다중키워드를 지원하며 선택암호문 공격에 강건한 선택적 프록시 재암호화 기법*

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

CCA-Secure Conditional Proxy Re-encryption to Support Multi-keyword*

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

요 약

프록시 재암호화란 프록시를 통해 자신의 복호권한을 다른 사용자에게 위임하는 기법을 말한다. 초기의 프록시 재암호화 기법은 모든 문서에 대한 복호권한을 한번에 위임해야 한다는 한계가 있었다. 이를 해결하기 위해 선택적 프록시 재암호화 기법이 제안되었다. 이 기법은 특정 상태(혹은 키워드)를 갖는 문서에 대해서만 복호권한을 위임하도록 지정할 수 있기 때문에, 기존의 기법보다 유연하게 적용이 가능하다는 장점이 있다. Weng 등이 제안한 선택적 프록시 재암호화 기법은 CCA 에는 강건하지만, 다중 키워드로의 확장을 정의하지 못하였다. 본 논문에서는 Weng 의 선택적 프록시 재암호화 기법을 확장하여 CCA 에 강건하며 다중키워드를 지원하는 프록시 재암호화 기법을 제안한다.

1. 서론

프록시 재암호화란 프록시를 통해 자신의 복호권한을 다른 사용자에게 위임하는 기법을 말한다. 초기의 프록시 재암호화 기법은 한번 권한을 위임하게 되면 사용자의 모든 문서에 대한 복호권한이 위임되는 한계가 있었다. 이를 해결하기 위해 선택적 프록시 재암호화 기법이 제안되었다. 선택적 프록시 재암호화 기법은 특정 상태(혹은 키워드)를 갖는 문서에 대해서만 복호권한을 위임할 수 있기 때문에, 복호권한의 위임을 더욱 유연하게 적용할 수 있다. 2009 년 Weng 등은 CCA(Chosen Ciphertext Attack)에 강건한 선택적 프록시 재암호화 기법을 제안했지만, 단일 홉(Single Hop)에 대해서만 적용이 가능하며, 다중 키워드에 대한 확장이 제시되지 않았다. 본 논문에서 Weng 등의 기법에 기반을 두어 다중 키워드를 지원하며 CCA 에 강건한 선택적 프록시 재암호화 기법을 제안한다.

이후의 구성은 2 장에서 배경지식들을, 3 장에서 기존에 진행된 프록시 재암호화 기법들을 소개한다. 4 장에서는 결합 키워드를 지원하는 선택적 재암호화 기법을 제안한다. 5 장에서는 제안한 기법을 분석하고 6 장에서 결론을 맺는다.

2. 배경지식

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
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	$\mathbb{G} \rightarrow \mathbb{Z}_p$

* "본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (NIPA-2012-H0301-12-1002)

2.2. 겹선형 맵(Bilinear Maps)

$\mathbb{G}$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 존재함.

2.3. 결정적 겹선형 디피-헬만 가정

(Decisional Bilinear Diffie-Hellman assumption)

그룹 $(\mathbb{G}, \mathbb{G}_T)$에서 DBDH 문제란, $(g, g^a, g^b,\ g^c, Q) \in \mathbb{G}^4 \times \mathbb{G}_T$ 일 때 알 수 없는 $a, b, c \in \mathbb{Z}_p$ 에 대해 $Q = e(g,g)^{abc}$를 만족하는 Q를 찾는 것을 말한다. 다항시간 알고리즘을 $\mathcal{B}$, 공격자의 이득을 ϵ이라 할 때 이 둘의 관계는 다음과 같아야 한다.

$$|\Pr[\mathcal{B}(g, g^a, g^b, g^c, Q = e(g,g)^{abc}) = 1] - \Pr[\mathcal{B}(g, g^a, g^b, g^c, Q = e(g,g)^d) = 1]| \geq \epsilon$$

이때 확률 Pr은 각각 Z_p에서 a, b, c, d를 임의로 선택할 확률과 $\mathbb{G}$에서 임의로 g를 선택활 확률이며, $\mathcal{B}$에서 임의의 비트를 소비하는 확률을 말한다.

그룹 $(\mathbb{G}, \mathbb{G}_T)$에서 DBDH 가정은 공격자가 DBDH 문제를 해결하기 위해 $\mathcal{B}$를 계산할 때 얻는 이득이 최소 ϵ보다 커야 한다는 것이다.

3. 관련연구

3.1. PRE, Proxy Re-Encryption

프록시 재암호화 기법이란 A 의 공개키로 암호화된 암호문을 B 의 공개키로 복호화할 수 있도록 암호문을 변환하는 기법을 말한다. 이때 재암호화 하는 과정에서 프록시는 평문이나 A 의 비밀키를 알 수 없어야 한다. 프록시 재암호화의 목적은 TTP(Trust Third-Party)의 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 생성한 재암호화키를 사용하는 기법으로서 하나의 재암호화 키로 Alice to Bob, Bob to Alice 재암호화가 모두 가능했다. 이 특징을 이후 제안되는 기법과 비교하여 양방향성이라고 부른다. 하지만 이 기법은 양방향성 때문에 Alice 와 Proxy 혹은 Bob 과 Proxy 가 공모하여 상대방의 비밀키를 알아낼 수 있기는 문제가 있었다. 따라서 이후 제안되는 기법들은 양방향성을 배제하는 방향으로 연구를 진행하였다.

