Gentry-Lee 기법을 활용한 동형암호상의 역행렬 계산 방법

이희수, 이용우
인하대학교 전기컴퓨터공학과
heesoo@inha.edu, yongwoo@inha.ac.kr

Homomorphic Matrix Inversion Using the Gentry-Lee Scheme

Heesoo Lee, Yongwoo Lee
Inha University Electrical and Computer Engineering

요 약

본 논문은 Chebyshev 다항식 초기화와 Newton-Schulz 반복을 결합한 동형암호 기반 역행렬 알고리즘을 제안한다. 정밀한 초기값 설정으로 필요한 반복 횟수를 최소화하여 multiplicative depth를 줄였으며, GL scheme의 trace 기반 행렬 곱셈과 호환되어 $\phi(p)$개 행렬을 단일 암호문에서 동시에 처리하여 높은 처리량을 제공한다. 평문 실험에서 총 depth 13에 1e-15의 정밀도를 달성하였다.

Ⅰ. 서 론

동형암호(Fully Homomorphhic Encryption, FHE)는 암호화된 상태에서 데이터 연산을 가능하게 하여 프라이버시를 보존하면서 클라우드 컴퓨팅이나 머신러닝을 수행할 수 있게 한다. BGV[1], BFV[2], CKKS[3]와 같은 RLWE 기반 FHE 스킴들은 덧셈과 곱셈 연산을 효율적으로 지원하지만, 링 구조 특성 상 나눗셈과 역수 연산은 직접하는 것이 불가능하다. 그러나 역행렬 계산은 선형 회귀 $\beta=(X^TX)^{-1}X^Ty$와 같은 통계 분석 및 머신러닝의 핵심 연산이다.

이러한 제약을 극복하기 위해 본 논문에서는 곱셈과 덧셈만을 사용하여 역행렬에 수렴하는 반복적 방법을 채택하였다. 수렴의 안정성을 보장하기 위해 정규화 전략을 도입하고, 기존 연구와 달리 Chebyshev 다항식을 통한 정밀한 초기값 설정으로 표준 Newton-Schulz 반복법의 회로 깊이 문제를 해결하여 필요한 반복 횟수를 최소화하였다. 또한 동형암호의 핵심 제약인 multiplicative depth 관리를 위해 Paterson-Stockmeyer 알고리즘을 적용하였다.

제안 알고리즘은 Gentry-Lee (GL) shceme[4]과의 호환성을 중요하게 고려하였다. GL scheme[4]은 다변수 링 구조를 통해 효율적인 SIMD 연산과 trace 기반 행렬 곱셈을 제공하므로, 역행렬 계산의 핵심인 반복적 행렬 곱셈을 효과적으로 수행할 수 있다. 특히 $\phi(p)$개의 행렬을 단일 암호문에 패킹하여 동시에 처리할 수 있어, 여러 행렬의 역행렬을 병렬로 계산할 수 있다.

Ⅱ. 관련 연구

동형암호 기반 행렬 연산에 관한 연구는 최근 활발히 진행되고 있다. Gentry와 Lee[4]는 다변수 링 구조 $R'_q = Z_q[i][X, Y, W]/\langle X^n - i, Y^n - i, \Phi_p(W)\rangle$를 활용하여 $\phi(p)$개의 $n \times n$ 행렬을 단일 다항식에 인코딩하고, 암호문 간 행렬 곱셈을 trace 연산을 통해 4번의 다항식 계수 행렬 곱셈으로 환원한다. 행렬이 슬롯에 직접 인코딩되므로 coefficient-slot 변환 오버헤드가 없으며, 행렬 크기를 링 차원과 독립적으로 조정 가능하다. 또한 $\phi(p)$개의 서로 다른 행렬을 단일 암호문에 패킹하여 동시에 연산할 수 있어, 반복적 행렬 곱셈인 역행렬 계산을 여러 행렬에 대해 병렬로 수행할 수 있는 구조이다.

동형암호 기반 역행렬 계산 연구에서 Newton-Schulz 반복법[5]의 표준 형태 $X_{k+1} = X_k(2I - AX_k)$는 적절한 초기값이 주어지면 2차 수렴을 보장한다. 그러나 동형암호 환경에서는 각 반복이 multiplicative depth 2를 소모하므로, 충분한 정밀도 달성을 위해 필요한 반복 횟수가 전체 회로 깊이를 결정하는 핵심 요소가 된다. 이러한 문제를 해결하기 위해 기존 연구들은 표준 Newton-Schulz 반복법을 대체하거나 변형하는 방식을 택하였다.

Cheon et al.[6]은 반복적 점화식 대신 $A^{-1} \approx \frac{1}{2^r}\prod_{j=0}^{r-1}(I+\hat{A}^{2^j})$ (여기서 $\hat{A}$는 정규화된 행렬) 형태의 곱셈 누적 구조를 사용하여 2의 거듭제곱 차수로 회로 깊이를 관리하였다. Kim et al.[7]은 반복 횟수를 줄이는 개선된 알고리즘으로 깊은 곱셈 회로와 부트스트래핑 비용을 감소시켰다.

