通信情報保護學會誌
第2卷, 第1號, 1992. 3

디지탈 서명과 해쉬함수

황석근* · 조한혁**

1. 서 론

컴퓨터가 인간생활의 여러 국면에 더욱 폭넓고 깊게 관여하게 됨에 따라 프로그램이나 데이타의 송수신 및 저장을 안전하고 완벽하게 통제해야 함에 있어서 요구되는 사항은 그런 공격을 찾아내는 일일 것이다. 인가 받은 자 또는 인가 받지 않은 자로부터, 또는 여하한 형태의 공격으로 부터 야기된 데이타 상의 변화를 찾아야 하는 필요성으로 부터 일방해쉬함수의 사용이 시발되었다. 따라서 해쉬함수는 MDS(manipulation detection code), finger print 등으로 불리기도 한다. 일방해쉬함수는 데이타 상의 변화를 신속하게 발견할 수 있는 한 편리한 방법이 되고 있다. 그리하여 오늘날 디지탈 서명에 필수적인 하나의 암호학적 도구가 되고 있는 해쉬함수는 1976년 Diffe와 Hellman[Di-He]이 일방함수(one way function)와 일방 trapdoor 함수(one way trapdoor function)의 개념 위에서 Rabin[Ra]과 Merkle[Me]에 의하여 시작되었다. 일방해쉬함수라는 것은 임의 길이의 input x를 받아서 일정 길이의 output y를 만들어 내는 함수 $y=F(x)$로서, y를 함수값으로 갖는 어떠한 다른 x'도 찾기 힘들다는 것이다. 이러한 성질로 말미암아 작은 길이의 y가 큰 길이의 x를 거의 유일하게 대표할 수 있는 것이다.

이제 일방해쉬함수에 대한 보다 수학적인 정의를 내리기 위하여 $V=\{0, 1\}$로 두고, $V^1 \cup V^2 \cup \cdots \cup V^m$, $V^1 \cup V^2 \cup \cdots$를 각각 V_m, V_∞로 나타내기로 한다. 단, V^k는 V의 k-fold Cartesian곱을 나타낸다.

정의 1. 함수 $h : V_\infty \to V^k$에 대하여, $h(x)=h(x')$되는 $x \neq x'$를 발견하는 일이 계산상 불가능할 때, h를 계산상 일대일 (*computationally one to one*)이라 하고, 이런 string의 쌍 x, x'를 h에 대한 충돌쌍(*colliding pair*)이라 한다.

정의 2. 함수 $h : V_\infty \to V^k$가 다음 조건

(1) 임의의 string $x \in V_\infty$이 주어졌을 때, h(x)는 쉽게 계산된다.

(2) x와 그 함수값 h(x)가 주어졌을 때, $h(x)=h(x')$되는 $x \neq x'$를 발견하는 일은 계산상 불가능하다 (computationally infeasible)

를 만족할때, h를 (k-bit) 일방해쉬함수(*one way hash function*)라 하고, 계산상 일대일인 일방해쉬함수를 충돌회피(*collision free*) 일방해쉬함수라 한다.

* 慶北大學校 副教授
** 서울大學校 助教授

2. 디지탈 서명용 해쉬함수

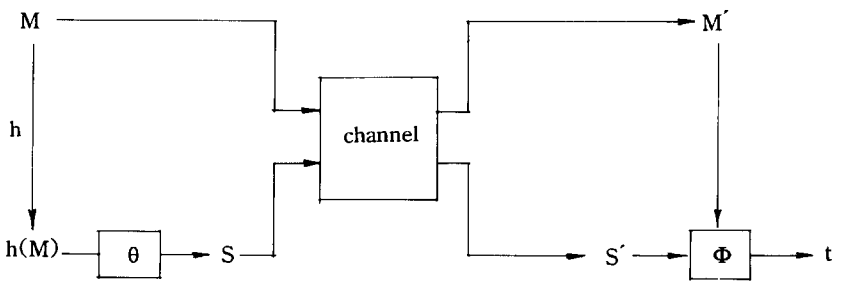
메세지 인증은 전달된 메세지가 공격받지 않은 원래 그대로의 메세지임을 보증하는 기능이다. 이는 사용자 A가 상대자에게 메세지를 보낼 때, 그가 바로 A임을 보증하는 기능으로 인증기능으로서의 가치를 갖게 하기 위해서

1. 수신자 B도 제삼의 사용자 C에게 A임을 증명할 수 없어야 할 것

2. 수신자 B는 B자신에게 조차도 사용자가 A임을 증명할 수 없어야 할 것

와 같은 제약조건을 둔다. 이 인증의 방법의 하나로 디지탈서명이 있다. 디지탈서명은 해쉬함수를 이용하여 다음과 같이 한다.

