타원곡선 디피-헬만에 기반하는 그룹 키 동의

한준호*, 김경훈**, 김종**, 홍성제**

*포항공과대학교, 전자전기공학과
**포항공과대학교, 컴퓨터공학과

Group Key Agreement based on Elliptic Curve Diffie-Hellman

Joon-Ho Han*, Kyong-Hoon Kim**, Jong Kim**, Sung-Je Hong**

*Dept. of Electrical Electronics Engineering, Pohang Univ. of Science and Technology
**Dept. of Computer Science & Engineering, Pohang Univ. of Science and Technology

요 약

그룹통신에 대한 관심이 높아지면서 이제 그룹통신 보안문제도 점점 관심을 얻어가고 있다. 보안문제 중에서 그룹보안통신에서 사용하는 그룹 키 관리가 보안의 초석이라고 할 수 있다. 그룹 키 관리는 그룹 키 분배와 그룹 키 동의가 있는데 본 논문에서는 그룹 키 동의에 대해 다룬다. 이제껏 그룹 키 동의는 디피-헬만(Diffie-Hellman)을 기반으로 키 동의를 해 왔다. 본 논문에서는 디피-헬만을 대신하여 타원곡선에서 이산로그문제의 어려움을 바탕으로 한 타원곡선 디피-헬만의 사용을 제시하며, 타원 곡선 디피-헬만을 기반으로 한 키 트리 기반 그룹 키 생성의 성능을 분석한다.

I. 서론

PGP를 사용하여 친구에게 이메일을 보내는 광경이 이제 우리에게는 더 이상 생경하지 않다. 감시와 자유, 그 끊임없는 변증법적 긴장은 네트워크 세계에 보안을 요청하기에 이르렀다. 지금까지 우리가 주로 봐왔던 것은 PGP 같은 일대일 통신에서의 보안이었다. 그런데 만약 어떤 회사의 중역들이 각 지사에서 회의를 한다고 생각해보자. 그들의 한마디 한마디는 회사 밖으로 나가서는 안 된다. 따라서 회의내용은 암호화가 필요하고, 암호화를 하기 위한 기본은 키 관리이다. 하지만 이 통신은 일대일 통신이 아니라 다대다 통신이다. 이 때, 각 중역들 간에 키를 가지는 것이 아니라, 중역들이 공통으로 하나의 키를 가진다.

앞에서 이야기 한 중역회의는 그룹보안통신의 한 예이다. 그리고 그룹보안통신은 그룹회원들이 공통의 키를 가짐으로 이루어지는데, 이 키를 그룹 키라고 한다. 그런데 문제는 그룹이 역동적인 특성을 가질 때 나타난다. 이합집산이 심한 그룹에서는 매번 회원이 바뀔 때마다 그룹 키를 갱신해야만 한다. 새 회원이 가입할 때에 이전 그룹 키를 준다면, 이전 통신물의 보안이 깨어지고, 회원이 탈퇴할 때 키를 바꾸지 않는다면, 탈퇴한 회원이 현재 통신을 엿들을 수 있다.

그룹 키를 생성, 관리하는 방식에는 그룹 키 분배와 그룹 키 동의가 있다. 본 논문은 그룹 키 관리 중에 타원곡선 디피-헬만을 기반으로 하는 그룹 키 동의를 제안하고 분석한다. 본 논문의 구성은 다음과 같다. 본문의 1장에서는 관련연구를 살펴보고, 2장에서는 제안하는 그룹 키 동의 방식을 설명한다. 그리고 3장에서는 성능 분석을 하고, 마지막으로 결론을 맺는다.

II. 본문

1. 관련연구

1) 그룹 키 분배

그룹 키 분배는 신뢰할만한 제 삼자가 키 서버가 되고, 키 서버가 각 그룹회원들과 비밀 키를 가지면서 그룹 키를 비밀 키로 암호화해서 보내주는 방식이다. 그래서 키 서버는 회원 가입, 탈퇴 시 키를 갱신해서 회원들에게 나누어준다. 그룹 키 분배의 장점은 키 생성이 수월하고 키를 분배하는데 큰 시간이 들지 않아, 규모가 큰 그룹에 적당하다는 점이다. 대신 키 서버에 대한 회원들의 신뢰문제와 결함이 생겼을 경우 통신전체에 결함이 생기는 문제가 있다.

