셀룰러 오토마타를 이용한 안전한 그룹 통신 프로토콜

이준석, 박영호, 이경현
부경대학교 전자계산학과
부경대학교 정보보호학과
부경대학교 전자컴퓨터정보통신공학부

Secure group communication protocol using a cellular automata

Jun-Seok Lee, Young-Ho Park, Kyung-Hyune Rhee
Department of Computer Science, Pukyong National University
Department of Information Security, Pukyong National University
Division of Electronic, Computer and Telecommunication Engineering, Pukyong National University

요 약

본 논문은 그룹 멤버들간의 안전한 통신을 위한 그룹키 관리(Group key management)에 대한 새로운 방법을 제안한다. 제안된 방식은 선형 셀룰러 오토마타를 이용해서 생성된 involution 특성을 갖는 기본 암호 프리미티브를 이용하여 비밀 공유키를 생성한다. 제안된 방식은 공모에 대한 위협을 근본적으로 방지할 수 있는 특징을 가지고 있다.

1. 서론

인터넷의 활용 영역이 다양한 분야로 확대되면서 여러 명의 사용자들에게 동일한 서비스를 제공해주기 위한 그룹 통신에 대한 요구가 증가하고 있다. 따라서 안전한 그룹 통신을 위해 그룹 사용자들에게 전송되는 정보에 대한 기밀성(confidentiality)과 무결성(integrity) 그리고 그룹 사용자에 대한 인증(authentication)과 같은 보안 요구사항이 만족되어야 한다.

그룹통신 환경에서의 위와 같은 요구사항을 만족하기 위해 그룹 멤버들간에 공유되는 그룹키를 관리하기 위한 다양한 방법들[1][2][8]이 제안되어 왔으며, 이러한 방법들은 크게 모든 멤버들이 신뢰하는 키 관리 센터(key management center) 또는 그룹관리자(group manager)가 그룹키를 생성하여 안전하게 멤버들에게 분배하는 그룹키 분배 프로토콜(group key distribution protocol)과 모든 멤버들이 그룹키를 생성하기 위해 키 생성 프로토콜에 동등하게 참여하는 그룹키 합의 프로토콜(group key agreement protocol)로 나누어진다.[1][2][8][10]

일반적으로 그룹키를 관리함에 있어서 다음과 같은 사항들이 고려되어야 한다.

- ○ 그룹키의 비밀성(group key secrecy)
  악의적인 공격자가 그룹키를 도출해 내는 것이 계산상 불가능하여야 한다.
- ○ 전방 비밀성(forward secrecy)
  악의적인 공격자가 이전 세션의 그룹키들에 대한 정

보로부터 이후의 그룹키를 계산할 수 없어야 한다.

- 후방 비밀성(backward secrecy)
  악의적인 공격자가 이후에 알려진 그룹키들의 정보로부터 이전 세션의 그룹키를 계산할 수 없어야 한다.
- 키 독립성(key independency)
  그룹키 집합 K의 적당한 부분집합 K'을 알고있는 공격자가 그룹키의 다른 부분집합 $\overline{K} \in (K - K')$를 계산할 수 없어야 한다.

본 논문은 셀룰러 오토마타(cellular automata)를 이용하여 암호학적으로 이용 가능한 기본 프리미티브를 생성하고 이를 연속적으로 적용함으로써 키 관리 센터가 그룹 내에서 공유할 수 있는 키를 생성하고 이를 그룹 멤버들에게 분배하기 위한 방안을 논의한다.

본 논문의 구성은 다음과 같다. 2장에서 기본 프리미티브를 구성하기 위한 셀룰러 오토마타의 응용에 대해서 논하고 3장에서 이를 응용하여 그룹 내 비밀 통신을 위한 비밀 공유키 생성알고리즘을 제안한다. 마지막으로 4장에서 결론과 향후과제를 논의한다.

