모바일 환경에서 음성데이터 보안을 위한 ECC 암호 알고리즘 설계

김현수*, 윤성열**, 박석천***
*, **경원대학교 일반대학원 전자계산학과
***경원대학교 IT대학
e-mail:scpark@kyungwon.ac.kr

Design of ECC Encryption Algorithm for Security of Voice data in Mobile Environment

Hyun-Soo Kim*, Sung-Yeol Yun**, Seok-Cheon Park***
*Dept of Computer Science, Kyungwon University

요 약

모바일 인터넷전화가 활성화됨에 따라 음성데이터에 대한 보안이 중요시 되고 있다. 이에 따라 보안의 강도가 강한 ECC 암호 알고리즘을 이용하여 인터넷전화 등에서 사용되는 음성 데이터를 암호화하고자 한다. 그러나 기존 암호화 방법은 암호화 횟수가 많아 자원 소모가 커서 모바일 환경에서는 제약적이다. 따라서 본 논문에서는 음성 데이터에 대한 암호화 횟수를 감소할 수 있는 암호화 알고리즘을 제안한다.

1. 서론

최근 스마트폰의 사용이 크게 증가함과 더불어 모바일 인터넷전화가 활성화됨에 따라 인터넷전화에서 전송되는 음성데이터에 대한 보안이 중요시 되고 있다. 이에 따라 보안의 강도가 강한 ECC 알고리즘을 적용하여 음성 데이터를 암호화 할 필요성이 있다. 그러나 공개키 방식인 ECC 암호 알고리즘의 암호 연산은 자원 소모가 매우 크기 때문에 모바일 등의 환경에서는 이용이 제약적일 수 있다. 따라서 본 논문에서는 ECC 알고리즘의 암호화 횟수를 대폭 감소할 수 있는 방법을 제시함으로써 암호 연산을 통한 자원 소모를 크게 감소시켜 빠르고 효율적으로 ECC 암호 알고리즘을 사용할 수 있게 하고자 한다.

2. 관련연구

2.1 G.711 음성코덱

G.711은 64Kbps에서 3KHz 전화 수준의 오디오 품질을 제공하기 위해 PCM 오디오 인코딩과 미국, 유럽에서 주로 이용하는 U-law 또는 A-law 방식을 사용한다. 펄스 코드변조(Pulse Code Modulation, PCM) 방식은 샘플들을 미국 방식인 U-law 또는 유럽 방식인 A-law 양자화 방식을 이용하여 한정된 재구성 세트 중의 하나로 양자화를 시켜주는 파형 코딩 방식이다. G.711 표준은 전화 대화 코딩을 위한 표준 방식으로 8Bit PCM을 정의하고 있다.

2.2 ECC 알고리즘

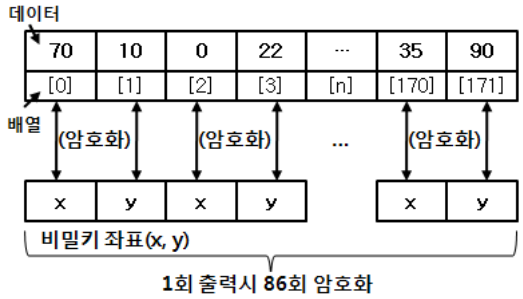
유한체(finite fields)위에서 정의된 타원곡선 군에서의 이산대수 문제에 기초한 타원곡선 암호시스템(ECC, Elliptic Curve Crypto-system)은 1985년에 Miller와 Koblitz가 독립적으로 제안한 공개키 암호알고리즘이다. 이는 최근 150여 년 전부터 정수론, 대수기하분야에서 집중적으로 연구되어 왔으며, Fermat의 마지막 정리의 증명에서도 타원곡선 이론이 아주 중요하게 이용되었다. 최근에는 타원곡선방법(ECM, Elliptic Curve Method)은 RSA 암호시스템의 근간이 되는 인수분해 문제와 소수 판정법 및 공개키 암호 등에 활용되고 있다.

2.3 음성 데이터에 대한 기존 ECC 암호화 방식

일반 ECC 암호 알고리즘은 타원곡선 위의 좌표끼리 덧셈연산을 함으로써 암호 데이터를 생산한다. 즉, 숫자와 숫자간의 연산이기 때문에 문자열이 음성데이터 또는 좌표 값에 포함될 수 없다. 따라서 암호화 과정에서 문자열, String 등의 데이터는 사용하기에 어려운 구조이다.

G.음성코덱 처리기는 음성 데이터를 바이트 타입의 배열 구조로 전송한다. 음성데이터를 기존의 ECC 암호 알고리즘 방식으로 암호화하면, ECDH 알고리즘을 통해 생성된 비밀키와 배열의 데이터를 꺼내어 각각 하나씩 연산을 해야 한다. 이에 대한 과정은 그림 1과 같다.

