복호화 권한을 양도할 수 있는 ID 기반의 대리 재 암호화 기법*

김기탁 박종환 이동훈
고려대학교 정보경영 공학 전문 대학원
{kitak, decartian, donghlee}@korea.ac.kr

Identity-Based Proxy Re-encryption with Multi-delegation

Ki Tak Kim Jong Hwan Park Dong Hoon Lee
Graduate School of Information Management and Security, Korea University

요약

1984년 Shamir에 의해 ID 기반의 암호시스템에 대한 개념이 소개된 이후로 많은 연구가 이루어져 왔다. ID 기반의 암호시스템에서는 복호화 할 수 있는 자를 암호화 하는 자가 선택하여 암호화 하기 때문에 정당한 복호화 권한을 가지고 있는 자만이 복호화를 할 수 있다. 이러한 복호화 권한은 어플리케이션에 따라 양도할 수 있어야 한다. 예를 들어 네트워크 스토리지의 경우는 정당한 권한을 가진 자에게 암호화 되어 저장되어 있는 컨텐츠를 복호화 할 수 있도록 권한을 양도해 주어야 한다. 대리 재 암호화(Proxy Re-encryption)은 복호화 권한을 다른 사람에게 양도할 수 있는 기법에 관한 것이다. 재 암호화 기법은 DRM과 같은 방송 통신 환경에 적합하게 사용될 수 있다. 본 논문에서는 ID 기반에서 복호화 권한을 적법하게 양도할 수 있는 재 암호화 기법을 제안한다.

1. 서론

대리 재 암호화는 대리자가 A의 공개키로 암호화 되어 있는 암호문 CA를 B의 공개키로 암호화 되어 있는 암호문 CB로 변형할 수 있도록 해 주는 기법이다. 이러한 기법은 A가 자신의 비밀 키를 B에게 알려주지 않고 암호화 된 메시지를 B가 복호화 할 수 있어야 하는 상황에 적합하게 사용될 수 있다. 대리 재 암호화 기법에서 대리자는 A 또는 B의 비밀 키를 알 수 없어야 하고 메시지에 대한 어떠한 정보도 얻을 수 없어야 한다.

공개키 기반의 대리 재 암호화 기법은 많은 연구가 이루어져 왔다 [1, 2, 3, 4, 5]. 최근에는 대리 재 암호화 기법을 ID 기반에 적합하도록 설계하는 연구가 많이 이루어지고 있다. ID 기반의 암호시스템에서는 메시지의 전송자는 수신자의 공개키로 수신자의 ID (예를 들어, 전화번호나 이-메일 주소)를 사용하여 메시지를 암호화 한다. 본 논문에서 제안하는 대리 재 암호화 기법은 A의 ID를 사용하여 암호화 한 암호문을 B의 ID를 사용하여 암호화 한 암호문으로 변형하는 기법이다. 제안 기법은 위임자의 어떠한 비밀 정보도 필요로 하지 않으며 위임자의 연산 부담이 없다. A가 B에게 복호화 권한을 양도해 주었다면, B는 다시 C에게 복호화 권한을 양도해 줄 수 있는 경우에는 재사용(multi-use) 가능하다라고 한다. 제안 기법은 재사용이 가능하다.

본 논문에서 제안하는 기법은 Boneh와 Boyen이 제안한 ID 기반의 암호화 기법 (BB-IBE)에 위임 기법을 추가하여 설계되었다 [6]. 제안 기법은 위임자에게 추가적인 알고리즘을 필요로 하지 않으며, 복호화 하는 자 역시 추가적인 비밀 키 또는 알고리즘을 필요로 하지 않는다. 즉, 복호화 권한의 수임자는 기반이 되는 BB-IBE의 복호화 알고리즘을 그대로 사용하면 된다. 이전에 제안되었던 ID 기반의 재 암호화 기법은 위임자의 비밀 키를 이용하여 재 암호화 키를 생성하여야 한다. 하지만 제안하는 기법은 위임자의 비밀 키도 필요로 하지 않는다는 점에서 더욱 다양한 어플리케이션에 적용 가능하다.

대리 재 암호화 기법은 네트워크 스토리지의 접근 제어 시스템에 활용할 수 있다. 즉, 대리 재 암호화 기법은 방송 컨텐츠를 네트워크 스토리지에 암호화 하여 저장한 뒤, 복호화 권한을 적법한 자에게만 양도하여 방송 컨텐츠를 정당하게 구매한 자에게만 컨텐츠를 얻을 수 있도록 제어하는 시스템을 구현하는데 적합하게 사용될 수 있다.

본 논문의 2절에서는 대리 재 암호화 기법에 필요한 기반 요소에 대하여 설명하고, 3절은 BB-IBE에 관하여 간략하게 설명한다. 4절에서 제안하는 기법을 서술하고, 5절에서 결론을 맺는다.

