보안공학연구논문지 *Journal of Security Engineering*
Vol.12, No.6 (2015), pp.545-552
http://dx.doi.org/10.14257/jse.2015.12.01

키에스크로를 최소화한 계층적 아이디기반 암호

이병천1)

Hierarchical ID-based Encryption with Minimized Key Escrow

Byoungcheon Lee[1)]

요 약

아이디기반 암호는 사용자의 아이디, 이메일주소 등 공개될 수 있는 임의의 정보를 공개키로 사용하고 이와 쌍이 되는 개인키는 개인키생성기관(PKG)이 생성하여 사용자에게 전달하는 공개키암호 기법이다[1][2]. 이것은 키분배를 효율적으로 수행할 수 있는 장점이 있으나 사용자의 개인키가 개인키생성기관(PKG)에게 노출된다는 키에스크로 단점이 있다. 아이디기반 암호는 그 특성상 독립적인 인증도메인을 갖는 복수개의 PKG가 사용되는 경우에는 아이디기반 암호만으로 인증을 확장하는 것이 어렵다고 생각되어 왔으나 Gentry, Silverberg[3]는 다수의 PKG가 계층적 구조로 연결된 일반적인 경우에도 아이디기반 암호만으로 인증을 확장할 수 있는 계층적 아이디기반 암호기법을 제시하였으며 이 논문은 많은 관련 연구들의 시발점이 되었다. 그런데 이 기법은 키에스크로 특성에 있어서 사용자의 모든 조상 PKG들이 사용자의 개인키를 가지고 있지 않음에도 불구하고 사용자에게 전송되는 암호문을 복호화할 수 있다는 단점이 있는데 이것은 매우 바람직하지 않은 특성이다. 본 연구에서는 이 기법을 수정하여 개인키를 가지고 있는 사용자와 사용자에게 개인키를 발급한 단말 PKG만이 복호화 능력을 가질 수 있도록 키에스크로 특성을 최소화할 수 있는 계층적 아이디기반 암호 기법을 제시한다.

핵심어 : 계층적 아이디기반 암호, 키에스크로 최소화, 개인키생성기관

Abstract

Identity-based cryptography is a public key cryptosystem in which any arbitrary string such as identity, email address of user can be used as a public key and the corresponding private key is generated by a private key generator (PKG) and given to the user through a secure channel[1][2]. It has advantage in key distribution, but also has drawback of key escrow that PKG knows user's private key. If multiple PKGs with independent certification domain are used and users belong to different PKGs, it was considered that expanding certification using only ID-based cryptography is difficult between two users who belong to different PKG domains. Gentry and Silverberg[3] presented a hierarchical identity based cryptography which successfully expands certification among multiple PKGs structured in hierarchical manner, thus lots of extended researches followed from it [4-10]. But this scheme has a drawback that all ancestor PKGs of a user can decrypt any message sent to the user even though they do not have the private key of the user, which is very undesirable feature. In this paper we modify Gentry and Silverberg's hierarchical identity based encryption (HIBE) scheme and present a new HIBE scheme which minimize the key escrow property

접수일(2015년10월27일), 심사의뢰일(2015년10월28일), 심사완료일(1차:2015년11월02일, 2차:2015년11월28일)
게재확정일(2015년12월07일), 게재일(2015년12월31일)

[1]312-702 충청남도 금산군 추부면 마전리 중부대학교 정보보호학과.
email: sultan@jbm.ac.kr

ISSN: 1738-7531 JSE

that only user and the end PKG who issued private key to the user can decrypt message.

Keywords : hierarchical identity based encryption (HIBE), minimized key escrow, private key generator

