

타원곡선 암호시스템에 기반한 복수의 키를 생성하는 AKC 프로토콜

안경모[†], 신성한[‡], 박지환[‡]

[†]부경대학교 전산교육전공, [‡]부경대학교 전자계산학과

An AKC Protocol Generating Multiple Secret Keys on Elliptic Curve Cryptosystems

KyeongMo An[†], SeongHan Shin^{‡†}, JiHwan Park^{‡‡}

[†]Education of Computer Science, PuKyong National Univ.

^{‡‡}Dept. of Computer Science, PuKyong National Univ.

E-mail : bido1878@yahoo.co.kr, shinsh@mail.pknu.ac.kr, jpark@pknu.ac.kr

요약

본 논문에서는 무선환경을 고려하여 타원곡선 암호시스템을 기반으로 하는 AKC 프로토콜(Authenticated Key Agreement with Key Confirmation Protocol)을 제안한다. 제안 프로토콜은 2명의 객체가 한번의 세션과정을 통해서 복수개의 공유키를 생성하며 주기적으로 키를 refresh함으로써, 현재 안전한 암호 알고리즘의 수출규제에 따른 대안으로 사용되어질 수 있다. 또한 이미 알려진 여러 공격에 대한 안전성을 상세히 고찰한다.

1. 서론

무선 전자상거래(Mobile-Commerce)가 활성화됨에 따라 무선 환경에서의 보안이 이슈가 되고 있다. 현재 무선상에서의 대표적인 보안 프로토콜로서 WAP 포럼에서 추진중인 WAP(Wireless Application Protocol), Microsoft가 주도하는 HTTP 기반의 ME(Mobile Explorer) 그리고 일본 NTT-Docomo의 i-mode등이 있다[1]. 그 중에서 WAP의 경우, 안전성을 보장하는 암호 알고리즘의 수출규제 때문에 프로토콜에 참여하는 당사자들이 어느 일정한 트랜잭션 이후에 키를 refresh하도록 하고 있다[2].

본 연구는 정보통신부 MSRC 연구지원에 의해 수행되었음

본 논문에서는 이러한 무선 환경을 고려한 키 확립 프로토콜을 다룬다. 키 확립 프로토콜은 2명 혹은 다수가 차후에 사용하게 될 암호 알고리즘에서 공유되는 비밀키(여기에서는 단순히 공유키로 명명한다)를 확립하기 위한 프로토콜로서 크게 키 전송 프로토콜과 키 동의 프로토콜로 나눌 수 있다. 전자는 한명이 키를 생성하여 상대방에게 전송하는 것이며, 후자는 프로토콜에 참여하는 당사자들의 정보를 가지고 키를 도출하는 것이다[3]. 여기에서는 무선상에서의 계산량과 통신량을 감안하면서 2명의 객체가 복수개의 공유키를 확립하는 AKC 프로토콜(Authenticated Key Agreement with Key Confirmation Protocol)을 제안한다. AKC 프로토콜은 객체를 인증하

는 키 공유 프로토콜이면서 동시에 공유되는 키를 확인하는 프로토콜이다.

본 논문의 구성은 다음과 같다. 2장에서는 제안하는 프로토콜에서 사용될 파라미터와 타원곡선 암호 그리고 프로토콜의 구성요소에 대해서 간략하게 설명한다. 3장에서 타원곡선 암호의 안전성에 기반하여 복수개의 키를 생성하는 프로토콜을 제안하고, 4장에서는 기존에 알려진 공격에 대한 안전성을 분석한다. 마지막으로 5장에서 결론을 맺는다.

2. 구성요소

2.1 파라미터

표1에 프로토콜에 사용될 파라미터들을 나타낸다. 일반적인 무선 전자상거래를 고려하여 프로토콜에 참여하는 두 객체를 각각 Alice와 Bob으로 두고, Alice는 무선상에 존재하는 Mobile User로, Bob은 유선상에서 서비스를 제공하는 서버로 가정한다.

