익명성을 제공하는 공평한 그룹 복호화 기법
(Allowing Anonymity in Fair Threshold Decryption)

김 진 일 † 서 정 주 †† 홍 정 대 ††† 박 근 수 ††††
(Jinil Kim) (Jungjoo Seo) (Jeongdae Hong) (Kunsoo Park)

요 약 그룹 복호화는 다수의 참여자 사이에서 수행되는 공개키 암호 시스템으로 하나의 암호문을 복호화하는데 지정된 수 이상의 참여자가 필요한 암호 시스템이다. 그룹 복호화를 실제 수행할 때에는 참여자의 공평성을 보장하기 위해 흔히 제3자를 도입하는데 이 때 제3자에 대해 필요한 신뢰의 수준 및 제3자에게 제공되는 정보를 줄이는 것이 중요하다. 본 논문에서는 제3자가 프로토콜을 잘 따르지만 중간 정보를 저장할 수 있는 모델(semi-honest model)을 가정하고 이와 같은 제3자(STTP, Semi-Trusted Third Party)를 그룹 복호화 기법에 이용하여 복호화 참여자는 평문을 얻을 수 있지만 STTP는 평문을 알 수 없을 뿐 아니라 복호화 참여자의 익명성도 유지할 수 있는 그룹 복호화 기법을 제안한다. 제안된 기법은 기존 프로토콜의 보안성, 공평성 등의 특징을 모두 유지하고 외부의 공격자가 STTP의 저장소를 볼 수 있는 경우에도 복호화 참여자를 알 수 없는 바람직한 특징을 가진다.

키워드 : 그룹 복호화, 공평성, 익명성, 믹스넷

Abstract A threshold decryption scheme is a multi-party public key cryptosystem that allows any sufficiently large subset of participants to decrypt a ciphertext, but disallows the decryption otherwise. When performing a threshold decryption, a third party is often involved to guarantee fairness among the participants. To maintain the security of the protocol as high as possible, it is desirable to lower the level of trust and the amount of information given to the third party. In this paper, we present a threshold decryption scheme which allows the anonymity of the participants as well as the fairness by employing a semi-trusted third party (STTP) which follows the protocol properly with the exception that it keeps a record of all its intermediate computations. Our solution preserves the security and fairness of the previous scheme and reveals no information about the identities of the participants and the plaintext even though an attacker is allowed to access the storage of the STTP.

Key words : threshold decryption, fairness, anonymity, mix-net

· 본 연구는 기초기술연구회의 NAP 과제 지원으로 수행되었음
이 연구를 위해 서울대학교 컴퓨터 연구소에서 연구장비를 지원하고 공간을 제공함

† 비 회 원 : 서울대학교 전기컴퓨터공학부
jikim@theory.snu.ac.kr
†† 학생회원 : 서울대학교 전기컴퓨터공학부
jjseo@theory.snu.ac.kr
††† 비 회 원 : 국방부 중령
jdhong@theory.snu.ac.kr
†††† 종신회원 : 서울대학교 전기컴퓨터공학부 교수
kpark@theory.snu.ac.kr

논문접수 : 2010년 7월 30일
심사완료 : 2010년 10월 25일

정보과학회논문지: 시스템 및 이론 제37권 제6호(2010.12)

1. 서 론

그룹 복호화는 다수의 참여자 사이에서 수행되는 공개키 암호 시스템으로 하나의 암호문을 복호화하는데 지정된 수 이상의 참여자가 필요한 암호 시스템이다. 그룹 복호화는 복호화 권한이 여러 참여자들에게 분배된다는 측면에서 중요한 데이터를 저장할 때 사용하거나 프라이버시를 보호하면서 공통의 결과를 계산하는 프로토콜의 핵심 요소로써 활용성이 다양한 기법이다[1].

그룹 복호화에서 비밀키는 보통 비밀 공유 기법(secret sharing scheme)을 이용하여 여러 개의 비밀키 조각으로 쪼개어진 다음 각자의 참여자들에게 분배된다. 일정 수 이상의 참여자들이 복호화를 수행할 때 각각의 참여자들은 암호문에 자신의 비밀키 조각을 적용하여 부분적으로 복호화된 복호화 조각을 계산한다. 일정 수 이상의 복호화 조각을 가진 참여자는 이를 이용하여 평문을

계산할 수 있다.

