그룹 서명 기법을 위한 호모모르픽 Proactive AVSS(Asynchronous Verifiable Secret Sharing)의 비잔틴 어그리먼트 프로토콜

성순화° 공은배
충남대학교 컴퓨터공학과 {shsung°, keb}@ce.cnu.ac.kr

Byzantine Agreement Protocol with Homomorphic Proactive AVSS for Group Signature Scheme

Soon Hwa Sung° Eun Bae Kong
Dept. of Computer Engineering, Chungnam University

요 약

인터넷과 같은 항상 변화하고 있는 거대한 네트워크에서는 안전한 전자거래를 위해 많은 키들과 메시지 확장 없이 그룹의 구성원이 다른 구성원이나 그룹에게 전해진 메시지 인증이 보장되어야 한다. 본 논문에서는 이를 위한 효율적인 그룹 서명 기법인 그룹의 공개키 수정없이 그리고 나머지 구성원들이 새로운 인증을 요구하지 않는 인증방법으로, 항상 변화하는 인터넷에서 신뢰기관인 중앙 인증 기관이 없는 쓰레시홀드 크립토그래피(Threshold Cryptography)를 가진 비잔틴 어그리먼트 프로토콜(Byzantine Agreement Protocol)을 제안한다. 아울러 쓰레시홀드 크립토그래피는 키 관리 문제를 피하고 키 분산을 하기 위해 신뢰된 분배자없이 호모모르픽 시크리트 쉐어링의 Proactive AVSS(Asynchronous Verifiable Secret Sharing)를 제시한다.

1. 서론

많은 통신은 각 개인에서 기관, 회사, 정부기관, 비영리 기관 등에서 영수증, 세금, 전문 기관의 회보 등의 형식으로 이루어진다. 이러한 기관 역시 서로의 통신을 필요로 하며 관련된 많은 안전성이 개인이 아니라 그룹으로 이루어진다. 그래서 많은 키들과 메시지 확장 없이 그룹의 구성원이 다른 구성원이나 그룹에게 전해진 메시지 인증이 보장되어야 한다. 보통 그룹 구성원은 기관과 그 공개키를 알지만 그 기관에 일하는 사람을 알 필요가 없을 뿐더러 기관의 이름으로 서명할 영향력을 누가 가지고 있는지 알 필요가 없다. 그러므로 키 관리 문제와 기관의 영향력을 분산시키기 위해 외부에 알려지지 않은 기관의 구성원들의 많은 공개키에 의존하는 대신 기관은 주로 하나의 공개키를 가져야만 한다. 또한 기관이 하나의 키를 가진다면 논쟁을 피하고 신뢰도를 보장하기 위해서 서명(복호화, 혹은 암호화시스템 사용) 영향력이 분산되어야만 한다[1,2,3]. 이러한 문제 해결을 위해 쓰레시홀드 크립토그래피(threshold cryptography)를 고려하려 한다.

인터넷과 같은 아주 큰 네트워크의 네트워크 그래프는 보통 잘 알려져 있지 않고 있다. 왜냐하면 네트워크는 항상 동적으로 새로운 컴퓨터와 링크가 네트워크에 더해지고 어떤 컴퓨터는 다운되며 변화하고 있기 때문이다. 그러나 비잔틴결함(Byzantine faults)[4,5]에 대한 전통적 연구는 네트워크가 알려진 경우에만 다루어진다. 네트워크가 알려지지 않은 경우 결함노드는 결함 데이터를 보낼 수 없으나 위조 노드들과 에지들(edges)이 존재하는 것처럼 흉내낼 수는 있다. 그러므로 본 논문은 신뢰할 수 있는 중앙 인증 기관없이 알려지지 않은 네트워크에서 비잔틴 결함을 다루어 향상된 인증기법인 그룹 서명 기법으로 발전시키려고 한다. 임의 방법과 하나의 목적을 위해 두가지 방법을 사용하여 오염된 파티들(corrupted parties)의 동작을 변경하는 비잔틴 적들(Byzantine adversaries)을 가진 오염된 파티들을 특히 고려한다. 이러한 오염된 파티들이 있음에도 불구하고 그룹 서명이 제대로 실행될 수 있는 방안을 살펴보기로 한다.