* 경원대학교 일반대학원 전자계산학과 석사과정
** 경원대학교 일반대학원 전자계산학과 박사과정
*** 경원대학교 IT대학 컴퓨터공학과 정교수(교신저자)

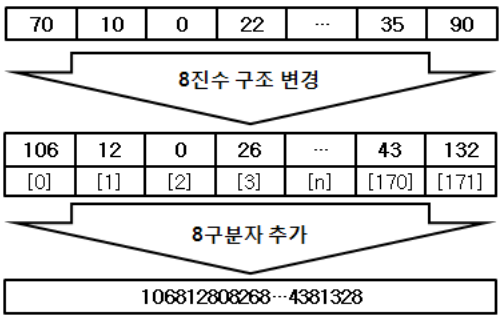


(그림 1) 기존 음성데이터 암호화 방식

기존 표준화되어있는 G.음성코덱의 1회 출력은 그림 1과 같이 172개의 바이트 배열에 담아 출력하게 된다. 따라서 각각 비밀키와 암호화 연산을 하게 될 경우, 비밀키의 구조인 좌표 x와 y값을 각각 암호화하기 때문에 1회 출력 시 86회의 암호화를 거쳐서 음성을 듣는 상대에게 전송된다. 따라서 실시간으로 출력되는 음성데이터를 86회 암호화 연산을 거쳐서 상대에게 전송하는 것은 자원 소모가 크기 때문에 모바일 환경에서는 큰 제약이 될 수 있다.

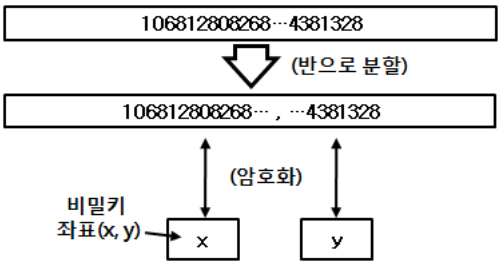
3. 음성 데이터 보안을 위한 효율적인 ECC 암호 알고리즘 설계

음성 데이터에 대한 암호화 연산의 횟수를 줄이기 위해서는 바이트 배열의 데이터 구조 변경이 필요하다. 음성 데이터가 인코딩되어 바이트 배열에 입력되기 전에 8진수의 데이터로 변경을 한다. 8진수로 된 데이터를 모두 순서대로 붙이고 구분자로 8을 이용한다. 8진수에는 8이 사용되지 않기 때문에 8을 데이터 사이마다 추가하여 데이터를 수의 상태로 유지한다. 그림 2는 이에 대한 설명을 나타낸다.



(그림 2) 음성 데이터 구조 변경

구분자를 통해서 변형된 데이터는 반으로 분할되어 비밀키 좌표 x, y와 암호 연산을 통해 암호화된 데이터를 생성한다. 그림 3은 데이터와 비밀키를 통해 암호화 연산하는 과정을 나타낸다.



(그림 3) 암호화 연산 과정

그림 3과 같은 과정을 통해 음성 코덱에서 음성 데이터 출력 시 단 한 번의 암호화 연산과정으로 기존의 암호화 알고리즘에 비해 암호화 연산 횟수가 큰 차이로 줄어들었다. 이에 따라 암호화 연산을 위한 자원 소모가 크게 줄기 때문에 더 효율적으로 음성 데이터 암호화에 적용이 가능하다.

4. 결론

기존 인터넷전화의 암호 알고리즘은 주로 대칭키 방식의 암호 알고리즘을 사용하였다. 그러나 본 논문에서는 음성 데이터에 대한 보안을 강화하기 위해 공개키 방식의 알고리즘인 ECC 암호 알고리즘을 이용하여 인터넷전화에 적용하였고, 더 효율적인 방법을 설계하였다. G.711 등의 G.계열의 음성 코덱은 약 170개 정도의 바이트 배열 구조에 음성을 처리하기 때문에 배열의 각 데이터를 암호화하게 되면 암호화 횟수에 따른 자원 소모가 많아서 모바일 등의 환경에서는 매우 제약적일 수 있다. 따라서 본 논문에서는 배열의 데이터 구조를 변경하여 암호화 횟수를 대폭 줄임으로써 처리 시간과 자원 소모를 대폭 감소시키고자 하였다. 본 알고리즘을 적용하여 모바일 인터넷전화 등의 실시간으로 처리되는 데이터의 암호화에 사용되면 보다 빠르고 효율적으로 처리가 가능할 것이다.

참고문헌

[1] Lief Uhsadel 외, “An Efficient General Purpose Elliptic Curve Cryptography Module for Ubiquitous Sensor Networks”, www.crypto.rub.de

[2] 진소라 외, “실시간 음성을 암호화한 통신 시스템 설계 및 구현”, 한국멀티미디어학회 추계학술지

[3] 변영준, “지능형 정보제공 시스템에서의 음성처리기술 활용”, 한국정보과학회 학술지

[4] http://blog.naver.com/websearch/70033938295