2. 기반 요소

가. Bilinear Map

G와 G_1을 소수인 위수 p를 갖는 곱셈 순환 그룹이라고 하자. G의 생성자를 g라고 하자. 다음과 같은 조건을 만족시킬 때 G_1은 admissible bilinear map $e: G \times G \rightarrow G_1$을 갖는다.

1. 모든 a, b에 대하여 $e(g^a, g^b) = e(g, g)^{ab}$.
2. $e(g, g) \neq 1$.
3. 모든 a, b와 g에 대하여 $e(g^a, g^b)$를 효율적으로 계산할 수 있는 알고리즘이 존재한다.

* "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

나. Identity-based Proxy Re-encryption

ID 기반의 대리 재 암호화 기법 (IB-PRE)은 다음과 같은 5개의 알고리즘으로 구성되어 있다.

Setup(k). 안전성 상수 k를 입력 받아 모든 사용자에게 공개 상수 $params$를 분배하고 mk를 마스터 비밀 키로 한다.

KeyGen($params$, mk, ID). 공개 상수 $params$, 마스터 비밀 키 mk와 ID를 입력 받아 ID에 대응하는 복화화 비밀 키 sk_{ID}를 생성한다.

Enc($params$, ID, M). 공개 상수 $params$와 ID와 메시지 M을 입력 받아 ID에 대한 메시지 M의 암호문 C_{ID}를 생성한다.

RKGen($params$, C_{ID_A}, ID_A, ID_B). ID_A가 복호화 할 수 있는 암호문 C_{ID_A}와, ID_A, ID_B를 입력 받아 재 암호화 키 $rk_{ID_A \to ID_B}$를 생성한다.

Re-enc($params$, $rk_{ID_A \to ID_B}$, C_{ID_A}). ID_A가 복호화 할 수 있는 암호문 C_{ID_A}와 재 암호화 키 $rk_{ID_A \to ID_B}$를 입력 받아 재 암호화 된 암호문 C_{ID_B}을 생성한다.

Dec($params$, sk_{ID}, C_{ID}). $params$와 비밀 키 sk_{ID}, 암호문 C_{ID}를 입력 받아 메시지 M을 출력한다.

올바름. 다음을 만족하면 대리 재 암호화 기법은 올바르다고 한다.

- $Dec(params, sk_{ID_A}, C_{ID_A}) = M.$
- $Dec(params, sk_{ID_B}, Re-enc(params, rk_{ID_A \to ID_B}, C_{ID_A})) = M.$

3. Boneh-Boyen Identity-based Encryption

본 논문의 제안 기법에 기반이 되는 BB-IBE는 다음과 같다[6].

SetUp(k). 안전성 상수 k가 주어졌을 때, 그룹 G의 임의의 생성자 g를 선택한다. 그리고 G의 임의의 원소 g_2와 h를 선택한다. Z_p^*의 원소 α를 선택하여 $g_1 = g^{\alpha}, mk = g_2^{\alpha}$로 $params = (g, g_1, g_2, h)$로 설정한다. α는 마스터 비밀 키 값으로 한다. $params$를 공개한다.

KeyGen(mk, $params$, ID). mk, $params$, ID를 입력 받는다. Z_p^*의 원소 u를 선택하여 다음과 같이 계산한다.

$$sk_{ID} = (d_0, d_1) = (g_2^{\alpha}(g_1^{ID}h)^u, g^u).$$

Enc(ID, $params$, M). 메시지 M을 ID로 암호화 하기 위하여 Z_p^*의 원소 r를 선택하고 다음과 같이 암호문을 생성한다.

$$C_{ID} = (g^r, (g_1^{ID}h)^r, M \cdot e(g_1, g_2)^r).$$

Dec(sk_{ID}, $params$, C_{ID}). 암호문 $C_{ID} = (C_1, C_2, C_3)$와 비밀 키 $sk_{ID} = (d_0, d_1)$, $params$를 입력 받아 다음과 같이 복호화 한다.

$$M = \frac{C_3 \cdot e(d_1, C_2)}{e(d_0, C_1)}.$$

4. 제안하는 Identity-based Proxy Re-encryption

제안하는 IB-PRE의 Setup, KeyGen, Enc, Dec 알고리즘은 BB-IBE와 동일하다. 여기서는 IB-PRE에 추가되는 알고리즘은 RKGen과 Re-enc 만 기술한다. 대리자는 RKGen과 Re-enc을 이용하여 재 암호화 된 암호문을 생성한다.

RKGen($params$, C_{ID_A}, ID_A, ID_B). $C_{ID_A} = (C_1, C_2, C_3)$라면 키 생성 기관 (KGC)에게 C_1을 전송하여 $C_1^{\alpha} = E$을 얻는다. Z_p^*의 원소 r_P를 선택하고 다음과 같이 계산한다.

$$X = g^{r_P},$$
$$Y = E^{(ID_B - ID_A)} \cdot g_1^{ID_B \cdot r_P} \cdot h^{r_P},$$
$$Z = e(g_1, g_2)^{r_P}.$$

$rk_{ID_A \to ID_B} = (X, Y, Z)$을 출력한다.

