타원곡선을 이용한 AMP 프로토콜

안창섭[0] 허 신
한양대학교 컴퓨터공학과
{csahn, shinheu}@cse.hanyang.ac.kr

Elliptic Curve AMP Protocol

Chang-sup Ahn[0] Shin Heu
Dept. of Computer Science & Engineering, Hanyang University

요 약

낮은 엔트로피의 패스워드를 이용하여 안전한 인증 및 키교환을 위해 Diffie-Hellman에 기반한 AMP(Authentication and key agreement via Memorable Password) 프로토콜이 제안되었다.

본 논문에서는 타원곡선 암호화가 가질수 있는 높은 보안성과 효율성을 위해 타원곡선이산대수문제(Elliptic Curve Discrete Logarithm Problem)에 기반한 EC-AMP(Elliptic Curve-AMP)프로토콜을 제안한다. EC-AMP는 랜덤 오라클(random oracle) 모델에서 여러 가지 공격에 대해 안전하므로 인증 및 키교환이 필요한 네트워크 환경에 패스워드를 이용함으로 얻을수 있는 편의성과 타원곡선이산대수문제가 제공하는 안전성을 보장할 수 있다.

1. 서론

사용자 인증 방법은 인증하고자 하는 대상에 따라 생체인식, 토큰검사, 패스워드 이용의 세가지로 나눌 수 있다. 패스워드를 이용하는 방법은 가장 간편하다는 장점을 가지고 있으나 인간의 기억력에 의존하는 방법이기 때문에 낮은 엔트로피를 가지고 있어, 사전공격이 가능하다. 또한 패스워드를 보관·관리하는 패스워드 파일이 유출될 경우에는 위장공격, 사전공격이 가능하게 된다는 문제점을 가지고 있다.

이러한 문제점의 해결 방안으로 AMP(Authentication and key agreement via Memorable Password)프로토콜이 제안 되었다[1]. AMP는 패스워드-확인자를 이용하고 이산대수문제를 기반으로 하는Diffie-Hellman[2][3] 방식의 프로토콜이며 증명가능한 접근(provable approach)으로 안전한 인증 및 키교환을 수행한다[1].

그러나 본 논문에서 제안하는 EC-AMP(Elliptic Curve-AMP)프로토콜은 이산대수문제대신에 타원곡선이산대수문제에 기반하여 상호인증 및 키교환을 수행한다. 이로 인해 보다 높은 보안성과 효율성을 가질수 있으며[4][5], 랜덤오라클모델(random oracle model)에서 여러 가지 공격에 대해 안정성을 제공한다.

본 논문은 2장에서 기존 연구에 대해 알아보고 3장에서는 파라미터 정의와 수치적 가정에 대해 기술한다. 4장에서는 EC-AMP 프로토콜을 설계하며 5장에서 프로토콜의 보안성에 대해 언급한다. 6장에서 효율성에 대해서 다루고 7장에서 결론을 맺는다.

2. 기존 연구

패스워드를 사용한 인증 및 키교환의 문제점들을 해결하고자 여러 프로토콜들이 제안되었다. EKE, DH-EKE, A-EKE 등과 같은 프로토콜로 인해 패스워드 인증 프로토콜 연구가 활성화 되게 되었고[1][3][6] SPEKE, S3P, SRP, GXY 등의 프로토콜이 제안되었다[1][7]. 그러나 이들 대부분의 프로토콜이 안전함을 증명하기에 불충분하거나 패스워드를 임시적인 방법으로 보호하기 때문에 [1][8][9], 이들 중 몇몇 프로토콜들은 이미 깨졌거나 해독중이다. 반면에 OKE를 시작으로 SNAPI, EKE2, AMP, PAK 등은 증명가능한 접근을 제시함으로써 발전된 패스워드 인증 프로토콜을 제시하였다[1][8][9].

A-EKE, B-SPEKE, SRP, AMP, GXY 등은 패스워드-확인자기반 프로토콜로, 클라이언트는 패스워드를 가지고 있는 반면 서버에서는 확인자만을 가지고 인증을 하게된다. 그러나 확인자기반 프로토콜이라도 서버의 파일이 유출될 경우 사전공격이나 서버위장이 가능하게 된다.

