DLP, ECDLP, ECC 자료 분석

세환 신

December 2024

요 약

이산 로그 문제에 속하는 방법으로 암호화를 수행하는 DLP와 ECDLP에 대해 알아보고, 특히 ECDLP를 응용한 ECC에 사용 분야와 효용성을 알아보고자 한다.

1 DLP와 ECDLP 비교하기

DLP와 ECDLP는 둘 다 이산 로그 문제에 속하는 알고리즘이다. 이산 로그 문제란 지수 계산을 수행하는 것은 빠르게 수행 가능하지만 역으로 로그를 계산하는 것은 어렵다는 점에서 착안한 암호화에 주로 사용되는 문제이다.

DLP는 $group$ 구조에서 정의된 문제로, g와 h, p(p는 적절히 큰 소수)값이 공개 키로 주어졌을 때 $g^x = h \mod p$를 찾는 게 목표이다. 즉 Z_p^*에서 $g^x = h$를 찾아야 한다는 뜻이다. DLP는 p를 큰 소수로 설정하고 적절한 g값을 선택하면 계산이 매우 어려워진다는 전형적인 이산 로그 문제의 형태를 띈다.

ECDLP의 경우 타원 곡선 위에서 이산 로그 문제를 정의한 것이다. 타원 곡선은 $y^2 = x^3 + ax + b$를 만족하는 점들의 집합이다. a와 b값은 임의로 정해진다. 주어진 타원 곡선 위의 점 P와 Q에 대해 $Q = k * P$를 만족하는 스칼라 값인 k를 찾는 문제이다. P는 생성점이고 Q가 점 덧셈의 결과가 되는 점이다. ECDLP도 마찬가지로 충분히 큰 소수 p를 사용하는 Z_p^*를 기반으로 한다. 즉 타원 곡선의 점을 찾을 때 유한체 내 점 덧셈을 기반으로 한다.

2 ECDLP가 DLP보다 어려운 문제로 해석되고 있는 이유

ECDLP가 왜 이산 로그 문제로 취급되는지 먼저 살펴보면 알 수 있다. ECDLP에서 P는 타원 곡선 위의 점이고 Q는 P를 k번 더한 값이다. 즉 점 덧셈을 반복하는 연산이다. 타원 곡선 상에서의 점 덧셈은 두 점을 직선으로 이었을 때 직선과 만나는 또 다른 점이 연산 결과이다. 이러한 연산을 k번 반복하는 것이 $Q = k * P$의 의미이다. 이는 곱하기를 k번 반복하는 것처럼 이산로그 문제로 생각할 수 있다. 타원곡선에서의 점 덧셈 연산 한 번을 여러 번, 즉 제곱으로 수행하는 상황으로 해석하는 것이다.

각 연산에 해당하는 점 덧셈 연산의 의미가 단순 곱하기가 아닌 타원 곡선 상에서 새로운 점을 찾는 연산이기 때문에 DLP에 비해 비선형적이고 예측하기 힘들다.

3 ECC의 주요한 특성과 최근 ECC를 활용한 기술 조사

3.1 ECC의 주요 특성

ECC는 기본적으로 ECDLP를 활용한 암호학적 프로토콜 설계 기술이고 공개 키 암호화 시스템 형식으로 사용한다. 공개 키 암호화 시스템 중에서는 RSA등의 다른 암호화 기법보다 더 작은 키 크기로 동등한 수준의 보안을 제공할 수 있다. 즉 고효율 암호화 방식이다. RSA체계에서 3072비트 크기의 키와 동일한 수준의 보안을 보장하기 위해서 ECC에서는 256비트로 동등한 보안 수준을 구현 가능하다. 즉, 암호화 요구 수준이 동일할 때 암호화하는 데 필요한 리소스가 상대적으로 더 적다는 뜻이다.

