몇가지 쌍짓기를 리용하는 무증명서쌍방인증열쇠합의규약에 대한 안전성분석

김영진, 김선경, 오충일

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《과학자, 기술자들은 현실에 튼튼히 발을 붙이고 사회주의건설의 실천이 제기하는 문제들을 연구대상으로 삼고 과학연구사업을 진행하여야 하며 연구성과를 생산에 도입하는데서 나서는 과학기술적문제들을 책임적으로 풀어야 합니다.》(《**김정일**선집》 증보판 제15권 492페지)

우리는 통신의 보안을 실현하는데서 중요한 의의를 가지는 두가지 무증명서쌍방인증열쇠합의(Cerfificatless Two-Party Authenticated Key Agreement, 략칭 CTAKA)규약에 대한 안전성분석을 진행하였다. CTAKA규약은 쌍짓기를 리용하는 규약과 리용하지 않는것이 있다. 쌍짓기에 기초한 CTAKA규약은 쌍짓기의 계산량이 많은것으로 하여 쌍짓기의 개수를 줄이는 방향으로 연구사업이 진행되고있으며 가장 최근의 연구결과는 XWZX-CTAKA와 L-CTAKA규약이다.

론문에서는 이 두가지 규약들에 대한 안전성을 분석하고 이 규약들이 내부적수의 중간침입공격에 불안전하다는것을 증명하였다.

1. 선행연구결과

CTAKA규약에서 통신에 참가하는 매 사용자는 자기의 세가지 비밀값 즉 부분비공개열쇠(KGC가 제공), 비공개열쇠(사용자가 선택), 림시비공개열쇠(사용자가 선택)를 가진다. 따라서 CTAKA규약에서 적수에게는 기껏 두가지 비밀값이 로출되거나 교체된다고 가정하며 이때 적수는 두가지 형태로 구분한다.

정의[1, 5] 통신에 참가하는 사용자(송/수신자)의 공개열쇠를 교체할수 있으나 KGC의 주열쇠는 알수 없는 적수를 외부적수라고 한다.

KGC의 주열쇠를 알수 있으나 사용자의 공개열쇠는 교체할수 없는 적수를 내부적수라고 한다.

2003년에 Al-Riyami와 Paterson에 의해 무증명서공개열쇠암호리론이 처음으로 제기된 후 Mandt는 CTAKA규약을 처음으로 제기하였으며 Wang, Shi 및 Li에 의해 보다 효률적인 CTAKA규약들이 제기되였다.

2008년 Xia 등은 Mandt의 규약이 열쇠절충중간침입공격에 불안전하다는것을 증명하고 개선된 규약을 제기하였고 2009년 Swanson와 Jao는 모든 CTAKA규약들의 안전성을 분석하고 Wang의 규약이 KCI공격에, Shi-Li의 규약이 중간대조공격에 불안전하다는것을 밝혔으며 처음으로 CTAKA규약의 형식적인 안전성모형을 제기하였다. 최근에 제기된 쌍짓기를 리용하는 CTAKA규약들을 비교하였다.(표)

표. CTAKA규약의 비교

규약 (년도)참고문헌	LBN-CTAKA (2009)[1]	LXX-CTAKA (2010)[2]	MHM-CTAKA (2011)[3]	L-CTAKA (2016)[4]	XWZX-CTAKA (2016)[5]
안전성모형	eCK	eCK	eCK	eCK	eCK
교환통보문수	2	2	2	1	1
통신통보문길이	$2\|G_1\|$	$2\|G_1\|$	$2\|G_1\|$	$\|G_1\|$	$\|G_1\|$
계산량	10B+5E	2B+4M+2E	B+3M	B+M+E	B+3M

B－쌍짓기계산시간, E－지수계산시간, M－스칼라점곱하기계산시간

2. XWZX-CTAKA규약에 대한 내부적수의 중간침입공격

여기서는 선행연구[5]에서 제기된 쌍짓기를 리용하는 무증명서쌍방인증열쇠합의규약 XWZX-CTAKA에 대한 중간침입공격을 진행한다.(그림 1)

정리 1 무증명서쌍방인증열쇠합의규약 XWZX-CTAKA는 내부적수의 림시공개열쇠교체에 의한 중간침입공격에 불안전하다.

