 역할을 하는 경우이다. 가블드 회로에서 garbler 는 공통된 회로를 암호화하는 역할을 수행하며, 암호화할 때 진리표에 맞는 128-bit 의 random string(label)을 생성한다. 그리고 입력 label 을 key 로 하여 출력 label 을 암호화한다. Garbler 위탁 방식에서는 사용자는 본인의 입력 label 을 생성하여 서버에게 전송하고, 서버는 나머지 역할을 수행한다. Whitewash[2]는 대표적인 garbler 위탁방식의 malicious secure 위탁 가블드 회로 프로토콜로, Carter et al.[3]의 많은 공개키 암호화 연산을 대칭 키 암호 방식을 활용하여 해결하였다. [3]은 evaluator 위탁 방식으로서 사용자가 입력 label 을 가져오기 oblivious transfer 에 일부 참여하여야 했으나 [2]는 이를 서버와 서비스 제공자에게 완전히 위탁함으로써 효율성을 높였다. Blanton et al[4]는 유전 정보를 활용한 건강 정보 및 유전적 유사도 검사 등을 가블드 회로 위탁 연산 프로토콜을 통해 수행하였고 garbler 위탁 방식을 채용하였다.

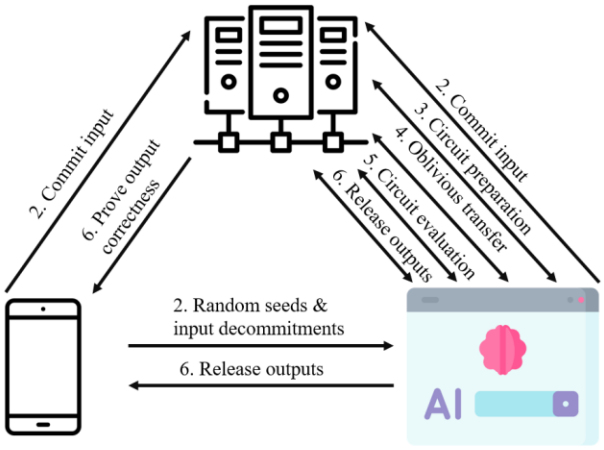


그림 2 Whitewash[2] 프로토콜

3-2 Evaluator 위탁 방식

다음으로 사용자 및 서버가 evaluator 역할을 하는 경우이며, 최근까지 지속적인 연구가 이루어지고 있다 [2], [5], [6], [7], [8]. 가블드 회로에서 evaluator 는 암호화된 회로 및 입력 label 을 받아 회로를 복호화 하는 역할을 수행한다. 서버와 사용자는 outsource oblivious transfer 를 통해 입력 label 을 받아오거나[3] [10]의 ideal functionality F 와 label 에 noise 를 추가하는 방식을 활용한다. Wu et al[7].는 서버를 활용한 가블드 회로 연산에 malicious security 를 위하여 최초로 [10]의 방식을 적용한 연구이며, 가장 최근 연구인 Liu et al[8].은 좀 더 효율성을 높인 [10]의 후속 연구 Katz et al[11].를 가블드 회로 위탁 연산에 적용한 연구이다. Liu et al.은 기존 최신 연구인 Wu et al.에 비해 약 1.32 배 속도가 향상되었다.