기존의 그룹 복호화 기법들은 흔히 조합자(combiner)라는 제3자를 도입하여 복호화를 수행하였다. 그러나 조합자는 다른 참여자들보다 먼저 평문을 얻기 때문에 모든 참여자로부터 완전히 신뢰받아야 한다는 비현실적인 요구사항을 가지고 있었다. 반면 조합자를 이용하지 않고 복호화를 수행하려고 하는 경우 참여자들이 복호화 조각을 서로 주고받아야 하는데 가장 먼저 복호화에 필요한 만큼의 복호화 조각을 모은 참여자가 먼저 복호화에 성공하게 되어 공평성의 문제가 발생하였다.

한편, Cleve[2]는 참여자의 절반 이상이 정직하지 않을 경우 제3자 없이는 공평한 프로토콜의 설계가 불가능함을 증명하였다. Hong 등은 [3] 그룹 복호화 문제에서 공평성을 보장하기 위해 제3자가 프로토콜을 잘 따르지만 중간 정보를 저장할 수 있는 모델(semi-honest model)을 가정하고 이와 같은 제3자(STTP, Semi-Trusted Third Party)를 그룹 복호화 기법에 도입한 공평한 그룹 복호화 기법을 제안하였다. 그들은 제안된 프로토콜에서 STTP가 복호화에 참여하지 않는 경우 복호화가 불가능함과 STTP가 평문에 대한 정보를 얻지 못함을 보이고 이로부터 프로토콜의 공평성을 증명하였다.

[3]에서 제안된 기법은 STTP가 평문에 대한 정보를 얻지 못하지만 비밀키 조각의 소유자에 대한 정보는 미리 알고 있다고 가정한다. 즉, STTP 또는 STTP의 저장소를 볼 수 있는 공격자는 각각의 비밀키 조각의 소유자의 ID(IP나 E-mail 등과 같은 정보)를 모두 알 수 있다. 이와 같은 복호화 권한의 소유자에 대한 정보는 외부의 공격자들에게 비밀키 소유자의 신상을 노출시키게 되어 테러나 스토킹 등의 문제를 야기할 수 있는 중요한 정보가 될 수 있다. 게다가 그룹 복호화의 참여자가 매우 많거나 STTP가 많은 세션을 관리하게 되면 STTP에 개인 정보가 축적되게 되어 프라이버시 침해의 위험성이 커질 수 있다.

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

관련연구: 그룹 복호화 방법은 다양한 스킴이 개발되어 있는데[4-6], 공평성에 대한 연구는 일반적으로 고려되지 않았다. Cleve[2]는 참여자의 절반 이상이 정직하지 않은 경우 완전히 공평한 프로토콜의 설계가 불가능함을 증명하였고 이를 피하기 위해 완전한 공평성 대신 서서히 암호문을 복호화해 나가는 방법의 완화된 공평성에 대한 연구가 진행되었다[7,8]. 그러나 그룹 복호화 과정에서의 익명성에 대한 연구는 현재까지 잘 알려져 있지 않다.

한편, Hong 등은[3] STTP를 도입하여 공평성의 정의를 완화하지 않고 정직한 참여자의 수에 관계없는 공평한 그룹 복호화 방법을 제안하였다. 그러나 이 방법은 STTP가 참여자를 알고 있다고 가정하였기 때문에 참여자가 익명인 경우 프로토콜의 안전성을 유지할 수 없다는 문제점을 가진다.

익명 통신에 대한 본격적인 연구는 Chaum이[9] 믹스(mix)라 불리는 릴레이 서버를 이용한 익명통신의 개념을 도입하면서 시작되었다. 이러한 믹스넷(Mix-net) 시스템을 이용하면 수신/발신자 간의 통신여부를 숨길 수 있고, 수신자 역시 발신자의 신원을 알지 못한 상태에서 교신을 할 수 있다[10].

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 사용하는 모델 및 정의들을 소개하고 3장에서는 주요 배경지식을 소개한다. 4장에서는 [3]에서 제안된 공평한 그룹 복호화 기법을 소개하고 5장에서는 익명성을 추가한 새로운 그룹 복호화 기법을 제안한다.