Re-enc($params$, $rk_{ID_A \to ID_B}$, C_{ID_A}). $params$, $rk_{ID_A \to ID_B}$, C_{ID_A}을 입력 받아 다음과 같이 계산한다.

$$C_1' = C_1 \cdot X,$$
$$C_2' = C_2 \cdot Y,$$
$$C_3' = C_3 \cdot Z.$$

재 암호화 된 암호문 $C_{ID_B} = (C_1', C_2', C_3')$을 출력한다.

올바름. $Dec(params, sk_{ID_A}, C_{ID_A}) = m$은 자명하므로 보이지 않는다.

$Dec(params, sk_{ID_B}, Re-enc(params, rk_{ID_A \to ID_B}, C_{ID_A})) = M$에 대하여 설명한다. 재 암호화 된 암호문 $C_{ID_B} = (C_1', C_2', C_3')$은 다음과 같다.

$$C_1' = g^{r + r_P},$$
$$C_2' = (g_1^{ID_B}h)^{r + r_P},$$
$$C_3' = M \cdot e(g_1, g_2)^{r + r_P}.$$

따라서 B의 비밀 키 $sk_{ID_B} = (d_0^B, d_1^B) = (g_2^{\alpha}(g_1^{ID_B}h)^{u_B}, g^{u_B})$라 할 때, Dec 알고리즘은 다음과 같이 메시지 M을 계산할 수 있다.

$$
\begin{aligned}
M &= \frac{C_3' \cdot e(d_1^B, C_2')}{e(d_0^B, C_1')} \\
&= \frac{M \cdot e(g_1, g_2)^{r+r_P} \cdot e(d_1^B, (g_1^{ID_B}h)^{r+r_P})}{e(d_0^B, g^{r+r_P})} \\
&= \frac{M \cdot e(g_1, g_2)^{r+r_P}}{e(g_2^{\alpha}(g_1^{ID_B}h)^{u_B}, g^{r+r_P})} \\
&= \frac{M \cdot e(g_1, g_2)^{r+r_P} \cdot e(g^{u_B}, (g_1^{ID_B}h)^{r+r_P})}{e(g_2^{\alpha}, g^{r+r_P}) \cdot e((g_1^{ID_B}h)^{u_B}, g^{r+r_P})} \\
&= \frac{M \cdot e(g_1, g_2)^{r+r_P}}{e(g_2^{r+r_P}, g^{\alpha})}.
\end{aligned}
$$

따라서 IB-PRE는 올바름을 만족한다.

제안 기법은 위임자에게 어떠한 계산적 부담을 주지 않는다. 또한 네트워크 스토리지의 경우를 생각해 볼 때 대리자가 같는 계산적 부담은 크지 않다고 볼 수 있다. 또한 C_{ID_B}는 동일한 위임 절차를 통해 복호화 권한을 C에게 양도할 수 있다. 즉, 대리자는 동일한 계산 과정을 통해 C_{ID_C}를 계산 할 수 있다. 따라서 제안 기법은 네트워크 스토리지에 저장될 컨텐츠를 BB-IBE의 기법으로 암호화 하여 저장한 뒤, 제안 기법을 이용하여 정당한 복호화 권한을 가진 자에게 복호화 권한을 위임 (즉, 정당한 복호화 권한을 가진 자가 복호화 할 수 있도록 재 암호화) 할 수 있다.

5. 결론

대리 재암호화 기법은 대리자를 통하여 복호화 권한을 다른 사람에게 위임할 수 있는 기법이다. 이러한 기법은 네트워크 스토리지의 접근 제어 시스템에 활용 가능하다. 본 논문에서는 네트워크 스토리지에 효율적으로 적용할 수 있는 대리 재 암호화 기법을 제안하였다. 하지만 제안 기법의 암호학적 안전성에 대한 증명은 앞으로 연구할 과제로 남아 있다.

6. 참고문헌

[1] Mambo, M, Okamoto, E, "Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts.", IEICE Trans. Fund. Electronics Communications and Computer Science E80-A/1, pp. 54-63, 1997.

[2] Blaze, M., Bleumer, G., Strauss, M., "Divertible protocols and atomic proxy cryptography.", In Proceedings of Eurocrypt '98, Vol. 1403, pp. 127-144, 1998.

[3] Ateniese, G. Fu, K., Green, M., Hohenberger, S., "Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage.", In the 12th Annual Network and Distributed System Security Symposium, pp. 29-43, 2005.

[4] Jakobsson, M., "On quorum controlled asymmetric proxy re-encryption.", In Proceedings of Public Key Cryptography, pp. 112-121, 1999.

[5] Dodis, Y., Ivan, A., "Proxy cryptography revisited.", In Proceedings of the Tenth Network and Distributed System Security Symposium, 2003.

[6] D. Boneh, X. Boyen, "Efficient selective-id secure identity based encryption without random oracles", In Advances in Cryptology - Eurocrypt '04, LNCS, Vol. 3152, pp. 443-459, Springer-Verlag, 2004.