3. EC-AMP

3.1. 파라미터 정의

EC-AMP 프로토콜은 Alice(클라이언트)와 Bob(서버)간의 프로토콜로 정의하며, Eve(공격자)는 수동공격 및 능동공격을 시도한다. π는 패스워드, τ는 임의의 솔트(salt)를 의미한다. $\{0,1\}^*$, $\{0,1\}^\infty$는 각각 한정된 길이의 이진수와 무한길이의 이진수를 나타낸다.

$h(): \{0,1\}^* \mapsto \{0,1\}^{l(k)}$는 SHA-1, HAS-160같은 충돌없는 단방향 해쉬함수이다. 또한 EC-AMP 프로토콜에 사용된 모든 해쉬함수는 랜덤오라클 성질을 가진다고 가정한다.

EC-AMP 프로토콜은 유한체(finite field) Z_q(q는 소수)위의 타원곡선 E의 원소 P가 주어지고 Q=aP일 때 a를 찾기가 계산상 불가능(computationally infeasible)하다[4][10][11]는 타원곡선이산대수문제에 기반한다. 여기서 타원곡선 E는

$$y^2 = x^3 + ax + b,$$
$$(a, b \in Z_q, 4a^3 + 27b^2 \neq 0 \bmod q) \quad --(1)$$

로 정의하고, E위의 점 P, Q의 덧셈연산 $P(x_1, y_1) + Q(x_2, y_2) = (x_3, y_3)$는 다음과 같이 정의한다.

$$\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1}, & \text{if } P = Q \\ \dfrac{y_2 - y_1}{x_2 - x_1}, & otherwise \end{cases}$$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \quad --(2)$$

모든 연산은 유한체 Z_q에서의 연산이므로 mod q는 생략한다.

3.2. EC-AMP 프로토콜의 설계

EC-AMP 프로토콜의 기본개념은 AMP와 마찬가지로 낮은 엔트로피의 패스워드를 높은 엔트로피로 "증폭"시키고 시간유동적인 파라미터를 추가하는 것이다[1]. 또한 패스워드에 대한 정보를 누출시키지 않으며 상호 인증이 가능하다. 패스워드 π대신에 임의의 x를 선택해서 $\pi + x \bmod q$를 사용한다. 또한 서버측의 패스워드 확인자가 누출되었을 경우에 서버사칭 공격, 사전공격 등을 막기위해 서버측 패스워드 파일도 증폭시킨다. 임의의 τ와 비밀키와 같은 ζ로 구성된 확인자를 가지며, ζ는 스마트카드 등의 보안성있는 저장장치에 보관할수 있다.

EC-AMP 프로토콜은 셋업과정과 프로토콜 실행의 두 단계로 나눌수 있다.

3.2.1. 프로토콜 셋업

1) 전역 파라미터; Alice와 Bob은 타원곡선과 P(타원곡선위의 한점), q(소수)를 공유한다.

2) 등록; 안전한 방법을 통해서 Alice는 선택한 패스워드를 Bob에게 전달한다. 예를 들어, 방문등록을 하거나 PKI방법을 통해서 $v = h_1(id, \pi)$를 Bob에게 전달한다.

3) 서버저장; Bob은 임의의 τ, ($\tau \in_R \{0,1\}^k$)를 선택한 뒤 다음을 확인자로 저장한다.

$$(id, \tau, \nu = g^{(\zeta + \tau)^{-1} v}) \quad --(3)$$

3.2.2. 프로토콜 실행

1) Alice는 $c_1 = aP$, ($a \in_R Z_q$) --(4)를 생성해 Bob에게 (id, c_1)을 보낸다.