2. 모델 및 정의들

2.1 참여자와 보안성 모델

공평한 그룹 복호화 프로토콜의 참여자들은 키 분배자(dealer), 키 소유자, STTP로 구성되며 다음과 같은 모델에서 동작한다.

키 분배자 (Dealer): 키 분배자는 그룹 복호화를 위해 키를 초기화하고 키 소유자들에게 분배하는 역할을 한다. 키 분배자는 프로토콜을 시작할 때에만 동작하는 신뢰할 수 있는 제3자인데 분산 키 생성 프로토콜[11]을 사용하면 제3자 없이 키 분배를 수행할 수 있다.

키 소유자(Shareholder): 키 소유자는 키 분배자로부터 비밀키 조각을 받아 그룹 복호화에 참여할 자격을 가진 참여자이다. 키 소유자는 악의적인 모델에서 동작하며 주어진 프로토콜에서 벗어난 동작을 하거나 프로토콜을 중단시킬 수 있다.

STTP(Semi-Trusted Third Party): STTP는 키 소유자들이 공평하게 복호화를 수행할 수 있도록 프로토콜을 중계하는 제3자로서 주어진 프로토콜을 잘 따르지만 그 과정에서 얻은 정보를 저장하여 평문에 대한 정보를 얻어내려고 하는(Honest-but-Curious) 참여자이다.

2.2 보안성 (Security)[1)]

$(t+1, l)$ 그룹 복호화의 보안성은 l 명의 키 소유자들

1) 게임에 기반한 보안성, STTP의 무지성, 공평성의 엄밀한 정의는 [3]을 참조한다.

이 있을 때 임의의 $(t+1)$ 명의 키 소유자들은 STTP의 도움을 얻어 복호화를 수행할 수 있지만 어떤 t 명 이하의 키 소유자들도 복호화를 수행할 수 없음을 의미한다. 보안성을 유지한 프로토콜은 공모한 t 명 이하의 키 소유자들이 키 소유자가 아닌 참여자를 추가하여 복호화를 시도할 때에도 복호화를 수행할 수 없도록 보장해야 한다.

2.3 STTP의 무지성(Obliviousness)

STTP가 프로토콜에 참여하는 경우 STTP가 프로토콜 수행 도중에 얻은 정보를 이용하여 평문에 대한 정보를 얻을 수 없어야 한다. 여기서는 STTP가 프로토콜에서 얻은 정보에 추가적으로 t 개의 비밀키 조각을 얻어도 평문에 대한 정보를 얻을 수 없음을 STTP의 무지성으로 정의한다.

2.4 공평성(Fairness)

공평성은 만약 어떤 키 소유자 P_i 가 그룹 복호화로부터 평문을 얻었다면 P_i 를 포함한 $t+1$ 명의 키 소유자들이 함께 그룹 복호화에 성공하여 평문을 얻을 수 있어야 함을 의미한다. 그룹 복호화에 참여하지 않은 키 소유자가 평문을 얻을 수 있는 방법은 복호화에 성공한 참여자로부터 직접 평문을 받는 것 이외에는 없어야 한다.

2.5 익명성(Anonymity)

익명성은 STTP가 키 소유자들이 누군지 알 수 없는 상태에서도 $t+1$ 명의 키 소유자들이 보안성 및 STTP의 무지성을 유지한 상태에서 복호화를 수행할 수 있도록 해야하고, 동시에 STTP가 프로토콜을 수행하는 과정에서 평문에 대한 정보 뿐 아니라 키 소유자들의 ID도 알 수 없어야 함을 의미한다.

키 소유자의 경우 함께 복호화를 수행할 다른 키 소유자들을 알아야 복호화 그룹을 형성할 수 있으므로 모든 키 소유자들의 ID를 안다고 가정한다. 키 소유자간의 익명성도 필요한 경우 키 분배자가 키 소유자들에게 가명(pseudonym)을 부여하여 키 소유자들간에도 익명 통신을 수행하게 할 수 있으나 본 논문에서는 편의상 가명에 기반한 통신을 가정하지 않는다.

3. Hash-ElGamal에 기반한 그룹 복호화 기법

본 논문에서는 간결성을 위해 Hash-ElGamal에 기반한 그룹 복호화 기법을 이용한다. Hash-ElGamal 그룹 복호화는 다음과 같이 동작한다.