이후 Ateniese 등은 단방향성을 갖는 Bilinear Pairing 기반 PRE 기법을 제안하였다. 이 기법은 위임자(Delegator)의 비밀키와 위임 받는자(Delegatee)의 공개키로 재암호화 키를 생성한다. 분석에 의하면 이 기법은 선택 평문 공격(CPA, Chosen Plain-text Attack)에 강건함을 갖지만, 선택 암호문 공격(CCA, Chosen Cipher-text Attack)에 취약한 것으로 밝혀졌으며, 이후 제안되는 기법들에서는 CCA 를 고려하여 설계하고 있다.

3.2. CPRE, Conditional Proxy Re-Encryption

선택적 재암호화 기법이란 A 의 공개키로 암호화된 암호문 중 특정 조건을 만족하는 암호문만 B 의 비밀키로 복호화할 수 있도록 암호문을 변환하는 기법을 말한다. 여기에서 특정 조건이란 키워드, 비트스트링, 의미 있는 문자열 등을 말하며, CPRE 에서는 이를 만족해야 복호화 할 수 있다.

2009 년 Weng 등은 n-Quotient Bilinear Diffie-Hellman Assumption 에 기반을 둔 CPRE 기법을 제안하였다[3]. Weng 은 이 기법을 제안할 때 CPA 뿐만이 아니라 CCA 도 강건하다고 주장하였으나, 얼마 후 자신의 기법이 CCA 에 취약함을 보이고 Decisional Bilinear Diffie-Hellman Assumption 에 기반을 둔 새로운 기법을 제안하였다[4]. Weng 등이 제안한 Efficient CPRE 는 CCA 에 안전하게 설계되었지만, 단일 키워드에 대해서만 정의가 되어있다.

3.3. Efficient CPRE

이 기법은 Weng 등이 2009 년에 제안한 기법으로서 CCA 에 안전하게 설계되어 있다. 먼저 사용자의 공개키 쌍은 다음과 같이 계산된다.

.

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

초기 권한 소유자의 비밀키로 풀 수 있는 암호문을 Second Level Ciphertext[1]라 하며, 이에 필요한 인자는 다음과 같이 계산된다.

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

초기 권한 소유자는 위의 암호문을 다음과 같이 복호화 할 수 있다.

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

위임하려는 사용자를 i, 위임 받을 사용자를 j, 사용자 j가 만족해야 하는 조건을 w라 할 때, 재암호화 키는 다음과 같이 결정된다.

[1] Level 에 의한 표기법은 Ateniese 등에 의해 처음 사용되었으며, 본 논문에서도 이 표기법을 따름.

$$RK_{i\to j}^{w} = (RK_1, RK_2) = \left(\left(H_2(PU_i, w)PU_j^{s\cdot H_5\left(PU_j^{s\cdot PR_i}\right)}\right)^{-PR_i}, PU_i^{s}\right)$$

위임 받을 사용자의 비밀키로 풀 수 있는 암호문을 First Level Ciphertext 라 하며 인자는 다음과 같이 계산된다.

$$\bar{s} = s \cdot PR_i$$
$$\overline{C_1} = g^R$$
$$\overline{C_2} = r \cdot e(g, PU_j)^{-R\cdot\bar{s}\cdot H_5\left(PU_j^{\bar{s}}\right)}$$
$$\overline{C_3} = m \oplus H_3(r)$$
$$\overline{C_4} = g^{\bar{s}}$$

복호권한을 위임 받은 사용자는 위의 암호문을 다음과 같이 복호화할 수 있다.

$$r = \overline{C_2} \cdot e(\overline{C_1}, \overline{C_4})^{PR_j\cdot H_5\left(\overline{C_4}^{PR_j}\right)}$$
$$m = \overline{C_3} \oplus H_3(r)$$
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 권한을 위임 받은 사용자는 자신의 비밀키로 초기 권한 소유자의 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.

$$\overline{C_1} = C_1 = g^R$$
$$\overline{C_2} = C_2 \cdot e(C_1, RK_1) = r \cdot e(g, PU_j)^{-R\cdot s\cdot PR_i\cdot H_5\left(PU_j^{s\cdot PR_i}\right)}$$
$$\overline{C_3} = C_3$$
$$\overline{C_4} = RK_2$$

4. 제안하는 기법

권한을 위임 받는 사용자가 가져야 하는 n 개의 상태를 $\{w_1, \ldots, w_n\}$이라고 하자. 사용자가 사용하는 공개키 쌍은 다음과 같이 생성한다.

