情 報 保 護 學 會 誌
第21卷 第2號, 2011. 4

ISO/IEC JTC1/SC27 WG2 (Cryptography & Security Mechanisms) 국제표준화 동향

이 필 중*

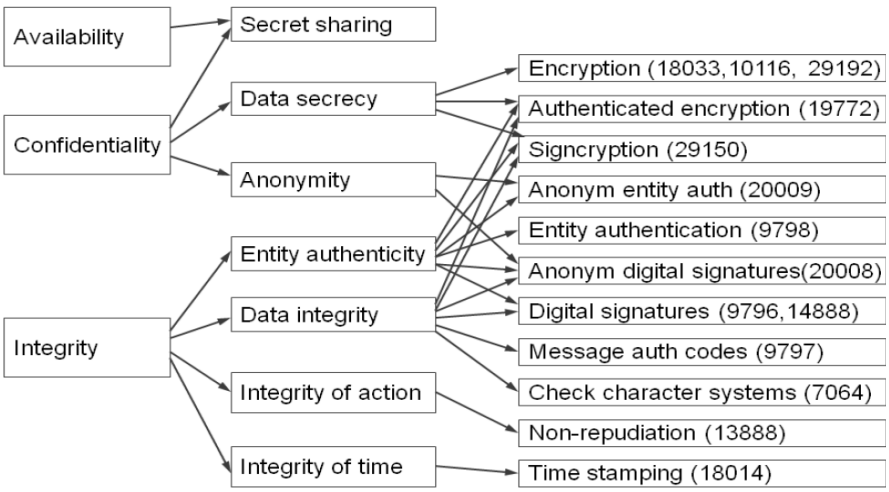
요 약

ISO/IEC JTC1/SC27 WG2의 역사 및 개요를 간단히 소개하고, 각 표준 별로 어떠한 내용인지, 어떤 기법들이 표준화되었는지를 살펴 본 후, 앞으로 WG2에서 표준화가 될 가능성이 있는 topic들을 살펴보고, 마지막으로 현재 가장 중요한 issue가 되고 있는 국제표준 암호알고리즘 선정기준에 대해 소개한다.

Ⅰ. WG2의 역사 및 개요

ISO와 IEC가 JTC1을 만들면서 암호학을 다루기 위해 SC20(Sub-Committee 20 - Data cryptographic techniques)이 만들었으나 1989년 6월 JTC1 총회에서 보다 넓은 범위의 보안 표준화를 위하여 SC27(IT security techniques)로 확대 개편하였고, WG(working group)들 중 WG2가 원래의 SC20을 계승한 "Cryptography and Security Mechanisms"라는 제목을 갖고 있다.

WG2에서는 데이터비밀성(Data secrecy), 익명성(Anonymity), 실체인증(Entity authentication), 데이터 무결성 (Data integrity), 행위 및 시간에 대한 무결성(Integrity)을 포함한 여러 보안 목표 자체 이루기 위해 필요한 표준들(그림 1 참조)과 이들 보안 목표를 이루는 것을 돕기 위한 표준들(그림 2 참조)을 만들고 있다. 2절에서부터는 해당 각 표준 별로 간단히 살펴보겠다.



〔그림 1〕 보안 목표 및 표준 기법들과의 관련성

* 포항공과대학교 전자전기공학과 (pjl@postech.ac.kr)

Ⅱ. 암호화 알고리즘 관련 표준들

2.1 ISO/IEC 18033 – Encryption algorithms

- ► Part 1: General (1ed 2005) - 암호알고리즘의 일반 개념, 용어 및 암호알고리즘 선정기준을 설명.
- ► Part 2: Asymmetric ciphers (1ed 2006) – 비대칭 암호알고리즘들인 ECIES-KEM, PSEC-KEM, ACE-KEM, RSAES, RSA-KEM, HIME(R)들이 표준화되었음.
- ► Part 3: Block ciphers (1ed 2005, 2ed 2010) – 원래는 64-bit block cipher들인 TDEA, MISTY1, CAST-128과 128-bit block cipher들인 AES, Camellia, SEED가 포함되어 있었으나, 2nd edition에는 본인이 editor가 되어 64-bit block cipher인 HIGHT를 추가하였음. 이들 중 SEED와 HIGHT는 한국의 알고리즘들임.
- ► Part 4: Stream ciphers (1ed 2005, Amd1 2009, 2ed FCD 투표 중) - MUGI, SNOW 2.0이 먼저, Rabbit, DECIMv2가 Amendment_1에 추가되었고, K2를 추가하기 위해 2nd edition이 진행 중. 그러나 BE를 중심으로 몇 NB(national body)들에서 ECRYPT-II의 주장을 바탕으로 잘 알려지지 않은 K2를 추가하지 말고 차라리 eStream에서 선정된 stream cipher들을 추가하라고 주장하는 중.

