

Acceptance rates for Cryptologic Conferences

Seungjoo Kim

skim@security.re.kr
<http://security.re.kr/>

August 29, 2005.

Conference : # of Submissions / # of Accepted papers / Ratio
--

제 1 절 Advances in Cryptology Series (Springer-Verlag's LNCS Volumes)

1.1 Advances in Cryptology – CRYPTO

CRYPTO'81 (Not LNCS) :	? / ? / ? (×)
CRYPTO'82 (Not LNCS) :	? / ? / ? (×)
CRYPTO'83 (Not LNCS) :	? / ? / ? (×)
CRYPTO'84 (LNCS 196) :	? / ? / ? (×)
CRYPTO'85 (LNCS 218) :	? / ? / ? (○)
CRYPTO'86 (LNCS 263) :	? / ? / ? (○)
CRYPTO'87 (LNCS 293) :	? / ? / ? (○)
CRYPTO'88 (LNCS 403) :	61 / 35 / 0.57 (○)
CRYPTO'89 (LNCS 435) :	93 / 43 / 0.46 (○)
CRYPTO'90 (LNCS 537) :	104 / 42 / 0.40 (pre)
CRYPTO'91 (LNCS 576) :	110 / 36 / 0.33 (○)
CRYPTO'92 (LNCS 740) :	135 / 38 / 0.28 (○)
CRYPTO'93 (LNCS 773) :	136 / 38 / 0.28 (○)
CRYPTO'94 (LNCS 839) :	114 / 38 / 0.33 (○)
CRYPTO'95 (LNCS 963) :	151 / 36 / 0.24 (○)
CRYPTO'96 (LNCS 1109) :	115 / 30 / 0.26 (○)
CRYPTO'97 (LNCS 1294) :	160 / 36 / 0.22 (○)
CRYPTO'98 (LNCS 1462) :	144 / 33 / 0.23 (○)
CRYPTO'99 (LNCS 1666) :	169 / 38 / 0.22 (○)
CRYPTO'00 (LNCS 1880) :	120 / 32 / 0.27 (○)
CRYPTO'01 (LNCS 2139) :	156 / 33 / 0.21 (○)
CRYPTO'02 (LNCS 2442) :	175 / 40 / 0.22 (○)
CRYPTO'03 (LNCS 2729) :	169 / 34 / 0.20 (○)
CRYPTO'04 (LNCS 3152) :	211 / 33 / 0.16 (○)

1.2 Advances in Cryptology – EUROCRYPT

EUROCRYPT'82 (LNCS 149) :	? / ? / ? (×)
EUROCRYPT'83 (LNCS ???) :	? / ? / ? (×)
EUROCRYPT'84 (LNCS 209) :	? / ? / ? (○)
EUROCRYPT'85 (LNCS 219) :	? / ? / ? (○)
EUROCRYPT'86 (LNCS ???) :	? / ? / ? (×)
EUROCRYPT'87 (LNCS 304) :	? / ? / 0.50 (○)
EUROCRYPT'88 (LNCS 330) :	? / ? / ? (○)
EUROCRYPT'89 (LNCS 434) :	? / ? / ? (pre)
EUROCRYPT'90 (LNCS 473) :	85 / 42 / 0.50 (○)
EUROCRYPT'91 (LNCS 547) :	? / ? / ? (○)
EUROCRYPT'92 (LNCS 658) :	? / ? / ? (pre)
EUROCRYPT'93 (LNCS 765) :	117 / 36 / 0.31 (○)
EUROCRYPT'94 (LNCS 950) :	137 / 36 / 0.26 (pre)
EUROCRYPT'95 (LNCS 921) :	113 / 33 / 0.29 (○)
EUROCRYPT'96 (LNCS 1070) :	126 / 34 / 0.27 (○)
EUROCRYPT'97 (LNCS 1233) :	104 / 34 / 0.33 (○)
EUROCRYPT'98 (LNCS 1403) :	161 / 44 / 0.27 (○)
EUROCRYPT'99 (LNCS 1592) :	122 / 32 / 0.26 (○)
EUROCRYPT'00 (LNCS 1807) :	150 / 39 / 0.26 (○)
EUROCRYPT'01 (LNCS 2045) :	155 / 33 / 0.22 (○)
EUROCRYPT'02 (LNCS 2332) :	122 / 33 / 0.27 (○)
EUROCRYPT'03 (LNCS 2656) :	156 / 37 / 0.24 (○)
EUROCRYPT'04 (LNCS 3027) :	206 / 36 / 0.17 (○)

1.3 Advances in Cryptology – ASIACRYPT

AUSCRYPT'90 (LNCS 453) :	? / ? / ? (○)
AUSCRYPT'92 (LNCS ???) :	? / ? / ? (pre)
ASIACRYPT'91 (LNCS 739) :	97 / 39 / 0.40 (○)
ASIACRYPT'94 (LNCS 917) :	94 / 30 / 0.32 (○)
ASIACRYPT'96 (LNCS 1163) :	124 / 31 / 0.25 (○)
ASIACRYPT'98 (LNCS 1514) :	118 / 32 / 0.27 (○)
ASIACRYPT'99 (LNCS 1716) :	96 / 31 / 0.32 (○)
ASIACRYPT'00 (LNCS 1976) :	140 / 45 / 0.32 (○)
ASIACRYPT'01 (LNCS 2248) :	153 / 33 / 0.32 (○)
ASIACRYPT'02 (LNCS 2501) :	173 / 34 / 0.20 (○)
ASIACRYPT'03 (LNCS 2894) :	188 / 33 / 0.18 (○)
ASIACRYPT'04 (LNCS 3329) :	208 / 36 / 0.17 (○)

제 2 절 Conference Proceedings as Springer-Verlag's LNCS Volumes

2.1 Algorithmic Number Theory

ANTS'94 (LNCS 877) : ? / 31 / ? (○)
ANTS'96 (LNCS 1122) : ? / 31 / ? (○)
ANTS'98 (LNCS 1423) : ? / 46 / ? (○)
ANTS'00 (LNCS 1838) : ? / 36 / ? (○)

2.2 Australasian Conference on Information Security and Privacy

ACISP'96 (LNCS 1172) : ? / 26 / ? (○)
ACISP'97 (LNCS 1270) : ? / 20 / ? (○)
ACISP'98 (LNCS 1438) : 66 / 35 / 0.53 (○)
ACISP'99 (LNCS 1587) : 53 / 26 / 0.49 (○)
ACISP'01 (LNCS 2119) : 91 / 38 / 0.42 (○)
ACISP'03 (LNCS 2727) : 158 / 42 / 0.27 (○)

2.3 Cryptographic Hardware and Embedded Systems

CHES'99 (LNCS 1717) : ? / ? / ? (×)
CHES'00 (LNCS 1965) : ? / ? / ? (×)
CHES'01 (LNCS ????) : 66 / 31 / 0.47 (○)
CHES'02 (LNCS 2162) : 101 / 39 / 0.39 (○)
CHES'03 (LNCS 2779) : 111 / 32 / 0.29 (○)
CHES'04 (LNCS 3156) : 125 / 32 / 0.26 (○)

2.4 European Symposium on Research in Computer Security

ESORICS'90 (LNCS ???) : ? / 24 / ? (×)
ESORICS'92 (LNCS ???) : ? / ? / ? (×)
ESORICS'94 (LNCS 875) : 71 / 26 / 0.37 (○)
ESORICS'96 (LNCS 1146) : 58 / 21 / 0.36 (○)
ESORICS'98 (LNCS 1485) : 57 / 23 / 0.40 (○)
ESORICS'00 (LNCS 1895) : 75 / 19 / 0.25 (○)
ESORICS'02 (LNCS 2502) : 83 / 16 / 0.19 (○)

2.5 Financial Cryptography

FC'97 (LNCS 1318) : ? / 31 / ? (o)
FC'98 (LNCS 1465) : ? / 28 / ? (o)
FC'99 (LNCS 1648) : ? / 19 / ? (o)

2.6 Fast Software Encryption

FSE'93 (LNCS 809) : ? / 26 / ? (o)
FSE'94 (LNCS 1008) : ? / 28 / ? (o)
FSE'96 (LNCS 1039) : ? / 18 / ? (o)
FSE'97 (LNCS 1267) : 44 / 23 / 0.52 (pre)
FSE'98 (LNCS 1372) : 39 / 20 / 0.51 (o)
FSE'99 (LNCS 1636) : 51 / 22 / 0.43 (o)
FSE'00 (LNCS 1978) : ? / ? / ? (x)
FSE'01 (LNCS 2355) : 46 / 27 / 0.59 (o)
FSE'02 (LNCS 2365) : 70 / 21 / 0.30 (o)

2.7 International Conference on Information and Communication Security

ICICS'97 (LNCS 1334) : 87 / 37(regular) + 11(short) / 0.55 (o)
ICICS'99 (LNCS 1726) : 62 / 24 / 0.39 (o)
ICICS'00 (LNCS 2015) : 56 / 20 / 0.38 (o)
ICICS'02 (LNCS 2513) : 161 / 41 / 0.25 (o)