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

초기 권한 소유자는 자신의 암호문에 사용할 키워드들을 다음과 같은 형태로 결합하여 Second Level Ciphertext 를 생성한다.

$$R = H_1(m, r)$$
$$C_1 = g^R$$
$$C_2 = r \cdot e(PU_i, \textstyle\prod_{t=1}^{n} H_2(PU_i, w_t))^R$$
$$C_3 = m \oplus H_3(r)$$
$$C_4 = H_4(C_1, C_2, C_3)^R$$

Second Level Ciphertext 의 형태가 변함에 따라 다음과 같이 복호화 과정이 변경된다.

If $e\left(C_1, H(C_1, C_2, C_3)\right) \neq e(g, C_4)$ Then return $\perp$
$r = C_2 / e(C_1, \prod_{t=1}^{n} H_2(PU_i\ w_t))^{PR_i}$
$m = C_3 \oplus H_3(r)$

위와 같이 키워드가 포함된 Second Level Ciphertext 를 First Level Ciphertext 로 변환해야 하는데, 이때 재암호화 키가 암호문 내의 키워드 부분을 소거할 수 있도록 다음과 같은 형태로 구성한다.

$$RK_{i\to j}^{w} = (RK_1, RK_2) = \left(\left(\prod_{t=1}^{n}(H_2(PU_i\ w_t))PU_j^{s\cdot H_5\left(PU_j^{s\cdot PR_i}\right)}\right)^{-PR_i}, PU_i^{s}\right)$$

위의 재암호화 키를 사용하면 권한을 위임 받는 사용자는 단일 키워드에 대한 First Level Ciphertext 와 동일한 형태의 암호문을 얻게 된다. 이후의 과정은 Efficient CPRE 와 동일하다.

5. 분석

제안하는 기법의 안전성은 결정적 겹선형 디피-헬만 가정에 의존하고 있으며, RK_1내부에 RK_2를 포함함으로써 CCA 로부터 안전하다. 만일 이와 같은 구조를 띄지 않는다면 다음과 같이 CCA 공격이 가능하다.

$$\overline{C_1}' = \overline{C_1} = g^R$$
$$\overline{C_2}' = \overline{C_2} \cdot e(\overline{C_1}, PU)^{-l} = r \cdot e(g, PU)^{-r\cdot(\bar{s}+l)}$$
$$\overline{C_3}' = \overline{C_3} = m_\delta \oplus H_3(r)$$
$$\overline{C_4}' = \overline{C_4} \cdot g^l = g^{\bar{s}+l}$$

위의 식에서 $\bar{s}' = \bar{s} + l$라 하면 공격자는 키 없이 암호문을 생성한 것이 된다. 하지만 본 기법은 Weng 의 기법에 따라 암호문에 사용자의 키를 포함하고 있기 때문에 CCA 로부터 안전하다.

제안하는 기법은 다중키를 지원하기 위해 암호문 생성과정, 재암호화키 생성과정, 복호화 과정에서 각각 n번의 곱셈과 해쉬연산이 소요된다. 해쉬 후의 곱셈은 $\mathbb{G}$상에서 이루어지므로 암호문의 크기에는 영향을 주지 않는다.

6. 결론 및 향후연구

본 논문은 Weng 의 기법을 확장하여 CCA 에 강건하며 다중키워드를 지원하는 선택적 프록시 재암호화 기법을 제안하였다. 제안된 기법은 Second Level Ciphertext 를 다루는 과정에서 n번의 곱셈와 해쉬연산이 소요되지만, 군에서 다루기 때문에 암호문의 크기에는 영향을 주지 않는다. 제안하는 기법은 여러 개의 키워드에 대해서는 관리할 수 있지만 여전히 결합 키워드(Conjunctive Keyword)에 대해서는 처리하지 못하는 한계가 있다. 따라서 향후에는 결합 키워드의 소유 여부를 판단하여 권한을 위임할 수 있는 선택적 프록시 재암호화 기법에 대한 연구가 필요하다.

참고문헌

[1] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography advances in cryptology — EUROCRYPT'98," in Advances in Cryptology — EUROCRYPT'98, ser. Lecture Notes in Computer Science, K. Nyberg, Ed. Berlin/Heidelberg: Springer Berlin / Heidelberg, 1998, vol. 1403, ch. 10, pp. 127-144.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1-30, 2006.

[3] J. Weng, R. H. Deng, X. Ding, C. K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS '09. New York, NY, USA: ACM, 2009, pp. 322-332.

[4] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, "Efficient conditional proxy re-encryption with Chosen-Ciphertext security information security," ser. Lecture Notes in Computer Science, P. Samarati, M. Yung, F. Martinelli, and C. A. Ardagna, Eds. Berlin, Heidelberg: Springer Berlin / Heidelberg, 2009, vol. 5735, ch. 13, pp. 151-166.