2.2 ISO/IEC 10116 – Modes of operation for an n-bit block cipher algorithm

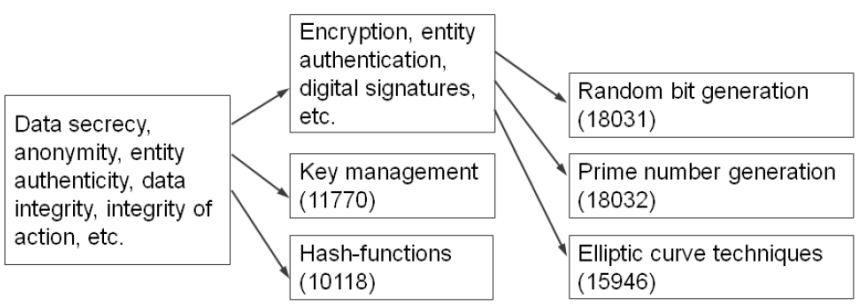
(1ed 1991, 2ed 1997, 3ed 2006) ECB(electronic codebook), CBC(cipher block chaining), CFB (cipher feedback), OFB(output feedback) mode들이 먼저 표준화 되었다가 3rd edition에 CTR(counter) mode가 추가되었음.

2.3 ISO/IEC 29192 – Lightweight cryptography

- ► Part 1: General (1ed 2CD 투표 중) - 경량암호알고리즘의 일반 개념, 용어를 설명함. 그러나 경량의 개념에 대한 논쟁이 끝나지 않았음.
- ► Part 2: Block ciphers (1ed FCD 투표 중) – 64-bit block cipher인 PRESENT와128-bit block cipher인 CLEFIA를 표준화하는 중.
- ► Part 3: Stream ciphers (1ed 1CD 투표 중) – Enocoro-128v2, Enocoro-80, Trivium을 표준화하는 중. 18033-4에서와 같이 몇 NB들에서 eStream에서 선정된 stream cipher들을 추가하라고 주장하는 중.
- ► Part 4: Mechanisms using asymmetric techniques (1ed 1CD 투표 중) - DL(EC)—based의 cryptoGPS, encryption-based의 ALIKE, 그리고 identity-based 기법 하나를 표준화하는 중.

2.4 ISO/IEC 19772 – Authenticated encryption

(1ed 2009) 무결성과 기밀성을 동시에 제공하는 기법들인 OCB2.0(offset codebook version 2), Key Wrap, CCM(counter with CBC-MAC), EAX, Encrypt-then-MAC 및 GCM(Galois/counter mode) 가 표준화되었음.



〔그림 2〕 보조 기법 표준들

2.5 ISO/IEC 29150 – Signcryption

(1ed 2FCD 투표 중) 부인봉쇄와 기밀성을 동시에 제공하는 DLSC(discrete logarithm based signcryption mechanism), ECDLSC(elliptic curve DLSC), IFDC (integer factorization based signcryption mechanism), EtS(encrypt-then-sign based mechanism)의 4개의 기법들을 표준화하는 중.

