Natural Logarithm 을 이용한 암호문간의 거듭제곱 동형연산 방법

최영진, 이용우
인하대학교

yj160727@inha.edu, yongwoo@inha.ac.kr

Ciphertext-Ciphertext Exponentiation For Homomorphic Encryption Using Natural Logarithm

Youngjin Choi, Yongwoo Lee
Inha Univ.

요 약

본 논문은 동형암호 환경에서 자연로그를 이용하여 암호문 간의 거듭제곱 연산을 수행하는 방법을 제안한다. 제안된 방법은 체비쇼프 근사를 활용하여 자연로그와 지수함수의 근사를 구하고, 이를 통해 암호화된 데이터 간의 거듭제곱 연산을 가능하게 한다. 해당 접근 방식은 기존 동형암호 스킴에서 지원하지 않는 연산을 정의하여, 동형암호의 연산범위를 확장하고 더 다양한 수학적 연산을 지원할 수 있게 한다.

Keywords: 개인정보 보호, 동형암호, 다항식 근사

Ⅰ. 서 론

동형암호(Homomorphic Encryption)는 암호화된 데이터에 대해 복호화 없이도 산술 연산을 수행할 수 있는 기술로, 데이터 프라이버시를 유지하면서 다양한 연산을 가능하게 한다. 동형암호는 클라우드 컴퓨팅, 금융 데이터 분석, 의료 데이터 보호 등 민감한 데이터를 다루는 여러가지 분야에서 중요한 역할을 한다. 본 논문에서는 실수 근사 연산을 제공하는 RLWE(Ring-Learning With Errors) 기반의 CKKS 스킴[1]을 채택하여, 암호화된 데이터 간의 거듭제곱 연산을 수행하는 방법을 제안한다.

Ⅱ. 동형암호(Homomorphic Encryption)

동형암호(HE)는 암호화된 데이터에 대해서 복호화 과정 없이 산술 연산을 수행할 수 있는 기술이다. HE 의 주요 연산 알고리즘은 다음과 같다.

1. $Add(evk,\ ct_1,\ ct_2)$:
   입력: 평가 키 evk , 메시지 $m_1,\ m_2$ 에 각각 대응되는 암호문 ct_1, ct_2
   출력: $m_1 + m_2$에 대응되는 ct_{add}
2. $Mult(evk,\ ct_1,\ ct_2)$:
   입력: 평가 키 evk , 메시지 $m_1,\ m_2$ 에 각각 대응되는 암호문 ct_1, ct_2
   출력: $m_1 \times m_2$에 대응되는 ct_{mult}

CKKS 스킴은 복소수 체 $\mathbb{C}$에서 메시지 벡터를 정의하고 이를 $\mathcal{R}_Q = \mathbb{Z}_Q[X]/< X^N + 1 >$상에서 암호화한다. 이때, 정수 N은 2의 거듭제곱수(power-of-two) 이다. HE 에서는 덧셈과 곱셈에 대한 연산은 지원하지만 초월함수, 부호함수(sgn), 대소비교, 나눗셈 등은 지원하지 않는다. 이러한 연산을 수행하기 위한 방법에는 근사를 이용하는 방법[2]이 있다. 하지만 암호문간의 거듭제곱 연산은 제안된 바가 없고 우리는 이를 제안한다.

Ⅲ. 체비쇼프 근사법(Chebyshev Approximation)

동형암호는 덧셈과 곱셈에 대한 동형연산을 지원하기 때문에 초월함수에 대해서는 다항함수의 근사를 이용해야한다. 그러므로 효율적인 근사법을 고려할 필요가 있다. 체비쇼프 근사는 최소최대 오차(minimax error)를 제공[3]하여 근사 함수와 실제 함수 사이의 절대오차의 최대치를 최소화해준다. 그리고 빠른 수렴속도를 가지기 때문에 매끄러운 함수(smooth function; C^∞)에 대해서 비교적 적은 차수의 다항식으로 높은 정확도의 근사치를 얻을 수 있다. 체비쇼프 근사법의 기저 다항식은 다음과 같은 재귀 관계로 정의된다.

$$T_0(x) = 1, T_1(x) = x$$

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \quad for \quad n \geq 1$$

체비쇼프 다항식은 닫힌 구간 $[-1,1]$ 에서 정의되며, 주어진 함수 $f(x)$에 대해서 다음과 같은 선형결합으로 근사한다.

$$f(x) \approx \sum_{k=0}^{n} a_k T_k(x)$$

이때, a_k 는 체비쇼프 계수로, 다음과 같이 계산된다.

$$a_k = \frac{2}{n+1}\sum_{j=0}^{n} f(x_j)T_k(x_j)$$

이때, x_j는 체비쇼프 다항식의 근이며, 다음과 같이 정의된다.

$$x_j = cos\left(\frac{(2j+1)\pi}{2(n+1)}\right) \quad for \quad j = 0,1,\dots,n$$

Ⅳ. 제안 방법

암호문 간의 동형 거듭제곱 연산을 정의하기 위해서 밑(base)에 대한 암호문을 c_1, 지수(power)에 대한 암호문을 c_2라고 하자. 우리가 목표로 하는 연산은 $c_1{}^{c_2}$이다. 이를 실현하기 위해 세 가지 주요 단계로 나누어 설명하겠다.