2. 기본 프리미티브 생성

셀룰러 오토마타는 규칙적인 셀의 배열로 구성된 유한상태기계(finite state machine)로써 많은 응용분야에서 이에 대한 연구가 있어왔다.[3][4][5] 또한 Wolfram 등에 의해서는 셀룰러 오토마타를 이용한 암호 알고리즘 개발에 대한 연구가 있었다.[6][7] 특히 Chaudhuri 등은 involution 특성을 갖는 기본 구조를 제안하고 이를 블록 및 스트림 암호 알고리즘에 적용하였다.[5][9]

3-이웃 Null Boundary 선형 셀룰러 오토마타를 이용하여 complement CA를 구성할 수 있고, 이는 그룹(group) 셀룰러 오토마타임이 증명되었다.[3] 즉, 법칙 51, 153, 195를 이용하여 셀룰러 오토마타를 구성함으로써 짝수개의 동일한 길이의 사이클 구조를 갖는 선형 셀룰러 오토마타를 구성할 수 있고 이를 거듭제곱함으로 involution 특성을 가지는 기본 구조를 생성할 수 있다.

complement CA에 대한 상태 천이 방정식은 다음과 같이 나타낼 수 있다.

$$s^{t+1} = [T] \cdot s^t + [F]$$

여기서, [T]는 셀룰러 오토마타에 대한 셀 갱신법칙을 나타내는 특성 매트릭스(characteristic matrix)이다. s^t와 s^{t+1}는 각각 시간 t와 t+1에 대한 셀룰러 오토마타의 상태를 나타낸다. 또한, [F]는 complement 법칙이 적용된 셀에 대하여 1 값을 가지는 벡터이다. 따라서 이를 법칙 R(153, 153, 153, 153)을 갖는 4-셀 NBCA(null boundary cellular automata)에 적용하면 다음과 같이 나타낼 수 있다.[ ]

$$s^{t+1} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot s^t + [1111]$$

또한 셀룰러 오토마타에 대한 상태 천이는 아래와 같이 치환(permutation)으로 표현할 수 있다. 이 표현은 또한 아래 식과 같이 서로 소(disjoint)인 순환(cycle)의 곱으로 표현할 수 있다. 여기서 각각의 숫자 표현은 셀룰러 오토마타 상태의 10진 표현이다.

$$\pi = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 15 & 12 & 9 & 10 & 3 & 0 & 5 & 6 & 7 & 4 & 1 & 2 & 11 & 8 & 13 & 14 \end{bmatrix}$$
$$= (0,15,14,13,8,7,6,5) \cdot (1,12,11,2,9,4,3,10)$$

여기서, 치환 π의 멱승을 반복함으로써 involution 특성을 가지는 새로운 치환구조를 얻을 수 있다.

$$\pi^2 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 11 & 4 & 1 & 10 & 15 & 0 & 5 & 6 & 3 & 12 & 9 & 2 & 7 & 8 & 13 \end{bmatrix}$$
$$= (0,14,8,6) \cdot (1,11,9,3) \cdot (2,4,10,12) \cdot (5,15,13,7)$$

$$\pi^4 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{bmatrix}$$
$$= (0,8) \cdot (1,9) \cdot (2,10) \cdot (3,11) \cdot (4,12) \cdot (5,13) \cdot (6,14) \cdot (7,15)$$

이 예제에서 π^4은 involution 특성을 가진다. 이를 본 논문에서 비밀 그룹 키 생성에 응용하고자 한다.

표 2. 짝수 길이의 동일 사이클을 갖는 Uniform CA의 구성 예

셀 개수	적용 법칙	사이클	
		길이	개수
4	51,51,51,51,	2	8
4	153,153,153,153	8	2
4	195,195,195,195	8	2
8	51,51,…,51,51	128	2
8	153,153,…,153,153	16	16
8	195,195,…,195,195	16	16

기존 연구에서 이와 같은 선형 complement CA를 구성함으로써 짝수 길이의 동일 사이클을 갖는 셀룰러 오토마타를 구성할 수 있음이 알려져 있다. 아래 표는 4-셀/8-셀에 대한 예를 보인다.[3][5]

표1에서 2, 3, 4행에 해당하는 치환 π_2, π_3, π_4 구조는 곧바로 involution 특성을 이용할 수 있고, 1행은 π_1^4을, 5, 6행의 경우는 π_5^8, π_6^8을 이용하여 involution 특성을 얻을 수 있다.

