情報保護學會論文誌
第13券 第3號, 2003. 6

보다 효율적인 Hierarchical ID-based Cryptosystem*

김 태 구**, 염 대 현***, 이 필 중****

More Efficient Hierarchical ID-based Cryptosystem

Tae Gu Kim**, Dae Hyun Yum***, and Pil Joong Lee****

요 약

C. Gentry와 A. Silverberg의 Hierarchical ID-based cryptography[3]에서는 계층에서 수신자의 단계가 깊어짐에 따라 암호문의 길이가 선형적으로 증가한다는 문제가 있었다. 본 논문에서는 HIDS(Hierarchical ID-based Signature)의 서명값을 활용해 암호문의 길이를 줄이는 새로운 방법을 제안한다.

ABSTRACT

Hierarchical ID-based Cryptography proposed by C. Gentry and A. Silverberg has the problem that the length of the ciphertext is proportional to the depth of the recipient in the hierarchy. In this paper, we propose the new methods to shorten the length of the ciphertext by using HIDS(Hierarchical ID-based Signature).

Keyword : ID-based cryptography, signature

Ⅰ. 서 론

ID-based cryptosystem은 1984년 A. Shamir에 의해 제안되었다. 송신자는 수신자의 ID로부터 암호키를 생성한 후 평문을 암호화한다. 수신자는 받은 암호문을 PKG(Private Key Generator)에서 받은 복호키를 사용해서 복호화한다. 이는 기존의 PKI(Public Key Infrastructure)에 사용되는 인증서를 사용하지 않고 사용자들이 이미 가지고 있는 ID(e-mail 주소 등)를 사용함으로써 인증서 관리의 불편함을 근본적으로 제거할 수 있다는 장점을 가지고 있다. 실제적인 ID-based encryption scheme[2]은 2001년에 D. Boneh와 M. Franklin에 의해 제안되었고, 최근에는 이를 계층적으로 구현한 Hierarchical ID-based cryptography[3]가 제안되었으나 계층에서 수신자의 단계가 깊어짐에 따라 암호문과 서명의 길이가 선형적으로 증가한다는 단점이 있다. 본 논문에서는 Hierarchical ID-based cryptography[3]의 이러한 단점을 서명을 통해 해결하는 보다 효율적인 방법을 제안한다.

Ⅱ. Hierarchical ID-based cryptography (C. Gentry & A. Silverberg)

이 장에서는 C. Gentry 와 A. Silverberg가 제안한 Hierarchical ID-based cryptography에 대해 알아본다.

---

* 본 논문은 2002년도 CISC 우수 논문임.

** KT 기술연구소(tgkim75@kt.co.kr)
*** 포항공과대학교 정보보안연구실(IS)(daehyun@oberon.postech.ac.kr)
**** 포항공과대학교 정보보안연구실(IS)(pjl@postech.ac.kr)

2.1 정 의

2.1.1 Admissible pairing

G_1과 G_2는 소수 위수 q를 가지는 가환군이라고 할 때, 다음과 같은 특성을 가지는 $G_1 \times G_1$에서 G_2로의 함수 $\hat{e}$를 admissible pairing이라고 한다.

- Bilinear: $\hat{e}(aQ, bR) = \hat{e}(Q, R)^{ab}$, $Q, R \in G_1, a, b \in Z$
- Non-degenerate: $\hat{e}$는 $G_1 \times G_1$의 모든 원소를 G_2의 항등원으로 보내지는 않는다.
- Computable: 임의의 $Q, R \in G_1$에 대한 $\hat{e}(Q, R)$값을 계산할 수 있는 효율적인 알고리즘이 존재한다.

2.1.2 BDH(Bilinear Diffie-Hellman) parameter generator

k에 polynomial한 시간 동안 소수 위수 q를 가지는 G_1, G_2 그리고 admissible pairing $\hat{e}$를 출력하는 랜덤 알고리즘이다. (여기서 k는 security parameter)

2.1.3 Bilinear Diffie-Hellman Assumption

G_1과 G_2를 큰 소수 위수 q를 가지는 가환군이라고 하자. G_1의 원소 P를 임의로 선택하고 Z_q의 원소 a, b, c를 임의로 선택해서 aP, bP, cP가 주어졌을 때, $\hat{e}(P, P)^{abc}$를 계산하는 것이 어렵다는 가정이다.