2.8 International Conference on Information Security and Cryptology

ICISC'98 (Not LNCS) : 53 / 18 / 0.34 (o)
ICISC'99 (LNCS 1787) : 61 / 20 / 0.33 (o)
ICISC'00 (LNCS ????) : 56 / 20 / 0.36 (o)
ICISC'01 (LNCS 2288) : 102 / 32 / 0.31 (o)
ICISC'04 (LNCS 3506) : 194 / 34 / 0.18 (o)

2.9 International Workshop on Information Hiding

IH'96 (LNCS 1174) : ? / 26 / ? (o)
IH'98 (LNCS 1525) : 41 / 25 / 0.61 (o)
IH'99 (LNCS 1768) : 68 / 33 / 0.49 (o)

2.10 IMA Cryptography and Coding

Cryptography and Coding'86	:	? / ? / ?	(×)
Cryptography and Coding'89	:	? / ? / ?	(×)
Cryptography and Coding'91	:	? / ? / ?	(×)
Cryptography and Coding'93	:	? / ? / ?	(×)
Cryptography and Coding'95 (LNCS 1025)	:	48 / 24 / 0.5	(○)
Cryptography and Coding'97 (LNCS 1355)	:	? / 35 / ?	(○)
Cryptography and Coding'99 (LNCS 1746)	:	? / 35 / ?	(○)
Cryptography and Coding'01 (LNCS 2260)	:	? / 38 / ?	(○)

2.11 INDOCRYPT

INDOCRYPT'00 (LNCS 1977)	:	54 / 25 / 0.46	(○)
INDOCRYPT'01 (LNCS 2247)	:	77 / 31 / 0.40	(○)

2.12 Information Security Workshop

ISW'97 (LNCS 1396)	:	39 / 25 / 0.64	(○)
ISW'99 (LNCS 1729)	:	38 / 19(regular) + 4(short)	/ 0.61 (○)
ISW'00 (LNCS 1975)	:	63 / 23 / 0.37	(○)
ISC'02 (LNCS 2433)	:	81 / 38 / 0.47	(○)

2.13 International Workshop on Practice and Theory in Public Key Cryptography

PKC'98 (LNCS 1431)	:	30 / 18 / 0.6	(○)
PKC'99 (LNCS 1560)	:	61 / 25 / 0.41	(○)
PKC'00 (LNCS 1751)	:	70 / 31 / 0.44	(○)

2.14 Recent Advances in Intrusion Detection

RAID'98 (LNCS ????)	:	? / ? / ?	(×)
RAID'99 (LNCS ????)	:	? / ? / ?	(×)
RAID'00 (LNCS 1907)	:	26 / 14 / 0.54	(○)

2.15 Workshop on Selected Areas in Cryptography

SAC'94	:	? / 17 / ?	(×)
SAC'95	:	? / 14 / ?	(○)
SAC'96	:	24 / 14 / 0.58	(○)
SAC'97	:	31 / 20 / 0.65	(○)

SAC'98 (LNCS 1556) : 39 / 26 / 0.67 (o)
SAC'99 : ? / ? / ? (x)
SAC'01 (LNCS 2259) : 57 / 25 / 0.44 (o)

2.16 International Workshop on Security Protocols

Security Protocols'96 (LNCS 1189) : ? / 17 / ? (o)
Security Protocols'97 (LNCS 1361) : ? / 17 / ? (o)
Security Protocols'98 : ? / 15 / ? (x)

2.17 Cryptographers' Track RSA Conference

CT-RSA'01 (LNCS 2020) : 65 / 33 / 0.51 (o)
CT-RSA'02 (LNCS 2271) : ? / ? / ? (x)
CT-RSA'03 (LNCS 2612) : 97 / 26 / 0.27 (o)

2.18 Workshop on Information Security Applications

WISA'00 : 29 / 20 / 0.69 (o)
WISA'02 : 76 / 36 / 0.47 (o)
WISA'03 (LNCS 2908) : 200 / 36 / 0.18 (o)
WISA'04 (LNCS 3325) : 169 / 37 / 0.22 (o)
WISA'05 (LNCS ?????) : 168 / 33 / 0.20 (o)

2.19 기타

AWIC'05 (LNAI 3528) (o)
PET'00 (LNCS 2009) (o)
DRM'01 (LNCS 2320) 50 / 15 / 0.3 (o)
MMM-ACNS'01 (LNCS 2052) 36 / 24 / 0.67 (o)
ECCV'02 (LNCS 2359) (o)
EC-Web'05 (LNCS 3590) 139 / 39 / 0.28 (o)
InfraSec'02 (LNCS 2437) 44 / 23 / 0.52 (o)
SAFECOMP'02 (LNCS 2434) 69 / 27 / 0.39 (o)
SPC'05 (LNCS 3450) : 48 / 14 / 0.29 (o)
ICCS'05 (LNCS 3515) (o)
ICCSA'03 (LNCS 2667, 2668, 2669) (o)
ICCSA'04 (LNCS 3043, 3044, 3045) (o)
ICCSA'05 (LNCS 3480) (o)
ICWE'03 (LNCS 2722) : 190 / 25 / 0.13 (o)
IWDW'03 (LNCS ?????) (o)

TrustBus'05 (LNCS 3592) (○)

제 3 절 Conference Proceedings as ACM Volumes

3.1 ACM Conference on Computer and Communications Security

ACM CCS'93 : 60 / 22(regular) + 5(short) / 0.45 (○)
ACM CCS'94 : ? / ? / ? (×)
ACM CCS'96 : ? / ? / ? (×)
ACM CCS'97 : 64 / 17 / 0.27 (○)
ACM CCS'98 : ? / ? / ? (×)
ACM CCS'99 : 83 / 16 / 0.19 (○)
ACM CCS'00 : 132 / 28 / 0.21 (○)

3.2 ACM Symposium on the Theory of Computing

STOC'93 : 227 / 85 / 0.37 (○)
STOC'94 : 241 / 82 / 0.34 (○)
STOC'96 : 201 / 74 / 0.37 (○)
STOC'97 : 211 / 75 / 0.36 (○)

제 4 절 Conference Proceedings as IEEE Volumes

4.1 IEEE Symposium on Security and Privacy

IEEE S&P'96 : 67 / 20 / 0.30 (○)
IEEE S&P'97 : 110 / 20 / 0.18 (○)
IEEE S&P'98 : 116 / 19 / 0.16 (○)
IEEE S&P'98 : 116 / 19 / 0.16 (○)
IEEE S&P'99 : 61 / 15 / 0.25 (○)
IEEE S&P'01 : 107 / 19 / 0.18 (○)

제 5 절 Etc.

5.1 Working Conference on Smart Card Research and Advanced Applications

CARDIS'00 : 36 / 21 / 0.58 (○)

5.2 Korea-Japan Joint Workshop on Information Security and Cryptology

JW-ISC'93 : ? / ? / ? (o)

JW-ISC'95 : ? / ? / ? (o)

JW-ISC'97 : ? / ? / ? (o)

5.3 Symposium on Cryptography and Information Security

SCIS'01 : (o)

Bibliography for Cryptology

Seungjoo Kim

skim@security.re.kr
<http://security.re.kr/>

August 6., 2010.

제 1 절 Mathematics

1. (성균관대) 김응태, 박승안, “정수론 (제3판)”, 경문사.
2. (성균관대) 김응태, 박승안, “현대대수학 (제3판)”, 경문사.
3. (성균관대) 데이비드 웰스 (심재관 옮김), “소수, 수학 최대의 미스터리”, 한승.
4. 사라 플래너리, “사라와 함께하면 수학이 즐겁다”, 나노미디어.
5. 이바스 피터슨 (김인수, 주형관 옮김), “현대수학의 여행자 (The Mathematical Tourist)”, 사이언스북스.
6. 정완상, “페르마가 들려주는 정수론 이야기”, (주)자음과모음.
7. 톰 펫시니스 (김연수 옮김), “프랑스 수학자 갈루아”, 이끌리오.
8. (성균관대) J. A. Bondy and U. S. R. Murty, “Graph Theory with Applications”, North Holland.
9. (성균관대) David M. Bressoud, “Factorization and Primality Testing”, Springer-Verlag.
10. (성균관대) Henri Cohen, “A Course in Computational Algebraic Number Theory”, Springer-Verlag.
11. (성균관대) S. C. Coutinho, “The Mathematics of Ciphers – Number Theory and RSA Cryptography –”, A K Peters, Ltd.
12. (성균관대) Persi Diaconis, “Group Representations in Probability and Statistics”, Institute of Mathematical Statistics.
13. (성균관대) C. Ding, D. Pei and A. Salomaa, “Chinese Remainder Theorem – Applications in Computing, Coding, Cryptography –”, World Scientific.
14. (성균관대) Dale Husemoller, “Elliptic Curves – With an Appendix by Ruth Lawrence –”, Springer-Verlag.