증명 적수는 송/수신자의 3개 비밀값들가운데서 기껏 2개까지 알수 있다. 여기서 내부적수는 KGC의 주열쇠 s를 알수 있으므로 송/수신자의 부분비공개열쇠 D_A와 D_B를 알수 있다. 그러므로 내부적수는 기껏 1개의 비밀값을 더 알수 있다. 그러나 송/수신자의 비공개열쇠는 알수 없으며 또 그에 대응하는 공개열쇠를 교체할수도 없으므로 따라서 내부적수는 림시비공개열쇠를 알거나 그에 대응하는 림시공개열쇠만을 교체할수 있다.

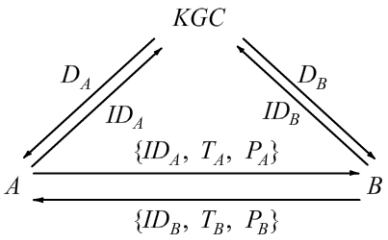

그림 1. XWZX-CTAKA규약의 실행과정

이로부터 내부적수는 A가 B에게 보내는 통보문 $\{ID_A,\ T_A,\ P_A\}$중에서 A의 림시공개열쇠 $T_A = t_A \cdot P_A$를 $T'_A = -P_A + P$로, B가 A에게 보내는 통보문 $\{ID_B,\ T_B,\ P_B\}$중에서 B의 림시공개열쇠 $T_B = t_B \cdot P_B$를 $T'_B = -P_B + P$로 교체하여 보낸다.

다음 내부적수는 A가 구하는 대화열쇠를 다음과 같이 알아내여 A와 공유함으로써 B로 위장한다. 즉 A가 현재 자기가 통신하는 상대방이 B로 잘못 생각하게 할수 있다.

① 송신자 A와의 대화열쇠공유, B로 위장

$$K_{A1} = (x_A + t_A)(P_B + T'_B) = (x_A + t_A)(P_B - P_B + P) = P_A + T_A$$

$$K_{A2} = e(D_A + t_A \cdot P_{KGC},\ H_1(ID_B) + T'_B) =$$

$$= e(s \cdot H_1(ID_A) + t_A \cdot P_{KGC},\ H_1(ID_B) + T'_B)$$

$$K_{A3} = t_A \cdot T'_B$$

$$sk_A = H_2(ID_A,\ ID_B,\ T_A,\ T'_B,\ K_{A1},\ K_{A2},\ K_{A3})$$

마찬가지로 내부적수는 수신자 B가 구하는 대화열쇠를 다음과 같이 알아내여 공유함으로써 송신자 A로 위장한다.

② 수신자 B와의 대화열쇠공유, A로 위장

$$K_{B1} = (x_B + t_B)(P_A + T'_A) = (x_B + t_B)(P_B - P_B + P) = P_B + T_B$$

$$K_{B2} = e(D_B + t_B \cdot P_{KGC},\ H_1(ID_A) + T'_A) = e(s \cdot H_1(ID_B) + t_B \cdot P_{KGC},\ H_1(ID_A) + T'_A)$$

$$K_{B3} = t_B \cdot T'_A$$
$$sk_B = H_2(ID_A,\ ID_B,\ T'_A,\ T_B,\ K_{A1},\ K_{A2},\ K_{A3})$$

$$A \xrightarrow{\{ID_A,\ T_A,\ P_A\}} C \xrightarrow{\{ID_A,\ T'_A,\ P_A\}} B$$
$$A \xleftarrow{\{ID_B,\ T'_B,\ P_B\}} C \xleftarrow{\{ID_B,\ T_B,\ P_B\}} B$$

그림 2. XWZX-CTAKA규약에 대한 중간침입공격과정

따라서 적수는 송신자 A와 대화열쇠 sk_A, 수신자 B와 sk_B를 공유하게 된다.(증명끝)

그림 2에 XWZX-CTAKA규약에 대한 중간침입공격과정을 주었다. 그림에서 A는 송신자, B는 수신자, C는 내부적수를 의미한다.

3. L-CTAKA규약에 대한 내부적수의 중간침입공격

여기서는 선행연구[4]에서 제기된 쌍짓기를 리용하는 무증명서쌍방인증열쇠합의규약 L-CTAKA에 대한 중간침입공격을 진행한다.

정리 2 무증명서쌍방인증열쇠합의규약 L-CTAKA는 내부적수의 림시공개열쇠교체에 의한 중간침입공격에 불안전하다.