메세지 M의 서명자는 서명키 e와 해쉬함수 h 및 서명생성 함수 Θ를 써서 서명 S=Θ(e, h(M))를 생성하고, 메세지 M과 서명 S를 수신자에게 보낸다. 여기서 해쉬함수는 압축된 메세지 H=h(M)을 생성하므로 Θ의 계산량을 줄여주므로 디지탈서명의 효율화를 도모하게 한다. 수신자는 검증키 d와 서명검증함수 Φ를 써서 t=Φ(d, S, h(M))로 두고, 서명이 옳으면 t=True, 옳지 않으면 t=False를 출력한다.



3. 해쉬함수의 기본 요건

디지탈 서명용 해쉬함수는 서명의 효율화를 기함이 목적이므로 컴퓨터가 용이하게 계산할 수 있어야 하며 아울러 내외적 부정을 방지할 수 있다는 의미에서 안전해야 한다. [IJSW]에서는 string의 길이를 축약하는 함수 $h : V_\infty \rightarrow V^k$가 해쉬함수로서 가치를 갖기 위한 요구조건으로서 효율성, 일방향성, 충돌회피성을 제안하고 있다. 이들은 각각 다음과 같다.

가) : 계산효율이 좋을 것

나) 일방향성 (약)(one-wayness, waek) :

해쉬값 H로 부터 h(M)=H되는 메세지 M을 역산하는 일은 계산상 불가능하다.

다) 일방향성 (강)(one-wayness, strong) :

어떤 메세지 M과 그 해쉬값 H가 주어졌을 때, h(M′)=H되는 메세지 M′≠M을 찾는 일은 계산상 불가능하다.

라) 충돌회피성(collision freeness) :

h(M)=h(M′)되는 메세지 M≠M을 찾는 일은 계산상 불가능하다.

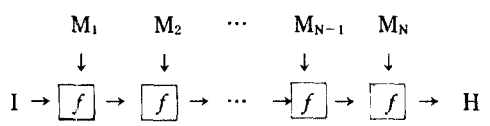
여기서 가)는 해쉬함수의 성능조건을 말하고, 나), 다), 라)는 해쉬함수의 안전성에 대한 제약이다. 안전성조건 나), 다)는 피압축메세지 H가 나왔을 때, 원래의 메세지 M을 역산 내지는 변조하는 일을

방지하기 위한 기능을 갖게 하기 위함이고, 라)는 이를테면 송신자가 처음 M을 보내놓고 나중에 M′를 보냈다고 주장하는 부정, 이른바 내부부정을 방지하기 위한 제약으로서 ISO/DP10118에서는 이것을 해쉬함수의 요구조건 중 가장 중요한 것으로 규정하고 있다.

4. 해쉬함수의 구성

임의의 길이의 string을 축약하는 일반적인 법칙을 설정하기는 지극히 어려우므로, 해쉬함수 h : $V_\infty \rightarrow V^k$는 보통 하나의 기초함수 $f : V^{m+k} \rightarrow V^k$를 바탕으로 다음과 같이 귀납적으로 정의한다.

1. 메세지 M을 m-bit string의 concatenation으로 나타낸다. : $M = M_1 \| M_2 \| \cdots \| M_N$. 여기서 필요하다면 적당한 길이의 00…0을 달아 M_N을 m-bit string으로 만든다.
2. $H_0 = I$를 초기치로 잡는다.
3. $H_i = f(M_i, H_{i-1})$ $(i = 1, 2, \cdots, N)$
4. $H = h(M, I) = H_N$ (해쉬값).



여기서 기초함수 f는 이를테면 1) $f(X, Y) = eX(Y)$, 또는 2) $f(X, Y) = eY(X)$ 내지는 이들의 변형된 함수로 잡는다. 단, $eK(M)$은 메세지 M을 키 K로 암호화한 것을 나타내며 atomic operation이라 부른다.

