Özgeçmiş

1. Adı Soyadı : Çetin Kaya Koç

2. Doğum Tarihi : 23 Ocak 1957

3. Ünvanı : Profesör

4. Öğrenim Durumu

Derece	Alan	Üniversite	Yıl
Lisans	Elektronik ve Haberleşme Mühendisliği	İstanbul Teknik Üniversitesi	1980
Y. Lisans	Elektronik ve Haberleşme Mühendisliği	İstanbul Teknik Üniversitesi	1982
Y. Lisans	Elektronik ve Bilgisayar Mühendisliği	Kaliforniya Üniversitesi	1985
Doktora	Elektronik ve Bilgisayar Mühendisliği	Kaliforniya Üniversitesi	1988

5. Akademik Ünvanlar

Yard. Doçent	Elek. ve Bilgisayar Müh.	Houston Üniversitesi (Texas)	1988-1992
Doçent	Elek. ve Bilgisayar Müh.	Oregon Devlet Üniversitesi	1992-1995
Profesör	Elek. ve Bilgisayar Müh.	Oregon Devlet Üniversitesi	1998-2007
Profesör	Bilgisayar Mühendisliği	Kaliforniya Üniversitesi	2008-2017
Profesör	Bilgisayar Mühendisliği	İstinye Üniversitesi	2017-bugüne

6. Yönetilen Yüksek Lisans ve Doktora Tezleri

6.1. Yüksek Lisans Tezleri

Houston Üniversitesi

1. S. N. Arachchige. *A Fast Algorithm for Gaussian Elimination over GF(2)*, 1990.
2. S. C. Gan. *Parallel Matrix Multiplication on Microcomputer Networks*, 1990.
3. C. Y. Hung. *Fast Algorithms and VLSI Structures for Modular Multiplication*, 1990.
4. A. Sharma. *Solution of Linear Recurrences on Hypercube Multiprocessors*, 1990.
4. B. N. Elkhoury. *Prefix Computation on Distributed Memory Multiprocessors*, 1990.
6. R. M. Piedra. *Exact Solution of Linear Equations on Multiprocessors*, 1990.
7. P. R. V. Subramaniam. *Two Algorithms for Mixed-Radix Conversion*, 1990.
8. X. Qian. *Fast Algorithms for Computation of Periodic Continued Fractions*, 1991.
9. L. C. Achour. *An Improved Congruence Algorithm*, 1991.
10. B. B. Youssef. *New Parallel Algorithms Chebyshev Polynomials*, 1991.
11. S. K. Gajawada. *New Packing Strategies for Convolution*, 1991.
12. S. Kuttalingam. *An Integrated Platform for Image Processing*, 1991.
13. M. N. K. Iyengar. *A Signal Acquisition and Analysis System*, 1992.
14. B. Bakkaloğlu. *Fast and Stable Algorithms for Matrix Sign Functions*, 1992.
15. A. A. Güvenç. *Improving the Performance of the Congruence Technique*, 1992.

Oregon Devlet Üniversitesi

16. Y. Peng. *High-Speed Implementations of the RSA Cryptosystem*, January 1995.
17. S. Johnson. *Hardware Implementations of Modular Multiplication*, March 1995.
18. C. K. Sandalcı. *Three Dimensional Monte Carlo Simulator*, May 1996.
19. J. B. Sessions. *Fast Software Implementations of Block Ciphers*, November 1998.
20. M. Musa. *Improved Montgomery Algorithms using Special Primes*, June 2000.
21. E. Turan. *ECDSA Optimizations on an ARM Processor*, June 2001.
22. H. Tanık. *ECDSA Optimizations on an ARM Processor*, June 2001.
23. A. W. Montville. *Random Number Generation on Handheld Devices*, May 2003.
24. S. Almanei. *Secure Instant Messaging: The Jabber Protocol*, June 2003.
25. U. Banerjee. *Hardware Encryption Using the MPC180 Co-Processor*, December 2003.
26. P. Godbole. *Optimizing the AES on Intel's SIMD Architecture*, January 2004.
27. O. Acıiçmez. *Fast Hashing on Pentium SIMD Architecture*, May 2004.
28. C. W. van Dyke. *An In-Depth Analysis of Software Vulnerabilities*, May 2004.
29. W.-C. Yang. *Hardware Realization for AES Key Generation*, May 2005.
30. L. Barlow. *Symmetric Encryption with Multiple Keys*, May 2005.
31. S. J. Park. *Design of Scalable and Unified Modular Multiplication*, June 2005.
32. R. Shamsuddin. *A Study of AES Implementations on ARM Processors*, June 2005.
33. A. A. Faresi. *Hardware Realization of the OCB Mode*, June 2005.