이에 따라 ECC는 모바일 기기나 임베디드 시스템 등 리소스가 제한되는 환경에 도입하기 유리할 수밖에 없다. 그리고 사용하는 비트 수가 적다는 것은 연산 속도 측면 뿐만 아니라 특히 네트워크 대역폭과 전송 지연을 줄이는 데 매우 좋다는 뜻이기도 하다. 이 때문에 블록체인이 ECC방식을 도입해서 사용하는 것이다.

또한 ECC는 현재 효율적으로 해결가능한 알고리즘이 존재하지 않다. 이는 ECC문제를 풀기 위해 시도할 수 있는 방법이 $Brute-force$밖에 없다는 뜻이다. 따라서 현재로서는 ECC는 지수시간 복잡도를 가지는 $NP-hard$문제라고 볼 수 있고 이는 ECC가 충분한 보안성을 가진다는 근거로 볼 수 있다.

그리고 ECC는 ECDSA(Elliptic Curve Digital Signature Algorithm)과 같은 서명 알고리즘으로 서명 생성, 검증 시 보안성과 빠른 속도를 보장할 수 있다.

3.2 ECC를 활용한 기술 조사

『A Construction of Three Party Post Quantum Secure Authenticated Key Exchange Using Ring Learning With Errors and ECC Cryptography』[1]

이 논문에 따르면, 양자 컴퓨터의 등장으로 기존의 많은 암호화 방식이 위협받고 있다. 양자 컴퓨터에서 Shor의 알고리즘을 활용하면 정수 인수분해나 이산 로그 문제를 다항 시간 내에 해결가능하기 때문이다. 이는 결국 RSA암호화 같은 기존 방식을 무력화시킬 수 있다는 의미이기에 이에 대비해 양자 내성을 갖춘 시스템이 필요하다.

이를 위해 논문에서는 RLWE(Lattice-based Authenticated Key Exchange) 방식과 ECC, 생체 인증 시 사용자의 익명성을 보장하기 위해 noise를 추가하는 방식까지 결합해서 시스템을 구축하고자 한다.

구체적으로 서버와 클라이언트가 RLWE를 사용해서 안전한 정보를 교환하고 이 정보에 대한 세션 키를 생성한다. 이후 ECC를 사용해서 서로의 신원을 확인하고 데이터에 대해 서명해서 무결성을 보장하는 방식이다.

RLWE를 활용하면 격자 기반 암호화 방식을 사용해서 양자 내성 보안을 보장할 수 있다. 여기에 ECC기반의 키 교환과 서명 방식을 제공해서 인증을 빠르게 하려고 시도하고 있다.

이처럼 ECC단독으로는 양자 내성을 갖추지 못하지만 양자 내성을 갖춘 다른 양자 내성 알고리즘과 함께 사용돼서 양자 내성 시스템을 효율적으로 동작하도록 사용되는 것을 볼 수 있다.

『**Double image encryption algorithm based on compressive sensing and elliptic curve**』[2]

논문에서는 이미지 데이터 트래픽이 점점 증가하는 상황에서 많은 이미지 트래픽을 효율적으로 암호화하기 위해 압축 센싱, 카오스 시스템, ECC를 도입한다.

압축 센싱을 활용해서 기존 이미지의 데이터를 훼손하지 않고도 낮은 샘플링 비율로 데이터를 가공하고 이에 초기값에 민감한 카오스 시스템과 복호화하기 어려운 ECC를 결합해서 많은 이미지 트래픽을 효율적으로 암호화하는 것이 가능하다는 내용의 논문이다.

카오스 시스템이란 초기값에 매우 민감한 시스템을 말한다. 일반적으로는 아주 미세한 오차는 계산 과정 중 무시하더라도 결과에 큰 영향을 미치지 않는다. 그러나 카오스 시스템에서는 아주 작은 오차가 생겨도 결과가 완전히 뒤바뀌기 때문에 원래의 값을 추정하기 어렵다. 이에 ECC를 결합해서 매우 비선형적으로 만들어 보안을 강화한 형태이다.