1. 서론

아이디기반 암호는 1984년 A. Shamir에 의해 제안된 암호기법으로서 사용자의 아이디, 이메일주소 등 공개될 수 있는 임의의 정보를 공개키로 사용할 수 있도록 하는 암호기법이다. 2001년 Boneh와 Franklin에 의해 실용적인 아이디기반 암호기법이 제시되었는데[2] 이 방법은 기존의 인증서 등 공개키기반구조(Public Key Infrastructure, PKI)를 사용하지 않고 키분배를 효율적으로 수행할 수 있다는 장점이 있어서 많은 연구가 이어지는 시발점이 되었다. 그런데 아이디기반 암호에서는 공개키와 쌍이 되는 개인키는 개인키생성기관(Private Key Generator, PKG)이 생성하여 사용자에게 안전하게 전달해 주어야 한다. 그러므로 PKG는 사용자의 개인키를 알게 된다는 키에스크로(Key Escrow) 특성을 가져서 사용자가 PKG를 절대적으로 신뢰할 수 있는 환경에서만 사용할 수 있으며 개인키를 사용자에게 안전하게 전달하기 위해서는 PKG와 사용자간에 안전한 비밀채널(secure channel)이 필요하게 된다는 단점이 있다. 그러므로 아이디기반 암호는 주로 신뢰도가 높은 폐쇄된 영역에서 활용될 것으로 예상된다.

아이디기반 암호는 하나의 PKG와 그 인증영역에 속한 사용자들 간에는 키분배가 간단한 장점이 있지만 그 특성상 여러개의 PKG가 서로 다른 인증영역을 가지고 활동하게 되는 환경에서는 다른 PKG 영역에 속한 사용자들과의 인증을 확인하기 위해서는 아이디기반 암호만으로 구현하는 것이 쉽지 않고 인증서기반 암호를 함께 사용하는 것이 필요하다고 생각되었다. 그런데 Gentry와 Silverberg[3]는 다수의 PKG가 계층적 구조로 연결된 일반적인 경우에도 아이디기반 암호만으로 신뢰를 확장할 수 있는 계층적 아이디 기반 암호(Hierarchical ID-based Encryption, HIBE) 기법을 제안하였으며 이 논문은 많은 관련 연구[4-10]의 시발점이 되었다.

그런데 Gentry와 Silverberg의 HIBE 기법은 키에스크로 특성에 있어서 사용자에게 개인키를 발급한 단말 PKG 뿐만 아니라 그 상위 레벨의 모든 조상 PKG들이 사용자의 개인키를 가지고 있지 않음에도 불구하고 사용자에게 전송되는 암호문을 복호화할 수 있다는 특성을 가지고 있는데 이것은 실제 환경에서 매우 바람직하지 않은 특성이다. 예를 들면 사장→이사→부장→과장→사원 등과 같이 직급별로 엄격한 계층구조를 갖는 조직내에서 상급자가 직속 부하에게 아이디기반 암호의 개인키를 발급하여 사용한다고 가정하면 사장은 이사에게 개인키를 발급하고, 이사는 부장에게, 부장은 과장에게, 과장은 사원에게 개인키를 발급하게 될 것이다. 과장은 사원에게 개인키를 발급해주었고 그것을 알고 있으므로 사원에게 전달된 암호문을 복호화해 볼 수 있고 심지어는 사원의 이름으로 서명문을 생성할 수도 있을 것이지만, 사장은 사원의 암호키를 모르므로 이러한 일을 할 수 없어야 할 것이다. 그런데 Gentry와 Silverberg의 HIBE 기법은 사원의 모든 상급자가 사원에게 전달되는 암호문을 복호화해볼 수 있는 기능을 가지게 되어 있다. 이것은 계층적 인증구조를 가지는

조직에서 키관리 권한을 분산하지 않고 중앙집중적으로 키관리를 하여 하급자의 모든 행동들을 모든 상급자들이 지켜보고 있는 것과 같아서 역할의 위임과 책임성이라는 측면에서 적절치 않다고 생각된다.

이 논문에서는 Gentry와 Silverberg의 HIBE 기법을 약간 수정하여 개인키를 가지고 있는 사용자와 사용자에게 개인키를 발급한 단말 PKG만이 복호화 능력을 가질 수 있도록 키에스크로 특성을 최소화한 계층적 아이디기반 암호 기법을 제시한다.

2. Gentry와 Silverberg의 HIBE 기법

여기에서는 Gentry와 Silverberg의 HIBE 기법에 대해 간단히 소개하고 이것의 키에스크로 문제점을 제시한다.

2.1 Gentry와 Silverberg의 HIBE 기법

이 논문에서는 복수의 PKG들이 계층적 인증구조를 가지고 있는 경우를 고려한다. 사용자는 $(ID_1, ID_2, \ldots, ID_t)$와 같이 아이디 튜플로 표시되는데 이것은 사용자의 아이디가 ID_t이며 사용자에게 개인키를 발행하는 단말 PKG는 ID_{t-1}이고 그 상위에 루트 PKG로부터 단말 PKG까지 $(ID_1, ID_2, \ldots, ID_{t-1})$의 계층적 레벨 구조를 가지고 있다는 것을 의미한다.