2. 알려지지 않은 네트워크에서 그룹 서명 기법

2.1 그룹 서명의 개념

그룹 서명 기법은 그룹 중의 일원이 그룹을 대표하여 익명으로 메시지를 사인하게 하는 기법이다. 나중에 논쟁이 있을 경우, 지정된 그룹 관리자가 익명성을 철회하여 원래 서명자를 확인할 수 있다. 간단한 그룹 서명 기법 구성은 그룹 공개키의 크기와 서명 길이가 그룹 구성원의 수에 독립적인 것이다. 그룹 공개키는 기본적으로 일반 디지털 서명 기법의 그룹 관리자의 공개키로 구성된다. 각 그룹 구성원은 많은 키쌍(공개키, 비밀키)을 생성하고, 멤버쉽 키라고 불리우는 그룹 구성원의 공개키가 그룹 관리자에 의해 사인되거나 인정된다. 그룹 구성원은 이러한 멤버쉽 키들 중 하나로 메시지를 사인할 수 있으며, 그룹 관리자가 멤버쉽 키가 어느 구성원에 속하는지 알고 있기 때문에 그룹 관리자는 쉽게 서명을 공개할 수 있다. 물론 멤버쉽 키는 한번만 사용

가능하며, 그렇지 않으면 서명이 링크될 수 있다. 이러한 해결은 멤버쉽 키와 인증서 지식만 제공함으로써 극복할 수 있다. 즉 Brassard et al.[6] 혹은 Boyar et al.[7]의 영지식 증명 기술을 사용할 수 있다. 게다가 멤버쉽 키는 더 이상 나타나지 않으므로 서명자는 그룹 관리자가 나중에 서명을 공개하는 정보를 제공해야만 한다. 이러한 기법은 멤버쉽 관리자 도움없이 멤버쉽 인증을 계산하기가 어렵다. 따라서 그룹의 공개키 수정없이 그리고 나머지 구성원들이 새로운 인증을 요구하지 않는 인증방법을 찾아야 한다. 이를 해결하기 위해 알려지지 않은 네트워크에서 신뢰할 수 있는 중앙 인증 기관없이 쓰레시홀드 크립토그래피를 가진 비잔틴 어그리먼트(Byzantine Agreement)를 제안한다. 아울러 쓰레시홀드 크립토그래피는 키 관리 문제를 피하고 키 분산을 하기 위해 신뢰자 없이 호모모르픽 시크리트 쉐어링의 Proactive AVSS(Asynchronous Verifiable Secret Sharing)를 제안한다.

2.2 알려지지 않은 네트워크에서 비잔틴 동의 문제

비잔틴 결함 모델은 네트워크가 알려진 경우에만 다루어진다. 그러므로 현재의 비잔틴 모델은 컴퓨터 안전성에 부적합하다. 알려지지 않은 네트워크에서 비잔틴 동의 문제는 임의 방법과 하나의 목적을 위해 두가지 방법에서 오염된 파티들의 동작을 변경하는 다음과 같은 비잔틴 적들을 사용한다. 비잔틴 동의 문제의 기본 형식은 다음과 같다: 일반 값에 동의하는 오염된 파티들을 허용하는 프로토콜을 디자인한다. 동의된 값은 오염되지 않은 파티들 중 하나의 입력 값이어야 한다.

본 논문은 오염된 파티들의 동작을 변경하는 비잔틴 적들의 오염된 파티들을 다룬다.

3. 쓰레시홀드 암호학

3.1 쓰레시홀드 암호학의 기본 개념

암호시스템은 두개의 입력을 가지는 함수 계산과 같다. 그들 중 하나는 키이고 다른 하나는 어플리케이션에서 어플리케이션으로 변하는 평문, 암호문, 서명문, 시드(seed) 등이다. 종종 이 함수는 파라미터가 키인 하나의 입력 함수 $f_{key}(input)$로 표현된다. 반면 파라미터가 입력인 하나의 키 함수 $g_{input}(key)$에도 유용하다.

$$f_{key}(input)=g_{input}(key) \qquad (1)$$

몇몇 중요한 암호 기법은 중요한 요소를 실행하는 함수 g가 호모모르픽이다. 즉

$$g_b(k_1+k_2)=g_b(k_1)*g_b(k_2) \qquad (2)$$

여기서 b는 파라미터 입력이고, k_1, k_2는 키 공간이다.