2) 그룹 키 동의

그룹 키 동의는 그룹 키를 회원들이 만드는데, 이 그룹 키에는 회원들의 독특한 정보가 새겨진다. 이 점이 키 생성을 키 서버가 점유하는 키 분배와 차이점이다. 또한 각 회원이 키 생성을 직접 한다. 그룹 키 동의의 장점은 신뢰할만한 제 삼자

없이 그룹을 만들 수 있다는 점이다. 키 서버에 대한 요청이 없기 때문에 번거롭지도 않다. 대신 키 생성에 회원들의 정보가 새겨지기 때문에 많은 시간이 걸릴 뿐 아니라 각 회원들이 키를 생성하는 과정도 있어 계산 오버헤드가 따른다. 따라서 규모가 큰 그룹에는 적합하지 않다.

그룹 키 동의에서 키 동의는 주로 유한체(finite field)의 이산로그 문제의 어려움을 기반으로 한 디피-헬만을 따른다. 디피-헬만 키 동의는 원래 일대일 키 동의로 제안되었다.[1] 디피-헬만 키 동의는 그룹 키 동의 연구에서 여럿이 키를 동의하도록 확장되었다.[2]

그룹 키 동의의 가장 큰 문제점은 확장성이다. 그룹의 변동에 따른 키의 갱신에 드는 계산비용이 그룹 키 분배보다 크다. 그룹 회원의 수가 n이라고 하면 계산은 O(n)의 복잡도를 가진다. 확장성을 해결하기 위해 논리적 구조로 키 트리가 제시되었다.[3][4] 키 트리의 키 갱신에 드는 계산의 복잡도는 O($logn$)이다. 현재 그룹 키 분배, 동의 모두 트리 구조를 기본으로 사용하고 있다.

3) 타원곡선 디피-헬만

1985년 Miller와 Koblitz는 각각 독립적으로 타원곡선을 이용한 암호시스템을 제안했다.[5] 이 암호시스템은 타원곡선에서의 이산로그 문제의 어려움을 기반으로 한다. 타원곡선을 이용한 암호시스템에서 기존의 디피-헬만에 해당하는 것이 타원곡선 디피-헬만이다.

타원곡선의 이산로그 문제는 타원곡선 상의 점 P와 Q가 주어졌을 때, 다음을 만족하는 k를 찾는 문제이다.

$$P \in E(F_q), Q \in (P, 2P, \ldots, lP), 1 \le k \le l$$

$$Q = kP, where P \in E(F_q) \quad (1)$$

다음 그림 1은 타원곡선 디피-헬만 키 동의의 동작을 간단히 보여준다.

앨리	빌리
K_i: 개인키, Q_i:공개키, G:베이스 포인트	
$Q_a = k_a G$	$Q_b = k_b G$
$Q_a \longrightarrow Q_b$	
$Z = k_a Q_b = k_a k_b G$	$Z = k_b Q_a = k_a k_b G$

그림 1: 타원곡선 디피-헬만

앨리와 빌리가 각각 개인키로 공개키를 만들어서 교환하고 교환한 공개키와 자신의 개인키로 서로 공유비밀 Z를 만들 수 있다.

타원곡선 디피-헬만 방식은 디피-헬만과 같은 안전도에서 비교할 때 훨씬 빠르고 효율적이며 짧은 키를 갖는 장점이 있다. 타원곡선 디피-헬만 키 동의는 사용되고 있으나 그룹 키 동의로 확장되지는 않았다. 따라서 본 연구는 타원곡선 디피-헬만을 그룹 키 동의로 확장하여 그룹 키 동의를 제시한다. 이전 그룹 키 동의에서는 대부분 유한체 Z_p에서 디피-헬만 키 동의를 그룹으로 확장해서 사용하고 있는데, 타원곡선 디피-헬만 키 동의를 그룹으로 확장해서 성능 향상을 보인다.

2. 제안하는 그룹 키 동의

1) 키 트리를 이용한 그룹 키 동의

본 논문에서는 타원곡선 디피-헬만을 기반으로 그룹 키 동의를 한다. 확장성을 고려하여 그룹 키 동의에 키 트리 구조를 사용한다. 다시 말해, 키 트리 구조에서 그룹 회원들이 그룹 키 동의를 하는데, 그 방식은 타원곡선 디피-헬만을 따른다.

표 2는 키 트리에서 사용하는 기호이다.