증명 정리 1에서와 마찬가지로 내부적수는 주열쇠 s를 알수 있으므로 D_A와 D_B를 안다고 가정한다. 다음 내부적수는 A의 림시공개열쇠 $T_A = t_A \cdot P_A$를 $T'_A = t_B^{-1} \cdot P$로, B의 림시공개열쇠 $T_B = t_B \cdot P_B$를 $T'_B = t_A^{-1} \cdot P$로 교체한다. 그러면 내부적수는 송신자 A가 구하는 대화열쇠를 다음과 같이 알아내여 A와 공유함으로써 수신자 B로 위장하고 중간침입공격을 할수 있다.

$$K_{A1} = e(H_1(ID_B),\ P_{KGC})^{x_A t_A} = e(D_B,\ T_A)$$
$$K_{A2} = e(D_A,\ T'_B)$$
$$K_{A3} = e(D_A,\ H_1(ID_B))$$
$$K_{A4} = t_A \cdot x_A \cdot T'_B = t_A \cdot x_A \cdot t_A^{-1} \cdot P = x_A \cdot P = P_A$$
$$sk_A = H_2(ID_A,\ ID_B,\ T_A,\ T'_B,\ K_{A1},\ K_{A2},\ K_{A3},\ K_{A4})$$

또한 수신자 B가 구하는 대화열쇠를 다음과 같이 알아낸다.

$$K_{B1} = e(D_B,\ T'_A)$$
$$K_{B2} = e(H_1(ID_A),\ P_{KGC})^{x_B t_B} = e(D_A,\ T_B)$$
$$K_{B3} = e(D_B,\ H_1(ID_A))$$
$$K_{B4} = t_B \cdot x_B \cdot T'_A = t_B \cdot x_B \cdot t_B^{-1} \cdot P = x_B \cdot P = P_B$$
$$sk_B = H_2(ID_A,\ ID_B,\ T'_A,\ T_B,\ K_{A1},\ K_{A2},\ K_{A3},\ K_{A4})$$

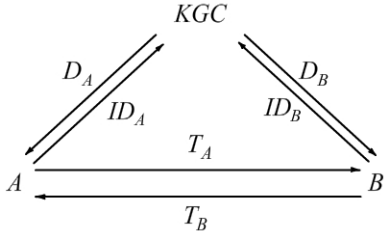

그림 3. L-CTAKA규약의 실행과정

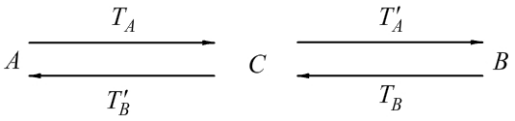

그림 4. L-CTAKA규약에 대한 중간침입공격과정

그림 3과 4에 L-CTAKA규약의 실행과정과 내부적수의 림시공개열쇠교체에 의한 중간침입공격과정을 주었다.(증명끝)

L-CTAKA규약에 대한 증명에서 K_4를 구하는것이 타원곡선우에서 BDH문제에 기초하고있다고 지적하였다. 그러나 내부적수가 중간침입공격을 하는 경우 $K_4 = t_A \cdot x_A \cdot t_B \cdot x_B \cdot P$에 대하여 송/수신자의 공개열쇠들을 교체함으로써 서로 다른 K_{A4}와 K_{B4}를 구하게 된다는것을 고려하지 못하였다. 따라서 내부적수는 송신자 A와 수신자 B사이에 중간침입하여 대화열쇠 sk_A와 sk_B를 각각 공유함으로써 쌍방사이의 통신을 조종할수 있게 된다.

우리는 앞으로 중간침입공격에 안전한 효률적인 쌍짓기를 리용하는 무증명서쌍방인증열쇠합의규약을 구성하려고 한다.

참 고 문 헌

[1] G. Lippold et al.; LNCS, 5671, Springer-Verlag, 206, 2009.

[2] W. Liu et al.; ICMINS, 520, 2010.

[3] R. Mokhtarnameh et al.; ICACT, 802, 2011.

[4] H-Y. Lin; Inf. Technol. Contr. 45, 1, 71, 2016.

[5] Y. Xie et al.; LNCS 10005, Springer-Verlag, 244, 2016.

주체108(2019)년 3월 15일 원고접수

Cryptanalysis of the Some Certificateless Two-Party Authenticated Key Agreement Protocols with Pairing

Kim Yong Jin, *Kim Son Gyong* and *O Chung Il*

In this paper we propose the intruder-in-the-middle attack of the inside attacker by replacing ephemeral public key for two Certificateless Two-Party Authenticated Key Agreement Protocols XWZX-CTAKA and L-CTAKA with pairing, and prove that the protocols are vulnerable to this attack.

Key word: Certificateless Two-Party Authenticated Key Agreement Protocol