15. Lee W. Johnson, R. Dean Riess and Jimmy T. Arnold, “Introduction to Linear Algebra (3rd Edition)”, Addison-Wesley Publishing Company.
16. (성균관대) Neal Koblitz, “Introduction to Elliptic Curves and Modular Forms”, Springer-Verlag.
17. (성균관대) Ramanujachary Kumanduri and Cristina Romero, “Number Theory with Computer Applications”, Prentice Hall.
18. (성균관대) A. K. Lenstra and H. W. Lenstra, Jr., “The Development of the Number Field Sieve”, Springer-Verlag.
19. (성균관대) Ming Li and Paul Vitanyi, “An Introduction to Kolmogorov Complexity and Its Applications”, Springer-Verlag.
20. (성균관대) Rudolf Lidl, Harald Niederreiter, and P.M. Cohn, “Encyclopedia of Mathematics and Its Applications – Finite Fields –”, Cambridge University Press.
21. (성균관대) Rudolf Lidl and Harald Niederreiter, “Introduction to Finite Fields and Their Applications”, Cambridge University Press.
22. (성균관대) Richard A. Mollin, “Quadratics”, CRC Press.
23. (성균관대) J. R. Norris, “Markov Chains”, Cambridge University Press.
24. (성균관대) Kenneth H. Rosen, “Elementary Number Theory and Its Applications (2nd Edition)”, Addison-Wesley Publishing Company.
25. (성균관대) M. R. Schroeder, “Number Theory in Science and Communications – With Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity –”, Springer-Verlag.
26. (성균관대) Joseph H. Silverman, “The Arithmetic of Elliptic Curves”, Springer-Verlag.

제 2 절 Computer Science

1. (성균관대) 데니스 샤샤, 캐시 레이저 (박영숙 옮김), “컴퓨터를 만든 15인의 과학자 (Out of Their Minds)”, 세종연구원.
2. (성균관대) 로버트 세지윅 (황정현 옮김), “C로 구현한 알고리즘 (Algorithms in C) – 기본편 –”, 피어슨 에듀케이션 코리아.
3. (성균관대) 류성열, 이남용, 오기성, “Software Testing”, 글로벌.
4. (성균관대) 문병로, “쉽게 배우는 알고리즘 – 관계 중심의 사고법 –”, 한빛미디어.

5. (성균관대) 문우식, “패턴 그리고 객체지향적 코딩의 법칙”, 한빛미디어.
6. (성균관대) 스티븐 스키에나, 미구엘 레비야 (서환수 옮김), “알고리즘 트레이닝북 (Programming Challenges)”, 한빛미디어.
7. (성균관대) 이성환, “패턴인식의 원리 (I권, II권)”, 홍릉과학출판사.
8. (성균관대) Hisao Yazawa (예승철 역), “성공과 실패를 결정하는 1%의 프로그래밍 원리”, 성안당.
9. (성균관대) John E. Hopcroft and Jeffrey D. Ullman (정인정 역), “오토마타와 계산이론 (Introduction to Automata Theory, Languages, and Computation)”, 홍릉과학출판사.
10. (성균관대) Daniel Pierre Bovet and Pierluigi Crescenzi, “Introduction to the Theory of Complexity”, Prentice Hall.
11. (성균관대) Gilles Brassard and Paul Bratley, “Fundamentals of Algorithmics”, Prentice Hall.
12. Cristian Calude, “Information and Randomness – An Algorithmic Perspective –”, Springer-Verlag.
13. (성균관대) Thomas H. Cormen, Charles E. Leiserson and Ronald L. Rivest, “Introduction to Algorithms”, The MIT Press and McGraw-Hill Book Company.
14. Elfriede Dustin, Jeff Rashka, John Paul, “Automated Software Testing – Introduction, Management, and Performance –”, Addison-Wesley.
15. (성균관대) Ding-Zhu Du and Ker-I Ko, “Theory of Computational Complexity”, John Wiley & Sons, Inc.
16. (성균관대) Mark Fewster and Dorothy Graham, “Software Test Automation – Effective use of test execution tools –”, Addison-Wesley.
17. (성균관대) Michael R. Garey and David S. Johnson, “Computers and Intractability – A Guide to the Theory of NP-Completeness –”, Bell Laboratories, Murray Hill, New Jersey.
18. (성균관대) David Hand, Heikki Mannila, and Padhraic Smyth, “Principles of Data Mining”, The MIT Press.
19. (성균관대) James L. Hein, “Theory of Computation – An Introduction –”, Jones and Bartlett Publishers.
20. (성균관대) John E. Hopcroft and Jeffrey D. Ullman, “Introduction to Automata Theory, Languages, and Computation”, Addison-Wesley Publishing Company.
21. (성균관대) Richard Johnsonbaugh, Marcus Schaefer, “Algorithms”, Prentice Hall.

22. (성균관대) Cem Kaner, James Bach, and Bret Pettichord, “Lessons Learned in Software Testing – A Context-Driven Approach –”, John Wiley & Sons, Inc.
23. (성균관대) Jon Kleinberg, Eva Tardos, “Algorithm Design”, Addison Wesley.
24. (성균관대) Donald E. Knuth, “The Art of Computer Programming (2nd Edition)”, Addison-Wesley Publishing Company.
25. (성균관대) Jan Van Leeuwen, “Handbook of Theoretical Computer Science (Volume A) : Algorithms and Complexity”, Elsevier.
26. Jean-Francois Monin, Michael G. Hinchey, “Understanding Formal Methods”, Springer.
27. (성균관대) Bernard M. Moret, “The Theory of Computation”, Addison-Wesley.
28. (성균관대) Michael A. Nielsen and Issac L. Chuang, “Quantum Computation and Quantum Information”, The Press Syndicate of the University of Cambridge.
29. James Noble, Charles Weir, “Small Memory Software”, Addison–Wesley.
30. (성균관대) Gerard O’Regan, “A Practical Approach to Software Quality”, Springer.
31. (성균관대) Christos H. Papadimitriou, “Computational Complexity”, Addison Wesley Longman.
32. (성균관대) William E. Perry, “Effective Methods for Software Testing (2nd Edition)”, John Wiley & Sons, Inc.
33. Richard J. Roiger, Michael W. Geatz, “Data Mining – A Tutorial-Based Primer –”, Addison–Wesley.
34. (성균관대) Michael Sipser, “Introduction to the Theory of Computation”, PWS Publishing Company.
35. (성균관대) Steven S. Skiena, Miguel A. Revilla, “Programming Challenges”, Springer.
36. Carl H. Smith, “A Recursive Introduction to the Theory of Computation”, Springer-Verlag.

제 3 절 Information Theory

1. (성균관대) Robert B. Ash, “Information Theory”, Dover Publications, Inc.
2. (성균관대) Thomas M. Cover and Joy A. Thomas, “Elements of Information Theory”, John Wiley & Sons, Inc.
3. (성균관대) George Cybenko, Dianne P. O’Leary and Jorma Rissanen, “The Mathematics of Information Coding, Extraction, and Distribution”, Springer-Verlag.
4. Richard W. Hamming, “Coding and Information Theory (2nd Edition)”, Prentice-Hall.
5. (성균관대) Robert J. McEliece, “Encyclopedia of Mathematics and Its Applications (Volume 3) – The Theory of Information and Coding –”, Addison-Wesley Publishing Company.
6. (성균관대) John R. Pierce, “An Introduction to Information Theory – Symbols, Signals & Noise – (Second, Revised Edition)”, Dover Publications, Inc.
7. (성균관대) Fazlollah M. Reza, “An Introduction to Information Theory”, Dover Publications, Inc.
8. (성균관대) N. J. A. Sloane and Aaron D. Wyner, “Claude Elwood Shannon Collected Papers”, IEEE Press.

제 4 절 Cryptography & Information Security

4.1 Book

1. “아무도 가르쳐주지 않은 인터넷 시큐리티의 구조”.
2. (성균관대) 강주성, 김재현, 박상우, 박춘식, 지성택, 하길찬, 한재우, “현대암호학”, 경문사.
3. 제임스 뱀포드 (곽미경, 박수미 옮김), “미 국가안보국 NSA (Body of Secrets)”, 서울문화사.
4. (성균관대) 김동균, 김은정, “공개키 암호학과 전자투표”, 청문각.
5. (성균관대) 루돌프 키펜한 (김시형 옮김), “암호의 세계 (Code Breaking)”, 이지북.
6. (성균관대) 루돌프 키펜한 (이일우 옮김), “머리를 쓰는 즐거움, 암호의 해석 (Code Breaking)”, 코리아하우스.