이 HIBE 기법의 안전성은 겹선형디피헬만(Bilinear Diffie-Hellman) 문제에 의존한다. G_1, G_2는 큰 소수 q를 위수로 가지는 순환군이며 각각 덧셈군, 곱셈군으로 표기한다. $e : G_1 \times G_1 \rightarrow G_2$는 겹선형사상을 나타내며 Weil pairing, Tate pairing 등으로부터 구성할 수 있다. $Level_i$를 계층구조에서 i번째 레벨을 가지는 객체들의 집합이라고 표시하자. 이때 $Level_0 = \{\text{루트}PKG\}$이다.

HIBE 기법은 다음과 같이 루트 PKG 설정, 나머지 PKG 설정, 개인키 생성, 암호화, 복호화 등의 알고리즘으로 구성된다.

2.1.1 루트 PKG 설정

큰 소수 q를 위수로 가지는 두 개의 순환군 G_1, G_2를 생성하고 겹선형사상 $e : G_1 \times G_1 \rightarrow G_2$를 생성한다.

임의의 생성자 $P_0 \in G_1$를 선택한다.

난수 $s_0 \in Z_q^*$를 선택하고 $Q_0 = s_0 P_0$를 계산한다.

두 개의 안전한 해쉬함수 $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : G_2 \rightarrow \{0,1\}^n$를 선택한다. 여기서 n은 암호화할 평문공간의 길이를 나타낸다.

루트 PKG는 s_0를 마스터키로 안전하게 저장하고 $param = (G_1, G_2, e, P_0, Q_0, H_1, H_2)$를 시스템

파라메터로 공개한다.

2.1.2 나머지 PKG 설정

루트 PKG 이외의 아이디 $(ID_1, ID_2, ..., ID_{t-1})$를 가지는 나머지 PKG들은 난수 $s_i \in Z_q^*$ $(i = 1, ..., t-1)$를 선택하고 안전하게 저장한다.

2.1.3 개인키 생성 (Extraction)

객체 E_t는 $Level_t$의 객체로서 $(ID_1, ID_2, ..., ID_t)$의 아이디 튜플을 가지고 있다고 하자. 이때 $(ID_1, ID_2, ..., ID_i)$ $(\text{for } 1 \le i < t)$는 $Level_i$의 조상 PKG를 나타내는 아이디 튜플이다. S_0는 G_1 순환군의 항등원이라고 하자. 객체 E_t의 부모 PKG E_{t-1}는 다음을 계산한다.

$P_t = H_1(ID_1, ..., ID_t) \in G_1$를 계산한다.

$S_t = S_{t-1} + s_{t-1}P_t = \sum_{i=1}^{t} s_{i-1}P_i$를 계산한다. 이것은 객체 E_t를 위한 비밀값으로 G_1군 위의 점이다. 여기서 S_{t-1}은 PKG E_{t-1}이 부모 PKG E_{t-2}로부터 발급받은 비밀값이다.

$Q_{t-1} = s_{t-1}P_0$ 를 계산한다.

부모 PKG E_{t-1}은 객체 E_t에게 $(S_t, Q_0, ..., Q_{t-1})$을 전달한다.

2.1.4 암호화

아이디 튜플 $(ID_1, ID_2, ..., ID_t)$을 가지는 수신자 E_t에게 메시지 M을 암호화하여 전달한다고 하자. 송신자는 다음을 계산한다.

$P_i = H_1(ID_1, ID_2, ..., ID_i) \in G_1 \text{ for } 1 \le i \le t$

난수 $r \in Z_q^*$을 선택하고 암호문을 다음과 같이 계산한다.

$C = [rP_0, rP_2, ..., rP_t, M \oplus H_2(g^r)]$

여기서 $g = e(Q_0, P_1) \in G_2$이다.

2.1.5 복호화

아이디 튜플 $(ID_1, ID_2, ..., ID_t)$을 가지는 수신자 E_t는 개인키 S_t와 조상 PKG들의 공개키 $(Q_0, ..., Q_{t-1})$를 가지고 있다. 수신한 암호문 $C = [U_0, U_2, ..., U_t, V]$를 복호화하기 위해서는 다음을 계산한다.