[표 1] 파라미터

E	$GF(p^m)$ 상의 타원곡선(공개정보) 여기에서 $p \geq 2^{160}$, $m = 1$ 이거나, $p = 2$, $m \geq 160$.
q	크기가 $ p^m $ 인 큰 소수(공개정보)
G	위수가 q 인 점(공개정보) G 는 타원곡선 상에서 랜덤하게 선택
H	안전한 일방향 해쉬함수
KH_k	k 를 키로 하는 안전한 일방향 해쉬함수
d_A, Q_A	Alice의 비밀키와 공개키 여기에서 $d_A \in _R [1, \Lambda, q-1]$. $Q_A = d_A G$.
d_B, Q_B	Bob의 비밀키와 공개키 여기에서 $d_B \in _R [1, \Lambda, q-1]$. $Q_B = d_B G$.
$Cert_A, Cert_B$	Alice와 Bob의 공개키 인증서 인증서는 그 객체의 공개키와 ID. 인증기관의 서명등을 포함
r_A, v, x	유일하게 선택된 Alice의 난수 $r_A, v, x \in _R [1, \Lambda, q-1]$

r_B	유일하게 선택된 Bob의 난수 $r_B \in _R [1, \Lambda, q-1]$
$E(\cdot), D(\cdot)$	비밀키 암호의 암/복호 알고리즘
K_{ENC}	암/복호 알고리즘에 사용되는 키
Key	Alice와 Bob의 공유된 비밀키(공유키)
TS	타임스탬프
$x \parallel y$	x 와 y 의 연결

2.2 타원곡선 암호[4][5]

유한체 $GF(p^m)$ 상에서 정의된 타원곡선 군은 아래의 3차 방정식을 만족하는 순서쌍 (x, y) 들과 무한원점 O 을 포함한 집합이며, 이 집합은 가환군 형태를 이룬다.

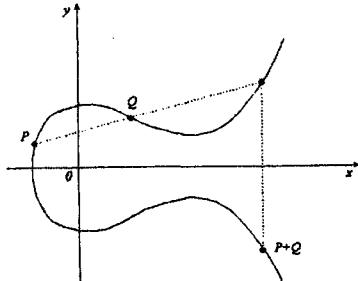
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$x, y, a_1, a_2, a_3, a_4, a_6 \in GF(p^m)$$

계산의 단순화를 위해, 이제부터 Weierstrass 형태의 타원곡선으로 설명한다.

$$y^2 = x^3 + ax + b$$

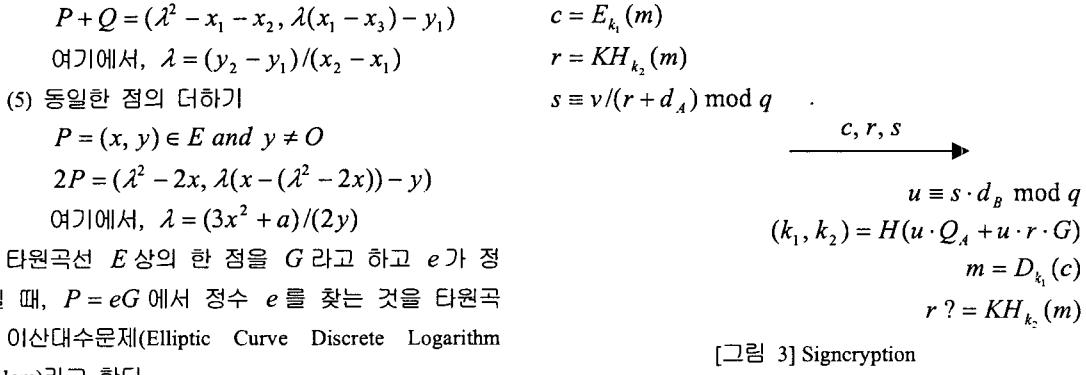
$$a, b \in GF(p) \text{ and } 4a^3 + 27b^2 \neq 0$$



[그림 1] 타원곡선에서의 더하기

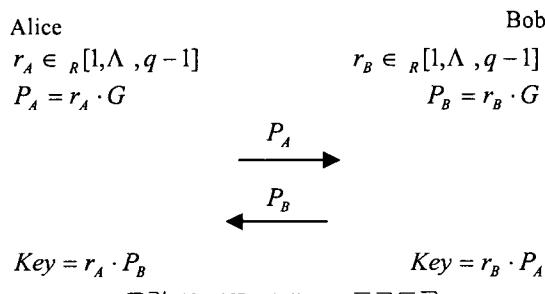
그림1과 같이, 타원곡선 상에서의 덧셈 연산은 다음 규칙들을 따른다.