2) Bob은 메시지를 받은 후 해당 사용자의 τ와 ν를 읽어온 뒤 c_2를 생성하여 Alice에게 보낸다.

$$c_2 = (c_1)y + (\zeta + \tau)y\nu, \ (y \in_R Z_q) \quad --(5)$$

3) Alice는 c_2를 기다리는동안 다음을 계산한다.

$$v = h_1(id, \pi), \ \chi = (x + v)^{-1} \bmod q \quad --(6)$$

c_2를 받으면,

$$e = h_2(c_1, c_2, id, Alice, Bob), \quad --(7)$$
$$\varpi = \chi(x + e) \bmod q, \ \alpha = c_2 \varpi$$

를 계산한다. 결과적으로,

$$\begin{aligned} \alpha &= c_2 \varpi = (x + v)yP\varpi \\ &= (x + v)yP(x + v)^{-1}(x + e) \\ &= (x + e)yP \end{aligned} \quad --(8)$$

를 계산하게 된다. 그 후에

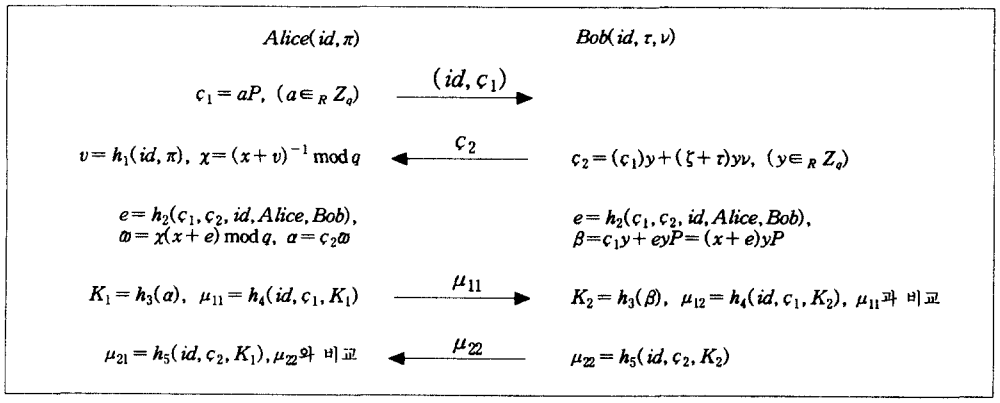
$$K_1 = h_3(\alpha), \ \mu_{11} = h_4(id, c_1, K_1) \quad --(9)$$

를 계산하여 Bob에게 μ_{11}를 보낸다.

4) 세 번째 메시지를 기다리는동안 Bob은

$$e = h_2(c_1, c_2, id, Alice, Bob), \quad --(10)$$
$$\beta = c_1 y + eyP = (x + e)yP$$

를 계산하고,



(그림 1)

$$K_2 = h_3(\beta),\ \mu_{12} = h_4(id, c_1, K_2) \quad --(11)$$

를 계산하여 도착된 μ_{11}와 μ_{12}를 비교하여 둘이 일치하면,

$$\mu_{22} = h_5(id, c_2, K_2) \quad --(12)$$

를 생성하여 Alice에게 보낸다. 만약 일치하지 않으면 모든 과정을 중단한다.

5) Alice는 네 번째 메시지를 기다리며

$$\mu_{21} = h_5(id, c_2, K_1) \quad --(13)$$

를 계산하고 수신된 μ_{22}와 일치하게 되면 상호인증이 완료된다. 만약 일치하지 않으면 모든 과정을 중단한다.

이 과정을 도식화하면 (그림1)과 같다. 결과적으로 상호인증을 통해 비밀키 $\alpha = \beta = (x+e)yP$를 서로 공유하게 된다.

4. 보안성 및 예측 효율성

4.1. 보안성

앞에서 언급했듯이 EC-AMP 프로토콜에 사용된 모든 해쉬함수는 랜덤오라클 성질을 가지고 타원곡선이산대수문제를 풀기는 계산적으로 불가능하다[4][10][11]고 가정한다. 이러한 가정하에서 다음의 특성들을 만족한다.

1. Perfect forward secrecy; 패스워드가 유출된 경우라도 타원곡선이산대수문제를 풀수 없기 때문에 이전에 사용된 세션키를 얻을수 없다.

2. Denning-Sacco 공격; 이전에 사용된 세션키가 유출되어도 타원곡선이산대수문제를 풀수 없기 때문에 사용자의 패스워드를 알아낼수 없다.

3. Replay 공격; c_1, c_2, μ_1, μ_2에는 일시적인 파라미터가 들어있는데 이러한 파라미터를 찾기는 타원곡선이산대수문제에 의하여 알아낼수 없다.

4. 온라인 추측공격; 온라인상에서 패스워드를 추측하여 시도하는 공격은 횟수를 제한하므로써 막을수 있다.