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

여기서 복호화되는 과정을 살펴보면

$$e(U_0, S_t) = e(rP_0, s_0P_1 + s_1P_2 + ... + s_{t-1}P_t)$$
$$= e(s_0P_0, rP_1)e(s_1P_0, rP_2)...e(s_{t-1}P_0, rP_t)$$
$$= e(Q_0, P_1)^r e(Q_1, U_2)...e(Q_{t-1}, U_t)$$

가 되어 해쉬함수 H_2의 입력값이 g^r과 동일해지는 것을 알 수 있다.

2.2 HIBE 기법의 키에스크로 문제점

위에서 제시한 HIBE 기법은 개인키 S_t를 가지고 있는 정당한 사용자 E_t와 이것을 발급한 단말 PKG E_{t-1}뿐만 아니라 모든 조상 PKG들도 복호화 가능하다는 문제점이 있다. 예를 들어 사용자 E_t의 조상 PKG인 $E_s\,(s < t-1)$는

$$V \oplus H_2(\frac{e(U_0, S_s)}{\prod_{i=2}^{s} e(Q_{i-1}, U_i)}) \Rightarrow M$$

와 같이 복호화 할 수 있으며 루트 PKG는 $V \oplus H_2(e(U_0, S_1)) \Rightarrow M$과 같이 복호화 할 수 있다. 이것이 가능한 이유는 암호화에 사용되는 $g = e(Q_0, P_1) \in G_2$ 값이 조상 PKG 누구나 계산할 수 있는 형태이기 때문이다.

이와 같이 사용자의 모든 조상 PKG들이 사용자의 모든 암호화된 메시지들을 복호화할 수 있다는 것은 매우 바람직하지 않으며 계층화된 인증구조에서 키관리 권한을 분산하지 않고 중앙집중적으로 키관리를 하는 것과 같다.

3. 키에스크로를 최소화하는 HIBE 기법

우리는 HIBE 기법의 키에스크로 특성을 최소화하여 개인키 S_t를 가지고 있는 정당한 사용자 E_t와 이것을 발급한 단말 PKG E_{t-1}만이 복호화할 수 있도록 수정하고자 한다. 위에서 보인 것처럼 암호화에 사용하는 g값을 $g = e(Q_0, P_1) \in G_2$와 같이 계산하여 사용하면 상위의 모든 조상 PKG들이 계산할 수 있게 되므로 이것을 $g = e(Q_{t-1}, P_t) \in G_2$와 같이 수정하면 사용자와 단말 PKG만이 복호화할 수 있게 된다. 제안된 방법에서 루트 PKG 설정, 나머지 PKG 설정, 개인키 생

성의 과정은 Gentry와 Silverberg의 HIBE 기법과 동일하다.

(1) 루트 PKG 설정 : 동일

(2) 나머지 PKG 설정 : 동일

(3) 개인키 생성 : 동일

(4) 암호화

아이디 튜플 $(ID_1, ID_2, ..., ID_t)$을 가지는 수신자 E_t에게 메시지 M을 암호화하여 전달한다고 하자. 송신자는 다음을 계산한다.

$P_i = H_1(ID_1, ID_2, ..., ID_i) \in G_1 \text{ for } 1 \le i \le t$

난수 $r \in Z_q^*$을 선택하고 암호문을 다음과 같이 계산한다.

$C = [rP_0, rP_1, rP_2, ..., rP_{t-1}, M \oplus H_2(g^r)]$

여기서 $g = e(Q_{t-1}, P_t) \in G_2$이다.

(5) 복호화

아이디 튜플 $(ID_1, ID_2, ..., ID_t)$을 가지는 수신자 E_t는 개인키 S_t와 조상 PKG들의 공개키 $(Q_0, ..., Q_{t-1})$를 가지고 있다. 수신한 암호문 $C = [U_0, U_1, U_2, ..., U_{t-1}, V]$를 복호화하기 위해서는 다음을 계산한다.