Işık Üniversitesi

34. Ö. A. Pamukçu. *IPCUBE: Personal Firewall on Linux*, June 2004.
35. E. Durak. *IPWALL: Gateway Firewall on Linux*, June 2004.
36. Ü. Kunter. *Risk Scalable and Modular Security Architectures*, April 2005.
37. M. Cihan. *Key Exchange Methods in Ad Hoc Networks*, April 2005.

Kaliforniya Üniversitesi

38. T. Cayton. *Analysis and Improvements of the AKS Algorithm*, June 2016.
39. A. Singh. *Decentralized Blockchain-Based Secure Messaging System*, March 2017.
40. P. M. Sosa. *Implementing a Lattice-Based Authenticated Key Exchange*, May 2017.

6.2. Doktora Tezleri

1. Bertan Bakkaloğlu. *Parallel and High-Performance Matrix Function Computations*, Oregon State University, December 1995.
2. Tolga Acar. *High-Speed Algorithms and Architectures for Cryptography*, Oregon State University, December 1997.
3. Berk Sunar. *Fast Galois Field Arithmetic for Elliptic Curve Cryptography and Error Control Codes*, Oregon State University, December 1998.
4. Alper Halbutoğulları. *Fast Bit-Level, Word-Level and Parallel Arithmetic in Finite Fields for Elliptic Curve Cryptosystems*, Oregon State University, December 1998.

5. Francisco Rodríguez-Henríquez. *New Algorithms and Architectures for Arithmetic in $GF(2^m)$ Suitable for Elliptic Curve Cryptography*, Oregon State University, June 2000.
6. Murat Aydos. *Efficient Wireless Security Protocols based on Elliptic Curve Cryptography*, Oregon State University, June 2000.
7. Erkay Savaş. *Implementation Aspects of Elliptic Curve Cryptography*, Oregon State University, June 2000.
8. Serdar Erdem. *Improving the Karatsuba-Ofman Multiplication Algorithm for Special Applications*, Oregon State University, November 2001.
9. Tuğrul Yanık. *New Methods for Finite Field Arithmetic*, Oregon State University, November 2001.
10. Adnan Abdul-Aziz Gutub. *New Hardware Algorithms and Designs for Montgomery Modular Inverse Computation in Galois Fields GF(p) and GF(2^n)*, (co-advised with Alex Tenca), Oregon State University, June 2002.
11. Lo'ai Tawalbeh. *A Novel Unified Algorithm and Hardware Architecture for Integrated Modular Division and Multiplication in GF(p) and GF(2^n) Suitable for Public-Key Cryptography*, Oregon State University, December 2004.
12. Gökay Saldamlı. *Spectral Modular Arithmetic*, Oregon State University, June 2005.
13. Colin William van Dyke. *Advances in Low-Level Software Protection*, Oregon State University, June 2005.
14. Minho Kim. *Cryptanalysis and Enhancement of Authentication Protocols*, Oregon State University, August 2006.
15. Onur Acıiçmez. *Advances in Side-Channel Cryptanalysis: Micro-Architectural Attacks*, Oregon State University, December 2006.
16. Samuel Green. *Reinforcement Learning for Cyber-Physical Safety Engineering*, University of California Santa Barbara, December 2018.