다음 정리는 해쉬함수와 그것의 기초함수 사이의 관계를 나타내는 중요한 결과로서 이로부터 안전한 해쉬함수의 구성에는 안전한 기초 일방함수의 구성이 필수적인 요건임을 알 수 있다.

정리 1. h가 f를 기초함수로 하는 해쉬함수라 할때, h가 충돌회필일 필요충분조건은 f가 충돌회피일 것이다.

증명 f가 충돌회피 함수라 하자. $N = 1$일 때는 명백히 h도 충돌회피 해쉬함수이다. 귀납법을 사용하기 위하여 $N-1$까지에 대하여 정리가 성립한다고 가정하자. 이제 메세지 $M' = M_1' \| M_2' \| \cdots \| M_N'$에 대하여 $H_N = H_N'$이라고 하면, $f(M_N, H_{N-1}) = f(M_N', H_{N-1}')$ 즉 $f(M_N, h(M_1 \| M_2 \| \cdots \| M_{N-1})) = f(M_N', h(M_1' \| M_2' \| \cdots \| M_{N-1}'))$. f의 충돌회피성으로 부터 $M_N = M_N'$ 및 $h(M_1 \| M_2 \| \cdots \| M_{N-1}) = h(M_1' \| M_2' \| \cdots \| M_{N-1}')$가 성립한다. 귀납법 가정으로 부터 $M_1 \| M_2 \| \cdots \| M_{N-1}) = M_1' \| M_2' \| \cdots \| M_{N-1}'$. 그러므로 $M = M'$이어야 한다. 따라서 해쉬함수는 h는 충돌회피 함수임이 증명되었다.

역으로 f에 대한 충돌쌍 M_1', M_1이 쉽게 발견되었다 하면 임의의 자연수 N에 대하여 메세지 $M_1 \| M_2 \| \cdots \| M_N$, $M_1' \| M_2' \| \cdots \| M_N'$는 h에 대한 충돌쌍이 되므로 h는 충돌회피 함수가 아니게 된다. ‖‖‖

보다 안전한 해쉬함수의 구성을 위하여, 위에서와 같이 정의된 함수 h를 바탕으로 다음과 같이 새로운 함수 g를 정의하는 방법을 생각할 수 있다. $\gamma : V_\infty \rightarrow V^m$을 계산상 일대일 함수라 하자. 이를테면 M의 길이를 $\gamma(M)$으로 생각할 수 있다. 이제 $M \in V_\infty$에 대하여 $g(M) = f(\gamma(M), h(M))$으로 함수 g를 정의한다.

정리 2. γ 또는 h 중 적어도 하나가 충돌회피이고 f가 충돌회피라고 하면, $g(M) = f(\gamma(M), h(M,))$으로 정의된 함수 g는 충돌회피이다.

증명 $g(M) = g(M')$를 만족하는 M, M′가 발견되었다면 $f(\gamma(M), h(M)) = f(\gamma(M'), h(M'))$이다. f가 충돌회피이므로 $(\gamma(M), h(M)) = (\gamma(M'), h(M'))$, 즉 $\gamma(M) = \gamma(M')$, $h(M) = h(M')$. 이제 γ 또는 h 중 적어도 하나가 충돌회피이라는 사실로부터 $M = M'$가 된다. 따라서 g는 충돌회피 함수이다. ‖‖‖

이와같이, 기초함수의 안전성은 그를 바탕으로 정의된 해쉬함수의 안전성에 직결되어 있는 것이다. 뿐만 아니라 다음 정리에서 보는 바와 같이 충돌회피인 기초 일방함수가 하나 있으면 이를 바탕으로 임의 길이 메세지를 축약하는 충돌회피 일방해쉬함수를 만들 수 있다.

정리 3. 충돌회피 일방해쉬함수 $f: V^{m+k} \to V^k$가 주어져 있다면, 임의의 자연수 i에 대하여 충돌회피 일방해쉬함수 $F: V^{m+k+i} \to V^k$를 만들 수 있다.

증명 $f: V^{m+k} \to V^k$를 주어진 충돌회피 일방해쉬함수라 하자. 자연수 n=1, 2, … 에 대하여 함수 $F_m: V^{nm+k} \to V^k$을 다음과 같이 점화식을 써서 정의한다.

