익명성을 제공하는 공평한 그룹 복호화 기법*

김진일 [10], 서정주 [1], 홍정대 [2], 박근수 [1]
서울대학교 전기컴퓨터공학부 [1]
{jikim, jjseo, kpark}@theory.snu.ac.kr
국방부 [2]
jdhong@theory.snu.ac.kr

Allowing Anonymity in Fair Threshold Decryption

Jinil Kim[10], Jungjoo Seo[1], Jeongdae Hong[2], Kunsoo Park[1]
School of Computer Science and Engineering, Seoul National University[1]
Ministry of National Defense[2]

1. 서 론

그룹 복호화 [1, 2] 는 다수의 참여자 사이에서 수행되는 공개키 암호 시스템으로 암호문을 복호화하는데 지정된 수 이상의 참여자가 필요한 암호 시스템이다. 기존의 그룹 복호화 기법에서는 흔히 조합자(combiner)라는 제 3 자가 평문을 복호화하여 참여자에게 주었기 때문에 조합자가 모든 참여자로부터 완전히 신뢰받아야 한다는 비현실적인 요구사항을 가지고 있었다. 반면 조합자를 이용하지 않으면 참여자들이 복호화 조각을 서로 주고받아야 하는데 가장 먼저 복호화 조각을 모은 참여자가 먼저 복호화에 성공하게 되어 공평성의 문제가 발생하였다.

Hong 등은 [3] 그룹 복호화 문제에서 공평성을 보장하기 위해 주어진 프로토콜을 따르는 제 3 자(STTP)를 도입하되 제 3 자가 평문에 대한 정보를 얻지 못하도록 하는 모델(semi-honest, honest-but-curious)에서 작동하게 하는 공평한 그룹 복호화 기법을 제안하였다. [3]에서 제안된 기법은 STTP 가 평문에 대한 정보를 얻지 못하지만 비밀키 조각의 소유자에 대한 정보는 미리 알고 있다고 가정한다. 즉, STTP 또는 STTP 의 저장소를 볼 수 있는 공격자는 각각의 비밀키 조각의 소유자의 ID (IP 나 E-mail 등과 같은 정보)를 모두 알 수 있다. 그러나 이와 같은 정보는 외부의 공격자들에게 비밀키 소유자의 신상을 노출시키게 되어 테러나 스토킹 등의 문제를 야기할 수 있기 때문에 STTP 에게 공개되지 않는 것이 바람직하다.

본 논문에서는 [3]에서 제안된 공평한 그룹 복호화를 개선하여 STTP 가 비밀키 조각의 소유자들의 익명성을 유지한 상태에서도 안전하게 그룹 복호화를 수행할 수 있는 기법을 제안한다. 제안된 방법은 비밀키 조각의 소유자들의 익명성을 유지하면서 STTP 가 필요로 하는 저장소 공간을 줄여준다는 바람직한 특징을 가진다.

2. 본 론

공평한 그룹 복호화 프로토콜의 참여자는 키 분배자(dealer), l 명의 키 소유자(shareholder) 및 STTP로 구성된다. 키 분배자는 공개키와 비밀키를 초기화하고 비밀키를 키 소유자들과 STTP에게 분배한다. STTP는 키 소유자들이 공평하게 복호화를 수행할 수 있도록 프로토콜을 중계하는 제 3자로써 주어진 프로토콜을 잘 따르지만 중간 정보를 저장하여 평문에 대한 정보를 얻어내려고 하는 참여자이다. 키 소유자들은 $(t+1)$명이 모이면 그룹 복호화 과정을 통해 암호문을 복호화할 수 있는 참여자로 악의적으로 프로토콜에서 벗어난 동작을 할 수 있다. 공평한 그룹 복호화 프로토콜이 익명성을 가진다는 의미는 STTP가 키 소유자들의 ID를 모르는 상태에서도 키 소유자들이 안전하고 공평하게 그룹 복호화를 수행할 수 있어야 함을 의미한다.

본 논문에서 제안하는 익명성을 제공하는 공평한 그룹 복호화 기법의 상세사항은 표 1과 같다. 이 프로토콜의 주요 아이디어는 비밀키 조각을 가진 키 소유자의 ID 를 미리 STTP에게 알려주는 대신 키 소유자가 자신이 비밀키 조각을 소유하고 있음을 STTP에게 증명해야 할 필요가 있을 때 zk-proof를 이용하여 비밀키 소유를 증명하는 것이다. STTP는 익명의 참여자가 비밀키 조각 $s_i = \log_g VK_i$ 에 대한 zk-proof를 보낼 수 있으면 통신 상대방이 키 소유자 P_i 라고 확신할 수 있다.

한편, 익명성을 유지하기 위해서는 통신 방법도 익명으로 이루어져야 하는데 이는 키 소유자와 STTP사이의 모든 통신에 믹스넷 [4] 을 이용함으로써 가능하다. STTP와 통신하는 키 소유자는 믹스넷에서 정의된 익명의 회신

* 본 연구는 기초기술연구회의 NAP 과제 지원으로 수행되었음. 이 연구를 위해 연구장비를 지원하고 공간을 제공한 서울대학교 컴퓨터연구소에 감사 드립니다.

주소를 이용하여 STTP로부터 응답을 받을 수 있다. 이 프로토콜에서 STTP와 키 소유자들의 통신은 모두 믹스넷을 통하고 STTP로부터 키 소유자로의 응답은 익명의 회신 주소를 이용한다고 가정한다.