샤미러(Shamir)의 비밀 공유 기법은 다음 특성을 가진다.

$$key=\sum_{i\in B} (constant_{i,B})(share_i) \qquad (3)$$

B는 모든 참가자들 집합 A의 부분 집합이며, 공유자 t=|B|이다. 샤미러의 비밀 공유 기법이 사용되고 g가 호모모르픽이면 (2), (3)을 사용하여 다음을 얻는다.

$$g_{input}(key)= g_{input}\left(\sum_{i\in B} (constant_{i,B})(share_i)\right) \quad (4)$$

$$=\prod_{i\in B} g_{input}(constant_{i,B} \bullet share_i)$$

$$=\prod_{i\in B} (g_{input}(share_i))^{constant\ i,B} \qquad (5)$$

(5)에서 $g_{input}(share_i)$는 공유자에 의해 계산되어 아이덴티티 i와 함께 신뢰성 있는 멤버쉽 관리자(combiner)에게 보내진다. 많은 공유자가 응답을 하면 아이덴티티를 알고 있는 멤버쉽 관리자는 공유자 t가 |B'| ≥t 인 집합 B'를 계산할 수 있다. 멤버쉽 관리자는 |B|=t인 B⊆B'를 선택하여 모든 i∈B에 대한 constant $_{i,B}$ 값을 얻어 (5)를 계산한다. 암호분석가는 t-1 할당이 영지식(zero-knowledge)[8]으로 시뮬레이션 될 수 있고 부분적 결과가 $g_{input\,i}(key)$이 minimal-knowledge[9]로 주어질 때 시뮬레이션 될 수 있다는 것을 안전성 목적으로 요구한다.

3.2 증명 가능한 호모모르픽 비밀 공유

비밀키의 분실이나 훼손을 대비하여 사용하는 기법이 비밀 공유(Secret Sharing:SS)[10,11]기법이다. 비밀 공유 기법은 비밀을 분산하여 보관하고 필요시 모아서 비밀을 복원하는 형식이다. 그 방법은 공유들을 참여자에게 분배한다. 참여자들은 비밀을 복원할 수 있는 권한이 부여된 단체 또는 개인들이다. 다음을 만족하는 비밀 공유 기법을 호모모르픽이라고 한다. 키 k 에 대한 공유 할당을 $(s_1, s_2, \cdots, s_l)$이라 하고 키 K'에 대한 공유 할당을 $(s'_1, s'_2, \cdots, s'_l)$ 이라 할 때 키 $k+K'$에 대한 공유 할당은 $((s_1+ s'_1), (s_2 + s'_2), \cdots, (s_l +s'_l))$을 만족한다. 이때 " +" 는 공유 공간과 키 공간을 정의한다. 샤미러의 비밀 공유 기법은 호모모르픽이다.

식 (3)을 만족하는 비밀 공유는 공유가 모듈에 속하고 constant $_{i,B}$ 는 스칼라이고 서버모듈에 속하는 키들은 호모모르픽이므로 검증하기가 쉽다. 전자선거에서 사용되는 (t-n)-threshold 비밀 공유 기법은 분배자가 배분하는 비밀 공유가 유효한지와 비밀 복원 시 참여자가 제출하는 비밀 공유가 유효한지를 판단할 수 없다는 것이다. 이에 대한 해결책을 [12]에서는 검증가능한 비밀공유(Verifiable Secret Sharing:VSS)개념으로 제시하였다. 그러나 제시된 구조가 공개적으로 검증 가능하지는 않았다. Stadler는 참여자들의 공개키를 비밀 공유에 사용하여 공개적으로 검증 가능한 비밀 공유(Publicly Verifiable Secret Sharing:PVSS)구조를 제시하였다[13]. [14]와 [15]에서는 Stadler의 PVSS방식을 개선하여 효율성을 증대시키고 비밀의 분배 및 복원이 정당하게 행하여졌음을 증명하였다.