7. Yayınlar

7.1. Uluslararası Hakemli Dergilerde Yayınlanan Yayınlar

1. Ö. Eğecioğlu and Ç. K. Koç. A fast algorithm for rational interpolation via orthogonal polynomials. *Mathematics of Computation*, 53(187):249-264, July 1989.
2. Ç. K. Koç and P. F. Ordung. Schwarz-Christoffel transformation for the simulation of two dimensional capacitance. *IEEE Transactions on Computer-Aided Design*, 8(9):1025-1027, September 1989.
3. Ö. Eğecioğlu, Ç. K. Koç, and A. J. Laub. A recursive doubling algorithm for solution of tridiagonal systems on hypercube multiprocessors. *Journal of Computational and Applied Mathematics*, 27(1+2):95-108, 1989.
4. Ö. Eğecioğlu, E. Gallopoulos, and Ç. K. Koç. Parallel Hermite interpolation: An algebraic approach. *Computing*, 42(4):291-307, 1989.
5. Ö. Eğecioğlu, E. Gallopoulos, and Ç. K. Koç. Fast computation of generalized divided differences and parallel Hermite interpolation. *Journal of Complexity*, 5(4):417-437, December 1989.
6. Ö. Eğecioğlu, E. Gallopoulos, and Ç. K. Koç. A parallel method for fast and practical high-order Newton interpolation. *BIT*, 30(2):268-288, 1990.

7. Ö. Eğecioğlu and Ç. K. Koç. Parallel rational interpolation. *International Journal of Computer Mathematics*, 32(3+4):217-231, 1990.
8. Ç. K. Koç and C. Y. Hung. Multi-operand modulo addition using carry save adders. *Electronics Letters*, 26(6):361-363, 15th March 1990.
9. Ç. K. Koç and C. Y. Hung. Carry save adders for computing the product AB modulo N. *Electronics Letters*, 26(13):899-900, 21st June 1990.
10. P. Cappello, E. Gallopoulos, and Ç. K. Koç. Systolic computation of interpolating polynomials. *Computing*, 45(2):95-117, 1990.
11. Ö. Eğecioğlu, Ç. K. Koç, and J. R. I. Coma. Fast computation of continued fractions. *Computers and Mathematics with Applications*, 21(2-3):167-169, 1991.
12. Ç. K. Koç, P. Cappello, and E. Gallopoulos. Decomposing polynomial interpolation for systolic arrays. *International Journal of Computer Mathematics*, 38(3+4):219-239, 1991.
13. Ç. K. Koç and C. Y. Hung. Bit-level systolic arrays for modular multiplication. *Journal of VLSI Signal Processing*, 3(3):215-223, 1991.
14. Ç. K. Koç and S. N. Arachchige. A fast algorithm for Gaussian elimination over GF(2) and its implementation on the GAPP. *Journal of Parallel and Distributed Computing*, 13(1):118-122, September 1991.
15. Ç. K. Koç and G. Chen. Parallel algorithms for Nevanlinna-Pick interpolation: The scalar case. *International Journal of Computer Mathematics*, 40(1+2):99-115, 1991.
16. Ç. K. Koç. Comments on "Residue arithmetic VLSI array architecture for manipulator pseudo-inverse Jacobian computation". *IEEE Transactions on Robotics and Automation*, 7(5):715-716, October 1991.
17. Ç. K. Koç. An improved algorithm for mixed-radix conversion of residue numbers. *Computers and Mathematics with Applications*, 22(8):63-71, 1991.
18. Ç. K. Koç. High-radix and bit recoding techniques for modular exponentiation. *International Journal of Computer Mathematics*, 40(3+4):139-156, 1991.
19. K. V. K. Iyer, H. Öğmen, and Ç. K. Koç. Landscape reshaping algorithm for additive neural networks with application to graph mapping problems. *Electronics Letters*, 28(2):109-111, 16th January 1992.
20. Ç. K. Koç and S. C. Gan. Parallel matrix multiplication on networked microcomputers. *Computers and Electrical Engineering*, 18(2):145-152, 1992.
21. Ç. K. Koç. A parallel algorithm for exact solution of linear equations via congruence technique. *Computers and Mathematics with Applications*, 23(12):13-24, 1992.
22. Ö. Eğecioğlu and Ç. K. Koç. A parallel algorithm for generating discrete orthogonal polynomials. *Parallel Computing*, 18(6):649-659, June 1992.
23. Ç. K. Koç and C. Y. Hung. Adaptive m-ary segmentation and canonical recoding algorithms for multiplication of large binary numbers. *Computers and Mathematics with Applications*, 24(3):3-12, 1992.
24. Ö. Eğecioğlu and Ç. K. Koç. Parallel prefix computation with few processors. *Computers and Mathematics with Applications*, 24(4):77-84, 1992.
25. Ç. K. Koç and G. Chen. A fast algorithm for scalar Nevanlinna-Pick interpolation. *Numerische Mathematik*, 64(1):115-126, 1993.

