OR 연산을 지원하는 조건부 프록시 재암호화 기법

은하수 [1†], 이훈정 [1], 오희국 [1], 김상진 [2‡]
[1] 한양대학교 컴퓨터공학과
[2] 한국기술교육대학교 컴퓨터공학과
e-mail : hseun@infosec.hanyang.ac.kr

Conditional Proxy Re-Encryption Scheme that Supports OR Operation

Hasoo Eun[1†], Hoonjung Lee[1], Heekuck Oh[1], Sangjin Kim[2‡]
[1]Dept. of Computer Science, Hanyang University
[2]School of Computer Science, Korea University of Technology and Education

요 약

프록시 재암호화 기법이란 위임하는 사람의 공개키로 암호화된 암호문을 신뢰기관의 도움 없이 위임 받는 사람의 개인키로 복호화할 수 있도록 변환하는 기법이다. 이후 특정 조건을 만족하는 사용자만 복호화할 수 있도록 하기 위해 조건부 프록시 재암호화 기법이 제안되었다. 2009 년 Weng 등에 의해 조건부 프록시 재암호화 기법이 제안된 이래 조건에 대해 Boolean 연산자를 모두 지원하는 방법은 아직까지 Open Problem 으로 남아있다. 현재 AND 연산에 대해서는 기존의 기법을 확장하여 지원할 수 있으나 OR, NOT 등에 대해서는 아직 제안되지 않았다. 본 논문에서는 기존의 기법을 확장하여 AND 연산과 함께 OR 연산도 지원할 수 있는 조건부 프록시 재암호화 기법을 제안한다

1. 서론

프록시 재암호화(PRE; Proxy Re-Encryption) 기법이란 Delegator(위임하는 사람)의 공개키로 암호화된 암호문을 신뢰기관의 도움 없이 Delegatee(위임 받은 사람)의 개인키로 복호화할 수 있도록 변환하는 기법이다[1]. 예를 들어 Alice 가 회사에서 암호화된 이메일을 사용하는 상황을 생각해보자. Alice 는 자신이 휴가로 자리를 비우는 동안 Bob 에게 메일을 포워딩하려 한다. 하지만 Bob 은 Alice 의 개인키가 없기 때문에 메일을 받을 수는 있지만 내용을 확인할 수 없다. 이때 프록시 재암호화 기법을 사용하면 Alice 가 포워딩한 메일을 Bob 이 확인하도록 할 수 있다.

처음 프록시 재암호화 기법이 제안된 이래 프록시에 의한 공격, 프록시와 Delegatee 의 공모를 통한 공격 등으로부터 보호하기 위한 다양한 기법들이 제안되었다[2, 3, 4]. 이와 더불어, 초기의 재암호화 기법은 복호화 권한(복호화 할 수 있는 권한)을 제어할 수 없었다. 한번 복호화 권한을 위임하게 되면 Delegatee 는 Delegator 의 모든 메시지를 복호화할 수 있다. 이후 Delegatee 가 특정 조건을 만족하는 메시지만 재암호화할 수 있는 조건부 프록시 재암호화(Conditional PRE) 기법이 제안되었다. 이 기법이 제안되면서 Delegator 는 복호화 권한을 더욱 유연하게 위임할 수 있게 되었다[5].

2009 년 Weng 등이 제안한 조건부 프록시 재암호화 기법은 단일한 키워드에 대해서만 복호화 권한을 위임할 수 있다. 이후 다중 키워드를 지원하기 위한 기법들이 연구가 되었으나, Boolean 연산자를 모두 지원하는 방법은 아직까지 Open Problem 으로 남아있다. 현재 AND 연산에 대해서는 기존의 기법을 확장하여 지원할 수 있으나 OR, NOT 등에 대해서는 아직 제안되지 않았다. 본 논문에서는 기존의 기법을 확장하여 AND 연산과 함께 OR 연산도 지원할 수 있는 조건부 프록시 재암호화 기법을 제안한다.

