이 력 서

*** 수석부회장 후보 약력**

성 명	박영호		
생년월일	1967.12.24	직 급	교수

*** 학 력**

학 위 취 득 기 간	출 신 교	전 공 분 야	학 위 명
1986.03. ~ 1990.02.	고려대학교	수학	이학사
1991.03. ~ 1993.02.	고려대학교	대수학	이학석사
1994.03. ~ 1997.02.	고려대학교	대수학	이학박사

*** 경 력**

경 력 기 간	재 직 기 관 명	직급 및 직위
2002.02. ~ 현재	세종사이버대학교	교수
2023.03. ~ 현재	세종사이버대학교	행정지원처장
2022.03. ~ 2023.02.	프랑스 Nantes 대학교	방문교수
2017.08. ~ 2021.08.	세종사이버대학교	대학원장, 콘텐츠정보처장
2010.09. ~ 2011.08.	미국 미주리주립대학교(MSU)	방문교수
2013.21. ~ 2016.02.	세종사이버대학교	정보보호통신학부장

*** 학회 및 사회활동**

활 동 기 간	활 동 내 역
2003.01. ~ 현재	한국정보보호학회 종신회원/ 이사 / 현 학술상임부회장
2022.01. ~ 현재	한국암호포럼 의장
2013.01. ~ 현재	한국정보보호학회 편집위원(2014년~ 2015년 편집위원장)
2013.01. ~ 현재	국가정보원 암호모듈검증 위원
2019.07. ~ 현재	IT보안인증사무국 인증위원회 인증위원
2014.01. ~ 현재	ICISC' 14, NetSec-KR 2021, ICISC' 23 외 한국정보보호학회 주관 다수 학술행사 프로그램/운영위원
2016.01. ~ 2016.12	한국정보보호학회 총무이사

*** 수 상**

년 도	수 상 내 역
2016.10	행정자치부 장관 표창
2015.07	한국과학기술단체총연합회 과학기술 우수 논문상
2016.12	한국정보보호산업협회 올해의 정보보호인 상(공로상)
2016.12	한국정보보호학회 공로상

*** 저서 및 논문 목록 (10편이내)**

2020	New Hybrid Method for Isogeny-Based Cryptosystems Using Edwards Curves, IEEE TRANSACTIONS ON INFORMATION THEORY, Vol.66, No.3, pp.1934-1943
2019	Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves, Advances in Cryptology -ASIACRYPT 2019, LNCS 11922, pp.273-292
2014	Practical RSA-PAKE for Low-Power Device in Imbalanced Wireless Network, International Journal of Distributed Sensor Networks,Vol. 2014, ID 125309, pp. 1-6
2013	Extended elliptic curve Montgomery ladder algorithm over binary fields with resistance to simple power analysis,INFORMATION SCIENCES,Vol. 245, pp. 304-312
2012	New Bit Parallel Multiplier With Low Space Complexity for All Irreducible Trinomials Over GF(2^n),EEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS,Vol. 20, No 10, pp. 1903-1908
2011	An efficient non-interactive deniable authentication scheme based on trapdoor commitment schemes,COMPUTER COMMUNICATIONS,Vol. 34, No. 3, pp. 353-357
2010	Security Analysis of an Unlinkable Secret Handshakes Scheme,IEEE COMMUNICATIONS LETTERS,Vol.14, No.1, pp. 4-5
2005	A note on the factorization method of Niederreiter,Finite Fields and Their Applications,Vol.11,Issue2 pp. 269-277
2002	Speeding Up Point Multiplication on Hyperelliptic Curves with Efficiently-computable Endomorphisms,Eurocrypt'02,LNCS 2332, pp. 197-208
2002	An improved method of multiplication on certain elliptic curves,PKC 2002, LNCS 2274,pp. 310-322