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*)

키 분배자가 비밀조각을 분배하는 과정

1. $SK = x \xleftarrow{R} G,\ PK = g^x \bmod q$
2. 다항식 $f(z) = \sum_{i=0}^{t} a_i z^i$를 선택
   단, $a_i \xleftarrow{R} G$, $f(0) = x$
3. $s_i = f(i) \bmod q,\ VK_i = g^{s_i}\ (1 \le i \le l)$
   P_i에게 s_i를 전송
4. $g,\ PK,\ \{(i, VK_i)\}_{1 \le i \le l}$를 공개

암호화 (*Encryption*)

메시지 m의 암호문 $E(m)$을 생성하는 과정

1. $r \xleftarrow{R} G$
2. $E(m) = (g^r,\ m \oplus H(g^{rx}))$

복호화 (*Decryption*)

암호문 $E(m) = (u, v)$를 복호화하는 과정

1. S : 복호화 그룹 $S \subset [1..l],\ |S| = t+1$
2. 각 P_i는 복호화 조각 $w_i = u^{rs_i}$과
   $\text{zk_proof}(log_g(VK_i) = log_u(w_i))$을 조합자에게 전송
3. 조합자는 $g^{rx} = \prod_{i \in S} w_i^{\lambda_i}$를 계산
   여기서 $\lambda_i = \prod_{b \in S \setminus \{i\}} \frac{i}{b-i}$ 는 Lagrange 계수
4. 조합자는 $m = v \oplus H(g^{rx})$를 계산

4. 기존의 공평한 그룹 복호화 기법

이 장에서는 [3]에서 제안된 공평한 그룹 복호화 기법을 간략하게 설명하고 이 프로토콜이 익명성을 만족시키지 못함을 설명한다. 그리고 이 프로토콜을 단순화하여 익명성을 허용하려고 한 경우 보안성을 깨뜨리는 공격 방법이 존재함을 설명하여 익명성 유지가 기술적으로 쉽지 않은 문제임을 보인다.

4.1 프로토콜 설명

[3]에서 제안된 공평한 그룹 복호화 기법의 아이디어는 프로토콜에 STTP를 도입하여 참여하는 키 소유자들간의 공평성을 보장하면서 STTP가 평문에 대한 정보를 얻지 못하게 하는 것이다. 이를 위해 키 분배자는 STTP를 위한 키 조각을 추가적으로 생성하여 복호화를 위해서는 $t+1$ 개의 키 조각과 STTP의 키 조각이 필요하게 한다. 그러면 STTP는 $t+1$ 명의 키 소유자들이 복호화 조각을 모두 주고받은 후 자신의 복호화 조각을 키 소유자들에게 공평하게 보내주어 평문을 계산하게 할 수 있다. 프로토콜은 아래와 같다.

키 생성 (*Key Generation*)

1. $x,\ R \xleftarrow{R} G$

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, $a_i \xleftarrow{R} G$, $f(0) = x - R$
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. $ID_{list} = \{(i, ID(P_i))\}_{1 \le i \le l}$를 P_i와 $STTP$에게 전송
6. $(g, PK, VK_{STTP}, \{(i, VK_i)\})$를 공개

키 생성 과정에서 키 분배자는 공개키와 비밀키, 확인키(verification key)를 생성하고 비밀키를 비밀 공유 방법을 사용하여 비밀키 조각으로 나눈다. 이때, STTP에 대응하는 비밀키 조각을 복호화에 꼭 필요하도록 하기 위해 비밀키 x를 STTP의 비밀키 조각 R과 나머지 비밀키 조각 $x-R$로 나누고 $x-R$을 다시 참여자들의 수 l만큼의 비밀키 조각으로 나눈다. 키 분배자는 각각의 비밀키 조각들을 키 소유자와 STTP에게 보낸다.

키 분배자는 키 소유자들의 ID 정보를 키 소유자들과 STTP에게 보내고 공개키 및 확인키를 공개한다.