2.2 HIDE(Hierarchical ID-based Encryption) Scheme

2.2.1 Root Setup

㉠ BDH parameter generator는 security parameter k를 입력으로 받아 소수 위수 q를 가지는 G_1, G_2, 그리고 $\hat{e}$을 생성한다.
㉡ 임의의 생성원 P_0를 G_1에서 선택한다.
㉢ 임의의 s_0 를 Z_q에서 선택한 후 $Q_0 = s_0P_0$를 계산한다.
㉣ 다음과 같은 해쉬 함수 H_1, H_2를 선택한다.
H_1: $\{0, 1\}^* \rightarrow G_1$, H_2: $G_2 \rightarrow \{0, 1\}^n$

여기서 t는 수신자의 단계이며, system parameter는 $<G_1, G_2, \hat{e}, P_0, Q_0, H_1, H_2>$이고 $s_0 \in Z_q$는 root PKG의 secret이다.

2.2.2 Lower-level Setup

$Level_i$를 i단계에 있는 entity들의 집합이라고 할 때 (여기서 $Level_0 = \{RootPKG\}$), entity $E_t \in Level_t$는 s_t를 Z_q에서 임의로 선택해서 그것을 안전하게 보관한다.

2.2.3 Extraction

E_t를 ID-tuple $(ID_1, ..., ID_t)$를 가지는 $Level_t$의 entity라고 하자. 이 때 $(ID_1, ..., ID_i)$ $(1 \le i < t)$은 E_t의 조상들의 ID-tuple이다. 그러면 E_t의 부모는 다음과 같은 과정을 수행한다.

㉠ $P_t = H_1(ID_1, ..., ID_t) \in G_1$를 계산한다.
㉡ E_t의 secret point S_t를 다음과 같이 계산한다.

$$S_t = S_{t-1} + s_{t-1}P_t = \sum_{i=1}^{t} s_{i-1}P_i$$

(S_0는 G_1의 항등원)

㉢ S_t와 $Q_i = s_iP_0$ $(1 \le i < t)$들을 E_t에게 전달한다.

2.2.4 Encryption

E_t에게 평문 $M \in \{0,1\}^n$을 암호화하여 보내기 위해서 다음과정을 수행한다.

㉠ $P_i = H_1(ID_1, ..., ID_i) \in G_1$ $(1 \le i \le t)$를 계산한다.
㉡ 임의의 r을 Z_q에서 선택한다.
㉢ 다음과 같은 암호문 $C \in G_1^t \times \{0,1\}^n$를 전송한다.

$$C = [rP_0, rP_2, ..., rP_t, M \oplus H_2(g^r)] \quad \text{(수식 1)}$$

여기서 $g = \hat{e}(Q_0, P_1) \in G_2$

2.2.5 Decryption

받은 암호문을 $C=[U_0, U_2, ..., U_t, V] \in G_1^t \times \{0,1\}^n$라고 하면, E_t는 다음과 같이 복호화한다.

$$V \oplus H_2\left(\frac{\hat{e}(U_0, S_t)}{\prod_{i=2}^{t} \hat{e}(Q_{i-1}, U_i)} \right) = M$$

2.3 HIDS(Hierarchical ID-based Signature) Scheme

2.3.1 Root Setup

㉠ BDH parameter generator는 security parameter k를 입력으로 받아 소수 위수 q를 가지는 G_1, G_2, 그리고 $\hat{e}$을 생성한다.
㉡ 임의의 생성원 P_0를 G_1에서 선택한다.
㉢ 임의의 s_0 를 Z_q에서 선택한 후 $Q_0 = s_0P_0$ 를 계산한다.

㉣ 다음과 같은 해쉬 함수 H_1, H_3를 선택한다.

$$H_1: \{0,1\}^* \rightarrow G_1, \quad H_3: \{0,1\}^* \rightarrow G_1$$

여기서 t는 서명자의 단계이며, system parameter는 $<G_1, G_2, \hat{e}, P_0, Q_0, H_1, H_3>$이고 $s_0 \in Z_q$는 root PKG의 secret이다.

2.3.2 Lower-level Setup: HIDE와 동일

2.3.3 Extraction: HIDE와 동일

2.3.4 Signing

평문 M을 서명하기 위해서 E_t는 다음 과정을 수행한다.

㉠ $P_M = H_3(ID_1, ..., ID_t, M) \in G_1$을 계산한다.

㉡ $Sig = S_t + s_t P_M$를 계산한다.