(i) Target map 설정

우리가 수행하고자 하는 연산은 두 암호문 c_1과 c_2에 대해 다음과 같은 형태의 map을 갖는다:

$$(c_1, c_2) \mapsto c_1^{c_2} \qquad (1)$$

이를 수행하기 위해서 로그 함수와 지수 함수를 활용한 변환을 고려하자.

(ii) log 변환

먼저, 다음과 같은 map을 정의한다:

$$(c_1, c_2) \mapsto c_2 \ln c_1 \qquad (2)$$

로그의 성질에 의해서 $c_2 \ln c_1$는 $\ln(c_1^{c_2})$와 같으므로, 우리의 목표 연산을 자연로그의 진수로 변환할 수 있다.

(iii) exp 변환

자연로그의 역함수를 이용하여 원래 목표 연산의 결과를 얻는다. 이를 위해 다음과 같은 map을 정의한다:

$$c_2 \ln c_1 \mapsto \mathrm{e}^{c_2 \ln c_1} \qquad (3)$$

지수와 로그의 성질에 의해서 $\mathrm{e}^{c_1 \ln c_2} = c_1^{c_2}$가 성립하므로, (2)와 (3)의 합성으로 (1)을 얻어낼 수 있다. 따라서 우리가 원하는 결과를 달성할 수 있다.

위에서 정의한 연산을 실제로 구현하기 위해, 로그 함수 $\ln x$와 지수 함수 e^x를 체비쇼프 근사를 통해 근사한다. 각각의 함수에 대해서 체비쇼프 계수를 구하여 체비쇼프 다항식과의 선형결합으로 근사함으로써 동형암호 환경에서 지수와 로그 연산을 수행할 수 있다. 이 과정은 다음과 같은 순서로 진행된다.

1. 암호문 c_1에 대해 로그 함수를 체비쇼프 근사를 이용해 계산한다.
2. 암호문 c_2와 로그 변환된 c_1을 곱하여 $c_2 \ln c_1$을 계산한다.
3. 이 결과에 대해 지수 함수를 체비쇼프 근사를 이용해 계산하여 최종 결과 $c_1^{c_2}$를 얻는다.

해당 알고리즘을 다음과 같은 의사코드로 나타낼 수 있다.

Algorithm 1 Homomorphic Exponentiation Using Natural Logarithm

Input: Ciphertexts c_1 (base) and c_2 (power)
Output: Ciphertext $c_1^{c_2}$

function HomomorphicExponentiation(c_1, c_2)
  $c_{log} \leftarrow$ ChebyshevApproxLog(c_1)
  $c_{target} \leftarrow$ Mult(c_2, c_{log})
  ▷ 곱셈의 동형연산 수행
  $target \leftarrow$ ChebyshevApproxExp(c_{target})
  ▷ $e^{c_2 \ln c_1}$
  return $target$
end function

제안된 방법의 성능은 체비쇼프 근사 다항식의 차수에 따라 달라진다. 최적의 성능을 위해 적절한 차수를 선택하고, 연산의 효율성을 높이기 위한 최적화 알고리즘을 적용할 수 있다. 이러한 접근은 연산 속도와 정확도 간의 균형을 맞추는데 도움이 될 것이다.

Ⅴ. 동형암호 환경에서의 구현

우리는 OpenFHE 라이브러리[4]를 이용하여 11th Gen Intel(R) Core(TM) i9-11900 @ 2.50GHz 의 CPU 환경에서 이를 구현하였다. 아래는 밑과 지수의 범위에 따른 수행시간과 절대오차를 나타낸 표이다.

밑 범위	지수 범위	수행시간	절대오차(평균)
[2, 6]	[2, 6]	0.3575s	1.6867×10^{-7}

2^{12}개의 sample 에 대해서 평균치를 구하였다. 실험에 사용한 Ring Dimension 과 Q(ScaleMod)는 각각 2^{13}, 50이다.

Ⅵ. 결 론

본 논문에서는 동형암호 환경에서 자연로그를 이용하여 암호문 간의 거듭제곱 연산을 수행하는 방법을 제안하였다. 제안된 방법은 동형암호의 연산 범위를 확장하고 다양한 수학적 연산을 지원할 수 있도록 한다. 하지만 밑이 0 에 매우 가깝거나 지수가 충분히 큰 경우에는 noise 가 커져서 복호화를 할 수 없게 된다. 향후 연구에서는 제안된 방법의 이러한 한계를 극복하고, 성능을 더욱 향상시키기 위한 최적화 방법과 다양한 응용 분야로의 적용 가능성을 탐구할 예정이다.

참 고 문 헌

[1] J. H. Cheon, A. Kim, M. Kim, and Y. Song. Homomorphic encryption for arithmetic of approximate numbers. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 409-437. Springer, 2017.

[2] J. H. Cheon, D. Kim, D. Kim, H. H. Lee, and K. Lee. Numerical method for comparison on homomorphically encrypted numbers. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 415-445. Springer, 2019.

[3] N. L. Carothers. *A short course on approximation theory*. Bowling Green State University.

[4] Ahmad AI Badawi et al. OpenFHE: Open-Source Fully Homomorphic Encryption Library. Cryptology ePrint Archive, Paper 2022/915, 2022.