강화학습 기반 GNFS 분석을 활용한 RSA 보안성 평가 연구

이영도, 김수리*, 윤기순

㈜엔에스에이치씨, *성신여자대학교

{ydlee, ksyoon}@nshc.net, *suhrikim@sungshin.ac.kr

RSA Security Evaluation Using Reinforcement Learning-based GNFS Analysis

Youngdo Lee, Suhri Kim*, Kisoon Yoon

NSHC Inc. (Associate Researcher, Chief Cryptographer),
*Sungshin Women's University (Assistant Professor)

요 약

RSA 암호체계는 큰 정수의 소인수분해 문제 기반하여 안전성을 보장하며, 그 안전성은 GNFS 알고리즘의 복잡도에 의해 평가된다. GNFS는 하지수 시간 복잡도를 가지는 현재까지 가장 효율적인 정수 인수분해 알고리즘으로 알려져 있으나, 실제 구현에서는 이론적 예측과 성능 간 차이가 존재한다. 이러한 차이는 알고리즘 단계별 파라미터 선택의 복잡성, 기존 휴리스틱 기반 접근법의 한계, 그리고 하드웨어적 제약에서 비롯되는 것으로 분석된다. 본 연구에서는 강화학습을 활용하여 GNFS의 파라미터 선택 과정을 자동화하고 최적화하는 새로운 접근법을 제안한다. 강화학습은 환경과의 상호작용을 통해 보상을 기반으로 최적 정책을 학습함으로써 기존 휴리스틱 기반 방식보다 효율적인 파라미터 조정과 실행 성능 향상을 가능하게 한다. 이를 통해 GNFS의 탐색 공간을 줄이고 인수분해 속도를 개선하며, 실제 환경에서 이론적 복잡도에 근접하는 성능 향상을 기대할 수 있다.

Ⅰ. 서 론

RSA(Rivest - Shamir - Adleman) 암호체계는 1977년 제안된 이후 전자서명, 키 교환 등 다양한 보안 프로토콜에서 핵심적인 역할을 수행하며 오늘날까지 가장 널리 사용되는 공개키 암호 알고리즘이다 [1],[2]. RSA의 안전성은 큰 정수의 소인수분해 문제를 기반으로, 현재까지 금융 및 네트워크 보안 분야에서 표준으로 활용되고 있다 [3].

RSA의 보안 수준은 키 길이 비트 n에 의해 결정되며, 이를 분석하는 대표적 알고리즘은 GNFS(General Number Field Sieve)이다 [4],[5]. GNFS는 하지수(sub-exponential) 시간 복잡도를 갖는 가장 효율적인 인수분해 알고리즘으로 알려져 있으며, RSA 안전성 평가의 핵심 지표로 활용된다. 그러나 이론적으로 RSA-1024 (n : 1024비트)가 2020년 이전에 인수분해 가능할 것으로 예측되었음에도 실제로는 RSA-250(n :829비트)까지만 인수분해가 성공하였다 [6]. 이는 이론적 복잡도 모델과 실제 하드웨어 환경 간의 차이, 파라미터 최적화의 한계 등이 복합적으로 작용한 결과로 분석된다.

GNFS는 크게 5단계로 구성되며, 각 단계의 파라미터 선택은 전체 성능에 중요한 영향을 미친다 [7]. 기존 연구는 주로 경험적 방법과 휴리스틱을 통해 파라미터를 조정해왔으나, 단계 간 복잡한 상호작용을 충분히 반영하기에는 한계가 있었다. 이에 본 연구에서는 강화학습(Reinforcement Learning)을 활용하여 GNFS 파라미터를 동적으로 최적화함으로써 실제 인수분해 성능을 향상시킬 수 있는 가능성을 연구한다.

Ⅱ. 관련 연구

RSA암호체계는 제안된 이후 현재까지 가장 널리 사용되는 공개키 암호 방식 중 하나로, 큰 정수의 소인수분해 문제의 계산 복잡도에 기반해 보안성을 보장한다. RSA는 두 개의 큰 소수를 선택해 곱한 값을 n으로 사용하며, 이를 효율적으로 소인수분해하지 않는 한 비밀키를 추론할 수 없다는 가정 위에서 동작한다[3].