㉢ 다음과 같은 서명값 $S \in G_1^{t+1}$를 전송한다.

$$S = [Sig, Q_1, ..., Q_t] \qquad \text{(수식 2)}$$

여기서 $Q_i = s_i P_0$ $(1 \le i \le t)$

2.3.5 Verification

받은 서명값 $[Sig, Q_1, ..., Q_t]$을 다음계산을 통해 검증한다.

$$\hat{e}(P_0, Sig) = \hat{e}(Q_0, P_1)\,\hat{e}(Q_t, P_M) \prod_{i=2}^{t} \hat{e}(Q_{i-1}, P_i)$$

2.4 Shortening the Ciphertext

(수식 1)을 보면 암호문의 길이가 계층에서 수신자의 단계가 깊어짐에 따라 늘어난다는 것을 알 수 있으며, (수식 2)를 보면 서명 역시 늘어남을 알 수 있다. 이러한 단점을 보완하기 위해 C. Gentry와 A. Silverberg는 다음과 같은 방법을 제안했다.

2.4.1 Authenticated Lower-level Root PKGs

Entity E_y가 CSU라는 대학에 있는 사람에게 자주 메일을 보낸다고 가정하면, CSU를 authenticated lower-level root PKG로 여기고 CSU의 서명을 사용해서 암호문의 길이를 줄이는 방법이다. 이를 위해 root PKG는 추가적으로 임의의 평문 M^*를 parameter로 가진다. S_t를 secret point로 가지는 CSU는 authenticated root PKG의 setup과정으로 M^*에 서명한다.

다음과 같은 ID-tuple $(ID_1, ..., ID_t, ..., ID_z)$을 가지는 CSU의 E_z라는 entity에게 E_y는 CSU의 서명 $[Sig(= S_t + s_t P_{M^*}), Q_1, ..., Q_t]$에서 Sig와 Q_t를 사용해서 다음과 같이 암호문의 길이를 줄일 수 있다.

1) Encryption

㉠ $P_i = H_1(ID_1, ..., ID_i)$ $(t+1 \le i \le z)$를 계산한다.

㉡ 임의의 r을 Z_q에서 선택한다.

㉢ 다음과 같은 암호문을 전송한다.

$$C = [rP_0, rP_{t+1}, ..., rP_z, M \oplus H_2(g_t^r)]$$

여기서 $g_t = \dfrac{\hat{e}(P_0, Sig)}{\hat{e}(Q_t, P_{M^*})} = \hat{e}(P_0, S_t)$

2) Decryption

받은 암호문을 $C = [U_0, U_{t+1}, ..., U_z, V]$라고 하면, E_z는 다음과 같이 복호화한다.

$$V \oplus H_2\left(\frac{\hat{e}(U_0, S_z)}{\prod_{i=t+1}^{z} \hat{e}(Q_{i-1}, U_i)}\right) = M$$

Ⅲ. Our result

3.1 받은 서명의 활용방법(1)

Ⅱ장에서 보였던 것과 같이 HIDE의 가장 큰 문제점은 암호문의 길이가 (수식 1)처럼 수신자의 단계가 깊어짐에 따라 선형적으로 증가한다는 것이다. 이의 개선을 위해 2.4와 같은 방법을 사용하는데, 여기서는 받은 서명의 Sig와 Q_t만 사용했다. 그러나 나머지 유효한 Q_t들을 사용하면 $Level_t$ 보다 상위 단계에 있는 entity들에게 암호문을 일정한 길이로 보낼 수 있다.

송신자 Alice가 다음과 같은 ID-tuple $(ID_1, ..., ID_t)$을 가지는 entity E_t의 서명 $[Sig, Q_1, ..., Q_t]$을 얻었다면, HIDS의 검증과정을 통해 $Q_1, ..., Q_t$값이 유효하다는 것을 알 수 있다. 그러면 Alice는 $Level_t$보다 위의 $Level_v$ $(v < t)$에 있고 E_t와 동일한 Q_i $(1 \le i < v)$를 가지는 entity E_v와 다음과 같은 과정을 거쳐 암호화된 통신을 할 수 있다.

3.1.1 Encryption

㉠ 임의의 r을 Z_q에서 선택한다.

㉡ 다음과 같은 암호문을 전송한다.

$$C = [rP_0, M \oplus H_2(g_v^r)]$$

여기서 $g_v = \hat{e}(Q_0, P_1)\hat{e}(Q_1, P_2) \cdots \hat{e}(Q_{v-1}, P_v)$

3.1.2 Decryption

받은 암호문을 $C = [U, V]$라고 하면, E_v는 다음과 같이 복호화한다.