26. Ç. K. Koç and P. Cappello. Systolic arrays for integer Chinese remaindering. *Parallel Computing*, 19(11):1303-1311, November 1993.
27. Ç. K. Koç and G. Chen. Inversion of all principal submatrices of a matrix. *IEEE Transactions on Aerospace and Electronic Systems*, 30(1):280-281, January 1994.
28. G. Chen and Ç. K. Koç. Computing matrix-valued Nevanlinna-Pick interpolation. *Linear Algebra and its Applications*, 203-204:253-263, 1994.
29. Ç. K. Koç and S. Johnson. Multiplication of signed-digit numbers. *Electronics Letters*, 30(11):840-841, 26th May 1994.
30. Ç. K. Koç, G. Chen, and C. K. Chui. Complexity analysis of wavelet signal decomposition and reconstruction. *IEEE Transactions on Aerospace and Electronic Systems*, 30(3):910-918, July 1994.
31. Ç. K. Koç, A. Güvenç, and B. Bakkaloğlu. Exact solution of linear equations on distributed-memory multiprocessors. *Parallel Algorithms and Applications*, 3:135-143, 1994.
32. Ö. Eğecioğlu and Ç. K. Koç. Exponentiation using canonical recoding. *Theoretical Computer Science*, 129(2):407-417, 1994.
33. Ç. K. Koç, B. Bakkaloğlu, and L. S. Shieh. Computation of the matrix sign function using continued fraction expansion. *IEEE Transactions on Automatic Control*, 39(8):1644-1647, August 1994.
34. Ç. K. Koç. Montgomery reduction with even modulus. *IEE Proceedings - Computers and Digital Techniques*, 141(5):314-316, September 1994.
35. Ç. K. Koç and B. Bakkaloğlu. Halley's method for the matrix sector function. *IEEE Transactions on Automatic Control*, 40(5):944-948, May 1995.
36. Ç. K. Koç. Analysis of sliding window techniques for exponentiation. *Computers and Mathematics with Applications*, 30(10):17-24, 1995.
37. Ç. K. Koç, T. Acar and B. S. Kaliski Jr. Analyzing and comparing Montgomery multiplication algorithms. *IEEE Micro*, 16(3):26-33, June 1996.
38. Ç. K. Koç and B. Bakkaloğlu. A parallel algorithm for functions of triangular matrices. *Computing*, 57(1):85-92, 1996.
39. Ç. K. Koç. Parallel canonical recoding. *Electronics Letters*, 32(22):2063-2065, 24th October 1996.
40. B. Bakkaloğlu, K. Erciyes, and Ç. K. Koç. A parallelization of Parlett's algorithm for functions of triangular matrices. *Parallel Algorithms and Applications*, 11(1-2):61-69, 1997.
41. Ç. K. Koç and A. M. Apohan. Inversion of cellular automata iterations. *IEE Proceedings - Computers and Digital Techniques*, 144(5):279-284, September 1997.
42. Ç. K. Koç and M. İnceoğlu. A parallel algorithm for principal nth roots of matrices. *Automatica*, 33(9):1735-1738, September 1997.
43. Ç. K. Koç. Parallel p-adic method for solving linear systems of equations. *Parallel Computing*, 23(13):2067-2074, December 15, 1997.
44. C. K. Sandalcı, Ç. K. Koç, and S. M. Goodnick. Three dimensional Monte Carlo device simulation with parallel multigrid solver. *International Journal of High Speed Computing*, 9(3):223-236, 1997.