3. 비밀 그룹 키 생성을 위한 제안 구조

제안 구조는 셀룰러 오토마타를 이용한 메시지 암호화 기법을 이용하므로 각 멤버에 대한 비밀키는 2장에서 소개한 involution 특성을 가지는 치환이며, 실제로는 그러한 치환을 셀룰러 오토마타를 이용하여 구성할 수 있는 법칙을 그룹관리자가 제공하게 될 것이다. 표2는 제안 시스템에서 사용되는 시스템 변수에 대한 설명이다.

표 3. 시스템 매개변수

G	그룹관리자
U_i	그룹 멤버
π_G	그룹관리자의 비밀 치환
π_i	G와 멤버 i 간에 공유되는 비밀 치환
π_K	그룹 공유 치환

3.1 시스템 설정(Setup)

그룹관리자 G는 자신의 치환 π_G와 n명의 멤버에 대한 각 멤버 $U_i\ (1 \le i \le n)$에 대해 involution 특성을 가지는 치환 π_i를 결정하고 π_i를 U_i에게 안전하게 전달한다. 이때 전달된 π_i가 그룹 관리자 G와 사용자 U_i간에 공유되는 비밀값이 되며 각 멤버는 이를 안전하게 보관한다.

$$G \rightarrow U_i : \pi_i \quad (1 \le i \le n)$$

그룹관리자는 아래와 같이 각 사용자들의 치환 π_i들을 임의의 순서로 합성하여 메시지 암호화를 위한 치환으로 π_K를 사용한다.

$$\pi_K = \pi_G \cdot (\pi_{i_1} \cdot \pi_{i_2} \cdot \ldots \cdot \pi_{i_n})\ ;\ \pi_{i_k} \in \{\ \pi_i \mid 1 \le i \le n\ \}$$

π_K를 계산한 그룹관리자는 각각의 그룹 멤버들에게 π_K를 아래와 같은 형태로 분배한다.

$$G \rightarrow U_i : p_i = \pi_K \cdot \pi_i \quad (1 \le i \le n)$$

p_i를 수신한 멤버는 자신의 비밀 치환 π_i를 적용하여 한번의 치환 연산으로 π_K를 계산할 수 있다.

$$U_i : \pi_K = p_i \cdot \pi_i = (\pi_K \cdot \pi_i) \cdot \pi_i$$

π_K를 수신한 모든 멤버들은 안전한 그룹 통신을 위해, 메시지 M에 대한 암호문 C를 생성하기 위해 아래와 같은 연산을 수행한다.

$$C = \pi_K \cdot [M]$$

암호문 C를 수신한 멤버들은 $M = \pi_K \cdot [C]$를 계산함으로써 원래의 평문 M을 획득할 수 있다.

3.2 멤버 참여에 대한 키 갱신

만일 새로운 사용자 U_j가 그룹의 멤버로 참여하는 경우, U_j는 그룹관리자 G를 통해 인증과정을 거치며 G는 U_j에 대한 치환 π_j를 생성하여 안전하게 전달하고 키 갱신을 위한 새로운 비밀 치환 π'_G를 생성하여 π_j를 포함하는 새로운 그룹키 π'_K로 갱신하고 멤

버들에게 분배한다

$$\pi'_K = \pi_K \cdot (\pi_j \cdot \pi'_G)$$

$$G \rightarrow U_i : p'_i = \pi'_K \cdot \pi_i$$

멤버의 추가로 인해 그룹키를 갱신하기 위해 그룹관리자는 두 개의 치환에 대한 두 번의 연산만을 필요로 한다. 그룹키를 갱신하기 위해 그룹관리자는 새로운 비밀 치환 π'_G를 사용하므로, 새로 참여한 U_j가 π'_K로부터 이전의 π_K를 계산할 수 없다.

3.3 멤버 탈퇴에 대한 키 갱신

어떤 멤버가 그룹에서 탈퇴하거나 삭제되는 경우, 그룹에서 삭제되는 멤버가 더 이상 그룹 멤버들간에 교환되는 메시지에 접근하지 못 하도록 하기 위해 그룹키를 갱신해야 한다.