표 2: 키 트리에 사용하는 기호

기호	의미
N_{ij}	트리의 노드 (i+1:높이, $0 \le j \le 2^i$)
M_i	i번째 그룹회원
G	타원곡선 상의 베이스 포인트
k_{ij}	노드N_{ij}의 개인키
$f(Q)$	타원곡선상의 점 Q를 q로 바꾸어주는 함수 $1 \le q \le l$
Q_{ij}	노드N_{ij}의 공개키
$L(N_{ij})$	노드N_{ij}의 왼편 자식노드
$R(N_{ij})$	노드N_{ij}의 오른편 자식노드

그림 2는 M_A, M_B, M_C가 가입한 그룹의 키 트리를 보여준다. 키 트리에서 단말 노드를 제외한 노드의 공개키와 개인키는 다음과 같은 생성과정을 거친다.

$$Q_{ij} = L(N_{ij})의\ k_{ij} \cdot R(N_{ij})의\ Q_{ij} \quad (2)$$

$$= R(N_{ij})의\ k_{ij} \cdot L(N_{ij})의\ Q_{ij} \quad (3)$$

$$k_{ij} = f(Q_{ij}) \quad (4)$$

키 트리에서 루트노드 N_{00}가 그룹 키에 해당하고 N_{20}, N_{21}, N_{11}은 각각 회원 M_A, M_B, M_C가 가진 개인키에 해당한다. 그림 2에서 그룹 키를 생성하는 과정은 다음과 같다.

1. M_A와 M_B가 N_{20}, N_{21}의 내용으로 타원곡선 키 동의를 해서 N_{10}에 해당하는 키를 만든다. $f(Q_{10})$가 N_{10}의 개인키가 된다. ($Q_{10}=k_{20}k_{21}G$)

2. M_A는 N_{10}의 개인키k_{10}과 N_{11}의 공개키 Q_{11}로 그룹 키를 만든다. M_B도 M_A와 같은 방식으로 그룹 키를 만들 수 있다. ($Q_{00}=k_{10}Q_{11}$)

3. M_C는 N_{11}의 개인키k_{11}과 N_{10}의 공개키 Q_{10}로 그룹 키를 만든다. ($Q_{00}=k_{11}Q_{10}$)

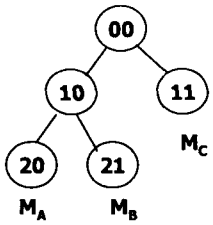

그림 2: 그룹 키 트리

2) 그룹 가입

가입은 하나의 회원이 가입하는 경우만 생각한다. 가입할 경우 이전 통신물의 보안을 위해 그룹 키의 갱신이 필요하다. 그림 3은 회원이 가입할 때 키 트리의 갱신을 보여준다.

트리의 높이는 작을수록 좋기 때문에 새로 들어온 회원은 N_{23}을 만들어서 N_{11}에 붙게 되고, M_C는 N_{22}를 생성하고 N_{11}에 붙게 된다. 키의 갱신은 변화가 생긴 노드에서 루트 노드까지의 경로에 위치하는 노드의 키들이 바뀌어야 한다. 따라서 N_{11}과 N_{00}이 바뀌어야 한다. 키 갱신 과정은 다음과 같다.

1. M_C와 M_D가 키 동의를 해서 N_{11}에 해당하는 키를 만든다. $Q_{11}=k_{22}k_{33}G$

2. M_A는 N_{10}의 개인키 k_{10}와 N_{11}에서 새로 만든 공개키로 그룹 키를 만든다. M_B도 M_A와 같은 방식으로 그룹 키를 만들 수 있다. ($Q_{00}=k_{10}Q_{11}$)

3. M_C는 N_{11}의 개인키 k_{11}와 N_{10}에서 새로 만든 공개키로 그룹 키를 만든다. M_D도 M_C와 같은 방식으로 그룹 키를 만들 수 있다. ($Q_{00}=k_{11}Q_{10}$)

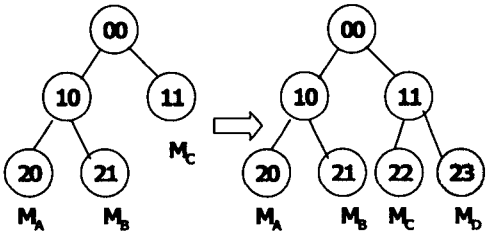

그림 3: 가입에서 그룹 키 트리 갱신

3) 그룹 탈퇴

회원이 탈퇴하는 경우 탈퇴한 회원에 해당하는 노드에서 루트 노드까지의 경로에 위치하는 노드의 키들이 바뀌어야 한다. 그림4는 회원이 탈퇴할 때 키 트리의 갱신이며, 키 갱신 과정은 다음과 같다.