Ⅲ. 실체 인증 관련 표준들

3.1 ISO/IEC 9798 – Entity authentication

- ► Part 1: General (1ed 1991, 2ed 1997, 3ed 2010) - 실체인증의 일반 개념 및 용어를 설명.
- ► Part 2: Mechanisms using symmetric encipherment algorithms (1ed 1994, 2ed 1999, 3ed 2008) – 1-pass 및 2-pass의 unilateral authentication, 2-pass 및 3-pass의 mutual authentication 그리고 4-pass 및 5-pass의 mechanism involving a trusted third party의 총 6개의 기법들을 표준화했음.
- ► Part 3: Mechanisms using digital signature techniques (1ed 1993, 2ed 1998, Amd1 2010) – 1-pass 및 2-pass의 unilateral authentication, 2-pass, 3-pass 및 4-pass 의 mutual authentication 그리고 2가지 5-pass의 mechanisms involving a trusted third party의 총 7개의 기법들을 표준화했음.
- ► Part 4: Mechanisms using a cryptographic check function (1ed 1995, 2ed 1999) - 1-pass 및 2-pass의 unilateral authentication, 2-pass 및 3-pass의 mutual authentication의 총 4개의 기법들을 표준화했음.
- ► Part 5: Mechanisms using zero knowledge techniques (1ed 1999, 2ed 2004, 3ed 2009) – Mechanisms based on (m.b.o.) identities (Fiat-Shamir, GQ1), m.b.o. integer factorization (GQ2), m.b.o. discrete logarithms with respect to (w.r.t.) prime numbers (Schnorr), m.b.o. discrete logarithms w.r.t. composite numbers (GPS1, GPS2), m.b.o. asymmetric encryption systems (Brandt, Damgard, Mitchell, Yuen), m.b.o. discrete logarithms w.r.t. elliptic curves (EC-GPS)의 총 11개의 기법들을 표준화했음.
- ► Part 6: Mechanisms using manual data transfer (1ed 2005, 2ed 2010) - 4 Mechanisms using a manual transfer of a short digest-value or a short key (One device with simple input, one device with simple output / One device with simple input, one device with simple output / Devices with simple input capabilities / Devices with simple input capabilities), 그리고2 Mechanisms using a MAC (Devices with simple output capabilities / One device with simple input, one device with simple output) 이렇게 총 8개의 기법들을 표준화했음.

3.2 ISO/IEC 20009 – Anonymous entity authentication

- ► Part 1: General (1ed 2WD 검토 중) – 익명성을 보장하는 실체인증의 일반 개념 및 용어를 설명.
- ► Part 2: Mechanisms based on anonymous digital signature schemes (1ed 2WD 검토 중) – ISO/IEC 20008-2에서 개발될 익명 디지털 서명을 사용하여 익명 실체인증을 하는 기법을 표준화하는 중. 본인이 현재 co-editor를 맡고 있음.

Ⅳ. 메시지 인증 관련 표준들

4.1 ISO/IEC 9797 – Message authentication codes (MACs)

- ► Part 1: Mechanisms using a block cipher (1ed 1989, 2ed 2011) - 블럭암호를 사용하여 MAC을 만드는 6개의 기법들을 표준화했음.
- ► Part 2: Mechanisms using a dedicated hash-function (1ed 2002, 2ed 2011) – HMAC, MDx-MAC, MDx-MAC optimized for short inputs의 총 3개의 기법들을 표준화했음.
- ► Part 3: Mechanisms using a universal hash-

function (1ed FCD 투표 중) – UMAC, Badger, Poly1305-AES, GMAC의 총 4개의 기법들을 표준화하는 중.

4.2 ISO/IEC 7064 – Check character system

(1ed 1983, 2ed 2003) 비암호학적인 방식으로 메시지인증을 주는 간단한 방식을 표준화했음.

Ⅴ. 디지털서명 관련 표준들

5.1 ISO/IEC 9796 – Digital signature schemes giving message recovery

- Part 1: Mechanisms using redundancy (1ed 1983, Withdrawn 2000) – 가장 빨리 표준화되었던, 잉여를 사용한 복원형 서명 표준은 안전도가 문제가 되어 2000년도에 철회되었음.
- Part 2: Integer factorization based mechanisms (1ed 1983, 2ed 2002, 3ed 2010) – 특별히 이름을 붙이지 않은 총 3개의 (부분)복원형 디지털서명 기법들을 표준화했음. 그 중 2번째의 것은 PSS-R이라고도 불리는 것으로 IEEE P1363a에서는 EMSR라고도 함.
- Part 3: Discrete logarithm based mechanisms (1ed 2000, 2ed 2006) – Nyberg-Rueppel (NR), ECNR, EC Miyaji (ECMR), EC Abe-Okamoto (ECAO), EC Pintsov-Vanstone (ECPV), ECK-CDSA/NR(ECKNR)의 총 6개의 기법들을 표준화했음. 마지막 것은 ECKCDSA를 바탕으로 NR 기법을 변형하여 한국의 것임.