이론적으로 RSA의 안전성은 현재 알려진 가장 효율적인 정수 인수분해 알고리즘인 GNFS(General Number Field Sieve)의 시간 복잡도를 통해 추정된다 [4],[5]. GNFS는 하지수(sub-exponential) 시간 복잡도를 가지며, 이론적 계산 모델에서는 컴퓨팅 파워의 발전 추세를 고려할 때 RSA-1024(1024비트)가 2020년경 실질적으로 인수분해될 수 있다는 예측도 제기된 바 있다. GNFS의 복잡도는 다음과 같으며,

$$L_n[1/3,(64/9)^{1/3}] = e^{(((64/9)^{1/3}+o(1))\cdot(\log N)^{1/3}(\log\log N)^{2/3})}$$

이는 알려진 알고리즘 중 가장 효율적인 것으로 알려져있다.

그러나 위 복잡도를 기반으로 실제 실험된 결과는 이론적인 복잡도와 간극이 존재한다. 2020년 기준으로 가장 큰 n을 성공적으로 인수분해된 것은 RSA-250(n :829비트)에 불과했으며[6], 이는 1024비트의 큰 수 n을 인수분해하기 위해 요구되는 계산 자원이 여전히 확보되지 않았음을 의미한다. 이러한 차이는 이론적 모델에서 가정한 최적화된 알고리즘, 완벽한 병렬화, 이상적인 하드웨어 환경과 실제 구현에서 발생하는 메모리 대역폭, 병렬 처리 오버헤드, 프로세서 성능 한계 등의 제약 사이에서 발생한다. 따라서 RSA의 보안성을 평가할 때는 단순히 이론적 복잡도 추정치에 의존하기보다, 실험적 분석 결과와 실제 구현상의 한계를 함께 고려할 필요가 있다.

GNFS는 현재까지 알려진 가장 빠른 정수 인수분해 알고리즘으로, 크게 (1) 다항식 선택(Polynomial Selection), (2) 체(Sieving), (3) 필터링(Filtering), (4) 선형대수(Linear Algebra), (5) 제곱근(Square Root) 단계로 구성된다. 특히 다항식 선택과 체 단계에서의 파라미터 설정은 알고리즘 전체 성능에 결정적인 영향을 미치며, 현재까지는 경험적 접근과 휴리스틱 기반 파라미터 수정에 의존하는 경우가 많다.

이러한 방식의 한계는 딥러닝, 특히 강화학습 기법을 활용하여 분석하고 개선 가능성을 탐구할 수 있을 것으로 판단된다. 강화학습은 환경과의 상호작용을 통해 보상을 기반으로 최적 정책을 학습함으로써, 기존의 수작업 기반 최적화보다 더 효율적이고 안정적인 인수분해 성능 향상을 기대할 수 있다.

Ⅲ. 강화학습 기반 GNFS 분석 제안 방법

강화학습(Reinforcement Learning, RL)은 에이전트가 환경과 상호작용하며 보상 함수를 최대화하는 방향으로 정책을 학습하는 기계학습 기법으로, 명시적인 지도(supervision) 없이도 순차적 의사결정 문제를 해결할 수 있는 장점을 가진다. GNFS는 초기 단계에서의 파라미터 선택이 이후 단계의 계산량과 인수분해 성공률에 큰 영향을 미친다. 이러한 특성은 강화학습에서 파라미터 조합을 탐색·학습·보상 기반으로 최적화할 수 있는 가능성을 제공한다.

본 연구에서는 GNFS 파라미터 최적화 문제를 강화학습 프레임워크로 정의하고, 알고리즘 수행 과정에서의 다항식 품질 평가 지표인 Murphy E-값을 보상으로 설정한다. Murphy E-값는 다항식의 소인수분해 가능성을 추정하는 척도로, 일반적으로 다음과 같이 정의된다[8].

$$\frac{6}{\pi^2}\int\int_{\Omega}\rho\left(\frac{\log|F(x,y)|+a(F)}{\log B_1}\right)\rho\left(\frac{\log|G(x,y)|+a(G)}{\log B_2}\right)dxdy$$

위 식에서 $\rho(u)$는 Dickman-de Brujin 함수로, 주어진 정수 또는 다항식 값이 특정 smoothness bound를 초과하지 않을 확률을 근사하며, a는 다항식의 값들이 특정 소수로 얼마나 잘 나눠지는 지를 측정하는 함수이며, B_1, B_2 는 smoothness bound를 나타낸다. 결과적으로 Murphy E-값이 높을수록 체(Sieving) 단계에서 더 많은 유용한 관계식(relations)을 발견할 가능성이 크다.

