M-Commerce를 위한 AMKC 프로토콜†

신성한*, 박지환*

*부경대학교 전자계산학과

A Novel AMKC Protocol for M-Commerce

Seong-Han Shin*, Ji-Hwan Park*

*Department of Computer Science, PuKyong National University

요 약

AKC 프로토콜(Authenticated Key Agreement with Key Confirmation protocol)은 2명 혹은 다수의 객체가 서로간에 차후에 사용하게 될 암호 알고리즘의 공유키를 확립하기 위한 프로토콜로서, 동시에 객체간의 인증과 확립된 공유키를 확인하는 것이다. 본 논문에서는 M-Commerce(Mobile-Commerce)를 고려한 인증서 기반의 실용적인 2자간 AKC 프로토콜에 초점을 맞춘다. 제안하는 프로토콜은 2명의 객체가 단 한번의 세션과정으로 복수의 공유키를 확립한다. 이것은 무선환경에서 암호 알고리즘의 수출규제에 대한 대안으로 적합하며, 계산량과 통신량을 고려하여 설계되었다. 그리고, 다양한 기존의 공격에 대한 내성에 대해서도 상세히 분석한다.

I. 서론

키 확립 프로토콜은 2명 혹은 다수의 객체가 차후에 사용하게 될 암호 알고리즘에서 공유되는 비밀키(여기에서는 단순히 공유키로 명명한다)를 확립하기 위한 프로토콜이다. 이 프로토콜은 크게 키 전송 프로토콜과 키 동의 프로토콜로 나눌 수 있다. 전자의 경우 한쪽의 객체에 의해 생성된 공유키는 다른 객체에게 안전하게 전송되며, 후자의 경우에는 객체들 각자의 정보에 의해 공유키가 생성되며 누구도 그 공유키를 사전에 계산할 수 없다[1].

본 논문에서는 무선 환경을 고려하면서 복수의 공유키를 확립하기 위한 2자간 AMKC 프로토콜(Authenticated Multiple Key Agreement with Key Confirmation protocol)에 초점을 맞춘다. 일례로 WAP의 경우, 적절한 안전성을 보장하는 암호 알고리즘의 수출규제에 의해 두 객체간의 공유키는 어느 일정한 트랜잭션 이후, refresh되어야만 그 안전성을 보장받을 수 있다[2].

본 논문의 구성은 다음과 같다. 2장에서는 제안되는 프로토콜에 사용되는 구성요소와 파라미터들에 대해서 설명하고, 3장에서는 PKI 기반에서 복수의 키를 생성하는 프로토콜을 제안한다. 4장에서는 제안된 프로토콜에 대해 기존에 알려진 공격에 대한 분석을 한다.

II. 구성요소 및 파라미터

본 논문에서는 전통적인 키 공유 프로토콜인 Diffie-Hellman 프로토콜[3]과 1997년 Y. Zheng에 의해 제안된 signcryption 기법을 이용한다[4,5]. Diffie-Hellman 프로토콜은 통신에 참여하고 있는 객체에 대한 인증 기능을 수행하지 못하므로, 공개키 암호와 서명 기법을 동시에 수행하여 계산량과 통신량을 줄인 signcryption을 이용한다. 하지만, signcryption 기법 자체로는 이전에 확립된 공유키에 대한 Forward Secrecy를 제공하지 못하는 단점이 있다.

제안하는 프로토콜에서 Alice라는 객체는 무선상에 존재하는 mobile user이고, Bob은 유선 상에서 서비스를 제공하는 서버라고 가정한다. 이것은 대부분의 M-Commerce에 해당되는 환경이다. 프로토콜에 사용되는 파라미터들은 다음과 같다.

†본 연구는 정보통신부 MSRC 연구지원에 의해 수행되었음

p, q는 큰 소수로서 q는 $p-1$의 소인수이며 적절한 안전성을 보장하기 위해서는 p의 크기는 1024비트, q의 크기는 160비트 이상이 되어야 한다[6]. g는 Z_p^*상에서 위수가 q인 원시근이다. Alice와 Bob의 비밀키와 공개키를 (x_a, y_a), (x_b, y_b)로 각각 두었을 때, x_a, x_b는 Z_q^*의 원소들이고 y_a, y_b는 다음과 같이 계산된다. $y_a \equiv g^{x_a} \bmod p, y_b \equiv g^{x_b} \bmod p$ 여기에서 Alice의 경우, 공개정보는 (y_a, g, p)이고 이 공개정보를 가지고 Alice의 비밀키 x_a를 구하는 것을 이산대수문제라고 한다. 또한, Alice와 Bob의 공개키, 소유자 ID 및 CA(Certification Authority)의 서명등이 포함된 인증서는 $Cert_A, Cert_B$로 나타낸다. $H()$는 안전한 일방향 해쉬함수를, $E(), D()$는 대칭키 암호시스템의 암/복호 알고리즘을 나타낸다.