- (1) $O + O = O$
- (2) $P + O = P$ 여기에서, 모든 $P = (x, y) \in E$
- (3) $P + Q = O$
여기에서, 모든 $P = (x, y), Q = (x, -y) \in E$
- (4) 다른 두 점의 더하기
 $P = (x_1, y_1), Q = (x_2, y_2) \in E \text{ and } x_1 \neq x_2$



2.3 Diffie-Hellman 프로토콜[6]

대표적인 키 공유 프로토콜인 Diffie-Hellman 프로토콜은 다음과 같다. 여기에서 Alice와 Bob은 보호되지 않는 통신로상에서 공유키를 확립한다.



이 프로토콜의 단점은 프로토콜에 참여하고 있는 객체에 대해서 인증 기능을 제공하지 않는다는 것이다.

2.3 Signcryption

Y. Zheng은 1997년 이산대수문제에 기반하여 공개키 암호와 서명 기법을 동시에 수행함으로써 계산량과 통신량을 줄인 Signcryption 기법을 제안하였다 [7][8]. 여기에서는 타원곡선 상에서 Y. Zheng 등이 제안한 Signcryption에 대해서 살펴본다[9][10].



Signcryption 기법에서 Alice는 암호 알고리즘과 서명에 쓰이는 키를 Bob의 공개키를 이용함으로써 수신자 지정 검증방식을 취하고 있다. 다시 말해서 Bob 이외의 어느 누구도 복호 및 서명의 검증을 할 수 없다. 하지만, Signcryption 기법을 이용한 키 공유 프로토콜은 Bob의 비밀키가 노출되었을 경우 이전에 확립된 공유키에 대한 Forward Secrecy를 보장하지 못하는 문제점이 있다.

3. 제안 프로토콜

3.1 Motivation

본 논문의 목적은 무선 환경을 고려하여 통신량과 계산량 측면에서 효율적인 타원곡선상의 Signcryption 기법을 이용하면서 Alice와 Bob 사이에 복수개의 공유키를 확립하는데 있다. 하지만, 이전에 제시된 AKC 프로토콜들은 복수개의 공유키를 확립하기 위해서는 그만큼의 세션을 반복해야 하는 비효율성이 있다[11][12]. 따라서 Signcryption의 서명 검증을 일반적인 서명과 동일하게 개선한 기법[13]으로 위의 문제점을 해결함과 동시에 실용적이고 효율적인 AKC 프로토콜을 제안한다.

3.2 Construction

제안하는 프로토콜에서 Alice와 Bob은 m 개의 공유키를 확립한다.

STEP1. Alice는 off-line상에서 유일한 난수 x 를 선택하고 T_A, x_m 을 계산한다. 한편, Bob은 자신이 선택한

난수 r_B 에 대한 공개값 T_B 를 계산하고 그 때의 타임스탬프 TS 와 인증서 $Cert_B$ 를 broadcast한다. 동시에 Bob은 r_B, TS 쌍을 자신의 데이터베이스에 보관한다.

$$x \in_R [1, \Lambda, q-1] \quad (1)$$

$$T_A = x \cdot G \quad (2)$$

$$x_m \equiv x + m \pmod{q} \quad (3)$$

$$r_B \in_R [1, \Lambda, q-1] \quad (4)$$

$$T_B = r_B \cdot G \quad (5)$$

STEP2. Alice는 Bob의 unknown key-share 공격을 막기 위해서 식 (6),(7)을 확인한다. 그리고 나서, Alice는 자신이 선택한 난수 x 와 Bob의 공유키 Q_B 를 사용하여 암호 알고리즘에 사용될 키를 계산하고, x_m 을 가지고 Bob과의 공유키를 구한다. 이것은 원래의 Signcryption 기법이 가지는 Forward Secrecy 문제점을 해결한다. 또한, Alice는 Bob이 공유키를 확인할 수 있도록 서명 생성시 공유키를 포함시켜 Signcryption 과정을 수행한다.

