지정된 검증자 서명기법의 비전가성+

*구영주 **천지영 ***최규영 ****이동훈

고려대학교, 정보경영공학전문대학원

*danmiluv@naver.com **jychun@korea.ac.kr ***young@cist.korea.ac.kr ****donghlee@korea.ac.kr

Delegation Attack on previous Designated Verifier Signature schemes

*Goo, Young Ju **Chun, Ji Young ***Choi, Kyu Young ****Lee, Dong Hoon

Graduate School of Information Management and Security CIST, Korea University

요약

최근 ICALP 2005에서 Lipmaa 등은 지정된 검증자 서명기법에서의 새로운 안전성 개념인 비전가성을 정의하였다. 지정된 검증자 서명기법(Designated Verifier Signature, DVS)이란 지정된 검증자만이 서명의 정당성을 검증할 수 있는 서명으로 제 삼자가 서명을 보고 서명자와 검증자 중에 누가 실제 서명자인지 알 수 없다는 특징이 있다. 그러나 Lipmaa 등이 제시한 '비전가성'을 만족하지 않은 지정된 검증자 서명기법의 경우, 서명자 또는 검증자가 개인키가 아닌 일부정보를 제 삼자에게 주어 정당한 서명을 만들어내는 것이 가능하다. 이러한 전가성은 전자투표나 컨텐츠 등에 있어서 심각한 문제이다. 본 논문에서는 2006년 Huang 등의 기법과 2007년 Zhang 등이 제안한 기법이 전가성에 안전하지 않음을 보인다.

1. 서론

지정된 검증자 서명 기법(DVS)은 1996년 Jakobsson [2] 등이 제안하였다. 지정된 검증자 서명 기법은 서명자가 검증자를 지정하고 서명하기 때문에 검증자 이외에는 서명을 검증해 볼 수 없으며 제 3자는 서명이 서명자로부터 나온 것인지 검증자로부터 생성된 것인지 확신할 수 없다. 검증자 또한 서명자가 생성한 서명과 구별 불가능한 서명을 생성할 능력이 있기 때문이다. 이러한 특징은 서명자의 프라이버시를 보호하고 따라서 전자 투표나 옥션, 전자 경매 등에 유용하게 쓰일 수 있다.

일반적으로 지정된 검증자 서명기법은 반드시 서명자와 검증자 이외에는 서명을 생성할 수 없어야 한다. 위조 불가능은 서명이 반드시 만족해야할 기본적인 안전성이다. 또한 지정된 검증자 서명 기법의 가장 큰 특징으로 서명자와 검증자 중 누가 실제로 서명을 생성하였는지 구분할 수 없어야 하는데, 이러한 source hiding의 안전성을 만족해야 한다. 2005년 Lipmaa[4] 등은 이러한 기본적인 안전성외에 지정된 검증자 서명기법이 갖춰야할 새로운 안전성에 대하여 정의하였다. Lipmaa등은 비전가성(non-delegatability)이라는 안전성 원칙을 제시하고 [JSI96, SKM03, SBWP03, SWP04, LV04]등의 지정된 검증자 서명기법이 전가성을 가진다는 것을 보였다. 전가성이란 서명자 또는 검증자가 자신의 비밀키를 노출하지 않고도 제 3자에게 약간의 정보를 줌으로써 제 3자가 정당한 서명을 생성할 수 있게 하는 것을 말한다. 비전가성을 만족하지 않는 DVS기법은, DVS기법이 적용되는 전자투표나 공개입찰, 옥션, 컨텐츠 이용 등에 심각한 문제를 야기할 수 있다. 전자투표의 경우, 서명자는 자신의 비밀키가 아닌 어떠한 정보를 제 3자에게 줌으로써 제 3자에게 자신의 투표 권리를 이행하도록 할 수 있으며, 컨텐츠 이용에서의 경우, 제 3자는 돈을 지불하지 않고도 서명자로부터 약간의 정보를 받음으로써 서명자가 유료로 이용하는 컨텐츠를 무료로 이용할 수 있게 된다. 따라서 비전가성은 지정된 검증자 서명에서 심각하게 고려되어야할 사항이다. 2005년 Li 등[3]은 [SKM03, SBWP03, SWP04, LV04a] 등의 4개의 지정된 검증자 서명기법이 전가 공격에 안전하지 않음을 보였다.