7. 오채환, “튜링이 들려주는 암호 이야기”, (주)자음과모음.
8. Lars Klander (김용권 역), “해커 프루프 (Hacker Proof)”, 정보문화사. 이지북.
9. (성균관대) Joel Scambray, Mike Schema (김태훈, 최창국, 김영진 옮김), “웹 기획·운영자를 위한 해킹과 보안 (Hacking Exposed)”, (주)사이버출판사.
10. (성균관대) 주식회사 니츠, “인터넷 보안 기술.I”, 도서출판 동서.
11. (성균관대) Michael Welschenbach (류대걸 역), “C와 C++로 구현하는 암호화 알고리즘 (Cryptography in C and C++)”, 인포북.
12. (성균관대) Greg Hoglund and Gary McGraw (류정욱, 한정애 공역), “소프트웨어 보안 : 코드 깨부수기 (Exploiting Software : How to break code)”, 정보문화사.
13. (성균관대) Hideki Imai (류춘열, 이경현, 박지환 옮김), “암호 이야기 - 정보 보안을 위한 새로운 키 -”, 동영출판사.
14. (성균관대) 마츠이 키네오, “컴퓨터를 이용한 암호조립법 입문”.
15. (성균관대) 박병익, 이강석, “리버스엔지니어링 역분석 구조와 원리”, 지앤선.
16. (성균관대) Paul Lunde (박세연 옮김), “시크릿코드 (The Secrets of Codes)”, 시그마북스.
17. (성균관대) 박영수, “역사 속에 숨겨진 암호 이야기”, 프리미엄북스.
18. (성균관대) 서광석, 김창한, “암호학과 대수학”, 북스힐.
19. (성균관대) 로버트 시코드 (서광열 옮김), “완벽한 보안을 위한 C와 C++ 코딩 (Secure Coding in C and C++)”, 피어슨 에듀케이션 코리아.
20. (성균관대) 서승우, “보안경제학 - CEO를 위한 정보보안 투자 가이드 -”, 서울대학교출판부.
21. (성균관대) 안교승, “서울에는 비밀이 없다 - 지금은 도청중 -”, 도서출판 그린.
22. (성균관대) 마크 스탬프 (안태남, 손용락, 이광석 옮김), “정보보안 이론과 실제”, 한빛미디어.
23. (성균관대) 여호영, 박근용, “디지털 네트워크 시큐리티”, 운정미디어.
24. (성균관대) 오카모토 타츠야키, 오오타 카즈오, “암호, 영지식증명, 수론”.
25. (성균관대) 원동호 역, “정보와 부호이론”, Ohm사.
26. (성균관대) 원동호, “현대 암호학”, 도서출판 그린.

27. (성균관대) 유영일, “침단보안 역해킹과 해커박스”, 삼각형프레스.
28. (성균관대) 사이먼 애덤스 (유정화 옮김), “특명, 암호를 풀어라!”, 삼성출판사
29. (성균관대) 윤중호, “윈도우 서버와 프로토콜 분석기를 활용한 네트워크 보안 프로토콜”, (주)교학사
30. (성균관대) 윤중호, “무선 LAN 보안 프로토콜”, (주)교학사
31. (성균관대) 이만영, 김지홍, 류재철, 송유진, 염홍열, 이임영, “전자상거래 보안 기술”, 생능출판사.
32. (성균관대) 이만영, 김지홍, 송유진, 염홍열, 이임영, “인터넷 정보보안”, 생능출판사
33. (성균관대) 이만영, 김지홍, 송유진, 염홍열, 이임영, “인터넷 보안기술”, 생능출판사
34. (성균관대) 이만영, 원동호, 이민섭, 송주석, 임종인, 박춘식, “현대 암호학 및 응용”, 생능출판사.
35. (성균관대) 이민섭, “현대암호학”, 교우사.
36. 이임영, “전자상거래보안입문”, 생능출판사.
37. (성균관대) 이지선, 이민순, 이병수, “해킹과 보안 마스터” 이한출판사.
38. (성균관대) 쓰지이 시게오 (이희구 옮김), “암호와 정보사회”, 한마음사.
39. (성균관대) 정기동, 김영주, 박성호, 유영중, “인터넷 및 개인용 컴퓨터 활용에서 컴퓨터 보안 바로알기”, 이한출판사.
40. (성균관대) 정완상, “원리와 개념의 과학나라, 정수와 암호의 원리”, (주)자음과모음.
41. (성균관대) H.X.Mel & Doris Baker 공저 (정재원, 류대걸, 강한 공역), “보안과 암호화 모든 것 (Cryptography Decrypted)”, 인포·북
42. (성균관대) 오스틴 프리먼 외 (정태원 옮김), “암호 미스터리 걸작선”, 국일미디어.
43. (성균관대) 데피드 스테다드, 마커스 핀토 (조도근, 김경곤, 장은경, 이현정 옮김), “웹 해킹 & 보안 완벽 가이드 (The Web Application Hacker's Handbook)”, 에이콘.
44. (성균관대) William Stallings (최용락, 소우영, 이재광, 이임영 옮김), “Cryptography and Network Security : Principles and Practice (3rd Edition)”, 도서출판 그린.
45. (성균관대) 브루스 슈나이어 (채윤기 옮김), “디지털 보안의 비밀과 거짓말 (Secrets & Lies)”, 나노미디어

46. (성균관대) 한국전자통신연구소, “컴퓨터범죄와 암호화 대책”.
47. 한국전자통신연구소, “현대암호학 (Modern Cryptology)”.
48. (성균관대) 한국전자통신연구원, “암호학의 기초”, 경문사.
49. (성균관대) Masaaki Mitani, Shinichi Satou (박인용, 이재원 옮김), “만화로 쉽게 배우는 암호”, 성안당.
50. (성균관대) Keiji Takeda, Hiroshi Isozaki, “네트워크 침입탐지 – 부정침입의 검출과 대책 –”,
51. (성균관대) Marshal D. Abrams, Sushil Jajodia, and Harold J. Podell, “Information Security – An Integrated Collection of Essays –”, IEEE Computer Society Press.
52. (성균관대) Jason Albanese and Wes Sonnenreich, “Network Security Illustrated”, McGraw-Hill.
53. (성균관대) Julia H. Allen, “The CERT Guide to System and Network Security Practices”, Addison-Wesley.
54. (성균관대) Edward G. Amoroso, “Intrusion Detection – An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response –”, Intrusion.Net Books.
55. (성균관대) Ross J. Anderson, “Security Engineering : A Guide to Building Dependable Distributed Systems”, John Wiley & Sons, Inc.
56. (성균관대) Paul Ashley and Mark Vandenwauver, “Practical Intranet Security – Overview of the State of the Art and Available Technologies –”, Kluwer Academic Publishers.
57. (성균관대) Mohan Atreya, Ben Hammond, Stephen Paine, Paul Starrett, and Stephen Wu, “Digital Signatures”, RSA Press.
58. (성균관대) Gregory V. Bard, “Algebraic Cryptanalysis”, Springer.
59. (성균관대) Friedrich L. Bauer, “Decrypted Secrets – Methods and Maxims of Cryptology –”, Springer-Verlag.
60. Frank Baylin, Richard Maddox and John McCormac, “World Satellite TV and Scrambling Methods – The Technicians’ Handbook – (2nd Edition)”, Baylin Publications.
61. Eli Biham and Adi Shamir, “Differential Cryptanalysis of the Data Encryption Standard”, Springer-Verlag.
62. (성균관대) David Bishop “Introduction to Cryptography with Java Applets”, Jones and Bartlett Publishers.
63. (성균관대) Matt Bishop “Computer Security”, Addison Wesley.

64. (성균관대) Matt Bishop “Introduction to Computer Security”, Addison Wesley.
65. (성균관대) Richard E. Blahut, Daniel J. Costello, Jr., Ueli Maurer, and Thomas Mittelholzer, “Communications and Cryptography – Two Sides of One Tapestry –”, Kluwer Academic Publishers.
66. (성균관대) I. F. Blake, G. Seroussi and N. P. Smart, “Elliptic Curves in Cryptography”, Cambridge University Press.
67. (성균관대) Antoon Bosselaers and Bart Preneel, “Integrity Primitives for Secure Information Systems – Final Report of RACE Integrity Primitive Evaluation RIPE-RACE 1040 –”, Springer.
68. (성균관대) Colin Boyd and Anish Mathuria, “Protocols for Authentication and Key Establishment”, Springer.
69. Gilles Brassard, “Modern Cryptology – A Tutorial –”, Springer-Verlag.
70. (성균관대) R. R. Brooks, “Disruptive Security Technologies with Mobile Code and Peer-to-Peer Networks”, CRC Press.
71. (성균관대) Steven Brown, “Implementing Virtual Private Networks”, McGraw-Hill.
72. (성균관대) Johannes A. Buchmann “Introduction to Cryptography”, Springer-Verlag.
73. (성균관대) J.Buchmann, T.Høholdt, H.Stichtenoth, H.Tapia-Recillas, “Coding Theory, Cryptography, and Related Areas”, Springer.
74. (성균관대) Steve Burnett and Stephen Paine, “RSA Security’s Official Guide to Cryptography”, RSA Press.
75. (성균관대) Paul Campbell, Ben Calvert, and Steven Boswell, “Security+ Guide to Network Security Fundamentals”, Thomson.
76. John E. Canavan, “Fundamentals of Network Security”, Artech House.
77. (성균관대) Jyh-Cheng Chen and Tao Zhang, “IP-Based Next-Generation Wireless Networks – Systems, Architectures, and Protocols –”, Wiley.
78. (성균관대) Michael Chissick and Alistair Kelman, “Electronic Commerce : Law and Practice (2nd Edition)”.
79. (성균관대) John Chirillo and Scott Blaul, “Storage Security – Protecting SANs, NAS, and DAS –”, Wiley.
80. (성균관대) Kim-Kwang Raymond Choo, “Secure Key Establishment”, Springer.