이후 논문 구성은 2 장에서 관련 연구에 대해 소개하고 3 장에서 제안하는 기법을 설명한다. 4 장에서 제안하는 기법을 분석하고 5 장에서 결론을 맺는다.

2. 관련연구

2.1. 표기법

본 논문에서 사용하는 표기법은 다음과 같다.

<표 1> 표기법

표기	의미
p	k 비트 소수
$\mathbb{G}$, $\mathbb{G}_T$	p를 위수로 갖는 순환 군
e	$\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$를 만족하는 겹선형 쌍함수
PU_i	i의 공개키
PR_i	i의 개인키
$RK_{i \rightarrow j}^{w}$	상태 w를 만족할 때 i에서 j로의 재암호키
m	메시지
w	키워드

* 이 논문은 2012 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2012-R1A2A2A01046986)
* 이 논문은 2012 년도 정부(교육과학기술부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임(No. 2012-R1A1A2009152)

s	$\mathbb{Z}_p$에 속하는 임의의 값
g	$\mathbb{G}$에 속하는 임의의 값
r	$\mathbb{G}_T$에 속하는 임의의 값
H_1	$\{0,1\}^* \rightarrow \mathbb{Z}_p$
H_2	$\{0,1\}^* \rightarrow \mathbb{G}$
H_3	$\mathbb{G} \rightarrow \{0,1\}^n$
H_4	$\{0,1\}^* \rightarrow \mathbb{G}$
H_5	$\mathbb{G} \rightarrow \mathbb{Z}_p$

2.2. 겹선형 맵

$\mathbb{G}$와 $\mathbb{G}_T$가 같은 위수를 갖는 곱셈 순환군일 때, $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$는 다음을 만족해야 한다.

- **Bilinearity**
  $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ where $\forall g_1, g_2 \in G, \forall a, b \in Z_p^*$
- **Non-degeneracy**
  $e(g_1, g_2) \neq 1_{\mathbb{G}_T}$ where $\exists g_1, g_2 \in \mathbb{G}$
- **Computability**
  $\forall g_1, g_2 \in \mathbb{G}$에 대해 $e(g_1, g_2)$를 효율적으로 계산하는 알고리즘이 존재

2.3. 프록시 재암호화 (Proxy Re-Encryption)

프록시 재암호화란 Delegator 의 공개키로 암호화된 암호문을 신뢰기관의 도움 없이 Delegatee 의 개인키로 복호화할 수 있도록 변환하는 기법이다. 이때 재암호화 하는 과정에서 프록시는 평문이나 Delegator 의 비밀키를 알 수 없어야 한다. 프록시 재암호화의 목적은 신뢰기관의 도움 없이 안전하게 암호문을 변환하는 것이다. PRE 의 초기 모델은 1998 년 Blaze 등에 의해 제안되었다[1]. 이 기법은 Alice 와 Bob 의 비밀키를 이용하여 재암호화키를 생성했다. 하나의 재암호화 키를 이용하여 Alice 가 Bob 에게 위임할 수 있었고, 그 반대로도 가능했다. 이 특징은 훗날의 기법들과 비교하여 양방향성이라고 부른다. 양방향성이 있으면 Alice 혹은 Bob 이 Proxy 와 공모하여 상대방의 비밀키를 알아낼 수 있기는 문제가 있었다. 따라서 이후의 기법들은 양방향성을 배제하는 방향으로 연구가 진행되었다.

이후 Ateniese 등은 단방향성을 갖는 Bilinear Pairing 기반 PRE 기법을 제안하였다. 이 기법은 Delegator 의 비밀키와 Delegatee 의 공개키로 재암호화 키를 생성한다. 이 기법은 양방향성에 의한 문제점은 해결하였으나, 선택 암호문 공격(CCA, Chosen Cipher-text Attack)에 취약하다는 문제점을 가지고 있었다.

프록시 재암호화 기법은 재암호화를 통해 복호화 권한을 위임해줄 수 있다. 하지만 한번 복호화 권한을 위임하게 되면 Delegator 의 모든 메시지를 Delegatee 가 복호화할 수 있다는 문제가 있다. 이를 해결하기 위해 복호화 권한의 범위를 제어할 수 있는 기법의 필요하게 되었다.