5.2 ISO/IEC 14888 – Digital signatures with appendix

- Part 1: General (1ed 1998, 2ed 2008) – 부가형 디지털서명의 일반 개념, 용어를 설명.
- Part 2: Integer factorization based mechanisms (1ed 1999, 2ed 2008) – RSA, RW (Rabin-Williams), GQ1, GQ2, GPS1, GPS2, ESIGN의 총 6개의 기법들을 표준화하고 있음.
- Part 3: Discrete logarithm based mechanisms (1ed 1998, 2ed 2006, Amd1 2010) – DSA, K-CDSA, Pointcheval/Vaudenay algorithm, ECDSA, EC-KCDSA, EC-GDSA, IBS-1, IBS-2, EC-RDSA, Schnorr DSA (SDSA), EC-SDSA 등 총 11개의 기법들을 표준화하고 있음. 본인이 2ed의 co-editor 이었고, 그 때 한국의 KCDSA, ECKCDSA, 및 IBS-2를 포함시켰음.

5.3 ISO/IEC 20008 – Anonymous digital signatures

- Part 1: General (1ed 2WD 검토 중) – 익명성을 보장하는 디지털서명의 일반 개념 및 용어를 설명.
- Part 2: Mechanisms using a group public key (1ed 2WD 검토 중) – 그룹 디지털 서명을 만드는 여러 기법들을 표준화하는 중. 한국에서 개발한 기법도 하나 포함하고 있음.

Ⅵ. 행위 및 시간 인증 관련 표준들

6.1 ISO/IEC 13888 – Non-repudiation

- Part 1: General (1ed1997, 2ed 2004, 3ed 2009) - 부인봉쇄의 일반 개념 및 용어를 설명.
- Part 2: Mechanisms using symmetric techniques (1ed 1998, 2ed 2010) – 대칭키암호를 사용하여 origin 및 delivery에 대한 부인봉쇄기법들과, time-stamping token을 얻는 기법을 표준화했음.
- Part 3: Mechanisms using asymmetric techniques (1ed 1997, 2ed 2009) – 비대칭키암호를 사용하여, origin, delivery, submission, transport에 대한 부인봉쇄기법들을 표준화했음.

6.2 ISO/IEC 18014 – Time stamping services and protocol

- Part 1: Framework (1ed 2002, 2ed 2008) – Time stamping service의 체계 및 용어를 설명.
- Part 2: Mechanisms producing independent tokens (1ed 2002, 2ed 2009) – 디지털서명이나

MAC을 사용하여 연결성이 없는 token을 시각인증용으로 발행하고 검증하는 기법을 표준화했음.

- Part 3: Mechanisms producing linked tokens (1ed 2004, 2ed 2009) – TSA(time stamping authority)를 서로 연결된token을 시각인증용으로 발행하고 검증하는 기법을 표준화했음.

Ⅶ. 보조 기법 표준들

7.1 ISO/IEC 11770 – Key management

- Part 1: Framework (1ed 1996, 2ed 2010) – 키 관리의 체계 및 용어를 설명.
- Part 2: Mechanisms using symmetric techniques (1ed 1996, 2ed 2008) – 대칭키암호방식을 이용하여 Point-to-point key establishment 기법 6개, Mechanisms using a Key Distribution Centre 4개, Mechanisms using a Key Translation Centre 3개를 표준화했음.
- Part 3: Mechanisms using asymmetric techniques (1ed 1999, 2ed 2008) – 비대칭키암호방식을 이용하여 secret key agreement 기법 11개, secret key transport 기법 6개, 그리고 public key transport를 TTP(trusted third party)를 이용하여 얻는 기법과 TTP를 이용하지 않고 얻는 기법을 표준화했음.
- Part 4: Mechanisms based on weak secret (1ed 2006) – Password-authenticated key agreement management 3개 및 Password-authenticated key retrieval management 1개를 표준화했음. IEEE P1363.2에서는 이들을 각기 BPKAS-SPEKE, DLAPKAS-SRP6, APKAS-AMP, PKRS-1라 불리며, AMP 기법은 한국의 것임.
- Part 5: Group key management (1ed FCD 투표중) – 한 그룹이 공유하는 키를 만든 기법으로 Tree based Key Establishment Mechanisms for Multiple Entities, Key Chain based Group Key Management(KCbKM), KCbKM with Unlimited Forward Key Chain, KCbKM with Limited Forward Key Chain, Key Chains with Tree based Key Distribution 의 5가지 기법을 표준화하고 있음.