81. (성균관대) Thomas W. Cusick, Cunsheng Ding and Ari Renvall, "Stream Ciphers and Number Theory", Elsevier.
82. (성균관대) Joan Daemen and Vincent Rijmen, "The Design of Rijndael", Springer.
83. (성균관대) Ivan Damgard, "Lectures on Data Security – Modern Cryptology in Theory and Practice –" Springer-Verlag.
84. (성균관대) Carlton R. Davis, "IPSec : Securing VPNs", RSA Press.
85. Donald W. Davies, "Tutorial : The Security of Data in Networks", IEEE Computer Society Press.
86. (성균관대) D. W. Davies and W. L. Price, "Security for Computer Networks – An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer –", John Wiley & Sons.
87. (성균관대) Peter T. Davis, "Securing Client/Server Computer Networks", McGraw-Hill.
88. Ed Dawson and Jovan Golić, "Cryptography : Policy and Algorithms", Springer.
89. (성균관대) Cipher A. Deavours, David Kahn, Louis Kruh, Greg Mellen and Brian J. Winkel, "Selections from CRYPTOLOGIA – History, People, and Technology –", Artech House.
90. (성균관대) Dorothy Denning, "Cryptography and Data Security", Addison-Wesley Publishing Company.
91. (성균관대) Alexander W. Dent and Chris J. Mitchell, "User's Guide to Cryptography and Standards", Artech House.
92. (성균관대) C. Ding, G. Xiao and W. Shan, "The Stability Theory of Stream Ciphers", Springer-Verlag.
93. (성균관대) Naganand Doraswamy and Dan Harkins, "IPSec – The New Security Standard for the Internet, Intranets, and Virtual Private Networks –", Prentice Hall PTR.
94. (성균관대) Blake Dournaee, "XML Security", McGraw-Hill.
95. (성균관대) Grady N. Drew, "Using SET for Secure Electronic Commerce", Prentice Hall PTR.
96. (성균관대) Electronic Frontier Foundation, "Cracking DES – Secrets of Encryption Research, Wiretap Politics & Chip Design –" O'Reilly & Associates, Inc.
97. (성균관대) Eldad Eilam, "Reversing – Secrets of Reverse Engineering –", Wiley Publishing, Inc.

98. (성균관대) Marc Farley, Tom Stearns, Jeffrey Hsu, “LAN TIMES : Guide to Security and Data Integrity – Protect Your Network from Hackers, System Failures, and Natural Disasters –”, Osborne.
99. Mark Fowler, “Codes & Ciphers”, Usborne Publishing Ltd.
100. (성균관대) Jalal Feghhi, Jalil Feghhi and Peter Williams, “Digital Certificates – Applied Internet Security –”, Addison-Wesley.
101. (성균관대) Niels Ferguson, Bruce Schneier, “Practical Cryptography”, Wiley Publishing, Inc.
102. (성균관대) Warwick Ford, “Computer Communications Security – Principles, Standard Protocols and Techniques –”, Prentice Hall.
103. Adam Freeman and Allen Jones, “Programming .NET Security”, O’Reilly.
104. (성균관대) Borko Furht and Darko Kirovski, “Multimedia Security Handbook”, CRC Press.
105. (성균관대) Brent Gale and Frank Baylin, “Satellite and Cable TV Scrambling and Descrambling”, Baylin/Gale Productions.
106. (성균관대) Simson Garfinkel, “PGP – Pretty Good Privacy –”, O’Reilly & Associates, Inc.
107. Simson Garfinkel and Gene Spafford, “Practical UNIX & Internet Security (2nd Edition)”, O’Reilly & Associates, Inc.
108. (성균관대) Jess Garms and Daniel Somerfield, “Professional Java Security”, Wrox Press, Ltd.
109. (성균관대) Paul Garrett, “Making, Breaking Codes : An Introduction to Cryptology”, Prentice Hall.
110. General Marcel Givierge, “Course in Cryptography”, Aegean Park Press.
111. Andrew M. Gleason, “Elementary Course in Probability for the Cryptanalyst (Revised Edition)”, Aegean Park Press.
112. (성균관대) Oded Goldreich, “Modern Cryptography, Probabilistic Proofs and Pseudorandomness”, Springer-Verlag.
113. (성균관대) Oded Goldreich, “Foundations of Cryptography – Volume I Basic Tools –”, Cambridge University Press.
114. (성균관대) Oded Goldreich, “Foundations of Cryptography – Volume II Basic Applications –”, Cambridge University Press.
115. (성균관대) Solomon W. Golomb, “Shift Register Sequences (Revised Edition)”, Aegean Park Press.

116. Walter Goralski and David Waclawski, "Virtual Private Networks – Achieving Secure Internet Commerce and Enterprisewide Communications –", Computer Technology Research Corp.
117. Jonathan S. Greenfield, "Distributed Programming Paradigms with Cryptography Applications", Springer-Verlag.
118. (성균관대) Dimitris A. Gritzalis, "Secure Electronic Voting", Kluwer Academic Publishers.
119. (성균관대) Peter Gutmann, "Cryptography Security Architecture : Design and Verification", Springer.
120. (성균관대) D.R.Hankerson, D.G.Hoffman, D.A.Leonard, C.C.Lindner, K.T.Phelps, C.A.Rodger, and J.R.Wall, "Coding Theory and Cryptography – The Essentials – (Second Edition, Revised and Expanded)", Marcel Dekker, Inc.
121. (성균관대) Darrel Hankerson, Alfred Menezes, Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer.
122. (성균관대) Thomas Hardjono and Lakshminath R. Dondeti, "Multicast and Group Security", Artech House.
123. (성균관대) Mike Hendry "Smart Card Security and Applications – Second Edition –", Artech House.
124. (성균관대) Debra S. Herrmann, "A Practical Guide to Security Engineering and Information Assurance", Auerbach Publications.
125. (성균관대) Debra S. Herrmann, "Using the Common Criteria for IT Security Evaluation", Auerbach Publications.
126. (성균관대) Lance J. Hoffman, "Building in Big Brother – The Cryptographic Policy Debate –", Springer-Verlag.
127. (성균관대) Russ Housley, and Tim Polk, "Planning for PKI – Best Practices Guide for Deploying Public Key Infrastructure –", John Wiley & Sons, Inc.
128. (성균관대) Tony Howlett, "Open Source Security Tools : A Practical Guide to Security Applications", Prentice Hall.
129. (성균관대) Andrew "Bunnie" Huang, "Hacking the Xbox – An Introduction to Reverse Engineering –", No Starch Press, Inc.
130. (성균관대) Larry J. Hughes, Jr., "Actually Useful Internet Security Techniques", New Riders Publishing.
131. (성균관대) Internet Security Systems, Inc., "Microsoft Windows 2000 Security Technical Reference", Microsoft Press.

132. (성균관대) Borja Jerman-Blazic, Wolfgang S. Schneider, and Tomaz Klobucar, “Advanced Security Technologies in Networking” IOS Press.
133. (성균관대) Neil F. Johnson, Zoran Duric, and Sushil Jajodia, “Information Hiding : Steganography and Watermarking – Attacks and Countermeasures” Kluwer Academic Publishers.
134. (성균관대) Marc Joye and Gregory Neven, “Identity-Based Cryptography” IOS Press.
135. Dieter Jungnickel, Jennifer D. Key, and Scott A. Vanstone, “Designs, Codes and Cryptography”, Kluwer Academic Publishers.
136. Merike Kaeo, “Designing Network Security”, Cisco Press.
137. (성균관대) Atul Kahate, “Cryptography and Network Security”, McGraw-Hill.
138. (성균관대) David Kahn, “The Codebreakers – The Story of Secret Writing –”, Scribner.
139. (성균관대) Stefan Katzenbeisser, “Recent Advances in RSA Cryptography”, Kluwer Academic Publishers.
140. (성균관대) Stefan Katzenbeisser and Fabien A. P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House.
141. (성균관대) Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security – PRIVATE Communication in a PUBLIC World –”, Prentice Hall.
142. (성균관대) Elizabeth Kaufman, and Andrew Newman, “Implementing IPsec : Making Security Work on VPNs, Intranets, and Extranets”, John Wiley & Sons, Inc.
143. (성균관대) Kevin Kenan, “Cryptography in the Database”, Symantec Press.
144. (성균관대) Christopher M. King, Curtis E. Dalton, and T. Ertem Osmanoglu, “Security Architecture : Design, Deployment & Operations”, RSA Press.
145. (성균관대) Jonathan Knudsen, “JAVA Cryptography”, O’Reilly.
146. (성균관대) Neal Koblitz, “A Course in Number Theory and Cryptography”, Springer-Verlag.
147. (성균관대) Neal Koblitz, “Algebraic Aspects of Cryptography”, Springer-Verlag.