2.4. 조건부 프록시 재암호화 (Conditional PRE)

조건부 프록시 재암호화란 Delegatee 의 공개키로 암호화된 암호문 중 특정 조건을 만족하는 암호문만 Delegator 의 비밀키로 복호화할 수 있다. 여기에서 특정 조건이란 키워드, 비트스트링, 의미 있는 문자열 등이 될 수 있다.

2009 년 Weng 등이 제안한 조건부 프록시 재암호화 기법은 단일한 키워드에 대해서만 복호화 권한을 위임할 수 있다. 이후 다중 키워드를 지원하기 위한 기법들이 연구가 되었으나, Boolean 연산자를 모두 지원하는 방법은 아직까지 Open Problem 으로 남아있다.

2.5. Weng 등의 CPRE

이 기법은 Weng 등이 2009 년에 제안한 기법으로서 먼저 사용자의 공개키 쌍은 다음과 같이 계산된다.

.

$$\begin{cases} PR_i = x_i \\ PU_i = g^{x_i} \end{cases} \quad \text{where} \quad x_i \in \mathbb{Z}_p$$

Delegator 와 Delegatee 가 풀 수 있는 암호문을 Second Level Ciphertext 라 하며, 이에 필요한 인자는 다음과 같이 계산된다.

$$R = H_1(m, r)$$
$$C_1 = g^R$$
$$C_2 = r \cdot e\left(PU_i, H_2(PU_i, w)\right)^R$$
$$C_3 = m \oplus H_3(r)$$
$$C_4 = H_4(C_1, C_2, C_3)^R$$

Delegator 는 위의 암호문을 다음과 같이 복호화 할 수 있다.

$$\text{If } e\left(C_1, H(C_1, C_2, C_3)\right) \neq e(g, C_4) \text{ Then return } \perp$$
$$r = C_2 / e\left(C_1, H_2(PU, w)\right)^{PR}$$
$$m = C_3 \oplus H_3(r)$$

Delegator 를 i, Delegatee 를 j, 사용자 j가 만족해야 하는 조건을 w라 할 때, 재암호화 키는 다음과 같이 결정된다.

$$RK_{i \rightarrow j}^{w} = (RK_1, RK_2)$$
$$= ((H_2(PU_i, w) PU_j^s)^{-PR_i}, PU_i^s)$$

재암호화 후 Delegatee 가 복호화 할 수 있는 암호문을 First Level Ciphertext 라 하며 인자는 다음과 같이 계산된다.

$$\bar{s} = s \cdot PR_i$$
$$\overline{C_1} = g^R$$
$$\overline{C_2} = r \cdot e\left(g, PU_j\right)^{-R \cdot \bar{s}}$$
$$\overline{C_3} = m \oplus H_3(r)$$
$$\overline{C_4} = g^{\bar{s}}$$

Delegatee 는 위의 암호문을 다음과 같이 복호화 할 수 있다.

$r = \overline{C_2} \cdot e(\overline{C_1}, \overline{C_4})^{PR_j \cdot H_5(\overline{C_4}^{PR_j})}$
$m = \overline{C_3} \oplus H_3(r)$
If $g^{H_1(m,r)} = \overline{C_1}$ Then return m else return $\perp$

이제 Second Level Ciphertext 를 First Level Ciphertext 로 변형하면 Delegatee 는 자신의 비밀키로 Delegator 의 암호문을 풀 수 있게 된다. 이를 위해 앞서 생성한 재암호화키 $RK_{i\to j}^{w}$ 를 사용한다. 재암호화 과정은 다음과 같이 각 인수를 재암호화 키를 이용하여 변환하며 진행된다.

$$\overline{C_1} = C_1 = g^R$$
$$\overline{C_2} = C_2 \cdot e(C_1, RK_1) = r \cdot e(g, PU_j)^{-R \cdot s \cdot PR_i}$$
$$\overline{C_3} = C_3$$
$$\overline{C_4} = RK_2$$