본 논문에서는 2006년 Huang 등이 제시한 Short Strong Designated Verifier Signature Schemes[1] 과 2007년 Zhang 등이 제시한 novel ID-based designated verifier signature scheme[5]이 전가 공격에 안전하지 않음을 보이겠다. 2장에서는 Huang 등의 short strong DVS기법과 Zhang 등의 의 ID 기반의 DVS기법에 대하여 소개하고 3장에서는 이들 기법이 전가 공격에 안전하지 않음을 보이겠다. 4장에서는 결론을 맺는다.

2. 제안된 DVS 기법

이 장에서는 Huang 등이 제안한 Short ID-Based SDVS(Short ID-Based Strong Designated Verifier Signature)[1]과 2007년 Zhang 등이 제안한 ID-based DVS기법[5]을 분석한다.

가. Huang 등의 Short ID-Based SDVS 기법

-Setup : KGC는 다음과 같이 시스템 파라미터와 master-key를 생성한다.

- $(G_1,+),(G_T,\bullet)$는 소수 $q(q \geq 2^l)$를 위수로 갖는 두 그룹이

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

고 e는 admissible bilinear map일 때 $\hat{e}: G_1 \times G_1 \rightarrow G_M$이다.

- 랜덤한 s∈Z_q^*를 고르고 G_1의 생성원 P를 선택하여 P_{pub} = sP를 계산한다. s는 마스터키로 공개되지 않는다.
- 암호학적 일방향 해쉬함수 $H_0 : \{0,1\}^* \rightarrow G_1$, $H_1 : \{0,1\}^* \rightarrow Z_q^*$를 생성한다. 시스템 파라미터는 params ={e, G_1, G_T, q, P, P_{pub}, H_0 ,H_0}이다.
- 각 사용자는 자신의 아이디, ID_i를 가지며 사용자의 공개키는 $Q_{ID} = H_0(ID)$와같이 계산하고 개인키는 $S_{ID} = sQ_{ID}$로 계산한다.

-Sign : 서명자를 A, 검증자를 B라 가정할 때, A는 먼저 자신의 개인키를 이용하여 $k = \hat{e}(Q_{ID_B}, S_{ID_A})$를 계산하고, 메시지 m에 대한 서명을 다음과 같이 생성한다.

$$\sigma = H_1(m,k)$$

-Verify : 수신자 B는 메시지 m에 대한 서명의 정당성을 다음과 같이 검증한다.

$$H_1(m, \hat{e}(Q_{ID_B}, S_{ID_B})) = \sigma \quad ?$$

등호가 성립한다면 accept를, 그렇지 않다면 reject를 출력한다.

-Transcript Simulation : 지정된 검증자 B는 A가 생성한 서명과 구별 불가능한 서명을 스스로 생성할 수 있어야 한다. 먼저 자신의 개인키를 이용하여 $k' = \hat{e}(Q_{ID_A}, S_{ID_B})$을 계산 후 구별 불가능한 서명을 다음과 같이 생성한다.

$$\sigma' = H_1(m,k)$$

B에 의해 생성된 메시지 m에 대한 서명 σ'은 A가 생성한 원래의 서명과 구별 불가능하다.

-Correctness :

$$\sigma = H_1(m, \hat{e}(Q_{ID_B}, S_{ID_A})) = H_1(m, \hat{e}(Q_{ID_B}, sQ_{ID_A}))$$
$$= H_1(m, \hat{e}(S_{ID_B}, Q_{ID_A})) = \sigma'$$

나. Zhang 등의 ID-Based DVS 기법

Zhang 등은[5] Correctness, Unforgeability, Source hiding, Non- delegatability 성질들을 만족하는 ID-Based DVS기법을 제안하였다. 그러나 실제로 Zhang 등의 기법은 전가 공격에 안전하지 않다. 이를 보임에 앞서 Zhang 등의 기법에 대하여 분석하고 Zhang의 기법이 전가 공격에 안전하지 않음을 3장에서 보이겠다.

-Setup : KGC는 다음과 같이 시스템 파라미터와 master-key를 생성한다.

