

이 력 서

* 수석부회장 후보 약력

성 명	하 재 철		
생년월일	1966. 8. 24	직 급	교수

* 학 력

학 위 취 득 기 간	출 신 교	전 공 분 야	학 위 명
1985. 3 ~ 1989. 2	경북대학교	전자공학	공학사
1989. 3 ~ 1993.8	경북대학교	전자공학	공학석사
1994. 3 ~ 1998. 2	경북대학교	전자공학	공학박사

* 경 력

경 력 기 간	재 직 기 관 명	직급 및 직위
1998. 3 ~ 2007. 2	나사렛대학교	부교수
2007. 3 ~ 현재	호서대학교	교수
2006. 7 ~ 2006. 12	호주 Queensland University of Technology	방문 교수
2014. 2 ~ 2015. 2	미국 Purdue University	방문 교수
2015. 5 ~ 2019. 10	호서대학교 공학교육혁신센터	센터장
2019. 10 ~ 2020. 11	호서대학교 전산센터	센터장

* 학회 및 사회활동

활 동 기 간	활 동 내 역
1991. 1 ~ 현재	한국정보보호학회 종신회원(현 총무부문 상임부회장)
2009. 1 ~ 현재	한국산학기술학회 종신회원 및 이사(현 학회지 편집위원)
2022. 1 ~ 현재	국제차세대융합기술학회 종신회원 및 이사(현 논문지 편집위원)
2001. 1 ~ 현재	한국인터넷정보학회 종신회원 및 논문지 편집위원
2007. 1 ~ 현재	정보보호제품 인증 위원 및 정보보호 관련 평가 및 심사 위원
2016. 1 ~ 2020. 12	한국정보보호학회 논문지 편집위원장
2003. 1 ~ 2016. 12	한국정보보호학회 주관 다수 학술행사 프로그램/조직/운영위원장
2012. 1 ~ 2012. 12	2012년 국가암호공모전 심사위원장

* 수 상

년 도	수 상 내 역
2022. 4	과학기술정보통신부 장관 표창장(정보보호 기술 발전)
2009. 12 ~	한국정보보호학회 공로상 5회 수상 (2009년, 2010년, 2012년, 2017년, 2020년)
2020. 9	호서대학교 총장 표창(교육 부문 우수교원)
2017. 7	미래창조과학부 장관 표창장(정보보호 유공)
2016. 7	한국과학기술단체총연합회 과학기술 우수 논문상
2013. 2	호서대학교 총장 표창(연구 부문 우수교원)

* 저서 및 논문 목록 (10편이내)

2022	Implementation of Disassembler on Microcontroller Using Side-Channel Power Consumption Leakage, MDPI Sensors, Vol. 22, No. 15, p. 5900, 2022. 08
2022	Deep Learning-based Attacks on Masked AES Implementation, Journal of Internet Technology, Vol. 23 No. 4, pp. 897-902, 2022, 07
2021	Performance Metric for Differential Deep Learning Analysis, Journal of Internet Services and Information Security (JISIS), Vol. 11, No. 2, pp. 22-33, 2021. 05
2018	Secure RSA implementation against horizontal correlation power analysis attack, Int. J. Internet Technology and Secured Transactions, Vol. 8, No. 1, pp. 62-77, 2018. 05
2016	An Improved Square-always Exponentiation Resistant to Side-channel Attacks on RSA Implementation, Intelligent Automation & Soft Computing, Vol. 22, No. 3, pp. 353-363, 2016. 07
2016	A secure exponentiation algorithm resistant to a combined attack on RSA implementation, International Journal of Computer Mathematics, Vol. 93, No. 2, pp. 258-272, 2016. 02
2021	연속 웨이블릿 변환을 사용한 비프로파일링 기반 전력 분석 공격, 한국정보보호학회 논문지, 31권, 6호, pp. 1127-1136, 2021. 12
2020	Performance Counter Monitor를 이용한 머신러닝 기반 캐시 부채널 공격 탐지, 한국정보보호학회 논문지, 30권, 6호, pp.1237-1246, 2020.1 2
2020	블록 암호 ARIA에 대한 Flush+Reload 캐시 부채널 공격, 한국정보보호학회 논문지, 30권, 6호, pp.1207-1216, 2020. 12
2000 ~	(C로 배우는) 암호학 프로그래밍, 미래컴, 2009. 2, 2018. 2(개정 2판, 현우사) (실무로 배우는) 네트워크 보안, 미래컴, 2008. 8 디지털 논리회로, 현우사, 2000년(초판), 2008년(개정 2판), 2021년(개정 3판)