$$V \oplus H_2(\hat{e}(U, S_v)) = M$$

여기서

$$\begin{aligned}
&\hat{e}(U, S_v) \\
&= \hat{e}(rP_0, s_0P_1)\hat{e}(rP_0, s_1P_2) \cdots \hat{e}(rP_0, s_{v-1}P_v) \\
&= \hat{e}(s_0P_0, rP_1)\hat{e}(s_1P_0, rP_2) \cdots \hat{e}(s_{v-1}P_0, rP_v) \\
&= \hat{e}(Q_0, rP_1)\hat{e}(Q_1, rP_2) \cdots \hat{e}(Q_{v-1}, rP_v) \\
&= (\hat{e}(Q_0, P_1)\hat{e}(Q_1, P_2) \cdots \hat{e}(Q_{v-1}, P_v))^r \\
&= g_v^r
\end{aligned}$$

그러므로

$$V \oplus H_2(\hat{e}(U, S_v)) = M \oplus H_2(g_v^r) \oplus H_2(g_v^r) = M$$

따라서 secret point S_v를 가진 E_v는 $U = rP_0$만 알면 Alice가 계산한 g_v^r을 얻을 수 있게 된다. S_v나 r을 모르는 경우 g_v^r을 구하는 것은 BDH문제로 볼 수 있고 이는 어려운 문제로 알려져 있다.

〔표 1〕 서명을 받은 경우에 HIDE와의 비교

		받은 서명의 활용방법(I)	HIDE
암호문의 길이		$G_1 \times \{0,1\}^n$	$G_1^v \times \{0,1\}^n$
pairing 연산	Alice	v	1
	E_v	1	v

위와 같이 하면 암호문이 계층의 깊이에 따라 선형적으로 늘어나지 않고 $G_1 \times \{0,1\}^n$로 고정된다. 참고로 Alice는 v번의 pairing연산이 필요하고, E_v는 1번의 pairing연산이 필요하다. 그러나 HIDS의 검증과정에서 필요한 pairing연산을 하므로, Alice가 그 값들을 저장해 두고 있다면, Alice는 추가적인 pairing연산을 할 필요가 없다. 다만 E_t의 서명을 얻어야 하는데, 이는 선택사항으로 사전에 system parameter로 정한 임의의 M^*에 대한 서명을 요구함으로써 해결할 수 있다. 더 하위단계에 있는 entity의 서명을 얻을수록 위와 같은 암호문을 보낼 수 있는 경우는 많아진다. 이와 같은 경우는 실제 응용에서 흔히 발생할 수 있으므로 본 논문에서 제안한 방법은 실제적으로 유용하게 사용될 수 있다. 만약 이 경우 받은 서명을 활용하지 않고 HIDE를 사용한다면 서명의 길이는 $G_1^v \times \{0,1\}^n$가 된다.

3.2 받은 서명의 활용방법(II)

또한 암호문을 보내고자 하는 entity의 모든 Q_i들은 모르지만 알고 있는 Q_i들을 사용해서 보내는 암호문의 길이를 줄일 수 있다.

$Level_w$에 있으면서 E_t와 같은 ID_1, ..., ID_v를 가지고 다음과 같은 ID-tuple $(ID_1, ..., ID_v, ..., ID_w)$을 가지는 entity E_w가 있다고 하자. Alice는 유효한 Q_i $(1 \le i \le v,\ v < t)$들을 이미 가지고 있으므로 다음과 같은 과정을 거쳐 암호화된 통신을 할 수 있다.

3.2.1 Encryption

㉠ 임의의 r을 Z_q에서 선택한다.

㉡ 다음과 같은 암호문을 전송한다.

$$C = [rP_0, rP_{v+2}, ..., rP_w, M \oplus H_2(g_w^r)]$$

여기서 $g_w = \hat{e}(Q_0, P_1)\hat{e}(Q_1, P_2) \cdots \hat{e}(Q_v, P_{v+1})$

3.2.2 Decryption

받은 암호문을 $C = [U_0, U_{v+2}, ..., U_w, V]$라고 하면, E_w는 다음과 같이 복호화한다.

$$V \oplus H_2\left(\frac{\hat{e}(U_0, S_w)}{\prod_{i=v+2}^{w} \hat{e}(Q_{i-1}, U_i)}\right) = M$$

여기서

$$\hat{e}(U_0, S_w) = \hat{e}(rP_0, s_0P_1)\hat{e}(rP_0, s_1P_2) \cdots \hat{e}(rP_0, s_{w-1}P_w)$$

이고

$$\begin{aligned}
&\prod_{i=v+2}^{w} \hat{e}(Q_{i-1}, U_i) \\
&= \hat{e}(Q_{v+1}, U_{v+2})\hat{e}(Q_{v+2}, U_{v+3}) \cdots \hat{e}(Q_{w-1}, U_w) \\
&= \hat{e}(s_{v+1}P_0, rP_{v+2})\hat{e}(s_{v+2}P_0, rP_{v+3}) \cdots \\
&\quad \hat{e}(s_{w-1}P_0, rP_w) \\
&= \hat{e}(rP_0, s_{v+1}P_{v+2})\hat{e}(rP_0, s_{v+2}P_{v+3}) \cdots \\
&\quad \hat{e}(rP_0, s_{w-1}P_w)
\end{aligned}$$