본 논문은 표준 Newton-Schulz 반복법을 사용하되 초기값 문제를 해결하는 방식을 택하였다. Chebyshev 다항식으로 1/x를 정밀하게 근사하여 우수한 초기값 X_0를 설정함으로써 필요한 반복 횟수를 최소화하고 전체 multiplicative depth를 최적화한다.

Ⅲ. 제안 방법

제안하는 알고리즘은 Newton-Schulz 반복법[5]을 기반으로 하며, 네 단계로 구성된다. Newton-Schulz 반복법은 $X_{k+1} = X_k(2I - AX_k)$의 형태로 역행렬을 근사한다. 초기값 X_0가 A^{-1}에 충분히 가까우면 2차 수렴을 보장하며, 오직 행렬 곱셈과 덧셈만을 사용하므로 동형암호 환경에 적합하다.

알고리즘의 전체 구조는 GL scheme[4]의 행렬 연산 특성을 고려하여 설계되었다. 첫 번째 단계는 정규화이다. Newton-Schulz 알고리즘의 수렴을 위해 Frobenius norm $\|A\|_F = \sqrt{\sum_{i,j}|a_{ij}|^2}$를 사용하여 $A' = A/\|A\|_F$로 행렬을 스케일링 한다. 이를 통해 A'의 모든 고윳값은 (0,1) 구간에 위치하게 된다.

두 번째 단계는 Chebyshev 다항식 근사를 이용한 초기화이다. Newton-Schulz 반복법의 수렴 속도는 초기 오차 $\|I - A'X_0\|_F$에 의해 결정되므로 정밀한 초기값이 필수적이다. 기존 연구들이 표준 Newton-Schulz 반복법

을 채택하지 않은 주요 이유는 단순한 초기화($X_0 = aI$)로는 많은 반복이 필요하여 회로 깊이가 과도하게 증가하기 때문이다. 본 논문은 함수 $f(x) = 1/x$를 구간 $[1, \epsilon]$에서 차수 d의 Chebyshev 다항식으로 근사하여 이 문제를 해결한다. Chebyshev 다항식은 최소 최대 오차(minimax error)를 달성하며, 초기값은 $X_0 = p_d(A')$로 설정된다. 오차는 차수 증가에 따라 지수적으로 감소하므로, 적절한 차수 선택으로 초기 오차를 충분히 작게 만들어 표준 Newton-Schulz 반복법을 유지하면서도 필요한 반복 횟수를 최소화할 수 있다.

다항식 평가의 효율성을 위해 Paterson-Stockmeyer 알고리즘[8]을 적용한다. 이 알고리즘은 차수 d_{poly}의 다항식 평가에 필요한 multiplicative depth를 $O(\sqrt{d_{poly}})$로 줄인다. $k = \lceil \sqrt{d_{poly}} \rceil$로 설정하고 $A^1, A^2, \cdots, A^k$를 미리 계산한 후, 다항식을 $p(A) = B_0 + A^k \cdot B_1 + A^{2k} \cdot B_2 + \cdots$의 형태로 재구성하여 전체 계산을 효율적으로 수행 가능하다.

세 번째 단계는 Newton-Schulz 반복이다. 초기값 X_0로부터 $X_{k+1} = X_k(2I - A'X_k)$를 반복 수행한다. 초기 오차를 $E_0 = I - A'X_0$라 하면, k번 반복 후 오차는 $E_k = E_0^{2^k}$로 지수적으로 감소한다. 각 반복은 2회의 행렬 곱셈을 요구하므로 multiplicative depth가 2씩 증가한다. GL scheme[4]의 패킹 구조를 활용하면, $\phi(p)$개의 서로 다른 행렬을 동시에 처리하여 $\phi(p)$배의 처리량을 달성할 수 있다.

네 번째 단계는 비정규화이다. 정규화된 행렬 A'에 대한 역행렬 근사 X_{final}을 얻은 후, $A^{-1} \approx X_{final} \cdot (1/\| A \|_F)$로 복원된다. GL scheme[4]에서는 동시에 처리되는 각 행렬마다 다른 정규화 계수를 적용해야 한다.

전체 multiplicative depth는 $D_{total} = D_{Cheby} + 2 \times n_{iter}$로 계산된다. 여기서 $D_{Cheby} = \lceil \sqrt{d} \rceil + 1$은 Paterson-Stockmeyer 알고리즘[8]을 적용한 다항식 평가의 depth로 대략 $O(\sqrt{d_{poly}})$이고, n_{iter}는 Newton-Schulz의 반복 횟수이다. 각 Newton-Schulz 반복은 depth 2를 소모한다.