$$\text{check } 1 < T_B < p \quad (6)$$

$$\text{check } q \cdot (T_B) \equiv O \pmod{p} \quad (7)$$

$$K_{ENC} = H(x \cdot Q_B) \quad (8)$$

$$Key = x_m \cdot (T_B) \quad (9)$$

$$r = H(Key \| T_B) \quad (10)$$

$$s \equiv x_m / (d_A + r) \pmod{q} \quad (11)$$

$$c = E_{K_{ENC}}(Cert_A \| r \| s \| TS) \quad (12)$$

STEP3. Bob은 Alice와 마찬가지로 받은 메시지 T_A, c 를 가지고 식 (13),(14)를 확인한다. 확인 후, 올바른 값이 아닐 시에는 프로토콜을 중단한다. 그렇지 않다면, Bob은 자신의 비밀키 d_B 를 가지고 복호키를 구한다. 이것이 Signcryption의 수신자 지정 검증방식이다. 암호문을 복호한 후, Bob은 TS 와 쌍을 이루는 난수 r_B 를 찾기 위해 데이터베이스를 검색한다. 데이터베이스에서 찾은 r_B 를 가지고 공유키를 생성하여 Alice의 서명을 검증함과 동시에 공유키 확인과정을 수행한다.

$$\text{check } 1 < T_A < p \quad (13)$$

$$\text{check } q \cdot (T_A) \equiv O \pmod{p} \quad (14)$$

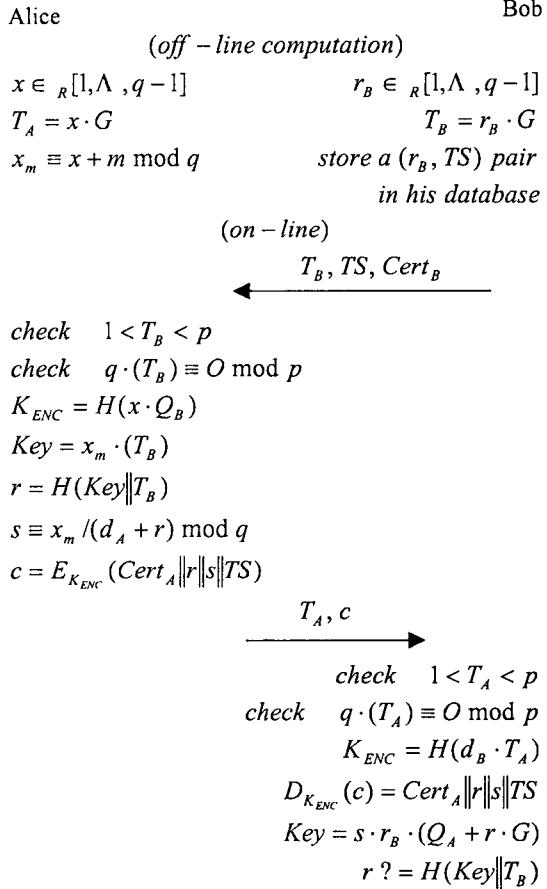
$$K_{ENC} = H(d_B \cdot T_A) \quad (15)$$

$$D_{K_{ENC}}(c) = Cert_A \| r \| s \| TS \quad (16)$$

$$Key = s \cdot r_B \cdot (Q_A + r \cdot G) \quad (17)$$

$$r ? = H(Key \| T_B) \quad (18)$$

위의 세션이 끝난 후, Alice와 Bob은 공유키 Key 를 확립하게 된다. 어느 일정한 트랜잭션 이후에 Alice와 Bob은 Key_2 로 refresh하고, 그 다음에 다시 Key_3 로 Key_4 로 결국에서 Key_m 으로 refresh한다. 다시 말해서 처음 확립된 키 이후에 $m-1$ 번까지 키를 refresh함으로써 사용하는 암호 알고리즘의 안전성을 보장하게 된다. 그림1에 전체 프로토콜을 나타내었다.



Generating $m-1$ secret keys

$$\begin{array}{ll} Key_2 = x_{m-1} \cdot (T_B) & Key_2 = Key + (-r_B) \cdot G \\ Key_3 = x_{m-2} \cdot (T_B) & Key_3 = Key_2 + (-r_B) \cdot G \end{array}$$

$$\begin{array}{ll} \text{N} & \text{N} \\ Key_m = x_1 \cdot (T_B) & Key_m = Key_{m-1} + (-r_B) \cdot G \end{array}$$

[그림 4] 제안 프로토콜

4. 안전성

여기에서는 제안된 프로토콜의 안전성을 분석한다. 우선 제안 프로토콜의 특징을 살펴보고 기준에 제시된 공격[14][15]에 대한 내성을 다룬다.

4.1 특징

제안 프로토콜은 타원곡선상의 Diffie-Hellman 문제와 이산대수문제에 안전성을 두고 있다. 또한 Random Oracle Model[16]을 고려하여 통신로상에 공개되는 정보를 최소화하였다.