2.6. AND 연산으로의 확장

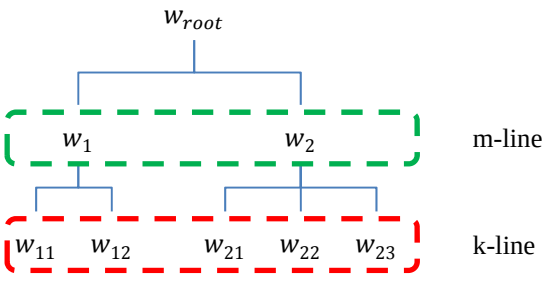
Boolean Algebra 에서 AND 연산은 곱셈과 동일하게 동작한다. 이는 조건부 프록시 재암호화 기법에도 바로 적용할 수 있다. Weng 등의 기법에서 하나의 조건 w 를 Delegatee 가 가지고 있는지 판단하기 위해 $H_2(PU, w)$ 를 사용했다. 만일 조건이 n 개로 확장된다면 사용자가 가지고 있어야 할 조건은 $\prod_{a=1}^{n} H_2(PU, w_a)$ 와 같은 형태가 될 수 있다. 이는 Weng 등의 기법에 바로 적용이 가능하다.

3. 제안하는 기법

본 논문에서는 Weng 등의 기법에 기반을 두되, AND 연산과 조금 다른 방법으로 OR 연산에 접근하였다. 본 논문에서 제안하는 기법의 첫 번째 아이디어는 OR 로 연결된 조건을 대신할 다른 조건을 사용하는 것이다. 예를 들어, 두 조건 w_{11} 과 w_{12} 중 하나만 가지고 있으면 w_1 을 풀 수 있다.

$$w_1 = w_{11} \text{ OR } w_{12}$$

이들을 포함관계로서 표현하면 (그림 1)과 같이 표현할 수 있다.



(그림 1) 키워드 사이의 관계

본 논문에서는 기존의 Condition 을 KC(Keyword Condition)라 하고, OR 연산을 위해 새로 생성한 조건들을 MC(Management Condition)라 한다.

실제 암호화에 사용되는 조건은 KC 와 MC 의 조합으로 구성되며, 사용자의 재암호화 키에는 MC 만 포함되어 있다. 사용자는 암호문에 포함된 MC 와 KC 의 조합에서 KC 를 제거함으로써 자신이 가지고 있는 재암호화 키로 해당 암호문을 재암호화 할 수 있게 된다. 이에 앞서 Delegator 는 KC 에 대해서는 공개하되, MC 에 대해서는 공개하지 않는다고 가정한다.

먼저 공개키와 개인키를 다음과 같이 생성한다.

$$\begin{cases} PR_i = x_i \\ PU_i = g^{x_i} \end{cases} \quad \text{where} \quad x_i \in \mathbb{Z}_p$$

Delegator 는 재암호화 조건으로 사용할 KC 와 그에 해당하는 MC 를 곱하여 암호문을 생성한다. 만일 KC 의 키워드를 w_{KC}, 이에 해당하는 MC 를 w_{MC} 라 했을 때 Second Level Ciphertext 는 다음과 같이 구성된다.

$$R = H_1(m, r)$$
$$C_1 = g^R$$
$$C_2 = r \cdot e(PU_i, H_2(PU_i, w_{MC}) \cdot H_2(PU_i, w_{KC}))^R$$
$$C_3 = m \oplus H_3(r)$$
$$C_4 = H_4(C_1, C_2, C_3)^R$$

Delegator 는 위의 암호문을 다음과 같이 복호화 할 수 있다.