$F_1(M, I) = f(M, I)$,

$F_m(M_1 \| M_2 \| \cdots \| M_N, I) = f(M_N, F_{n-1}(M_1 \| M_2 \| \cdots \| M_{N-1}, I))$ $(n=2, 3, \cdots)$.

단, 각 M_i m-bit이다. 이제 정리를 i가 m의 배수일 때와 그렇지 않을 때의 두가지로 나누어 증명한다.

경우 1 : i가 m의 배수일 때.

$i=(N-1)m$이라 하면 $F_N: V^{Nm+k} \to V^k$가 되므로 F를 F_N으로 잡을 수 있다. 이제 F_N이 충돌회피 일방해쉬함수임을 보이면 된다. 그러나 이것은 정리 1로 부터 바로 알 수 있는 사실이다.

경우 2 : i가 m의 배수가 아닐 때.

$i=(N-1)m+r$ $(0<r<m)$라 하고 $M' \in V^{m+i}$라 하자. $M'=M_1 \| M_2 \| \cdots \| M_N \| E$(단, E는 r-bit)라고 할 때, $M=M_0 \| M_1 \| \cdots \| M_N \| M_{N+1}$ (단, $M_0=1^{m-r} \| 0^r$, $M_{N+1}=E \| 0^{m-r}$이고 여기서 u^t은 u로 된 t-bit string uu…u을 나타낸다.)로 두면 (m+k+i)-bit string (M', I)는 ((N+1)m+k)-bit string (M, I)로 확장된다. 이제 $F(M', I)=F_{N+2}(M', I)$로 정의하면 경우 1에서와 마찬가지로 F는 충돌회피 일방해쉬함수가 된다. ‖‖‖

5. 해쉬함수의 안전성

디지탈 서명 scheme의 기본적인 특성은 첫째 각 메세지 M은 그것의 서명 S와 함께 전송된다는 것과 둘째 서명 scheme은 $f(S)=M$을 만족하는 트랩도어 함수 f를 토대로 하고 있으며 전송자만이 이 함수 f를 역산하는 트랩도어 정보를 가지고 서명을 구할 수 있다는 것이다. 이러한 서명 scheme에 대한 공격법으로 중요한 것으로는, Direct attack, Known Message attack, Generic chosen-message attack, Directed chosen-message attack, Adaptive chosen-message attack 등이 있다[GMR]. 한편 서명 scheme 자체를 무의미하게 만드는 경우로는 Totalbreak(송신자의 트랩도어 정보(비밀키)가 유출된 경우),

Universal forgery(공격자가 송신자의 서명 알고리즘과 같은 효과를 가진 능률적인 서명 알고리즘을 발견할 수 있는 경우, 이를테면 공개키를 factoring하지 않고 RSA 함수를 계산할 수 있게 되는 경우)

Selective forgery(공격자가 미리 선택한 메세지의 서명을 위조할 수 있는 경우)

Existential forgery(공격자가 적어도 하나의 메세지의 서명을 위조할 수 있는 경우) 등이 있다.

위에 언급한 의미로 서명 scheme이 깨어졌다고 하는 것은 무시할 수 없는 정도의 확률로 위의 경우 중 하나가 발생했다는 것을 뜻한다. 그러나 서명 scheme의 파괴정도는 공격법과 병행하여 언급될 문제이지 일률적으로 이 scheme은 깨어져서 못쓴다고 말할 수 있는 성질의 문제가 아니다. 이를테면 RSAScheme을 사용한 서명 시스템에 있어서, (M_1, S_1), (M_2, S_2)가 동일인이 서명한 메세지라면 S_2 S_2는 M_1 M_2의 서명임을 쉽게 증명할 수 있으므로, RSA Scheme은 Directed chosen-message attack를 써서 Selectively forgeable하다.

- Meet-in-the-middle 공격

앞서 언급한 바와 같이 해쉬함수에 관련된 주된 문제는 첫째 계산이 용이할 것과 둘째 안전한 해쉬함수의 구성 문제이다. 서명 시스템의 안전성의 문제는 결국 해쉬함수의 안전성의 문제로 귀착된다. 위의 첫째 문제는 빠른 속도의 칩(이를테면

DES[Dat])이 제작되어 있는 비밀키 블락암호 알고리즘을 써서 가능하다. 그러나 둘째 문제에 대해서는 아직 완전한 답이 없다. 해쉬함수에 대한 일반적인 몇가지의 공격법이 [Ca-Gi]에 설명되어 있다. 그중 대표적인 것으로 Yuval[Yu]의 공격과 Meet-in-the-middle[Co]공격이 있는데 이들은 이른바 유명한 "Birthday panadox"의 변형이다. 이 파라독스는 다음과 같다.