Ⅳ. 실험 결과

제안 알고리즘을 평문 환경에서 검증하였다. $d = 16$으로 설정한 뒤, $A = XX^T$로 양정부호 행렬을 생성하였다. Chebyshev 근사는 차수 15, 구간 $[\epsilon, 1]$에서 $\epsilon = 0.01$로 설정하였다.

Chebyshev 초기화 후 초기 오차 $\| I - A'X_0 \|_F$는 0.292로 수렴 조건을 만족하였다. 표 1은 Newton-Schulz 반복의 2차 수렴 특성을 보여준다. 4회 반복 후 $1e-12$ 미만의 정밀도 수준에 도달하였으며, 최종 상대 오차는 1.21×10^{-15}이었다.

Iteration	Error $\| I - A'X_k \|_F$
0	2.92×10^{-1}
1	2.52×10^{-2}
2	2.12×10^{-4}
3	1.74×10^{-8}
4	5.46×10^{-15}

[표 1] Newton-Schulz 반복 과정의 수렴 ($d = 16$, Chebyshev 차수 15)

Chebyshev 차수	초기 오차 $\| I - A'X_0 \|_F$	Iteraton	D_{Cheby}	총 Depth
6	1.47	6	3	15
9	0.76	5	4	14
12	0.52	5	5	15
15	0.29	4	5	13
18	0.15	4	6	14

[표 2] Chebyshev 차수에 따른 성능 비교

표 2는 Chebyshev 차수가 초기화 성능에 미치는 영향을 보여준다. 차수가 증가할수록 초기 오차가 감소하여 반복 횟수가 줄어든다. 차수 15가 총 depth 13으로 가장 최적의 선택임을 확인하였다.

Ⅴ. 결론

본 논문에서는 GL scheme과의 호환성을 고려한 동형암호 기반 역행렬 계산 알고리즘을 제안하였다. Newton-Schulz 반복법과 Chebyshev 초기화를 결합하여 행렬 곱셈과 덧셈으로 구성된 알고리즘을 설계하였으며, 이는 GL scheme의 효율적인 배치 연산과 trace 기반 행렬 곱셈을 직접 활용할 수 있다.

평문 실험에서 $d = 16$인 행렬에 대해 Chebyshev 차수 15, Newton-Schulz 반복 4회로 1e-15의 정밀도를 달성하였으며, 총 multiplicative depth는 13이다.

실용화를 위한 핵심 과제는 정규화 과정의 동형암호 구현이다. Frobenius norm의 계산은 각 원소의 제곱, 전체 합, 그리고 제곱근으로 구성된다. 제곱과 전체 합은 Hadamard 곱셈과 회전 합으로 계산 가능하지만, 제곱근 $\sqrt{\sum_{i,j} |a_{ij}|^2}$와 $1/\| A \|_F$는 다항식 근사가 필요하여 추가 depth를 소모한다. 이러한 비선형 연산을 효율적으로 근사하고 전체 depth를 최소화하는 것이 주요 과제이다. 제안 알고리즘은 선형 회귀, PCA 등 다양한 privacy-preserving machine learning 응용에 활용될 수 있다.

ACKNOWLEDGMENT

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(RS-2024-00399401, 양자안전 보안 인프라 전환 및 대양자 복합 안전성 검증기술 개발)

참 고 문 헌

[1] Brakerski, Z., Gentry, C., and Vaikuntanathan, V., "(Leveled) Fully Homomorphic Encryption without Bootstrapping," in Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS), ACM, 2012, pp. 309-325.

[2] Fan, J., and Vercauteren, F., "Somewhat Practical Fully Homomorphic Encryption," Cryptology ePrint Archive, Report 2012/144, 2012.

[3] Cheon, J. H., Kim, A., Kim, M., and Song, Y., "Homomorphic Encryption for Arithmetic of Approximate Numbers," in Advances in Cryptology – ASIACRYPT 2017, Lecture Notes in Computer Science, Vol. 10624, Springer, Cham, 2017, pp. 409-437.

[4] Gentry, C., and Lee, Y., "Fully Homomorphic Encryption for Matrix Arithmetic," Cryptology ePrint Archive, Report 2025/1935, 2025.

[5] Schulz, G., "Iterative Berechnung der reziproken Matrix," Zeitschrift für Angewandte Mathematik und Mechanik (ZAMM), Vol. 13, No. 1, pp. 57-59, 1933.

[6] Cheon, J. H., Kim, A., and Yhee, D., "Multi-dimensional Packing for HEAAN for Approximate Matrix Arithmetics," Cryptology ePrint Archive, Report 2018/1245, 2018.

[7] Kim, S., et al., "Improved Matrix Inversion with Packed Ciphertexts using Fully Homomorphic Encryption," Cryptology ePrint Archive, Report 2025/1274, 2025.

[8] Paterson, M. S., and Stockmeyer, L. J., "On the Number of Nonscalar Multiplications Necessary to Evaluate Polynomials," SIAM Journal on Computing, Vol. 2, No. 1, 1973, pp. 60-66.