III. AMKC 프로토콜

여기에서는 Diffie-Hellman문제의 안전성을 기반한 복수의 키를 생성하는 AMKC 프로토콜(Authenticated Multiple Key Agreement with Key Confirmation protocol)을 제안한다. 기존의 AKC 프로토콜은 random oracle[7] 환경에서 공유키의 안전성이 취약할 수 있는 구조를 가지며, 복수의 키를 공유하기 위해서는 그만큼 세션과정을 반복해야 한다[8]. 아래에 제안하는 프로토콜의 전체 과정을 설명한다.

Step1. Alice는 Bob과 n개의 공유키를 확립하기 전에, off-line상에서 유일한 난수 x를 선택해서 x_n, T를 계산한다. 반면에, Bob은 자신이 선택한 난수 r_B로 계산한 공개값 g^{r_B}와 그 때의 타임스탬프 TS 그리고 인증서 $Cert_B$를 broadcast한다.

$$x \in Z_q^* \tag{1}$$

$$x_n \equiv x \cdot n \bmod q \tag{2}$$

$$T \equiv g^x \bmod p \tag{3}$$

Step2. Bob으로부터 메시지를 받고 나서 Alice는 unknown key-share 공격을 막기 위해 아래의 식 (4),(5)를 확인한다. 그리고 나서, Alice는 x를 이용해서 암호 알고리즘에 사용될 키와 x_n을 가지고 공유키를 계산한다. 이것은 공유키의 perfect forward secrecy를 보장한다. signcryption을 한 후, Alice는 Bob에게 공개값 T와 암호문 c를 보낸다.

$$1 < g^{r_B} < p \tag{4}$$

$$(g^{r_B})^q \equiv 1 \bmod p \tag{5}$$

$$K_{ENC} = H(y_b^x \bmod p) \tag{6}$$

$$Key \equiv (g^{r_B})^{x_n} \bmod p \tag{7}$$

$$r = H(Key \| g^{r_B}) \tag{8}$$

$$s \equiv x_n/(x_a + r) \bmod q \tag{9}$$

$$c = E_{K_{ENC}}(Cert_A \| r \| s \| TS) \tag{10}$$

Step3. 마찬가지로, Bob은 Alice가 보내온 메시지를 가지고 식 (11),(12)를 확인하고 signcryption의 수신자 지정 검증방식으로 복호키를 생성한다. 수신한 암호문을 복호한 후, Bob은 TS와 pair를 이루는 r_B를 가지고 Alice와의 공유키를 생성한다. 마지막으로 식 (16)으로 서명의 검증과 공유키 확인을 한다.

$$1 < T < p \tag{11}$$

$$T^q \equiv 1 \bmod p \tag{12}$$

$$K_{ENC} = H(T^{x_b} \bmod p) \tag{13}$$

$$D_{K_{ENC}}(c) = Cert_A \| r \| s \| TS \tag{14}$$

$$Key \equiv (y_a \cdot g^r)^{s \cdot r_B} \bmod p \tag{15}$$

$$r ?= H(Key \| g^{r_B}) \tag{16}$$

이 프로토콜이 끝나고 난 후, Alice와 Bob은 일정한 트랜잭션 이후에 $n-1$번까지 키를 refresh 할 수 있다. 그림1에 전체 프로토콜을 나타내었다.

IV. 안전성 분석

여기에서는 제안된 프로토콜의 특징과 기존에 제시된 공격[9-11]에 대한 내성을 다룬다. 프로토콜의 효율성을 보이기 위해서 기존에 제안되었던 AKC 프로토콜과 비교한다.

1. 특징

Explicit key authentication of Alice to Bob: 일반적으로 명시적 키 인증이라는 것은 암시적 키 인증과 키 확인이 제공될 때에 보장된다. Step2에서 Alice는 선택한 난수 x로 계산된 x_n을 가지고