- $(G_1, +), (G_T, \bullet)$는 소수 $q(q \geq 2^l)$를 위수로 갖는 두 그룹이고 e는 admissible bilinear map일 때 $\hat{e}: G_1 \times G_1 \rightarrow G_M$이다.
- 랜덤한 s∈Z_q^*를 고르고 G_1의 생성원 P를 선택하여 P_{pub} = sP를 계산한다. s는 마스터키로 공개되지 않는다.
- 암호학적 일방향 해쉬함수 $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \times G_1 \times G_1 \rightarrow G_1$를 생성한다. 시스템 파라미터는 params ={e, G_1, G_2, q, P, P_{pub}, H_1 ,H_2}이다.

-KeyExtract : 주어진 ID에 대하여 공개키는 $Q_{ID} = H_0(ID)$와 같이 계산하고 개인키는 $S_{ID} = sQ_{ID}$로 계산한다.

-Sign : 서명자 A는 메시지 m에 관하여 지정된 검증자 B에 대한 서명을 다음과 같이 생성한다. 랜덤한 두 수 $r_1, r_2 \in Z_q^*$를 선택하고

$$U_1 = r_1 Q_{ID_B}$$
$$U_2 = r_1 r_2 Q_{ID_B}$$
$$H = H_2(m, U_1, U_2)$$
$$V = r_2 H + r_1^{-1} S_{ID_A}$$

를 계산한다. 메시지 m에 대하여 지정된 검증자 B에 대한 A의 서명은 (U_1, U_2, V)이다.

-Verify : 지정된 검증자 B는 먼저 $H = H_2(M, U_1, U_2)$를 계산하고 $e(U_1, V) = e(U_2, H)e(S_{ID_B}, Q_{ID_A})$?를 체크한다. 등호가 성립한다면 accept를 그렇지 않다면 reject를 출력한다.

-Transcript simulation : B는 원래의 서명과 구별 불가능한 서명을 생성하기 위하여 먼저 랜덤한 $r_1', r_2' \in Z_q^*$를 뽑고 다음과 같이 구별 불가능한 서명을 생성한다.

$$U_1' = r_1' Q_{ID_B}$$
$$U_2' = r_1' r_2' Q_{ID_B}$$
$$H' = H_2(M, U_1', U_2')$$
$$V' = r_2' H' + r_1'^{-1} S_{ID_A}$$

B가 생성한 서명 (U_1', U_2', V')는 정당하게 검증을 통과한다. 따라서 제 삼자는 B가 생성한 것과 A가 생성한 서명을 구별할 수 없다.

3. 제안된 DVS 기법의 전가성

이 장에서는 앞에서 살펴본 Huang 등과 Zhang 등의 DVS기법의 전가안전성에 대하여 분석한다. 비전가성(Non-delegatability)이란 서명자 또는 검증자가 자신의 비밀키를 제외한 어떠한 정보를 제 3자에게 주더라도, 지정된 검증자에 대하여 정당한 서명을 생성할 수 없는 것을 말한다. 이러한 성질은 2005년 Lipmaa 등[4]에 의해 정의된 것으로 DVS기법에 있어서 고려되어야 할 중요한 안전성이다. 전가 공격에 대하여 기법이 안전하지 않다면 서명자 또는 검증자가 지정된 검증자에 대하여 자신의 서명 생성 능력을 다른 이에게 위임하는 것이 가능해 짐으로써 심각한 문제를 유발할 수 있다.

가. Huang 등의 기법에 대한 전가 공격

Huang등의 기법에서는 서명자 A와 지정된 검증자 B가 자신의 개인키와 상대방의 공개키를 이용해 같은 $k = \hat{e}(Q_{ID_B}, S_{ID_A}) = \hat{e}(S_{ID_B}, Q_{ID_A}) = k'$를 계산함으로써 서명과 구별 불가능한 transcript를 생성한다. 따라서 서명자 또는 지정된 검증자가 랜덤한 $r \in Z_q^*$에 대하여,

$$T_1 = rS_{ID_A} (\text{or } rS_{ID_B}),\ T_2 = r^{-1} H_1(ID_B) (\text{or } r^{-1} H_1(ID_A))$$

의 정보를 제 3자에게 주게 되면 제 3자는 지정된 검증자 B에 대한 A의 서명을 다음과 같이 생성할 수 있다.

$$\sigma = H_1(m, \hat{e}(T_1, T_2))$$

A 또는 B가 주는 정보로는 제 3자가 개인키를 얻는 것은 Discrete Logarithm 문제를 푸는 것과 같으므로 제 3자가 개인키를 알아낼 가능성은 없다.