복호화 과정 (*Decryption*)

S : 복호화 그룹 $S \subset [1..l]$, $|S| = t+1$

Round 1 : 복호화 조각 교환

S의 모든 참여자 P_i, P_j에 대해

1. P_i 는 $w_i = u^{s_i}$와 zk_proof$(log_g(VK_i) = log_u(w_i))$를 P_j에게 보냄
2. P_i가 $t+1$개의 복호화 조각을 받으면

   $(i, ID(P_i), READY, S, E(m))$을 $STTP$에게 보냄

Round 2 : $STTP$가 자신의 복호화 조각을 보냄

1. $STTP$는 각 $READY$에 대해 $(i, ID(P_i)) \in ID_{list}$임을 확인하고 아닌 경우는 무시
2. 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 3 : 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

복호화 과정(그림 1)에서는 복호화에 참여하려고 하는 키 소유자들이 복호화 조각을 상호 교환한 후 STTP에게 $READY$ 신호를 보낸다. STTP는 미리 가지고 있는 ID의 목록인 ID_{list}를 통해 $READY$ 신호가 실제 키 소유자로부터 온 것인지 확인하고 자신의 복호화 조각과 zk-proof를 참여한 키 소유자들 모두에게 공평하게 보낸다. 그러면 STTP의 복호화 조각을 받은 키 소유자들은 복호화 조각들을 조합하여 평문을 계산한다.

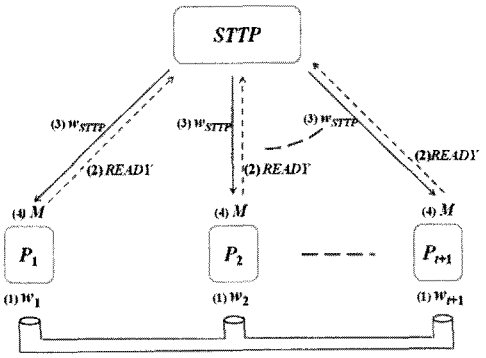

그림 1 공평한 그룹 복호화 기법

4.2 프로토콜의 안전성

이 프로토콜은 랜덤 오라클 모델에서 CDH 가정(Computational Diffie-Hellman 가정)을 만족할 때 보안성, STTP의 무지성 및 공평성이 증명되었다. [3] 증명은 게임에 기반한 방법으로 보안성이나 STTP의 무지성을 무시할 수 없는 확률로 깰 수 있는 공격자가 존재할 경우 이를 이용하여 CDH 문제를 풀 수 있음을 보임으로써 모순을 이끌어내는 방법을 이용하였다. 공평성은 프로토콜에서 STTP가 프로토콜에 참여한 모든 키 소유자들에게 동시에 STTP 자신의 복호화 조각을 보내주는 것으로부터 보장된다.

4.3 익명성의 부재

이 프로토콜은 STTP가 모든 키 소유자들의 ID를 모두 가지고 있는 상태에서 동작한다. 이는 STTP의 저장소가 외부의 공격자에게 노출될 경우 키 소유자들의 신원이 노출된다는 위험을 가진다. 게다가 STTP가 키 소유자들의 ID를 모두 저장하고 있어야 하므로 $O(l)$ 만큼의 저장소가 필요하게 되어 키 소유자가 많거나 STTP가 다수의 세션에 참여할 경우 STTP가 큰 부하를 받는다는 문제점도 가진다.

한편, STTP가 키 소유자들과 직접 통신하게 되므로 STTP가 프로토콜 수행 전에 키 소유자들의 ID를 몰랐다고 하더라도 프로토콜을 수행하고 나면 STTP가 참여한 키 소유자들의 ID를 알게 된다.

4.4 프로토콜을 단순화한 경우의 공격 방법

익명성을 유지하기 위해 프로토콜을 수정하여 STTP가 키 소유자들의 ID 목록을 가지지 않도록 수정한 경우 t명의 키 소유자들이 공모하면 다음과 같은 공격이 가능하다. 먼저 공모한 t명의 키 소유자들이 정직한 키 소유자 P_i와 함께 프로토콜을 초기화한다. P_i가 자신의 복호화 조각을 공모한 키 소유자들 중 한 명에게 보내

면 공모한 키 소유자들은 프로토콜을 중단시킨다. 그리고 실제 키 소유자가 아닌 가짜 키 소유자 P_i' 에게 P_i로부터 받은 복호화 조각을 주어 P_i 대신 프로토콜에 참여하게 한다. 이 경우 STTP가 ID 리스트를 가지고 있지 않아 P_i와 P_i'를 구분하지 못하므로 복호화가 정상적으로 수행되게 된다. 이는 결과적으로 공모한 t 명의 키 소유자들이 복호화에 성공하게 되어 프로토콜의 보안성이 깨지게 되는 원인이 된다.