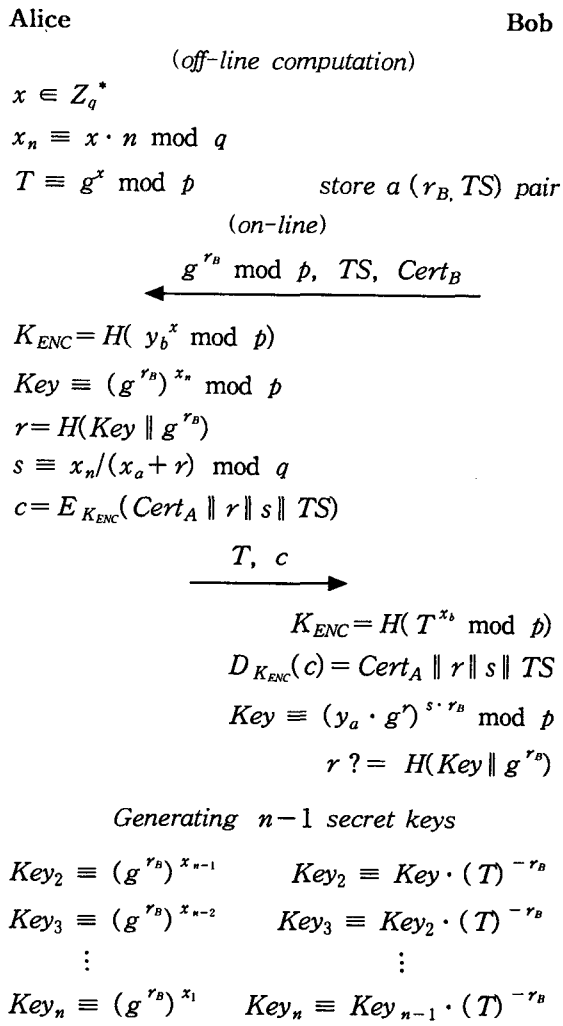

그림1. AMKC protocol.

공유키를 생성하여 서명을 한 후, Bob에게 보낸다. 이 과정에서 Bob은 Alice 이외에는 누구도 이 공유키를 계산할 수 없음을 확신한다. 왜냐하면, 공유키에 사용된 x_n이 Alice의 서명검증과정에서 나타나기 때문이다. 또한, Bob은 Alice가 실제로 공유키를 계산하였다는 것을 식 (16)으로 확신할 수 있다.

Implicit key authentication of Bob to Alice: Step3에서 Bob은 자신의 공개키에 대응하는 비밀키를 가지고 대칭키 암호시스템에 쓰인 복호키를 도출할 수 있다. 그 후에, 암호문을 복호하고 난수 r_B를 가지고 공유키를 계산하게 된다(식 (13-16)). 이것을 signcryption의 수신자 지정 검증방식이라고 한다. 따라서, Alice는 오직 Bob만이 공유키를 구할 수 있음을 확신할 수 있다.

Entity authentication & Non-repudiation of Alice: Step2에서 Alice는 Bob이 보내온 공개값 g^{r_B}와 공유키에 대한 서명을 생성한다. 따라서 PKI기반에서 Bob은 Alice라는 객체를 인증할 수 있다. 또한, 부인불가기능은 원래의 signcryption과 동일하게 수행될 수 있다.

Anonymity of Alice: Alice의 인증서는 식 (10)에 의해 암호화된 형태로 Bob에게 보내진다. 이것은 Bob의 비밀키를 알지 못하는 한, Alice의 익명성이 보장된다는 것을 의미한다. 따라서 공격자는 Bob이 누구와 통신을 하고 있는지 알 수 없다. Alice와 Bob이 보다 민감한 통신을 하는 경우에 익명성은 유용하다.

2. 공격에 대한 안전성

Known-key security(key freshness): Alice와 Bob 사이에 AKC 프로토콜이 수행되면 유일한 공유키를 생성하게 되는데, 이것을 일반적으로 세션키라고 한다. 제안된 프로토콜에서 Alice와 Bob 모두 공유키가 유일한 값이라는 것을 확신할 수 있다. 그 이유는 만약 Alice가 동일한 난수를 다시 사용하게 된다면 Bob은 식 (9)에 의해 Alice의 비밀키를 도출할 수 있게 된다. 따라서 공유된 세션키는 유일하게 된다. 이러한 성질을 Alice의 self-enforcement property라고 한다.

Perfect forward secrecy: 만약 어느 한쪽의 공개키에 대응하는 비밀키가 노출되더라도, 그 이전 공유키의 안전성은 보장되어야 한다. 공격자가 Alice의 비밀키를 알게 되더라도 이전의 통신문은 암호화된 형태를 취하므로 Bob의 비밀키 없이는 복호할 수 없다. 또한, Bob의 비밀키를 알게 되어 암호문을 복호하더라도 Bob이 선택한 난수가 없으면 공유키를 구할 수 없다. 따라서, 이 프로토콜은 perfect forward secrecy를 보장한다고 할 수 있다.