If $e(C_1, H(C_1, C_2, C_3)) \neq e(g, C_4)$ Then return $\perp$
$r = C_2 / e(C_1, H_2(PU, w_{MC}) \cdot H_2(PU, w_{KC}))^{PR}$
$m = C_3 \oplus H_3(r)$

Delegator 를 i, Delegatee 를 j 라 할 때, 재암호화 키는 다음과 같이 결정된다.

$$RK_{i\to j}^{w} = (RK_1, RK_2) = ((H_2(PU_i, w_{MC}) PU_j^s)^{-PR_i}, PU_i^s)$$

본 논문에서는 재암호화의 결과로 얻을 수 있는 First Level Ciphertext 를 기존의 기법과 동일한 형태로 구성하려 한다. 동일하게 구성하면 단일 키워드와 AND 연산을 포함하여 OR 연산도 동시에 지원할 수 있기 때문이다. 사용자는 Second Level Ciphertext 에서 다음과 같이 First Level Ciphertext 를 얻을 수 있다. 이 때 Delegatee 는 w_{KC} 를 알고 있다고 가정하자.

$$\overline{C_1} = C_1 = g^R$$
$$\overline{C_2} = C_2 \cdot \hat{e}\left(C_1, RK_1^{H_2(PU_j, w_{KC})}\right) = r \cdot e(g, PU_j)^{-R \cdot s \cdot PR_i}$$
$$\overline{C_3} = C_3$$
$$\overline{C_4} = RK_2$$

4. 분석

OR 연산은 복수의 재암호화키를 이용하여 여러 번 시도하는 방법으로 대치될 수도 있다. 하지만 이 경우 모든 조건에 대해 재암호화키가 필요하다. 즉, n개의 조건에 대해 n개의 재암호화 키가 필요하다. 반면

제안하는 기법을 사용하게 되면 n개의 조건이 같은 MC 의 서브트리에 속할 때, 1 개의 키만으로도 재암호화가 가능해진다. 이를 통해 사용자는 자신의 키를 효율적으로 관리할 수 있다.

제안하는 기법은 Weng 등의 CPRE 에서 추가적으로 OR 연산을 지원하기 위해 1 회의 지수연산이 추가되었다. 이 지수연산은 사용자가 OR 연산을 하기 위해서만 필요하며 그 외의 경우에는 필요 치 않다.

5. 결론

조건부 재암호화 기법은 특정 메시지의 복호화 권한을 다른 사람에게 위임할 수 있다는 특징 때문에 클라우드 컴퓨팅 애플리케이션으로서 많은 관심을 받고 있다. 하지만 아직까지 Boolean 연산자를 완벽히 지원하는 기법은 발표되지 않았다. 본 논문에서는 Weng 등의 기법을 기반으로 여러 조건이 OR 로 연결된 키워드를 대신할 Management Keyword 를 이용하여 AND 와 OR 를 지원하는 조건부 재암호화 기법을 제안하였다. 제안된 기법은 사용자 측면에서 재암호화 키를 여러 개 둘 필요 없이 하나의 재암호화 키 만 이용함으로써 복호화 권한을 효율적으로 관리할 수 있다. 제안하는 기법은 메시지를 암호화하는 사람이 키워드의 구성을 미리 알고 있어야 한다는 한계가 있다. 하지만 클라우드 컴퓨팅과 같이 사용자가 직접 자신의 데이터를 관리하는 환경에서는 효율적으로 사용될 수 있다.

참고문헌

[1] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” Proc. of Advances in Cryptology - EUROCRYPT 1998, LNCS 1403, pp. 127-144, May 1998.

[2] Y. Dodis and A. Ivan, “Proxy cryptography revisited,” in Proc. Network and Distributed System Security Symposium (NDSS), Feb. 2003.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. “Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage,” ACM Transactions on Information and System Security (TISSEC), Vol. 9, No. 1, pp. 1-30, Feb. 2006.

[4] M. Green and G. Ateniese. “Identity-based proxy re-encryption,” The 5th International Conference on Applied Cryptography and Network Security (ACNS), LNCS 4521, pp. 288-306, June 2007.

[5] J. Weng, R.H. Deng, C. Chu, X. Ding, and J. Lai, “Conditional proxy re-encryption secure against chosen-ciphertext attack,” Proc. Of the 4th International Symposium on Information, Computer and Communications Security (ASIA CCS 09), pp. 322-332, Mar. 2009.