7.2 ISO/IEC 10118 – Hash-functions

- Part 1: General (1ed 1994, 2ed 2000) – 해쉬함수의 일반 사항들 및 용어를 설명.
- Part 2: Hash-functions using an n-bit block cipher algorithm (1ed 1994, 2ed 2000, 3ed 2010) – 블록암호알고리즘을 이용하여 4가지 해쉬함수를 만드는 기법을 표준화했음.
- Part 3: Dedicated hash-functions (1ed 1998, 2ed 2003, 3ed 2004, Amd1 2006) – RIPEMD-160, RIPEMD-128, SHA-1, SHA-256, SHA-512, SHA-384, WHIRLPOOL, SHA-224의 총 8개의 해쉬함수들을 표준화했음.
- Part 4: Hash-functions using modular arithmetic (1ed 1998) – 이왕 HW로 modular연산기를 만들어 놓은 경우 이를 이용하여 해쉬함수를 만들어 사용하면 좋겠다는 생각에 2가지 기법을 표준화했음.

7.3 ISO/IEC 18031 – Random bit generation

(1ed 2005, 2ed 2FCD 투표 중) RBG (random bit generator)의 model과 type들, 그리고 NRBG (non-deterministic RBG) 및 DRBG (deterministic RBG)의 요구사항들을 서술하고, test방법들, 그리고 Hash_DRBG (hash-function DRBG), CTR_DRBG, OFB_DRBG, Dual_EC_DRBG (dual elliptic curve DRBG), MS_DRBG (Micali Schnorr DRBG)의 기법들을 표준화하는 중

7.4 ISO/IEC 18032 – Prime number generation

(1ed 2005) Miller-Rabin, Frobenius-Grantham, Lehmann의 3가지 probabilistic primality test, 그리고 Elliptic Curve Primality Certificate와 Primality Certificate Based on Maurer's Algorithm을 이용한 2가지 Deterministic Primality Verification Methods 및 이들을 이용한 Prime Number Generation 기법들을 표준화했음

7.5 ISO/IEC 15946 – Cryptographic techniques

- Part 1: General (1ed 2002, 2ed 2008) – 타원곡

선 자체 및 타원곡선기반 암호학의 일반 사항들 및 용어를 설명.

- Part 2: Digital Signatures (1ed 2002, Withdrawn 2007) - 여기에 들어있던 (EC-KCDSA를 포함한) 타원곡선기반 부가형서명기법들을 ISO/IEC 14888-3의 개정 시 ISO/IEC 14888-3에 포함시켰고, ISO/IEC 14888-3의 2ed가 출판된 후 Withdrawn.
- Part 3: Key establishment (1ed 2002, Withdrawn 2008) - 여기에 타원곡선기반 키 설립 기법들을 ISO/IEC 11770-3 개정 시 ISO/IEC 11770-3에 포함시켰고, ISO/IEC 11770-3의 2ed가 출판된 후 Withdrawn.
- Part 4: Digital Signatures with Message Recovery (1ed 2004, Withdrawn 2007) - 여기에 들어있던 (ECKNR를 포함한) 타원곡선기반 복원형서명기법들을 ISO/IEC 9796-3의 개정 시 ISO/IEC 9796-3에 포함시켰고, ISO/IEC 9796-3의 2ed이 출판된 후 Withdrawn.
- Part 5: Elliptic curve generation (1ed 2009) - 어떻게 안전하게 타원곡선 파라미터들을 설정하고 타원곡선을 만들고, 안정성을 검증하는 가에 대한 기법들을 표준화했음

Ⅷ. Study Period에 있거나 향후 표준화될 가능성이 있는 과제들

아직 정식 과제가 되지는 않았으나 그럴 가능성이 있는 topic들이 study period에 있거나 roadmap에 list되어 있다. 그들은 다음과 같다.

- Blind signature
- Identity-based cryptosystem
- Certificateless (or token-based) cryptosystem
- Cryptosystem allowing flexible access
- Secret sharing schemes
- Threshold cryptography
- Protection against side channel attacks
- Evaluation of lightweight algorithms
- Hyper-elliptic curve cryptography
- Lattice-based public-key cryptography
- Cryptographic techniques for digital right management
- Broadcast Encryption
- Achieving long-term security with unconditional schemes
- Quantum cryptography