148. (성균관대) Alan G. Konheim, “Cryptography A Primer”, John Wiley & Sons.
149. (성균관대) Bert-Jaap Koops, “The Crypto Controversy – A Key Conflict in the Information Society –”, Kluwer Law International.
150. (성균관대) Weidong Kou, “Networking Security and Standards”, Kluwer Academic Publishers.
151. (성균관대) Evangelos Kranakis, “Primality and Cryptography”, John Wiley & Sons.
152. (성균관대) Micki Krause and Harold F. Tipton, “Handbook of Information Security Management 1999”, Auerbach.
153. Solomon Kullback, “Statistical Methods in Cryptanalysis”, Aegean Park Press.
154. (성균관대) Gerard Lacoste, Birgit Pfitzmann, Michael Steiner, and Michael Waidner, “SEMPER – Secure Electronic Marketplace for Europe”, Springer-Verlag.
155. (성균관대) Kerstin Lemke, Christof Paar, and Marko Wolf, “Embedded Security in Cars – Securing Current and Future Automotive IT Applications –”, Springer.
156. (성균관대) Johnny Long, “Google Hacking”, Syngress.
157. (성균관대) G. Longo “Secure Digital Communications”, Springer-Verlag.
158. (성균관대) Pete Loshin “Big Book of IPsec RFCs”, Morgan Kaufmann.
159. (성균관대) Pete Loshin “Personal Encryption Clearly Explained”, AP Professional.
160. (성균관대) Michael Luby, “Pseudorandomness and Cryptographic Applications”, Princeton University Press.
161. (성균관대) Stefan Mangard, Elisabeth Oswald, Thomas Popp, “Power Analysis Attacks – Revealing the Secrets of Smart Cards –”, Springer.
162. (성균관대) Wenbo Mao, “Modern Cryptography – Theory & Practice –”, Prentice Hall.
163. Donis Marshall, “.NET Security Programming”, Wiley Publishing, Inc.
164. (성균관대) James L. Massey, “Cryptography : Fundamentals and Applications (Copies of Transparencies)”, Advanced Technology Seminars.
165. (성균관대) Máire McLoone, John V. McCanny, “System-On-Chip Architectures and Implementations for Private-Key Data Encryption”, Kluwer Academic/Plenum Publishers.

166. (성균관대) Gary McGraw, “Software Security”, Addison-Wesley.
167. (성균관대) H. X. Mel and Doris Baker, “Cryptography Decrypted”, Addison-Wesley.
168. (성균관대) David Melnick, Mark Dinman, and Alexander Muratov, “PDA Security – Incorporating Handhelds into the Enterprise –” McGraw-Hill.
169. (성균관대) Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC Press.
170. (성균관대) Alfred J. Menezes, “Elliptic Curve Public Key Cryptosystems”, Kluwer Academic Publishers.
171. (성균관대) Carl H. Meyer and Stephen M. Matyas, “Cryptography : A New Dimension in Computer Data Security – A Guide for the Design and Implementation of Secure Systems –”, John Wiley & Sons.
172. (성균관대) Stewart S. Miller, “WiFi Security, McGraw-Hill.
173. (성균관대) Richard A. Mollin, “An Introduction to Cryptography”, Chapman & Hall / CRC
174. (성균관대) Ed Moyle and Diana Kelley, “Cryptographic Libraries for Developers”, Charles River Media, Inc.
175. (성균관대) Andrew Nash, William Duane, Celia Joseph, and Derek Brink, “PKI : Implementing and Managing E-Security”, McGraw-Hill.
176. James Nechvatal, “Public-Key Cryptography”, NIST.
177. (성균관대) David E. Newton, “Encyclopedia of Cryptology”, ABC-Clio.
178. (성균관대) Randall K. Nichols, “ICSA Guide to Cryptography”, McGraw-Hill.
179. Randall K. Nichols, “Classical Cryptography Course (Volume I)”, Aegean Park Press.
180. Randall K. Nichols, “Classical Cryptography Course (Volume II)”, Aegean Park Press.
181. (성균관대) Valteri Niemi, Kaisa Nyberg, “UMTS Security”, Wiley.
182. (성균관대) Rolf Oppliger, “Authentication Systems for Secure Networks”, Artech House.
183. (성균관대) Rolf Oppliger, “Secure Messaging with PGP and S/MIME”, Artech House.
184. (성균관대) Christof Paar, Jan Pelzl, “Understanding Cryptography – A Textbook for Students and Practitioners –”, Springer.

185. (성균관대) Raymond R. Panko, “Corporate Computer and Network Security”, Prentice Hall.
186. (성균관대) Wayne Patterson, “Mathematical Cryptology – for Computer Scientists and Mathematicians –”, Rowman & Littlefield.
187. (성균관대) Adrian Perring and J.D. Tygar, “Secure Broadcast Communication in Wired and Wireless Networks”, Kluwer Academic Publishers.
188. (성균관대) Birgit Pfitzmann, “Digital Signature Schemes – General Framework and Fail-Stop Signatures –”, Springer-Verlag.
189. (성균관대) Charles P. Pfleeger, “Security in Computing (2nd Edition)”, Prentice-Hall, Inc.
190. (성균관대) Charles P. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing (3rd Edition)”, Prentice-Hall, Inc.
191. (성균관대) Clifford A. Pickover, “Cryptorunes – Codes and Secret Writing –”, Pomegranate Communications, Inc.
192. (성균관대) Marco Pistoia, Duane F. Reller, Deepak Gupta, Milind Nagpur, and Ashok K. Ramani, “JAVATM 2 Network Security”, Prentice-Hall, Inc.
193. Bruce Potter and Bob Fleck, “802.11 Security”, O’Reilly.
194. (성균관대) Bart Preneel and Vincent Rijmen, “State of the Art in Applied Cryptography”, Springer-Verlag
195. (성균관대) Bart Preneel, René Govaerts and Joos Vandewalle, “Computer Security and Industrial Cryptography – State of the Art and Evolution –”, Springer-Verlag
196. (성균관대) Eric Rescorla, “SSL and TLS – Designing and Building Secure Systems –”, Addison-Wesley.
197. (성균관대) Man Young Rhee, “Cryptography and Secure Communications”, McGraw-Hill Book Co.
198. (성균관대) Man Young Rhee, “Internet Security – Cryptographic principles, algorithms and protocols”, WILEY
199. (성균관대) Man Young Rhee, “Mobile Communication Systems and Security”, WILEY
200. (성균관대) Michael Rosing, “Implementing Elliptic Curve Cryptography”, Manning Publications Co.
201. (성균관대) Jorg Rothe, “Complexity Theory and Cryptology – An Introduction to Cryptocomplexity –”, Springer.

202. (성균관대) Rainer A. Rueppel, “Analysis and Design of Stream Ciphers”, Springer-Verlag.
203. (성균관대) Deborah Russell and G. T. Gangemi Sr., “Computer Security Basics”, O’Reilly & Associates, Inc.
204. (성균관대) P.Y.A. Ryan and S.A. Schneider, “The Modelling and Analysis of Security Protocols : the CSP Approach”, Addison-Wesley.
205. (성균관대) Arto Salomaa, “Public-Key Cryptography (2nd, Enlarged Edition)”, Springer-Verlag.
206. (성균관대) Günter Schäfer, “Security in Fixed and Wireless Networks – An Introduction to Securing Data Communications –”, Wiley.
207. Mike Schiffman, “Building Open Source Network Security Tools – Components and Techniques –”, Wiley Publishing, Inc.
208. (성균관대) Klaus Schmech, “Cryptography and Public Key Infrastructure on the Internet”, Wiley.
209. Bruce Schneier, “Applied Cryptography – Protocols, Algorithms, and Source Code in C –”, John Wiley & Sons, Inc.
210. (성균관대) Bruce Schneier, “Applied Cryptography (2nd Edition) – Protocols, Algorithms, and Source Code in C –”, John Wiley & Sons, Inc.
211. (성균관대) Bruce Schneier, “Secrets and Lies – Digital Security in a Networked World –”, John Wiley & Sons, Inc.
212. (성균관대) Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson, “The Twofish Encryption Algorithm – A 128-Bit Block Cipher”, John Wiley & Sons, Inc.
213. (성균관대) Jennifer Seberry and Josef Pieprzyk, “Cryptography – An Introduction to Computer Security –”, Prentice Hall.
214. (성균관대) Alexander V. Sergienko, “Quantum Communications and Cryptography”, Taylor & Francis Group.
215. (성균관대) Igor Shparlinski, “Number Theoretic Methods in Cryptography – Complexity Lower Bounds –”, Progress in Computer Science and Applied Logic, Vol.17.
216. (성균관대) Igor Shparlinski, “Cryptographic Applications of Analytic Number Theory – Complexity Lower Bounds and Pseudorandomness –”, Progress in Computer Science and Applied Logic, Vol.22.
217. (성균관대) Mostafa Hashem Sherif, “Protocols for Secure Electronic Commerce”, CRC Press.