Explicit Key Authentication of Alice to Bob : 일반적으로 명시적 키 인증이라는 것은 임시적 키 인증과 키 확인이 제공될 때 보장된다. STEP2에서 Alice는 난수 x 로 계산된 x_m 을 가지고 공유키 Key 를 생성한다. 식 (10),(11)과 같이 x_m 과 공유키가 Alice의 서명 생성시 사용된다. 이 과정에서 Bob은 Alice 이외의 어느 누구도 이 공유키를 계산할 수 없다는 것을 확신한다. 왜냐하면 공유키에 사용된 x_m 의 공유값이 Bob의 서명검증 과정에서 나타나기 때문이다(식 (17)). 또한 Bob은 Alice가 실제로 이 공유키를 생성하였다는 것을 식 (18)로 확신할 수 있다.

Implicit Key Authentication of Bob to Alice : STEP3에서 Alice로부터 메시지를 수신한 Bob은 자신의 공개키에 해당하는 비밀키 d_B 를 가지고 암호 알고리즘에 쓰일 복호키를 도출하게 된다(식 (15)). 그리고 나서 자신의 난수 r_B 를 가지고 공유키 Key 를 계산한다(식 (17)). 이것은 Signcryption의 수신자 지정 검증방식이다. 따라서 Alice는 오직 Bob만이 자신이 생성한 공유키를 구할 수 있다고 확신할 수 있다.

Entity Authentication : STEP2에서 Alice는 Bob으로부터 수신한 공개값 T_B 와 공유키 Key 에 대한 서명을 생성한다. 따라서 Bob은 PKI(Public-Key Infrastructure) 기반에서 Alice라는 객체를 암호문에 포함된 인증서 $Cert_A$ 와 서명검증 과정을 통해서 인증할 수 있다. 또한, 서명의 부인불가(Non-repudiation)기능은 원래의

Signcryption 기법과 동일하게 수행될 수 있다.

Anonymity of Alice : 전자상거래에서 구매자를 특정할 수 없도록 익명성을 보장하는 것은 중요하다. 제안 프로토콜에서 Alice의 인증서 $Cert_A$ 는 식 (12)에 의해 암호화된 형태로 Bob에게 전송된다. 이것은 Bob의 비밀키가 노출되지 않는 한, Alice의 익명성이 보장된다는 것을 의미한다. 따라서 공격자는 Bob이 누구와 통신을 하고 있는지 알 수 없다.

4.2 공격에 대한 안전성

Known-Key Security(Key Freshness) : Alice와 Bob이 통상의 AKC 프로토콜을 수행하게 되면 유일한 공유키를 확립하게 되는데, 이것을 일반적으로 세션키라고 한다. 제안된 프로토콜에서 Alice와 Bob은 모두 공유키가 유일한 값이라는 것을 확신할 수 있다. 그 이유는 만약 Alice가 이전과 동일한 난수 x 를 가지고 계산된 동일한 값 x_m 을 다시 사용하여 공유키를 확립한다면 아래의 연립일차 합동식(식 (19),(20))에 의해 식 (21)과 같이 Alice의 비밀키가 도출된다. 따라서 공유된 세션키는 유일하게 된다. 이러한 성질을 Alice의 Self-Enforcement Property라고 한다.

$$s \equiv x_m / (d_A + r) \pmod{q} \quad (19)$$

$$s' \equiv x_m / (d_A + r') \pmod{q} \quad (20)$$

$$d_A \equiv (s'r' - sr) / (s - s') \pmod{q} \quad (21)$$

Perfect Forward Secrecy : 만약 어느 한쪽의 공개키에 대응하는 비밀키가 노출되더라도, 그 이전에 확립된 공유키의 안전성이 보장될 때 Perfect Forward Secrecy를 만족한다고 할 수 있다. 우선 공격자가 Alice의 비밀키 d_A 를 알게 되더라도 그 이전 세션과정의 메시지 c 는 암호화된 형태를 취하므로 Bob의 비밀키 d_B 없이는 복호할 수 없다. 또한 Bob의 비밀키를 알게 되어 암호문을 복호하더라도, Bob이 그 때에 선택했던 난수 r_B 를 알지 못하면 공유키를 구할 수 없다. 따라서, 제안된 프로토콜은 Perfect Forward Secrecy를 제공한다고 할 수 있다.