Ⅸ. 기타 중요 사항 - 국제표준 암호알고리즘 선정 기준

지난 2010년 10월 베를린에서 열린 WG2 회의에서 중요한 결정이 있었다. 원인은 ECRYPT II에서 수년간 stream cipher의 전문가 100여명 이상 모여 제안하고 검토하고 판단하여 7개의 stream cipher를 골라 놓았는데 그 중 18033-4와 29192-3에는 하나씩만 포함되어 있고, eStream에서 고려되었다가 탈락된 Decim_v2나 stream cipher의 전문가들에게 잘 알려지지도 않아 충분한 검토를 받지 못한 K2가 포함되는 것은 말이 되질 않는다며 이들 대신 자신들이 고른 stream cipher들을 표준화 해 달라는 협력문서 LS(liaison statement)를 보내왔기 때문이었다. 이 LS 처리를 위해 모인 자리에서 18033-1의 Annex A에 있는 selection criteria 가 informative인 것에 불만이었던 사람들의 목소리가 커졌고, 현재 표준화된 것들이 과연 잘 결정된 것이냐는 의문들을 표시하는 사람들이 많았다. 제안 당시에만 깨어지지 않았다고 해서 표준을 제정한다면 몇 년 못 가서 그 표준을 폐기하는 일이 발생하게 되어 표준의 공신력에 손상이 간다며, 충분한 기간 동안 충분한 검토를 거친 것 소위 mature하고 안전한 것만 표준으로 해야 한다는 원칙론이 강조되었다. 한편 새로 선정되는 기준도 잘 만들어져야 하겠지만, 국제적인 사용이 (거의) 없는 표준이라면 빼도 무방하지 않겠느냐는 의견도 있었고 받아들이는 분위기였다. 결론적으로 “Criteria for the standardization of encryption algorithms”이란 제목의 study period를 갖기로 했고, 구체적인 문항을 만들어 각 NB(national body)들에게 답을 달라는 요청이 있었고, 그 답들을 가지고 이번 4월 싱가포르에서 열릴 WG2 회의에서 토의할 예정이다. Stream cipher에서 시작된 암호알고리즘 선택 논의가 block cipher를 포함하는 것으로 되어 우리나라에서 표준화 한 SEED나 HIGHT에도 영향을 미칠 수 있을 것으로 판단되며, 추

후에는 hash, MAC, 키교환 기법, 서명 기법들로 모두 확산이 될 수도 있을 것이다. 따라서 기존에 우리나라에서 만들어 표준화 해 놓은 알고리즘이나 기법들을 국제표준으로 유지시키기 위해 우리나라 안에서의 활용도를 높이고, 국제적으로도 많이 사용하게 만드는 노력에 게을리 하지 말아야 하겠다.

X. 결 론

본고에서는 ISO/IEC JTC1/SC27의 WG2 (Cryptography & Security Mechanisms)의 역사 및 개요, 그리고 각 표준에 어떤 알고리즘들이 들어있는지 등을 살펴보았고, 앞으로 다루어질 가능성이 있는 주제들도 알아보았다. 그리고 현재 한국에서 만든 암호알고리즘 2개, 디지털서명알고리즘 4개, 키교환기법 1개가 표준화되어 있고, 익명서명기법 1개를 표준화하는 중인데, 새로 표준을 만드는 것도 중요하지만 만들어진 표준을 널리 사용하게 만드는 것 역시 중요하다는 것을 최근 이슈가 된 국제표준 암호알고리즘 선정기준 관련 논의를 보면서 다시 한 번 강조하고자 한다.

〈著者紹介〉

이 필 중 (Pil Joong Lee)
종신회원

1974년 2월: 서울대학교 전자공학과 졸업
1977년 3월: 한국대학교 전자공학과 석사
1982년 6월: U.C.L.A System Science. Engineer
1985년 6월: U.C.L.A Electrical Engineering. Ph.D
1980년 3월~1985년 8월: Jet Propulsion Laboratory. Senior Engineer
1985년 8월~1990년 2월: Bell Communication Research. M.T.S
1990년 2월~현재: 포항공과대학교 전자전기공학과 교수
1996년 2월~1997년 2월: NEC Research Institute 방문 연구원
2000년 9월~2003년 8월: 포항공과대학교 정보통신 연구소장 (정보통신대학원장 겸임)
2004년 1월~2004년 12월: 한국정보보호학회 회장
2004년 1월~2004년 12월: KT 정보보호 자문위원
2008년 7월~2008년 12월: POSDATA 정보보호 자문위원
2007년 1월~현재: 한국공학한림원 정회원
관심분야 : 정보보호 전반