표 1. 익명성을 제공하는 공평한 그룹 복호화 프로토콜 (Hash-ElGamal 기반)

설정 ($Set-Up$)

G : 큰 소수 q의 위수를 가지는 군(group) $\cong Z_q^*$
H : G에서 평문길이의 비트열로의 해쉬 함수
g : G의 생성자(generater)

키 생성 (*Key Generation*)

1. $x,\ R \underset{R}{\leftarrow} G$
2. $PK = g^x \bmod q,\ s_{STTP} = R,\ VK_{STTP} = g^R$
3. 다항식 $f(z) = \sum_{i=0}^{t} a_i z^i$를 선택
   단, $a_i \underset{R}{\leftarrow} G,\ f(0) = x - R$
4. $s_i = f(i) \bmod q,\ VK_i = g^{s_i}\ (1 \le i \le l)$
   P_i에게 s_i를 전송, $STTP$에게 s_{STTP}를 전송
5. $(g,\ PK,\ VK_{STTP},\ \{(i,\ VK_i)\})$를 공개

암호화 (*Encryption*)

메시지 m의 암호문 $E(m)$을 생성하는 과정
1. $r \underset{R}{\leftarrow} G$
2. $E(m) = \left(g^r,\ m \oplus H(g^{rx})\right)$

복호화 과정 (*Decryption*)

S : 복호화 그룹 $S \subset [1..l],\ |S| = t+1$
P_i와 $STTP$ 사이의 통신은 모두 믹스넷을 이용
$STTP$는 익명의 회신 주소를 통해 P_i에게 회신
***Round* 1** : ($Schnorr\ style\ zk\_proof$)
1. P_i는 $r_i \underset{R}{\leftarrow} G$를 선택하고
2. $(i, E(m), g^{r_i}, S)$를 $STTP$에게 전송
3. $STTP$는 $c_i \underset{R}{\leftarrow} G$를 P_i에게 전송
4. P_i는 $z_i = (c_i s_i + r_i) \bmod q$ 를 $STTP$ 에게 보냄
5. $STTP$는 모든 P_i에 대해 $g^{z_i} = VK_i^{c_i} g^{r_i}$를
   확인하고 $START$ 신호를 P_i에게 전송

***Round* 2** : 복호화 조각 교환
1. P_i 는 $w_i = u^{s_i}$와 zk_proof($log_g(VK_i) = log_u(w_i)$)를 P_j에게 전송
2. P_i가 $t+1$개의 복호화 조각을 받으면
   $(i,\ READY,\ S,\ E(m))$을 $STTP$ 에게 전송

***Round* 3** : $STTP$가 자신의 복호화 조각을 보냄
1. S의 $t+1$개의 $READY$를 받으면
   P_i에게 $w_{STTP} = u^{s_{STTP}}$ 와 zk_proof($log_g(VK_{STTP}) = log_u(w_{STTP})$)를 보냄

***Round* 4** : 평문 계산
1. P_i는 $g^{rx} = w_{STTP} \prod_{i \in S} w_i^{\lambda_i}$를 계산
   (여기서 $\lambda_i = \prod_{b \in S \setminus \{i\}} \frac{i}{b-i}$ 는 Lagrange 계수)
2. P_i는 $m = v \oplus H(g^{rx})$를 계산

키 소유자의 익명성은 믹스넷의 익명성에 의해 STTP가 키 소유자들의 ID를 얻을 수 없다는 점에 기인한다. 기존의 프로토콜에서는 STTP가 미리 키 소유자의 ID 리스트를 가지고 있어 어떤 키 소유자와 통신하고 있는지 식별할 수 있었으나 이 프로토콜에서는 STTP가 ID 정보를 가지지 않을 뿐 아니라 키 소유자들이 STTP와 주고받는 모든 정보가 ID와 무관하므로 믹스넷이 STTP로부터 키 소유자들의 익명성을 보호할 수 있다. 반면에 STTP는 키 소유자들의 ID를 모르는 상태에서도 zk-proof를 통해 상대방이 키 소유자인지 확인할 수 있으므로 안전하게 그룹 복호화할 수 있도록 동작할 수 있다.

3 결 론

본 논문에서는 [3]에서 제안한 공평한 그룹 복호화 기법에 익명성을 추가할 수 있는 프로토콜을 제안하였다. 제안된 프로토콜은 기존 프로토콜의 보안성과 공평성 등의 성질을 그대로 충족할 뿐 아니라 STTP가 키 소유자들에 대한 정보를 가지지 않아도 안전하게 그룹 복호화를 수행할 수 있도록 하여 키 소유자들이 안전하게 그룹 복호화에 참여할 수 있게 하였다.

4 참조문헌

[1] P. Fouque, G. Poupard, J. Stern: Sharing decryption in the context of voting of lotteries, Financial Cryptography 2000, 2000.
[2] V. Shoup: Practical threshold signatures, In Eurocrypt 2000, 2000
[3] J. Hong, J. Kim, J. Kim, M. K. Franklin, K. Park: Fair Threshold Decryption with Semi-Trusted Third Parties, in ACISP 2009, pages 309-326, 2009.
[4] G. Danezis, C. Diaz: A Survey of Anonymous Communication Channels, Microsoft Technical Report MSR-TR-2008-35, 2008.