1. M_A는 노드 N_{10}으로 옮기고, N_{20},N_{21}은 없앤다.

2. M_A는 N_{10}의 개인키k_{10}를 새 것으로 바꾸고 공개키 Q_{10}을 만든다.

3. M_A는 N_{10}의 개인키k_{10}과 N_{11}의 공개키 Q_{11}로 그룹 키를 만든다.

4. M_C는 N_{11}의 개인키 k_{11}와 N_{10}에서 새로 만든 공개키로 그룹 키를 만든다. M_D도 M_C와 같은 방식으로 그룹 키를 만들 수 있다. ($Q_{00}=k_{11}Q_{10}$)

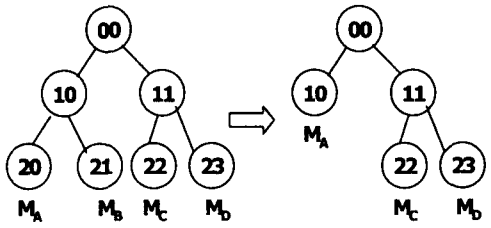

그림 4: 탈퇴에서 그룹 키 트리 갱신

3. 성능 분석

타원곡선 디피-헬만을 이용한 그룹 키 생성에 걸리는 시간을 생각해보자. 키 트리는 균형 잡힌 트리(Balanced Tree)를 가정하고, 통신 전송시간은 동일하다고 가정한다. 표 3은 생성시간 측정 파라미터들이다.

표 3: 그룹 키 생성 시간 파라미터

n	그룹의 회원 수
t_{pub}	공개키 생성시간
t_{secret}	공유비밀 생성시간
p	데이터 크기
l	전송시간

회원의 수가 n 명 있을 때, 생성되는 트리의 깊이는 $\lceil log_2 n \rceil + 1$이 되며, 단말 노드에서 루트 노드까지 각 레벨 당 $(t_{pub} + t_{secret} + p \square l)$이 걸린다. 따라서, 모든 그룹 회원이 그룹 키를 생성하는데 걸리는 시간은 $\lceil log_2 n \rceil (t_{pub} + t_{secret} + p \square l)$이 된다. 이 식을 이용하여, 키 트리를 기반으로 한 디피-헬만 키 동의(TGDH)와 키 트리를 기반으로 한 타원곡선 디피-헬만 키 동의(TG-ECDH)의 그룹 키 생성 속도를 그룹 크기에 따라 비교하면 그림 5와 같다. 그림 5에서 사용한 파라미터는 표 4와 같다.

표 4: 디피-헬만/ 타원곡선 디피-헬만 성능비교[6]

	디피-헬만	타원곡선 디피-헬만
p	1024 bits	320 bits
t_{pub}	1.788 msec	0.516 msec
t_{secret}	8.148 msec	1.695 msec

그림 5에서 대역폭은 10Mbps, 1Mbps, 100Kbps로 두고 그룹 키 생성 속도를 비교했다. 그림에서 보듯이, 타원곡선 디피-헬만 키 동의가 적어도 3배 이상 빠른 것을 볼 수 있다.

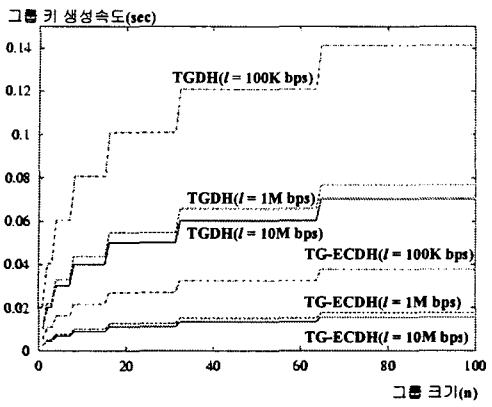

그림 5: 그룹 키 생성속도의 비교

4. 결론

본 논문에서는 키 트리 구조를 사용해서 타원곡선 디피-헬만 방식으로 키를 생성하고 그룹 가입과 탈퇴가 어떻게 이루어지는지 살펴보았다. 제안하는 그룹 키 동의 방법은 타원곡선 디피-헬만 방식을 사용함으로써, 이전 방법보다 약 3~5배 정도의 성능 향상을 보였다. 향후 연구 계획은 제안하는 그룹 키 동의 방법을 구현하고, 보다 효율적인 프로토콜을 제안하는 것이다.

참고문헌

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644-654, November 1976.

[2] M. Steiner, G. Tsudik, and M. Waidner, "CLIQUES: a New Approach to Group Key Agreement," *In Proceedings of the 18th International Conference on Distributed Computing Systems*, pp. 380-387, May 1998.

[3] D. M. Wallner, E. G. Harder, and R. C. Agee, "Key Management for Multicast: Issues and Architecture," internet draft draft-wallner-key-arch-01.txt, September 1998.

[4] Y. Kim, A. Perrig, and G. Tsudik, "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups," *In Proceedings of the 7th ACM Conference on Computer and Communications Security*, pp. 235-244, November 2000.

[5] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203-209, 1987.

[6] 이동훈, 황효선, 임채훈, "타원 곡선 암호의 기초와 응용," *퓨처시스템 암호체계센터 기술보고서 FS-TR01-03*, 2001년 8월.