5. 익명성을 허용한 그룹 복호화 기법

이 장에서는 기존의 STTP를 이용한 공평한 그룹 복호화 방법을 개선하여 STTP가 참여자의 비밀키 조각뿐 아니라 참여자의 ID도 얻지 못하도록 익명성을 유지하는 방법을 제안한다.

5.1 프로토콜 설명

이 프로토콜의 주요 아이디어는 비밀키 조각을 가진 키 소유자의 ID를 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 P_i라고 확신할 수 있다.

한편, 익명성을 유지하기 위해서는 통신 방법도 익명으로 이루어져야 하는데 이는 키 소유자와 STTP사이의 모든 통신에 믹스넷을 이용함으로써 가능하다. STTP와 통신하는 키 소유자는 믹스넷에서 정의된 익명의 회신 주소를 이용하여 STTP로부터 응답을 받을 수 있다. 그림 2는 프로토콜의 통신 방법을 도식화한 것이다.

키 생성과정은 키 분배자가 ID 목록을 키 소유자에게만 보내고 STTP에게는 보내지 않는 점을 제외하고는 동일하다. (4.1절 참조)

복호화 과정은 다음과 같다. 프로토콜에서 STTP와 키 소유자들의 통신은 모두 믹스넷을 통하고 STTP로부터 키 소유자로의 응답은 익명의 회신 주소를 이용한다고 가정한다.

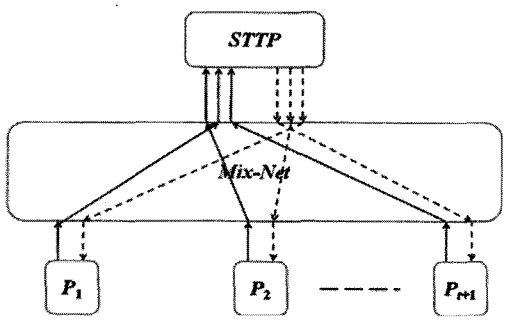

그림 2 익명성을 허용하는 공평한 그룹 복호화에서의 통신 방법

복호화 과정 (*Decryption*)

S : 복호화 그룹 $S \subset [1..l]$, $|S| = t+1$

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

Round 2 : *STTP*가 자신의 복호화 조각을 보냄
1. *STTP*는 각 *READY*에 대해 $(i, ID(P_i)) \in ID_{list}$ 임을 확인하고 아닌 경우는 무시
2. 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 3 : 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

복호화 과정은 먼저 복호화에 참여하려고 하는 키 소유자들이 STTP에게 자신이 비밀키를 가지고 있음을 zk-proof를 통해 증명하면 STTP는 모든 키 소유자들의 zk-proof를 확인한 후 믹스넷을 통해 키 소유자들에게 *START* 신호를 보낸다. *START* 신호를 받은 키 소유자들은 서로 복호화 조각을 교환한다. 이 때 키 소유자들은 서로의 ID를 알고 있으므로 직접 통신을 통해 복호화 조각을 교환할 수 있다. 복호화 조각의 교환이 끝나면 각 키 소유자들은 STTP에게 *READY* 신호를 보내고 STTP는 자신의 복호화 조각을 키 소유자들에게 보냄으로써 복호화를 가능하게 한다.

5.2 프로토콜의 안전성

이 프로토콜에서 STTP는 믹스넷을 통해서만 키 소유자들과 통신하기 때문에 키 소유자의 ID를 알 수 없다. 그러나 STTP는 키 소유자들이 보낸 익명의 회신 주소를 이용하여 믹스넷을 통해 키 소유자들에게 응답할 수 있고 zk-proof를 통해 자신이 실제 키 소유자와 통신하고 있음을 확신할 수 있다. 그러므로 이 프로토콜은 기존의 프로토콜이 가지고 있었던 보안성, STTP의 무지성, 공평성의 특징을 모두 유지할 수 있다.