한 학급의 학생 수를 r이라 하고, 이 학급의 학생중 적어도 2명의 생일이 같을 확률을 p(r)이라 하자. $p(r)\geq 1/2$이기 위한 최소의 자연수 r은 무엇인가? 이 문제의 답은 23으로서 우리가 직관적으로 추측하는 답보다 훨씬 작은 수이다.

정리 4. [Yu] h를 주어진 k-bit 해쉬함수, S_1, S_2를 $|S_1| = |S_2| = 2^{k/2}$인 임의의 메세지의 집합이라 하면, $h(M_1)=h(M_2)$를 만족하는 $M_i \in S_i$, i=1, 2, 가 존재할 확률은 1/2이상이다.

Coppersmith[Co]는 위의 정리를 이용하여 RSA scheme을 사용하는 Rabin scheme[Ra] 및 Davies-Price scheme[Dav-Pr1]은 meet-in-the-middle 공격에 약함을 보였다. 즉 공격자는 정당한 메세지 M에 대한 서명 $f(M)=S$를 알고, 같은 서명값 $f(M')=S$를 갖는 위조 메세지 M'를, 수용할만한 정도의 회수의 trial로, 찾을 수 있다는 것이다. 다음 정리에서 우리는 imprint의 길이가 크지 않는 임의의 서명 scheme은 meet-in-the-middle 공격에 약함을 증명한다.

정리 5. 임의의 k-bit 해쉬함수에 대하여, $2^{k/2+1}$회의 trial로 충돌쌍이 발견될 확률은 1/2이상이다.

증명 $h : V_* \rightarrow V_k$를 주어진 해쉬함수라 하자. $|S_1| = |S_2| = 2^{k/2}$인 임의의 메세지의 집합S_1, S_2를 잡는다. 이런 집합은 한개의 메세지로 부터 몇개의 변조 메세지를 만들고 이들을 결합하여 쉽게 구성할 수 있다. S_1, S_2의 각 메세지에 h를 적용, imprint를 구하는데는 $2\times 2^{k/2}=2^{k/2+1}=2^{k/2}$회의 trial로 충분하다. 이제 이들 imprint들을 sorting하여 비교하면 같은 것이 있을 확률은, Yuval의 정리로부터, 1/2 이상이다. ||||

지금까지 알려진 최선의 sorting 방법을 적용할 때의 time-complexity는 O(NlogN) 알려져 있다(단, N은 프로그램 list의 크기). 그러므로 이런 종류의 공격을 무력화하기 위해서는 $k/2>32$일 필요가 있다. 따라서 $k>64$ 즉, imprint를 128-bit 이상으로 함이 요구된다.

- Atomic operation의 특성에 의한 공격

지금까지 제안된 해쉬함수의 기초 함수에 있어서 연산의 핵심이 되는 atomic operation으로서는 보통 다음과 같이 공개키 시스템이 사용되고 있다.

1. RSA system,
2. FEAL system,
3. Knapsack problem based system,
4. Modular squaring based system,
5. Discrete logarithm based system,
6. Error correcting code based system.

대칭블락암호키 e(예 : DES)를 atomic operation으로 하는 해쉬함수에 있어서는 다음과 같은 약점으로 인하여 충돌쌍이 쉽게 발견되기도 한다.

e의 보수속성 (Complementary property) : $e\underline{K}(\underline{M})=\underline{e}k(\underline{M})$ 단, $\underline{X}$는 X의 보수.

e의 weak key property : $eK_1(eK_2(M))=M$ 단, $K_1=K_2$ 또는 $K_1\neq K_2$.

참 고 문 헌

[Ca-Gi] M. Campana and M. Girault, *Comment utiliser les fonctions de condensation dans la protection des données*, SECUROCOM 1988, 91-110.

[Ca-We] Carter and Wegman, *Universal clases of hash functions*, *J.* Computer and system Sci. 18 (1979), 91-110.