218. (성균관대) Gustavus J. Simmons, “Contemporary Cryptography – The Science of Information Integrity –”, IEEE Press.
219. (성균관대) Simon Singh, “The Code Book”, Fourth Estate.
220. (성균관대) Richard E. Smith “Authentication – From Passwords to Public Keys –”, Addison-Wesley.
221. (성균관대) Richard J. Spillman, “Classical and Contemporary Cryptology”, Prentice Hall.
222. (성균관대) Frank Stajano, “Security for Ubiquitous Computing”, John Wiley & Sons, Ltd.
223. (성균관대) William Stallings, “Cryptography and Network Security : Principles and Practice (2nd Edition)”, Prentice Hall.
224. (성균관대) William Stallings, “Cryptography and Network Security : Principles and Practice (3rd Edition)”, Prentice Hall.
225. (성균관대) William Stallings, “Network and Internetwork Security – Principles and Practice –”, IEEE Press.
226. (성균관대) William Stallings, “Network Security Essentials – Applications and Standards –”, Prentice Hall.
227. William Stallings, “Practical Cryptography for Data Internetworks”, IEEE Computer Society Press.
228. (성균관대) Mark Stamp and Richard M. Low, “Applied Cryptanalysis – Breaking Ciphers in the Real World –”, Wiley - Interscience.
229. (성균관대) Douglas R. Stinson, “Cryptography – Theory and Practice –”, CRC Press.
230. (성균관대) Douglas R. Stinson, “Cryptography – Theory and Practice – (Second Edition)”, CRC Press.
231. (성균관대) Rita C. Summers, “Secure Computing – Threats and Safeguards –”, McGraw-Hill.
232. (성균관대) Peter Szor, “The Art of Computer Virus Research and Defense”, Symantec Press.
233. (성균관대) Laura Taylor, “FISMA Certification & Accreditation”, Syngress.
234. (성균관대) Stephen A. Thomas, “SSL & TLS Essentials – Securing the Web –”, John Wiley & Sons, Inc.
235. (성균관대) Frank Thornton, Brad Haines, Anand M. Das, Hersh Bhargava, Anita Campbell, John Kleinschmidt, “RFID Security”, Syngress.

236. (성균관대) John R. Vacca, "Satellite Encryption", Academic Press.
237. (성균관대) Jan C. A. Van Der Lubbe, "Basic Methods of Cryptography", Cambridge University Press.
238. (성균관대) John Viega and Gary McGraw, "Building Secure Software", Addison-Wesley.
239. (성균관대) John Viega and Matt Messier, "Secure Programming Cookbook for C and C++", O'Reilly.
240. John Viega, Matt Messier, and Pravir Chandra, "Network Security with OpenSSL", O'Reilly.
241. (성균관대) Serge Vaudenay, "A Classical Introduction to Cryptography: Applications for Communications Security", Springer.
242. (성균관대) Jan Vitek and Christian D. Jensen, "Secure Internet Programming – Security Issues for Mobile and Distributed Objects –", Springer.
243. (성균관대) Peter Wayner, "Digital Copyright Protection", AP Professional.
244. (성균관대) Peter Wayner, "Disappearing Cryptography – Being and Nothing on the Net –", AP Professional.
245. Peter Wayner, "Digital Cash – Commerce on the Net – (2nd Edition)", AP Professional.
246. (성균관대) Jason Weiss, "Java Cryptography Extensions – Practical Guide for Programmers –", Elsevier.
247. (성균관대) Michael Welschenbach, "Cryptography in C and C++" Apress.
248. (성균관대) Dominic Welsh, "Codes and Cryptography", Clarendon Press.
249. (성균관대) James A. Whittaker, "How to Break Software – A Practical Guide to Testing –", Addison Wesley.
250. (성균관대) James A. Whittaker and Herbert H. Thompson, "How to Break Software Security – Effective Techniques for Security Testing –", Addison Wesley.
251. (성균관대) Brian J. Winkel, Cipher A. Deavours, David Kahn, Louis Kruh, "The German Enigma Cipher Machine – Beginnings, Success, and Ultimate Failure –", Artech House.
252. (성균관대) John D. Woodward, Jr., Nicholas M. Orlans, Peter T. Higgins, "Biometrics – Identity Assurance in the Information Age –", McGraw-Hill/Osborne.

253. (성균관대) Song Y. Yan, “Primality Testing and Integer Factorization in Public-Key Cryptography”, Kluwer Academic Publishers.
254. (성균관대) Adam L. Young and Moti Yung, “Malicious Cryptography : Exposing Cryptovirology”, Wiley.
255. (성균관대) Jianying Zhou, “Non-repudiation in Electronic Commerce”, Artech House.

4.2 Thesis

1. N. Asokan, “Fairness in Electronic Commerce”, Ph.D. Thesis.
2. Mustafa Atici, “Hash Families : Recursive Constructions and Applications to Cryptography”, UMI Dissertation Services.
3. Donald Rozinak Beaver, “Security, Fault Tolerance, and Communication Complexity in Distributed Systems”, UMI Dissertation Services.
4. (성균관대) John R. Black, JR., “Message Authentication Codes”, Ph.D. Thesis.
5. Daniel Bleichenbacher, “Efficiency and Security of Cryptosystems based on Number Theory”, Nachdruck der Diss. ETH No.11404.
6. Dan Boneh, “Studies in Computational Number Theory with Applications to Cryptography”, Ph.D. Thesis.
7. Victor Boyko, “A Pre-Computation Scheme for Speeding Up Public-Key Cryptosystems”, Ms.D. Thesis.
8. Victor Boyko, “On All-or-Nothing Transforms and Password-Authenticated Key Exchange Protocols”, Ph.D. Thesis.
9. Stefan A. Brands, “Rethinking Public Key Infrastructures and Digital Certificates – Building in Privacy –”, The MIT Press.
10. Jan Camenisch, “Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem”, Nachdruck der Diss. ETH No.12520.
11. Claude Crepeau, “Correct and Private Reductions Among Oblivious Transfers”, Ph.D. Thesis.
12. (성균관대) Joan Daemen, “Cipher and Hash Function Design, Strategies based on Linear and Differential Cryptanalysis”, Ph.D. Thesis.
13. Michael Hilton Dawson, “A Unified Framework for Substitution Box Design Based on Information Theory”, UMI Dissertation Services.

14. Jean-Francois Dhem, "Design of an Efficient Public-Key Cryptographic Library for RISC-based Smart Cards", Ph.D. Thesis.
15. Taher A. ElGamal, "Cryptography and Logarithms Over Finite Fields", UMI Dissertation Services.
16. Rosario Gennaro, "On the Definitions and the Properties of Zero-Knowledge Arguments", Ms.D. Thesis.
17. Shafrira Goldwasser, "Probabilistic Encryption : Theory and Applications", UMI Dissertation Services.
18. Li Gong, "Cryptographic Protocols for Distributed Systems", Ph.D. Thesis.
19. Helen May Gustafson, "Statistical Analysis of Symmetric Ciphers", Ph.D. Thesis.
20. Russell Impagliazzo, "Pseudo-Random Generators for Probabilistic Algorithms and Cryptography", Ph.D. Thesis.
21. Ian W. Jackson, "Who goes here ? Confidentiality of Location through Anonymity", Ph.D. Thesis.
22. Markus Jakobsson, "Privacy vs. Authenticity", Ph.D. Thesis.
23. Stanislaw Jarecki, "Proactive Secret Sharing and Public Key Cryptosystems", Ms.D. Thesis.
24. Marc Joye, "Security Analysis of RSA-type Cryptosystems", Ph.D. Thesis.
25. Ryan Junee, "Power Analysis Attacks : A Weakness in Cryptographic Smart Cards and Microprocessors", Ms.D. Thesis.
26. Michael K. Just, "Methods of Multi-Party Cryptographic Key Establishment", Ms.D. Thesis.
27. (성균관대) Joe Kilian, "Uses of Randomness in Algorithms and Protocols", The MIT Press.
28. (성균관대) Lars Ramkilde Knudsen, "Block Ciphers – Analysis, Design and Applications", Computer Science Department Aarhus University.
29. Xuejia Lai, "On the Design and Security of Block Ciphers", Nachdruck der Diss. ETH No.9752.
30. Douglas Low, "Java Control Flow Obfuscation", Ms.D. Thesis.
31. (성균관대) Stefan Mangard, "Calculation and Simulation of the Susceptibility of Cryptographic Devices to Power-Analysis Attacks", TUG Diploma Thesis.