Key-COMPROMISE Impersonation : 이것은 만약 Bob의 비밀키가 노출되었을 때 공격자가 다른 객체(공격자 자신이 아닌 다른 객체)처럼 가장하여 Bob을 속이는 것을 말한다. 하지만 제안된 프로토콜에서 확립되는

공유키는 Bob이 선택하는 난수 r_B 에 의존한다. 또한 제안 프로토콜과 같은 인증서 기반 프로토콜에서 이 공격은 의미가 별로 없다.

Unknown Key-Share(Joint Control of a Shared Secret Key) : Bob이 우연히 혹은 고의적으로 츠약한 공개값 T_B 를 가지고 Alice와 공유키를 확립하려고 한다면 Alice는 그것을 확인할 수 있어야 한다. 마찬가지로 Bob도 동일하게 확인할 수 있어야 한다. 제안된 프로토콜에서 Alice와 Bob은 모두 식 (6),(7)과 식 (13),(14)에서 공개값을 확인한다. 이것은 Alice와 Bob이 츠약한 공개값을 선택하지 않았다는 것을 보장한다.

5. 결론

본 논문에서는 현재 이슈가 되고 있는 Mobile-Commerce에 적합한 AKC 프로토콜을 제안하였다. 제안 프로토콜은 무선 환경을 고려하여 타원곡선 암호 시스템을 기반으로 하고 2명의 객체가 복수개의 키를 생성하여 주기적으로 키를 refresh함으로써 안전한 암호 알고리즘의 수출규제에 따른 대안으로 사용되어질 수 있다. 또한 기존에 제시된 공격에 대해서도 상세히 분석하였다.

[참고문헌]

- [1] “무선인터넷 백서”, 소프트뱅크미디어, 2001
- [2] <http://www.wapforum.org>
- [3] A. Menezes, P. van Oorschot, S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1997
- [4] K. Araki, T. Satoh, S. Miura, “Overview of Elliptic Curve Cryptography(Extended Abstract)”, Proceedings of PKC’98, Pacifico Yokohama, Japan, 5-6 February, 1998
- [5] ISO/IEC JTC1/SC27, “Information Technology-Security Techniques”, May 2000
- [6] W. Diffie, M. Hellman, “New Directions in Cryptography”, IEEE Transactions on Information Theory, IT-22, pp.644-654, 1976
- [7] 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
- [8] Y. Zheng, “Shortened Digital Signature Signcryption and Compact and Unforgeable Key Agreement Schemes”, IEEE P1363 Submissions to the Study Group for Future Public-Key Cryptography Standards
- [9] Y. Zheng, H. Imai, “How to Construct Efficient Signcryption Schemes on Elliptic Curves”, Information Processing Letters, Vol.68, N.5, pp.227-233, 1998
- [10] Y. Zheng, H. Imai, “Efficient Signcryption Schemes On Elliptic Curves”, Proceedings of the IFIP 14th International Information Security Conference (IFIP/SEC’98), Chapman & Hall, September 1998
- [11] L. Law, A. Menezes, “An Efficient Protocol for Authenticated Key Agreement”, Technical report CORR 98-5, Department of C&O, University of Waterloo, March 1998
- [12] B. Y. Song, K. J. Kim, “Two-Pass Authenticated Key Agreement Protocol with Key Confirmation”, Proc. of Indocrypt2000, LNCS Vol.1997, pp.237-249, Calcutta India, Dec. 10-13, 2000
- [13] F. Bao, R. H. Deng, “A Signcryption Scheme with Signature Directly Verifiable by Public Key”, PKC’98, Springer-Verlag, LNCS 1431, pp.55-59, 1998
- [14] G. Horn, K. M. Martin, C. J. Mitchell, “Authenticated Protocols for Mobile Network Environment Value-added Services”, IEEE Transactions on Vehicular Technology, available at (http://isg.rhbnc.ac.uk/cjm/Chris_Mitchell.htm)
- [15] S. B. Wilson, A. Menezes, “Authenticated Diffie-Hellman Key Agreement Protocols”, Proc. of the 5th Annual Workshop on Selected Area in Cryptography(SAC’98), LNCS 1556, pp.339-361, 1998
- [16] M. Bellare, P. Rogaway, “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols”, Proceeding of the 1st ACM Conference on Computer and Communications Security, ACM, 1993