4.4의 공격은 STTP가 실제 키 소유자와 비밀키 조각은 없으나 복호화 조각을 가진 공격자를 구분하지 못하기

때문에 가능한 공격인데 이 프로토콜에서는 zk-proof의 성질에 의해 이와 같은 공격이 원천적으로 차단된다.

5.3 익명성의 유지

이 프로토콜의 익명성은 믹스넷의 익명성에 의해 STTP가 키 소유자들의 ID를 얻을 수 없다는 점에 기인한다. 기존의 프로토콜에서는 STTP가 미리 ID 리스트를 가지고 있어 올바른 키 소유자와 통신하고 있는지 식별하였으나 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. STTP는 참여한 키 소유자들이 어떤 확인키에 해당하는 비밀키 조각을 가지고 있는지 알 수 있지만 키 소유자들의 ID 자체는 얻을 수 없다.

한편, STTP가 ID 목록을 저장하지 않아도 되므로 STTP의 저장 공간이 절감되어 STTP가 한꺼번에 다수의 그룹 복호화 세션을 처리할 수 있게 된다. 그리고 STTP의 저장 공간이 외부인에 의해 노출될 경우에도 개인 정보를 누출시키지 않을 수 있게 된다.

6. 결 론

본 논문에서는 [3]에서 제안한 공평한 그룹 복호화 기법에 익명성을 추가할 수 있는 프로토콜을 제안하였다. 제안된 프로토콜은 기존 프로토콜의 보안성, STTP의 무지성, 공평성 등의 성질을 그대로 충족할 뿐 아니라 STTP가 키 소유자들에 대한 정보를 가지지 않아도 안전하게 그룹 복호화를 수행할 수 있도록 하여 키 소유자들의 프라이버시를 보호할 수 있게 하였다.

참 조 문 헌

[1] L. Kissner and D. Song: Privacy-preserving set operations, CRYPTO 2005, volume 3621 of Lecture Notes in Computer Science, pp.241-257, Springer-Verlag, 2005.

[2] R. Cleve: Limits on the security of coin flips when half the processors are faulty(extended abstract), in STOC, pp.364-369, 1986.

[3] J. Hong, J. Kim, J. Kim, M. K. Franklin, K. Park: Fair Threshold Decryption with Semi-Trusted Third Parties, in ACISP 2009, pp.309-326, 2009.

[4] R. Gennaro, S. Halevi, H. Krawczyk, T. Rabin: Threshold RSA for dynamic and ad-hoc groups, In Eurocrypt 2008, LNCS, vol.4965, pp.88-107, Springer, 2008.

[5] P. Fouque, G. Poupard, J. Stern: Sharing decryption in the context of voting of lotteries, Financial Cryptography 2000, 2000.

[6] V. Shoup: Practical threshold signatures, In Eurocrypt 2000, 2000.

[7] B. Pinkas: Fair secure two-party computation, Eurocrypt 2003, 2003.

[8] J. A. Garay, P. D. MacKenzie, M. Prabhakaran, K. Yang: Resource Fairness and Composability of Cryptographic Protocols, TCC 2006.

[9] D. Chaum: Untraceable electronic mail, return addresses, and digital pseudo-nyms, Communications of the ACM, 4(2), February 1982.

[10] G. Danezis, C. Diaz: A Survey of Anonymous Communication Channels, Microsoft Technical Report MSR-TR-2008-35, 2008.

[11] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin: Secure distributed key generation for discrete-log based cryptosystems, J. Cryptology, 20(1):51-83, 2007.

김 진 일

정보과학회논문지 : 시스템 및 이론
제 37 권 제 1 호 참조

서 정 주

2009년 성균관대학교 컴퓨터공학부 학사
2009년~현재 서울대학교 전기·컴퓨터공학부 석박사통합과정. 관심분야는 암호학, 컴퓨터이론, 병렬처리

홍 정 대

1993년 육군사관학교 기계공학과 학사
2005년 서울대학교 전기·컴퓨터공학부 석사. 2010년 서울대학교 전기·컴퓨터공학부 박사. 관심분야는 암호학, 군사보안

박 근 수

정보과학회논문지 : 시스템 및 이론
제 37 권 제 1 호 참조