[Co] D. Coppersmith, *Another birthday attack*,

Advances in cryptology, Proc. of Crypto '85, LNCS 128, Springer (1986), 14-17.

[Dam] I.B. Damgård, *A design principle for hash functions*, Crypto'89(Abstract),

[Dat] *Data Encryption Standard*, FIPS Pub. 46, N.B.S., U.S. Dept. of Comm., Jan., 1977.

[Dav] D.W. Davies, *Applying the RSA digital signature to electronic mail*, IEEE Computer 16 No. 2(1983), 55-62

[Dav-Pr1] D.W. Davies and W.L. Price, *The application of digital signatures based on public key cryptosystems*, NPL Report DNACS 39/80, National Phisical Laboratory, Teddington, Middlesex, England, 1980.

[Dav-Pr2] D.W. Davies and W.L. Price, *Digital signatures-An update*, Proc. 7th Internat. Conference on Computer Communications, (1984), 845-849.

[Dav-Pr3] D.W. Davies and W.L. Price, *Security for computer networks*, 1983, 280.

[Di-He] W. Diffie and M.E. Hellman, *New directions in cryptography*, IEEE Trans Inform. Theory, IT22.6 (1976), 644-654.

[GMR] S. Goldwasser, S. Micali and R.L. Rivest, *A' paradoxical' solution to signature problem*, IEEE (1984), 441-448.

[Go-Ga] Godlewski and Camion, *Manipulation and errors, Localization and detection*, Proceedings of Eurocrypt'88, Springer.

[Is-Dp] ISO/DP 10118, *Hash functions for digital signatures*, (Oct. 1989 version)

[IJSW] ISO/IEC/JTC1/SC20/WG2N 118 : *Hash function for digital signatures*, Apr. 1988.

[Me] R.C. Merkle, *One way hash functions and DES*, CRYPTO'89 Abstract, Aug. 1989, to appear in the Proceedings.

[Me-Ma] C.H. Meyer and S.M. Matyas, *Cryptography : A new dimension in computer data security*, John Wiley and Sons, New York, 1982.

[MOI] S. Miyaguchi, K Ohta and M. Iwata, *128-bit hash function (N-Hash)*, NTT Review 2, 6(1990), 128-132.

[Ra] M. Rabin, *Digitalize signatures*, In R. DeMillo et al., editor, Foundation of Secure Computation, Academic Press, 1978, 155-166.

[Qu-Gil] J.J. Quisquarter and M. Girault, *2n-bit hash functions using n-bit symmetric block cipher algorithms*, EUROCRYPTO'89(Abstract)

[Qu-Gi2] J.J. Quisquarter and M. Girault, *2n-bit hash functions using n-bit symmetric block cipher algorithms*, Eurocrypto'89 for Lecture Note

[Se-Pi] Cryptography, An Introduction to Computer Security, Prentice Hall, 1989.

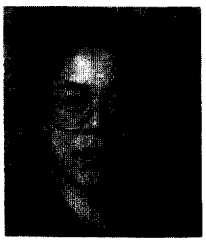
[Sha] A. Shamir, *Identity-based cryptosystems and signature scheme*, Proceedings of Crypto'84, Lecture Notes in Comp. Sci. 196, Springer, 1985.

[We] D. Welsh, Codes and Cryptography, Clarendon Press, Oxford, 1989.

[Yu] G. Yuval, *How to swindle Rabin*, Cryptologia 3 No. 3(1979), 187-189.

□ 著者紹介

黃 石 根(正會員)



1972年 2月 慶北大學校 師範大學 數學教育科 卒業(理學士)
1977年 2月 慶北大學校 大學院 數學科 卒業(理學碩士)
1985年 8月 Univ. of Wisconsin-Madison 大學院 數學科 卒業(Ph. D.)
1979年 4月～1990年 2月 慶北大學校 專任講師-助教授
1990年 3月～1991年 3月 成均館大學校 副教授
1991年 3月～現在 慶北大學校 副教授

조 한 혁(正會員)

1979年 2月 서울大學校 師範大學 數學教育科 卒業(理學士)
1981年 2月 서울大學校 大學院 數學科 卒業(理學碩士)
1988年 8月 Univ. of Wisconsin-Madison 大學院 數學科 卒業(Ph. D.)
1988年 9月～1989年 2月 Bowling Green State Univ. 專任講師
1989年 3月～현재 서울大學校 助教授