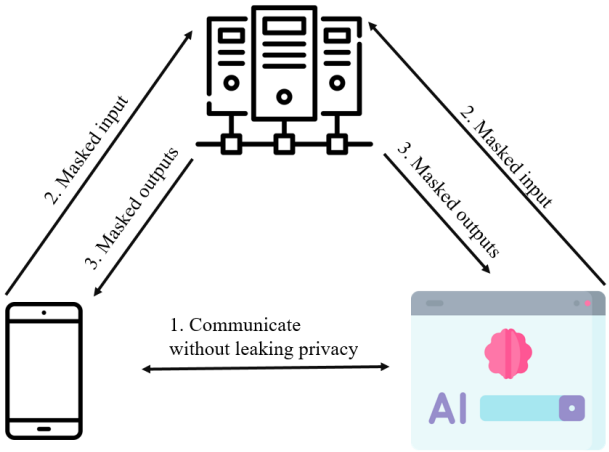


그림 3 Liu et al[8]. 프로토콜

4. 결론

클라우드 컴퓨팅 서비스를 활용하기 위해 사용자는 데이터를 클라우드로 전송해야 하기 때문에 데이터 프라이버시 문제가 부각되고 있다. Garbled circuit 은 이를 해결하기 위한 프라이버시 보호 기술 중 하나이다. 하지만 secure computation 의 특성으로 많은 연산 및 통신 부하가 발생하고 이를 해결하기 위해 제 3 의 클라우드 서버에 연산을 위탁하여 사용자의 부담을 최소로 하는 연구가 지속적으로 이루어졌다. Garbled circuit 의 두 역할 garbler 혹은 evaluator 의 역할을 서버에 위탁하였고 새로운 참여자가 등장함으로써 발생하는 보안 취약점에 대한 방어 기법이 추가되었다. 위탁 방식에 따라 장단점이 존재하지만 유저의 연산을 최소화하기 용이한 evaluator 위탁 방식이 최근까지 지속적으로 연구되고 있다. 또한 실제 어플리케이션에서 공격자의 악의적인 행위로부터 보안성을 유지하기 위해 효율성을 조금 포기하더라도 semi-honest security 보다 보안성이 더 강화된 malicious security 를 보장하는 방향으로 연구가 주로 이루어지고 있다.

5. ACKNOWLEDGEMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구이며 (IITP-2023-RS-2023-00256081), 2024 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구이며 (RS-2023-00277326), 2024 년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원되었음. 이 논문은 2024 년도 정부(산업통상자원부)의 재원으로 한국산업기술기획평가원의 지원을 받아 수행된 연구임.(No. RS-2024-00406121, 자동차보안취약점기반위협분석시스템개발(R&D)). 이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구결과임(No.RS-2024-00438729, 익명화된 기밀실행을 이용한 전주기적 데이터 프라이버시 보호 기술 개발). 본 연구는 반도체 공동연구소 지원의 결과물임을 밝힙니다. 이 연구를 위해 연구장비를 지원하고 공간을 제공한 서울대학교 컴퓨터연구소에 감사드립니다.

참고문헌

[1] Yao, Andrew Chi-Chih. "How to generate and exchange secrets." 27th annual symposium on foundations of computer science (Sfcs 1986). IEEE, 1986.

[2] Carter, Henry, Charles Lever, and Patrick Traynor. "Whitewash: Outsourcing garbled circuit generation for mobile devices." Proceedings of the 30th Annual Computer Security Applications Conference. 2014.

[3] Carter, Henry, et al. "Secure Outsourced Garbled Circuit Evaluation for Mobile Devices." 22nd USENIX Security Symposium (USENIX Security 13). 2013.

[4] Blanton, Marina, and Fattaneh Bayatbabolghani. "Efficient server-aided secure two-party function evaluation with applications to genomic computation." Proceedings on Privacy Enhancing Technologies (2016).

[5] Kamara, Seny, Payman Mohassel, and Ben Riva. "Salus: a system for server-aided secure function evaluation." Proceedings of the 2012 ACM conference on Computer and communications security. 2012.

[6] Baldimtsi, Foteini, et al. "Server-aided secure computation with off-line parties." Computer Security–ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part I 22. Springer International Publishing, 2017.

[7] Wu, Yulin, et al. "Efficient server-aided secure two-party computation in heterogeneous mobile cloud computing." IEEE Transactions on Dependable and Secure Computing 18.6 (2020): 2820-2834.

[8] Liu, Zhusen, et al. "Efficient and Privacy-Preserving Cloud-Assisted Two-Party Computation Scheme in Heterogeneous Networks." IEEE Transactions on Industrial Informatics (2024).

[9] Lindell, Yehuda, and Benny Pinkas. "An efficient protocol for secure two-party computation in the presence of malicious adversaries." Advances in Cryptology-EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007. Proceedings 26. Springer Berlin Heidelberg, 2007.

[10] Wang, Xiao, Samuel Ranellucci, and Jonathan Katz. "Authenticated garbling and efficient maliciously secure two-party computation." Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. 2017.

[11] Katz, Jonathan, et al. "Optimizing authenticated garbling for faster secure two-party computation." Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38. Springer International Publishing, 2018.