나. Zhang 등의 기법에 대한 전가 공격

Zhang 등은 제안한 기법이 비전가성을 가짐을 증명하였으나 제안된 기법은 전가 공격에 안전하지 않다. 이는 다음과 같이 보일 수 있다. 서명자 A 또는 지정된 검증자 B가 제 3자에게 (T_1, T_2)의 정보를 다음과 같이 주게 되면,

$$T_1 = r^{-1}H_1(ID_B)(\text{or } r^{-1}H_1(ID_A)),\ T_2 = rS_{ID_A}(\text{or } rS_{ID_B})$$

이를 이용하여 제 3자는 서명자 A와 지정된 검증자 B에 대한 정당한 서명을 만들어 낼 수 있다. 제 3자는 랜덤한 두 수 $s_1, s_2 \in Z_q^*$를 선택하고 아래와 같이 계산한다.

$$\begin{aligned} U_1 &= s_1 T_1 \\ U_2 &= s_1 s_2 T_2 \\ H &= H_2(m, U_1, U_2) \\ V &= s_2 H + s_1^{-1} T_2 \end{aligned}$$

이때 서명은 (U_1, U_2, V)가 되며 메시지 m에 대하여 제 3자가 생성한 서명은 정당하다.

$$\begin{aligned} e(U_1, V) &= e(s_1 T_1, s_2 H) e(s_1 T_1, s_1^{-1} T_2) \\ &= e(U_2, H) e(T_1, T_2) \\ &= e(U_2, H) e(S_{ID_B}, Q_{ID_A}) \end{aligned}$$

따라서 제 3자는 서명자 또는 검증자의 개인키를 모르고도 주어진 정보를 가지고 정당한 서명을 만들 수 있게 된다.

4. 결론

본 논문에서는 지정된 검증자 기법에서의 새로운 안전성 성질인 비전가성에 대하여 알아보고 이전의 두 기법이 전가 공격에 안전하지 않음을 보였다. 지정된 검증자 기법은 지정된 자만이 검증 가능하고 제 3자가 실제 서명자가 누구인지 구별 할 수 없는 성질을 가지기 때문에 서명자에 대한 프라이버시를 보장한다. 이러한 특성은 전자투표나 공개입찰, 옥션 등에 활용될 수 있다. 그러나 지정된 검증자 기법이 전가성을 지닐 경우 서명자 또는 검증자가 개인키를 드러내지 않고도 지정된 검증자에 대하여 자신의 서명 권리를 다른 이에게 위임할 수 있으므로 전자투표나 입찰등에 있어서 심각한 문제를 일으킬 수 있으므로 전가성에 대한 안전성의 고려가 필요하다. 기존의 ID 기반의 지정된 검증자 서명기법은 대부분이 전가 공격에 안전하지 않다. 따라서 비전가성을 만족하는 지정된 검증자 기법에 관한 연구가 더욱 필요할 것이다.

5. 참고문헌

[1] X.Huang, W. Susilo, Y. Mu, and F. Zhang, Short(Identity-Based) Strong Designated Verifier Signature Schemes, ISPEC 2006, LNCS 3903,pp. 214-225, Springer-Verlag, 2006.

[2] M.Jakobsson,K.Sako,R.Impagliazzo,Designated verifier proofs and their applications, in : Advances in Cryptology-Eurocrypt96, LNCS,vol.1070,Springer-Verlag,1996,pp.143-154

[3] Y. Li, H. Lipmaa, and D. Pei, On Delegatability of Four Designated Verifier Signatures, ICICS 2005, LNCS 3783,p. 61-71, Springer-Verlag, 2005.

[4] H. Lipmaa, G. Wang and F. Bao, Designated verifier signature schemes: attacks, new security notions and a new construction, in: ICAP 2005, LNCS, vol. 3580,Springer-Verlag, 2004, pp. 459-471

[5] J.Zhang, J. Mao, A novel ID-based designated verifier signature scheme, Information Sciences 178 (2008) 766-773