32. Michael John Merritt, "Cryptographic Protocols", UMI Dissertation Services.
33. Mats Naslund, "Bit Extraction, Hard-Core Predicates, and the Bit Security of RSA", Ph.D. Thesis.
34. Noam Nisan, "Using Hard Problems to Create Pseudorandom Generators", The MIT Press.
35. Takeshi Okamoto, "Studies on Identity-Based Fault-Tolerant Key Distribution Systems", Ms.D. Thesis.
36. Sophia A. Paleologou, "Probabilistic Decision Making in Games and Cryptographic Protocols", UMI Dissertation Services.
37. Giuseppe Persiano, "Interaction in Zero-Knowledge Proof Systems", UMI Dissertation Services.
38. David Pointcheval, "Les Preuves de Connaissance et leurs Preuves de Sécurité", Ph.D. Thesis.
39. C. Radu, "Analysis and Design of Off-Line Electronic Payment Systems", Ph.D. Thesis.
40. Zulfikar Amin Ramzan, "Group Blind Digital Signatures : Theory and Applications", Ms.D. Thesis.
41. Sunil Kumar Rottou, "A Survey of Zero-Knowledge Techniques and Their Applications", UMI Dissertation Services.
42. (성균관대) Hermann Schneider, "Analysis of the Resistance of Different Logic Styles against SPA & DPA Attacks", TUG Diploma Thesis.
43. Daniel Ron Simon, "On Defining and Achieving Cryptographic Security in a Multiparty Network", UMI Dissertation Services.
44. Markus Stadler, "Cryptographic Protocols for Revocable Privacy", Nachdruck der Diss. ETH No.11651.
45. (성균관대) Stefan Tillich, "Evaluation of Side-Channel Attack Resistivity with Rapid Prototyping", TUG Diploma Thesis.
46. Stephen Trilling, "Some Implications of Complexity Theory on Pseudo-Random Bit Generation", Ms.D. Thesis.
47. Amr Mohamed Youssef, "Analysis and Design of Block Ciphers", Ph.D. Thesis.
48. Mei Zhang, "Information Leakage of Boolean Functions", UMI Dissertation Services.

49. Yuliang Zheng, “A Study on Probabilistic Cryptosystems and Zero-Knowledge Protocols”, Ms.D. Thesis.
50. Jianying Zhou, “Non-repudiation”, Ph.D. Thesis.

제 5 절 Etc.

1. (성균관대) “누구나 이해할 수 있는 상대성 이론”, Newton HIGHLIGHT.
2. (성균관대) “누구나 이해할 수 있는 양자론”, Newton HIGHLIGHT.
3. (성균관대) 김중태, “대한민국 IT사 100 - 파콤222에서 미네르바까지 -”, e비즈북스.
4. (성균관대) 존 더비셔 (박병철 옮김), “리만 가설 - 베른하르트 리만과 소수의 비밀 -”, 승산.
5. (성균관대) 랜디 포시 (심은우 옮김), “마지막 강의”, 살림.
6. (성균관대) 리처드 파인만, “일반인을 위한 파인만의 QED 강의”, 승산.
7. (성균관대) 리처드 파인만 (승영조, 김희봉 옮김), “발견하는 즐거움”, 승산.
8. (성균관대) 리처드 파인만 (박병철 옮김), “파인만의 여섯가지 물리이야기”, 승산.
9. (성균관대) 리처드 파인만 (박병철 옮김), “파인만의 또다른 물리이야기”, 승산.
10. (성균관대) 리처드 파인만 (정무광, 정재승 옮김), “파인만의 과학이란 무엇인가?”, 승산.
11. (성균관대) 리처드 파인만, 로버트 레이턴, 매슈 샌즈 (박병철 옮김), “파인만의 물리학 강의 (Vol.1)”, 승산.
12. (성균관대) 리처드 파인만, 로버트 레이턴, 매슈 샌즈 (김인보, 박병철 외 6명 옮김), “파인만의 물리학 강의 (Vol.2)”, 승산.
13. (성균관대) 리처드 파인만, 마이클 고틀리브, 랠프 레이턴 (박병철 옮김), “파인만의 물리학 길라잡이 - 강의록에 딸린 문제 풀이 -”, 승산.
14. (성균관대) 마이클 바 (이석주 옮김), “C·C++로 작성하는 임베디드 시스템 프로그래밍 (Programming Embedded Systems in C and C++)”, 한빛 미디어.
15. (성균관대) 매일경제신문 산업부, “반도체 이야기”, 이지북.
16. 박명순, “컴퓨터 바이러스 - 분석, 제작 및 예/치방 -”, 기한제.

17. (성균관대) 박영환, “임베디드 시스템 + 임베디드 리눅스”, 사이텍미디어.
18. 박재호, “임베디드 리눅스”, 한빛미디어.
19. (성균관대) 박지훈, “누가 소프트웨어의 심장을 만들었는가”, 한빛미디어.
20. 스티븐 호킹 (김동광 옮김), “그림으로 보는 시간의 역사”, 까치.
21. 스티븐 호킹 (김동광 옮김), “호두껍질 속의 우주”, 까치.
22. (성균관대) 신영석, 박동선, 주수중, “Embedded Linux 이론과 실습”, 홍릉과학출판사.
23. 안철수, “바이러스 분석과 백신 제작”, (주)정보시대.
24. (성균관대) ANK Co., Ltd., (이영란 옮김), “TCP/IP가 보이는 그림책”, 성안당.
25. 이귀영 “Add-on Linux Kernel Programming”, 글로벌.
26. (성균관대) 임재춘, “한국의 이공계는 글쓰기가 두렵다”, 마이너
27. (성균관대) 임재춘, “한국의 직장인은 글쓰기가 두렵다”, 북코리아
28. (성균관대) 조지 가모브 (승영조 옮김), “조지 가모브 물리열차를 타다”, 승산.
29. (성균관대) 조지 존슨 (김재완 옮김), “양자 컴퓨터 - 이보다 더 빠른 컴퓨터는 있을 수 없다 -”, 한승.
30. (성균관대) 존 윌리엄 토이고 (김민아, 정윤이, 조경숙 옮김), “재해 복구 전략 (Disaster Recovery Planning - Preparing for the Unthinkable -)”, 한빛미디어.
31. 존 캣슬리스 (박재호, 이해영 옮김), “임베디드 하드웨어 이해와 설계 (Designing Embedded Hardware)”, O'Reilly.
32. 지원우, “컴퓨터 바이러스 - 예방과 치료 -”, 도서출판 지산사.
33. (성균관대) Steven Shepard (정교일 역), “알기쉬운 전파식별”, 홍릉과학출판사
34. (성균관대) Tsutomu Tone (김성훈 옮김), “성공과 실패를 결정하는 1%의 네트워크 원리”, 성안당.
35. (성균관대) 탁승호, “Let's Smart Card 스마트카드”, 성안당.
36. Sinan Si Alhir, “Learning UML”, O'Reilly.
37. (성균관대) Zhiqun Chen, “Java Card™ Technology for Smart Cards - Architecture and Programmer's Guide -”, Addison-Wesley.

38. (성균관대) Gordon Clarke, Deon Reynders, “Practical Modern SCADA Protocols – DNP3, IEC 60870.5 and Related Systems –”, Newnes.
39. (성균관대) Olivier Dubuisson (Philippe Fouquart 옮김), “ASN.1 Communication Between Heterogeneous Systems”, Morgan Kaufmann.
40. (성균관대) Klaus Finkenzeller (Rachel Waddington 옮김) “RFID Handbook – Fundamentals and Applications in Contactless Smart Cards and Identification – (Second Edition)”, WILEY.
41. (성균관대) Bill Glover and Himanshu Bhatt, “RFID Essentials”, O’Reilly.
42. (성균관대) Yahya Haghiri and Thomas Tarantino, “Smart Card Manufacturing – A Practical Guide –”, John Wiley & Sons, Ltd.
43. (성균관대) Uwe Hansmann, Martin S. Nicklous, Thomas Schack, Achim Schneider, and Frank Seliger, “Smart Card Application Development Using Java – Second Edition –”, Springer.
44. Greg Lehey, “The Complete FreeBSD – Documentation from the Source –”, O’Reilly.
45. Robert Love, “Linux Kernel Development”, Developer’s Library.
46. (성균관대) Charles Petzold, “하드웨어와 소프트웨어 CODE”, 정보문화사.
47. Sara Radicati, “Electronic Mail – An Introduction to the X.400 Message Handling Standards –”, McGraw-Hill, Inc.
48. (성균관대) Khalid Sayood, “Introduction to Data Compression”, Morgan Kaufmann Publishers, Inc.
49. (성균관대) Matthew Syme and Philip Goldie, “Optimizing Network Performance with Content Switching – Server, Firewall, and Cache Load Balancing –”, Prentice Hall.
50. Michael J. Young (김용권 옮김), “Step by Step XML”, 정보문화사.
51. Jose Luis Zoreda and Jose Manuel Oton, “Smart Cards”, Artech House.