이므로

$$\frac{\hat{e}(U_0, S_w)}{\prod_{i=v+2}^{w} \hat{e}(Q_{i-1}, U_i)}$$

$$= \hat{e}(rP_0, s_0P_1)\hat{e}(rP_0, s_1P_2) \cdots \hat{e}(rP_0, s_vP_{v+1})$$

$$= \hat{e}(s_0P_0, rP_1)\hat{e}(s_1P_0, rP_2) \cdots \hat{e}(s_vP_0, rP_{v+1})$$

$$= (\hat{e}(Q_0, P_1)\hat{e}(Q_1, P_2) \cdots \hat{e}(Q_v, P_{v+1}))^r$$

$$= g_w^r$$

그러므로

$$V \oplus H_2\left(\frac{\hat{e}(U_0, S_w)}{\prod_{i=v+2}^{w} \hat{e}(Q_{i-1}, U_i)}\right)$$

$$= M \oplus H_2(g_w^r) \oplus H_2(g_w^r) = M$$

위와 같이 하면 암호문의 길이가 서명을 활용하지 않고 HIDE를 사용했을 때의 $G_1^w \times \{0,1\}^n$에서 $G_1^{w-v} \times \{0,1\}^n$로 줄어들고, Alice는 $v+1$번, E_w는 $w-v$번의 pairing연산이 필요하다. 여기서도 Alice가 HIDS의 검증과정에서 필요한 값들을 저장해 두고 있다면, Alice는 추가적인 pairing연산을 할 필요가 없다.

〔표 2〕 서명을 받은 경우에 HIDE와의 비교

		받은 서명의 활용방법(II)	HIDE
암호문의 길이		$G_1^{w-v} \times \{0,1\}^n$	$G_1^w \times \{0,1\}^n$
pairing 연산	Alice	$v+1$	1
	E_w	$w-v$	w

Ⅳ. Conclusion

HIDE의 가장 큰 문제는 암호문의 길이가 수신자의 계층의 단계가 깊어짐에 따라 선형적으로 길어진다는 것이었다. 이 문제를 개선하기 위해 Authenticated lower-level root PKG와 같은 방법을 사용했는데, 기존에는 HIDS 서명의 Sig와 Q_i만 사용하여 그보다 하위 단계의 암호문 길이를 줄였다. 본 논문에서는 서명의 나머지 유효한 Q_i값들을 사용하여 상위 단계의 암호문을 일정하게 하는 방법과 암호문의 길이를 줄이는 방법을 제안하였다.

참 고 문 헌

[1] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology - Crypto '84, Lecture Notes in Computer Science 196, Springer-Verlag, pp.47~53, 1984.

[2] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing", Advances in Cryptology - Crypto 2001, Lecture Notes in Computer Science 2139, Springer-Verlag, pp.213~229, 2001.

[3] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography", Advances in Cryptology - Asiacrypt 2002, Lecture Notes in Computer Science 2501, Springer-Verlag, pp.548~566, 2002.

〈著者紹介〉

김 태 구 (Tae Gu Kim) 정회원
2000년 8월 : 연세대학교 전자공학과 졸업
2003년 2월 : 포항공과대학교 전자전기공학과 석사
2003년 2월~현재 : KT 기술본부 기술연구소
<관심분야> 전자공학, 통신공학, 정보보호

염 대 현 (Dae Hyun Yum)
1998년 2월 : 포항공과대학교 전자전기공학과 졸업
2000년 2월 : 포항공과대학교 전자전기공학과 석사
2000년 3월~현재 : 포항공과대학교 전자전기공학과 박사과정
<관심분야> 정보보호, 암호 프로토콜, 이동 네트워크

이 필 중 (Pil Joong Lee) 종신회원
1974년 2월 : 서울대학교 전자공학과 졸업
1977년 2월 : 서울대학교 전자공학과 석사 졸업
1982년 6월 : U.C.L.A. System Science, Engineer
1985년 6월 : U.C.L.A. Electrical Engineer, Ph.D.
1980년 6월~1985년 8월 : Jet Propulsion Laboratory, Senior Engineer
1985년 8월~1990년 2월 : Bell Communications Research, M.T.S
1990년 2월~현재 : 포항공과대학교 전자전기공학과, 교수
<관심분야> 정보보호, 암호이론, 암호 프로토콜