Key-compromise impersonation: 이것은 Bob의 비밀키가 노출되었을 때 공격자가 다른 객체(공격자 자신이 아닌 다른 객체)처럼 Bob을 속이는 것을 말한다. 하지만, 인증서 기반 프로토콜에서는 이 공격 자체가 의미가 없다.

Unknown key-share(joint control of a shared secret key): 이것은 Bob이 우연히 혹은 고의적으로 취약한 공개값을 가지고 Alice와 공유키를 확립하려고 한다는 것을 Alice가 알아야 한다는 것을 의미한

다. 즉, Alice는 Chris(제3자)와 세션키를 공유하였는데, Bob은 Alice와 공유키를 확립하였다고 믿게 되는 것이다. 제안된 프로토콜에서는 Alice와 Bob 모두 Step2,3에서 공유키를 생성하기 전에 식 (4),(5)와 식 (11),(12)로 공개값을 확인하게 된다. 이것은 Alice와 Bob이 취약한 공개값을 선택하지 않도록 한다.

3. 기존 프로토콜과의 비교

표1에서 제안된 프로토콜을 기존에 제시되었던 것과 비교한다. 계산량의 경우, 무선 상에 존재하는 Alice만을 고려한다. Alice와 Bob이 n개의 공유키를 확립하는 경우에는 제안된 프로토콜이 계산량과 통신량을 크게 줄이는 것을 알 수 있다. 그 이유는 암호화에 사용되는 키와 공유키에 사용되는 난수를 분리함으로써 부가적인 통신 없이도 $n-1$개까지의 공유키를 생성할 수 있기 때문이다.

표 1: AKC 프로토콜들의 비교.

	3-pass 프로토콜[8]	AMKC 프로토콜
통신수	3	2
계산량 (사전계산량)	3	3 (2)
n개의 경우	$3n$	$n+4$
통신량	$3\|p\|+2\|H\|$	$3\|p\|$
n개의 경우	$(2n+1)\|p\|+2n\|H\|$	$3\|p\|$
DVP	X	O
KKS	X	O
PFS	O	O
KCI	O	O
UKS	X	O

여기서 DVP(Designated Verifier Proof)는 수신자 지정 검증방식을 KKS는 Known-Key Security, PFS는 Perfect Forward Secrecy, KCI는 Key-Compromise Impersonation 그리고 UKS는 Unknown Key-Share를 나타낸다.

V. 결론

본 논문에서는 2자간 AKC 프로토콜에서 복수의 키를 생성할 수 있는 프로토콜을 제안하였다. 이 프로토콜은 현재 이슈가 되고 있는 M-Commerce에 적합하도록 고안되었으며, 무선환경에서의 안전한 암호 알고리즘의 수출규제에 대한 대안으로 사용되어질 수 있다. 또한, 기존에 제시된 여러 가지 공격에 대한 내성도 분석하였다.

참고문헌

[1] A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.

[2] http://www.wapforum.org

[3] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22, pp.644-654, 1976.

[4] Y. Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature)+Cost(Encryption)", Crypto'97, Springer-Verlag, LNCS 1294, pp.165-179, 1997.

[5] Y. Zheng, "Shortened Digital Signature, Signcryption and Compact and Unforgeable Key Agreement Schemes", P1363 Submissions to the Study Group for Future Public-Key Cryptography Standards.

[6] Michael J. Wiener, "Performance Comparison of Public-Key Cryptosystems", CryptoBytes, The technical newsletter of RSA Laboratories, Vol.4, No.1, 1998.

[7] R. Canetti, O. Goldreich, S. Halevi, "The Random Oracle Methodology, Revised", Proc. of the 30th Annual ACM Symposium on the Theory of Computing(STOC'98), pp.209-218, 1998.

[8] K. H. Lee, S. J. Moon, "AKA Protocols for Mobile Communicatioins", Proc. of Australasian Conference(ACISP2000), pp.400-411, 2000.

[9] K. Nyberg, R. A. Rueppel, "Weaknesses in Some Recent Key Agreement Protocols", IEE Electronic Letters, Vol.30, No.1, 1994.

[10] G. Horn, K. M. Martin, C. J. Mitchell, "Authentication Protocols for Mobile Network Environment Vaule-added Services", IEEE Trans. on Vehicular Technology, available at http://isg.rhbnc.ac.uk/cjm/Chris_Mithchell.htm

[11] Simon Blake-Wilson, Alfred Menezes, "Authenticated Diffie-Hellman Key Agreement Protocols", Proc. of the 5th Annual Workshop on Selected Area in Cryptography, LNCS1556, pp.339-361, 1998.