5. 확인자 유출; 패스워드파일이 유출될 경우라도 ζ를 모르면 침투할수 없다.

4.2. 예측 효율성

이미 널리 쓰이는 RSA(인수분해문제)나 DSA(이산대수문제)같은 알고리즘은 현재 허용되는 보안기준(10^{12} MIPS year)를 만족하려면 1024비트 크기의 유한체를 사용하여야 하는 반면에 ECC(Elliptic Curve Cryptography)는 160비트 크기의 유한체로도 충분하다[4]. 더 나아가 보다 높은 보안성이 필요할 경우에 RSA, DSA는 2차 함수적인 많은 비트수를 필요로 하는것에 비해 ECC는 약간의 추가 비트수로도 훨씬 높은 보안성을 만족한다.

160비트의 ECDSA와 1024비트의 DSA를 비교했을 때, ECC가 대략 6~10배 정도 빠르면서 비슷한 정도의 보안성을 가진다[4][5]. 따라서 프로토콜 수행시간의 큰 비중을 차지하는 지수곱셈을 타원곱셈으로 대치하므로써 Diffie-Hellman기반의 AMP 프로토콜보다 ECC기반의 EC-AMP 프로토콜이 더욱 빠른 수행시간을 보장한다.

또한 통신부하측면에서도 총 4개-그 중 큰 데이터는 c_1과 c_2뿐이다-의 데이터만이 전송되므로 다른 여러 프로토콜에 비해 효율적이다.

5. 결론

본 논문에서는 이산대수문제를 사용하는 AMP 프로토콜을 향상시킨 타원곡선이산대수문제에 기반한 EC-AMP 프로토콜을 제안하였다. 기존에 하드웨어를 이용하는 등의 여러 가지 강력한 인증 방법들이 있으나 장치휴대, 편의성이 취약하다. 반면에 EC-AMP 등의 패스워드를 이용한 편리하고도 안전한 인증방법을 통해서 분산환경에 보안성을 더할수 있을 것이다. 앞으로 더욱 효율적인 타원곡선 덧셈을 이용하여 보다 높은 수행속도를 얻을 수 있을 것이다.

참고문헌

[1] Taekyoung Kwon, "Authentication and Key Agreement via Memorable Password" , IACR ePrint, 2000.

[2] Alfred J. Menezes, Paul C.van Oorschot and Scott A. Van stone, *Handbook of Applied Cryptography*, CRC Press, pp.49-125, 1997.

[3] Bruce Schneier, *Applied Cryptography*, Wiley, pp.513-522, 1995.

[4] Certicom Corp., "Remarks on the security of the Elliptic curve cryptosystem" , http://www.certicom.com, 2000.

[5] Julio Lopez and Ricardo Dahab, "Performance of Elliptic Curve Cryptosystems" , *Technical report IC-00-08*, http://www.dcc.unicamp.br/ic-main/publications-e.html, 2000.

[6] S.Bellovin and M.Merritt, "Encrypted Key Exchange: password-based protocols secure against dictionary attcks," *Proceeding of the 1992 IEEE Computer Society conference on Research in Security and Privacy*, pp.72-84, 1992.

[7] T.Wu, "Secure Remote Password protocol," *Internet Society Symposium on Network and Distributed System Security*, 1998.

[8] Victor Boyko, Philip MacKenzie and Sarvar Patel, "Provably Secure Password-Authenticated Key Exchange Using Diffe-Hellman," *Eurocrypt2000*, 2000.

[9] Phil MacKenzie, "More Efficient Password Authenticated Key Exchange," *RSA2001*, 2001.

[10] Gareth Jones, "Cryptography and Elliptic curves" , Project report of Univ. of Southampton, 1999.

[11] 이성우, "ECC 개론" , 고려대학교 정보보호기술연구소, http://www.cipher.or.kr, 2000.