『**Enhancing security by using GIFT and ECC encryption method in multi-tenant datacenters**』[3]

이 논문에서는 DCN, 즉 데이터 센터 네트워크에서 다뤄야 하는 트래픽을 어떻게 효율적으로 암호화시킬 것인지와 관련해서 ECC를 도입한다. DCN에서 다루는 트래픽을 크게 short flow와 long flow로 나눈다. Short flow는 latency에 민감하다는 특징이 있고 long flow는 더 중요한 정보가 담기기 때문에 보안성이 더 요구된다.

기존 단일 암호화 방식을 적용했을 때는 short flow에 대해서는 latency가 너무 길고 long flow에서는 보안 강도가 충분하지 않다는 문제가 있다. 따라서 long flow에는 비대칭 키 알고리즘인 ECC를 적용하고 short flow에는 경량화된 대칭 키 알고리즘인 GIFT를 적용해서 개선하겠다는 내용이다. 네트워크 환경에서 long flow에 대해 ECC를 적용해 보안 강도를 높이려는 시도를 확인할 수 있다.

『**An Efficient and Provably Secure ECC-Based Conditional Privacy-Preserving Authentication for Vehicle-to-Vehicle Communication in VANETs**』[4]

기술 중 VANETs란 차량과 차량 간(V2V) 또는 차량과 인프라 간(V2I) 통

신을 수행해서 교통 안전과 차량 트래픽 관리 등을 개선하기 위한 네트워크이다. 차량 내에 OBU라는 유닛을 설치하고 이를 활용해서 주변 차량, 인프라와 안전과 관련된 메시지를 주고받는 형식이다. 이 때 보안 수준이 충분하지 않다면 공격자가 심각한 사고를 일으킬 수 있기 때문에 높은 수준의 보안이 필요하다. 그러나 Bilinear Pairing, Map-to-Point 해시 함수를 사용하는 기존 방식은 연산량이 너무 많아서 교통 밀집 상황이 발생한다면 요구 성능을 만족하지 못할 가능성이 높다. 따라서 연산이 비교적 간단한 일반 해시 함수를 사용하고 여러 서명을 병렬적으로 한 번에 검증하는 알고리즘을 구현한다는 내용이다.

ECC 기반 조건부 프라이버시 인증 방식을 사용해서 차량의 신원을 기본적으로는 primary하게 관리하지만 필요 기관이 경우에 따라 신원을 확인가능하도록 구현한다. 이를 통해 교통 밀집 지역의 실시간 통신 상황에서도 높은 처리량을 유지할 수 있다는 내용이다.

4 결론

이처럼 ECC기반 암호화 방식을 적용하면 기존 암호화 방식을 더 효율적으로 바꿀 수 있고 이에 따라 기존에는 리소스 문제로 구현이 어려운 문제에도 암호화를 도입하는게 가능하다.

참고 문헌

[1] Dharminder Chaudhary, Uddeshaya Kumar, and Kashif Saleem. A construction of three party post quantum secure authenticated key exchange using ring learning with errors and ecc cryptography. *IEEE Access*, 2023.

[2] Guodong Ye, Min Liu, and Mingfa Wu. Double image encryption algorithm based on compressive sensing and elliptic curve. *Alexandria engineering journal*, 61(9):6785–6795, 2022.

[3] Jin Wang, Ying Liu, Shuying Rao, R Simon Sherratt, and Jinbin Hu. Enhancing security by using gift and ecc encryption method in multi-tenant datacenters. *Computers, Materials & Continua*, 75(2):3849–3865, 2023.

[4] Ikram Ali, Yong Chen, Niamat Ullah, Rajesh Kumar, and Wen He. An efficient and provably secure ecc-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in vanets. *IEEE Transactions on Vehicular Technology*, 70(2):1278–1291, 2021.