4.Byzantine Agreement Protocol of Proactive AVSS without a trusted dealer

Proactive AVSS 기법은 두개의 프로토콜로 구성된다:Sharing Protocol(S), Reconstruction Protocol(R). 공유 프로토콜은 세 단계로 이루어진다:먼저 각 파티는 분배자로부터 비밀 공유를 기다린다. 그 다음, 파티들은 그들의 공유가 유일한 비밀을 정의한다는 것을 함께 검증하려고 한다. 각 파티가 유일한 비밀로 정의되었다는 것이 한번 확인되면, 각 파티는 지역적으로 계산하여 검증 단계에서 모여진 정보를 사용하여 정확한 비밀 공유를 출력한다. 재구성 프로토콜에서는 각 파티가 미

리 정의한 집합 R에 있는 파티들에게 공유를 보낸다. 그 다음, R에 있는 각 파티는 유일한 비밀을 결정하기 위해 충분한 공유를 기다려서 재구성된 비밀을 출력한다[16]. 잘못된 공유($\sum_{j\in B} s'_{j,i}$)를 다루기 위해 본 논문에서는 새로운 알고리즘[17]을 사용한다. 따라서 재구성에 있어서 [18]과 [19]기법에서는 비밀 재구성에서 조금의 에러 확률을 가지는 반면, 제안한 기법은 재구성에서 에러 확률이 없으며 지연도 없다.

호모모르픽 비밀 공유의 다음과 같은 사용은 신뢰된 분배자의 필요없이 활용될 수 있다. 첫번째 참가자는 유일하게 임의의 키 k_1를 선택하여 이 키를 생성하는 공유들($s_{1,1}$, $s_{1,2}$,''' ,$s_{1,l}$ /: 공유자 수)의 분배자를 실행시킨다. 첫번째 참가자가 안전한 채널을 사용하여 참가자 i에 대한 공유 $s_{1,i}$ 와 $1 \le i \le l$ 를 보낸다. $B \subset A$에서 t참가자는 독립적으로 랜덤을 선택하는 비슷한 기능을 형성할 것이고 $s_{1,i}$ 대신 $s_{j,i}$ 공유들을 생성하여 비밀리 참가자 i에게 보낸다. 이때 참가자 i는 공유 $s_i = \sum_{j\in B} s_{j,i}$ 를 계산할 수 있으며, 공유 기법이 호모모르픽이기 때문에 s_i 는 키 $k = \sum_{j\in B} k_j$ 의 공유이다. 쓰레시홀드 크립토그래피 아이디어의 처음 사용은 [20]에 있었고 Pedersen 기법[21] 역시 분산이 검증 가능하다는 것을 보장한다. 즉 공유자가 돌려받은 공유는 항상 같은 비밀키를 다시 계산할 수 있으며, 이때 비밀키는 공개적으로 생성된 공개키와 일치한다는 것을 보장한다.

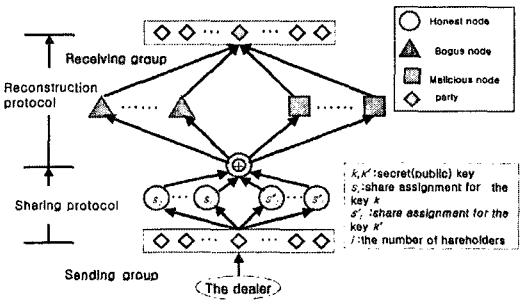

그림 1. Byzantine Agreement Protocol with Proactive AVSS

5. 결론

그룹 서명 기법은 그룹 중의 일원이 그룹을 대표하여 익명으로 메시지를 사인하게 하는 기법이다. 나중에 논쟁이 있을 경우, 지정된 그룹 관리자가 익명성을 철회하여 원래 서명자를 확인할 수 있다. 본 논문에서 제안한 그룹 서명 기법은 그룹의 공개키 크기와 서명의 길이뿐만 아니라 사인과 검증에 대한 계산적 결과까지도 그룹 구성원 수에 독립적이다. 따라서 항상 변화하고 있는 인터넷과 같은 거대한 네트워크에서의 안전한 전자거래를 위하여, 변화에 능동적으로 대처할 수 있는 그룹 서명 기법으로 신뢰된 분배자없이 호모모르픽 Proactive AVSS를 가진 비잔틴 어그리먼트 프로토콜로 악의적인 환경에서도 안전한 그룹 서명이 이루어진다.