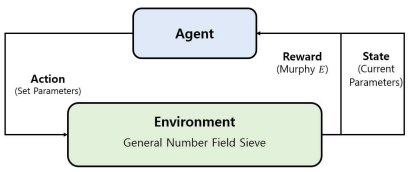

그림 1 강화학습 기반 GNFS 분석 제안 방법

본 논문에서 제안하는 방식은 [그림 1] 과 같다. 강화학습에서의 에이전트(Agent)는 환경(Environment)에서 다양한 파라미터 조합을 실험하며, 장기적으로 계산 비용을 최소화하고 높은 Murphy E-값을 유도하는 최적 전략을 학습한다. 이를 통해 기존 휴리스틱 기반 접근이 놓칠 수 있는 비직관적 최적 해를 발견하고, 동일한 계산 자원으로 더 큰 n를 인수분해할 가능성을 높일 수 있다. 강화학습 기반 접근법은 특히 다항식 선택 단계에서 후보 다항식의 Murphy E-값을 보상으로 활용해 품질을 평가하고 최적 후보를 선택하는 과정, 체 단계에서 소수 체 크기 등의 매개변수를 조정하는 과정에서 강력한 개선 효과를 기대할 수 있다. 본 논문에서 제안하는 방법은 GNFS를 활용한 RSA 분석을 보다 효율적으로 수행할 수 있는 새로운 최적화 패러다임을 제시하며, 대규모 정수 인수분해 문제의 실질적 계산 가능성 평가에 기여할 것으로 전망된다.

Ⅳ. 기대효과 및 향후 과제

본 연구에서 제안하는 강화학습 기반 GNFS 분석 방법은 기존 휴리스틱 또는 경험적 접근법으로는 발견하기 어려운 최적 파라미터 조합을 인공지능을 이용하여, 효율적으로 탐색할 수 있는 가능성을 제공한다. 이를 통해 동일한 하드웨어 자원에서 더 빠르고 효율적인 인수분해를 수행하거나, 제한된 자원으로도 기존보다 큰 n에 대한 실질적 분석 가능성을 높이는 데 기여할 수 있다. 특히 RSA 암호체계의 보안성 평가 과정에서 기존 이론적 복잡도 분석과 실제 구현 간의 간극을 줄이고, 보다 정밀한 실험 기반 보안 수준 추정치를 제공할 수 있을 것으로 기대된다.

향후 과제는 다음과 같다. 첫째, 강화학습 모델을 GNFS 환경에 적합하도록 구체화하고, 실제 인수분해 시뮬레이션 데이터를 기반으로 학습 효율을 높이는 방법을 마련해야 한다. 둘째, GNFS 단계별로 독립적 파라미터 최적화뿐 아니라 단계 간 상호 의존성을 고려한 통합 정책 학습 기법을 개발할 필요가 있다. 셋째, 제안된 강화학습 기반 최적화 기법을 대규모 분산 환경 또는 GPU 가속 기반 클러스터에서 실험하여, 실제 고성능 컴퓨팅(HPC) 환경에서의 확장성과 실효성을 검증해야 한다. 마지막으로, 강화학습 모델이 GNFS 알고리즘의 근본적인 계산 복잡도를 줄일 수 있는 잠재적인 패턴을 학습하는지, 아니면 단순히 기존 휴리스틱을 근사하는지에 대한 이론적 분석이 필요하다.

본 연구는 강화학습을 활용한 새로운 정수 인수분해 최적화 접근법을 제안함으로써 RSA 보안성 평가 및 암호 강도 측정에 있어, 보다 실질적이고 정량적인 근거를 마련할 수 있는 기반을 제공하며, 향후 고전적 인수분해 알고리즘의 효율화와 차세대 암호 안전성 분석 분야에서 중요한 연구 방향으로 확장될 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

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

참 고 문 헌

[1] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120 - 126, 1978.

[2] W. Stallings, “Cryptography and Network Security: Principles and Practice”, 8th ed., Pearson, 2023.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.

[4] A. K. Lenstra and H. W. Lenstra Jr., “The Development of the Number Field Sieve”, Springer, 1993.

[5] R. P. Brent, “Recent Progress and Prospects for Integer Factorisation Algorithms,” Computational Methods in Number Theory, 1995.

[6] B. B. Arjen Lenstra et al., “The Factorization of RSA-250,” Mathematics of Computation, 2020. [Online]. Available: https://eprint.iacr.org/2020/1492

[7] T. Kleinjung, “Polynomial Selection for the General Number Field Sieve,” Mathematics of Computation, vol. 75, pp. 2037 - 2047, 2006.

[8] B. A. Murphy, “Polynomial Selection for the Number Field Sieve Integer Factorization Algorithm”, Ph.D. Thesis, The Australian National University, 1999.