만일 멤버 U_j가 그룹에서 탈퇴하는 경우, 그룹관리자는 U_j의 치환 π_j를 삭제하고 남아있는 멤버들에 대한 치환들을 임의로 합성하여 새로운 그룹키를 갱신하고 남아있는 멤버들에게 전달한다.

$$\pi'_K = \pi'_G \cdot (\pi_{i_1} \cdot \pi_{i_2} \cdot \cdots \cdot \pi_{i_n}) \quad (\pi_{i_k} \neq \pi_j)$$

$$G \rightarrow U_i : p'_i = \pi'_K \cdot \pi_i \quad (1 \leq i \leq n,\ i \neq j)$$

U_j를 제외한 모든 멤버 U_i들은 $p'_i \cdot \pi_i$를 계산함으로써 갱신된 그룹키 π'_K를 쉽게 획득할 수 있으며, 삭제된 멤버 U_j는 π_j를 사용하여 p'_i로부터 갱신된 π'_K를 계산하는 것이 어렵다. 그러므로 U_j는 더 이상 그룹 통신에 참여할 수 없게 된다.

4. 결론 및 향후과제

본 논문은 그룹 비밀키 생성에 대한 새로운 방향을 제시하고 있다. 이는 셀룰러 오토마타를 이용하여 암호학적으로 응용할 수 있는 involution 구조를 생성하고 이를 그룹 사용자에 대한 비밀 정보로 할당함으로써 그룹 키 생성에 있어서 간단한 특성 매트릭스 연산으로 생성할 수 있다. 또한 이와 같은 구조는 사용자들의 공모에 대하여 견고함을 보인다.

현재 제안 시스템에서는 그룹키를 획득하기 위해 각각의 멤버들은 단지 한번의 치환연산만이 요구되지만, 그룹관리자는 갱신된 그룹키를 전달하기 위해 n명의 멤버에 대해 멤버 추가시에는 2번의 치환 연산을 요구하고 멤버 삭제 시에는 n번의 치환 연산을 요구되며, 그룹키를 멤버들에게 전달하기 위해 n번의 통신량이 요구된다. 대부분의 그룹키 분배 프로토콜에서는 그룹관리자의 오버헤드를 줄이기 위해 트리 기반의 그룹키 관리 기법을 사용하고 있으며, 향후 제안 기법을 트리 구조와 결합하는 방안에 대해서도 연구가 되어야 할 것이다. 또한 그룹키 분배뿐만 아니라 그룹 키 합의 알고리즘에 셀룰러 오토마타를 응용할 수 있는 방안에 대하여 보다 많은 연구가 있어야 할 것이다.

[참고문헌]

[1] Y. Amir, Yongdae Kim, C. Nita-Rotaru, J. Schultz, J. Stanton, G. Tsudik, "Exploring robustness in group key agreement", 21st International Conference on Distributed Computing Systems, Apr 2001, pp.399-408

[2] D. Balenson, D. McGrew, A. Sherman. "Key management for large dynamic groups: One-way function trees and amortized initialization", Internet-Draft: draft-balensongroupkeymgmt-oft-00.txt, Feb., 1999.

[3] P. P. Chaudhuri, D. R. Chowdhury, S. Nandi, S. Chattopadhyay, "Additive Cellular Automata Theory and Applications Volume 1", IEEE Computer Society Press, 1997.

[4] M. Mihaljevic, H. Imai, "A Family of Fast Keystream Generations Based on Programmable Linear Cellular Automata over GF(q) and Time-Variant Table", IEICE Transactions on Fundamentals, vol.E82-A, no.1, pp.32-39, 1999.

[5] S. Nandi, B. K. Kar, P. P. Chaudhuri, "Theory and applications of cellular automata in cryptography", IEEE Transactions of Computers, vol.43, pp.1346-1357, Dec., 1994.

[6] S. Wolfram, "Cellular Automata and Complexity", Addison Welsely Publishing Company, 1994.

[7] S. Wolfram, "Cryptography with Cellular Automata", in Advanced in Cryptology, Crypto 85 Proceedings, LNCS 218, pp.1346-1357, 1986.

[8] C. K. Wong, M. Gouda, S. S. Lam, "Secure group communications using key graphs", In Proceedings of ACM SIGCOMM '98, pp.68-79, September 1998.

[9] Alfres J. Menezes, Paul C. vaz Oorschot, Scott A. nanstone, "Handbook of Applied Cryptography", CRC Press, 1997.

[10] 박영희, 정병천, 윤현수, "트리를 이용한 효율적인 그룹키 동의 프로토콜", 한국정보보호학회 종합학술발표회 논문집, vol.12, no.1, 20, 2002.