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

여기서 복호화되는 과정을 살펴보면

$$\begin{aligned} & e(U_0, S_t) = e(rP_0, s_0P_1 + s_1P_2 + ... + s_{t-1}P_t) \\ & = e(s_0P_0, rP_1)e(s_1P_0, rP_2)...e(s_{t-2}P_0, rP_{t-1})e(s_{t-1}P_0, P_t)^r \\ & = e(Q_0, U_1)e(Q_1, U_2)...e(Q_{t-2}, U_{t-1})e(Q_{t-1}, P_t)^r \end{aligned}$$

가 되어 해쉬함수 H_2의 입력값이 g^r과 동일해지는 것을 알 수 있다.

이렇게 수정된 HIBE 기법에서는 암호화에서 사용되는 $g^r = e(Q_{t-1}, P_t)^r \in G_2$ 값은 개인키 S_t

를 알고 있는 수신자 E_t와 단말 PKG E_{t-1} 만이 계산할 수 있으며 사용자 E_t의 조상 PKG인 $E_s\,(s < t-1)$는 복호화를 수행할 수 없게 된다.

4. 결론

이 논문에서는 Gentry와 Silverberg의 HIBE 기법에서 모든 조상 PKG들이 사용자에게 전달되는 암호화된 메시지를 복호화할 수 있는 과도한 키에스크로 기능을 가지게 되는 문제점이 있다는 것을 지적하였다. 이를 해결하기 위하여 암호화/복호화 알고리즘을 수정한 기법을 제시하였으며 그 결과 제안된 방식에서는 개인키 S_t를 알고 있는 수신자 E_t와 단말 PKG E_{t-1} 만이 복호화 계산을 수행할 수 있게 되었다.

이와 같이 HIBE 기법의 키에스크로 문제를 해결함으로써 복수의 PKG들이 계층적으로 활용되는 대규모 네트워크에서도 키관리 권한을 분산하는 방식으로 ID기반 암호를 안전하게 활용할 수 있는 기반이 마련되었다고 볼 수 있다.

References

[1] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, Advances in Cryptology - CRYPTO '84 (1985), LNCS 196, pp. 47-53.

[2] D. Boneh and M. Franklin, Identity based encryption from the Weil pairing, Advances in Cryptology – Crypto 2001 (2001), LNCS 2139, Springer, pages 213-229.

[3] C. Gentry and A. Silverberg, Hierarchical ID-based Cryptography, Advances in Cryptology - Asiacrypt 2002 (2002), LNCS 2501, pages 548–66.

[4] J. Horwitz and B. Lynn, Toward Hierarchical Identity-Based Encryption, Advances in Cryptology - EUROCRYPT 2002 (2002), LNCS 2332, pp. 466–481.

[5] D. Boneh, X. Boyen, E. Goh, Hierarchical Identity Based Encryption with Constant Size Ciphertext, Advances in Cryptology – Eurocrypt 2005 (2005), LNCS 3494, pp. 440-456.

[6] X. Boyen and B. Waters, Anonymous Hierarchical Identity-Based Encryption (Without Random Oracle), Advances in Cryptology – Crypto 2006 (2006), LNCS 4117, pp. 290-307.

[7] M. Abdalla, E. Kiltz, and G. Neven, Generalized Key Delegation for Hierarchical Identity-Based Encryption, Computer Security – ESORICS 2007 (2007), LNCS 4734, pp. 139-154.

[8] C. Gentry and S. Halevi, Hierarchical Identity Based Encryption with Polynomially Many Levels, 6th Theory of Cryptography Conference, TCC 2009 (2009), LNCS 5444, pp. 437-456.

[9] J. H. Seo, T. Kobayashi, M. Ohkubo, and K. Suzuki, Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts, Public Key Cryptography – PKC 2009 (2009), LNCS 5443, pp. 215-234.

[10] Man Ho Au, Joseph K. Liu, Tsz Hon Yuen, and Duncan S. Wong, Practical Hierarchical Identity Based Encryption and Signature schemes Without Random Oracles, https://eprint.iacr.org/2006/368.pdf (2006).

Author

이병천 (Byoungcheon Lee)

1986년 2월 : 서울대학교 물리학과 학사
1988년 2월 : 서울대학교 물리학과 석사
2002년 2월 : KAIST 정보보호 박사
2002년 3월 ~ 현재 : 중부대학교 정보보호학과 교수
관심분야 : 암호 프로토콜, 네트워크 보안, 인증