참고문헌

[1] G. R. Blakley, " Safeguarding cryptographic keys" , In Proc. Nat. Computer Conf. AFIPS Conf. Proc., pp. 313-317, 1979. vol.48.

[2] M. Ito, A. Saito, and T. Nishizeki, " Secret sharing schemes realizing general access structures" , In Proc. IEEE Global Telecommunications Conf., Globalcom' 87, pp.99-102. IEEE Communications Soc. Press, 1987.

[3] A. Shamir, " How to share a secret" , Commun. ACM, 22, pp.612-613, November 1979.

[4] L. Lamport, R. Shostak, and M. Pease, " The Byzantine Generals Problem" , ACM Transactions on programming languages and systems, 4(2), pp. 382-401, 1982

[5] D. Dolev, C. Dwork, O. Waatz, and M. Yung, " Perfectly Secure Message Transmission" , Journal of the ACM, 40(1), pp.17-47, January 1993.

[6]Gilles Brassard,David Chaum,and Claude Crepeau," Minimum disclosure proofs of knowledge" ,Joural of Computer and System Sciences, 37(2):pp156-189,Oct.1988.

[7]Joan Boyar,Rene Peralta, " Short discreet proofs" , Advances in Cryptology-EUROCRYPT' 96, volume 1070 of Lecture notes in computer Science, pp131-142,Springer Verlag, 1996

[8] S. Goldwasser, S. Micali, and C. Rackoff. " The knowledge complexity of interactive proof systems" , SIAM J. Comput., 18(1), pp. 186-208, February 1989.

[9] Z. Galil, S. Haber, and M. Yung. " Minimum-knowledge interactive proofs for decision problems" , SIAM J. Comput.,18(4), pp.711-739, August 1989.

[10]A. Shamir, " How to share a secret' , Communication of the ACM, 22(11):pp.612-613, 1979.

[11]G.R.Blakley, " Safeguarding cryptographic keys' ' , In Proceeding of the National Computer Conference 1979, Vol. 48 of AFIPS Conference Proceedings, pp.313-317, 1979.

[12]B.Chor, S. Goldwasser, S. Micali, and B. Awerbuch, " Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults" , In Proceeding of the 26th IEEE Symposium on the foundations of Computer Science(FOCS), pp.383-395, 1985.

[13]M. Stadler, " Publicly Verifiable Secret Sharing" , Advances in Cryptology-Eurocrypto96, LNCS Vol.1070, pp. 190-199, Springer-Verlag, 1996.

[14]E. Fujisaki, T. Okamoto, " A Pratical and Provably Secure Scheme for Publicly Verifiable Secret Sharing and Its Applications" , Advances in Cryptology-Eurocrypto98, LNCS Vol., pp.32-46, Springer-Verlag, 1998.

[15]B. Schoenmakers, " A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting" , Advances in Cryptology-Crypto99, LNCS Vol., pp.148-164, Springer-Verlag, 1999.

[16] Ran Canetti, "Studies in Secure Multiparty Computation and Applications", pp73-79, March 1996.

[17]Soon Hwa Sung, Eun Bae Kong," Byzantine Agreement with Threshold Cryptography in Unknown Networks" , SAM' 04, pp.68-74, Las Vegas, Nevad, USA, June 21-24,2004

[18] P. Feldman, "Asynchronous Byzantine Agreement in Constant ExpectedTime", unpublished manuscript, 1989.

[19] R. Canetti and T. Rabin, "Optimal Asynchronous Byzantine Agreement", 25th STOC, 1993, pp.42-51.

[20] T. P. Pedersen, "A threshold cryptosystem without a trusted party", In D.W. Davies, editor, Advances in Cryptology, Proc. of Eurocrypt '91(Lecture Notes in Computer Science 547), pp.522-526, Springer-Verlag, April 1991, Brighton, U.K.

[21]H.Petersen and P. Horster, "Self-certified keys Concepts and Applications", In Proc. Communications and Multimedia security'97, 1997.