45. S. S. Pennathur, C. K. Sandalcı, Ç. K. Koç, and S. M. Goodnick. 3D parallel Monte Carlo simulation of GaAs MESFETs. *VLSI Design*, 6(1-4):273-276, 1998.
46. Ç. K. Koç and B. Sunar. Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields. *IEEE Transactions on Computers*, 47(3):353-356, March 1998.
47. Ç. K. Koç and T. Acar. Montgomery multiplication in GF(2^k). *Designs, Codes and Cryptography*, 14(1):57-69, April 1998.
48. Ç. K. Koç and C. Y. Hung. Fast algorithm for modular reduction. *IEE Proceedings - Computers and Digital Techniques*, 145(4):265-271, July 1998.
49. B. Sunar and Ç. K. Koç. Mastrovito multiplier for all trinomials. *IEEE Transactions on Computers*, 48(5):522-527, May 1999.
50. A. Halbutoğulları and Ç. K. Koç. Mastrovito multiplier for general irreducible polynomials. *IEEE Transactions on Computers*, 49(5):503-518, May 2000.
51. A. Halbutoğulları and Ç. K. Koç. Parallel multiplication in GF(2^k) using polynomial residue arithmetic. *Designs, Codes and Cryptography*, 20(2):155-173, June 2000.
52. E. Savaş and Ç. K. Koç. The Montgomery modular inverse - revisited. *IEEE Transactions on Computers*, 49(7):763-766, July 2000.
53. B. Sunar and Ç. K. Koç. An efficient optimal normal basis type II multiplier. *IEEE Transactions on Computers*, 50(1):83-87, January 2001.
54. A. Levi and Ç. K. Koç. Risks in email security. *Communications of the ACM*, 44(8):112-112, August 2001.
55. M. Aydos, T. Yanık, and Ç. K. Koç. High-speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor. *IEE Proceedings - Communications*, 148(5):273-279, October 2001.
56. T. Yanık, E. Savaş, and Ç. K. Koç. Incomplete reduction in modular arithmetic. *IEE Proceedings - Computers and Digital Techniques*, 149(2):46-52, March 2002.
57. Ç. K. Koç and C. Paar. Guest editors' introduction to special section on cryptographic hardware and embedded systems. *IEEE Transactions on Computers*, 52(4):401-402, April 2003.
58. A. F. Tenca and Ç. K. Koç. A scalable architecture for modular multiplication based on Montgomery's algorithm. *IEEE Transactions on Computers*, 52(9):1215-1221, September 2003.
59. B. Sunar, E. Savaş, and Ç. K. Koç. Constructing composite field representations for efficient conversion. *IEEE Transactions on Computers*, 52(11):1391-1398, November 2003.
60. F. Rodríguez-Henríquez and Ç. K. Koç. Parallel multipliers based on special irreducible pentanomials. *IEEE Transactions on Computers*, 52(12):1535-1542, December 2003.
61. A. Levi, M. U. Çağlayan, and Ç. K. Koç. Use of nested certificates for efficient, dynamic and trust preserving public key infrastructure. *ACM Transactions on Information and System Security*, 7(1):21-59, February 2004.

62. E. Savaş, A. F. Tenca, M. E. Çiftçibaşı, and Ç. K. Koç. Novel multiplier architectures for $GF(p)$ and $GF(2^n)$. *IEE Proceedings - Computers and Digital Techniques*, 151(2):147-160, March 2004.
63. T. Wollinger, J. Pelzl, V. Wittelsberger, C. Paar, G. Saldamlı, and Ç. K. Koç. Elliptic and hyperelliptic curves on embedded μP. *ACM Transactions on Embedded Computing Systems*, 3(3):509-533, August 2004.
64. A. F. Tenca, E. Savaş, and Ç. K. Koç. A design framework for scalable and unified architectures that perform multiplication in $GF(p)$ and $GF(2^m)$. *International Journal of Computer Research*, 13(1):68-83, 2004.
65. E. Savaş, M. Naseer, A. A.-A. Gutub, and Ç. K. Koç. Efficient unified Montgomery inversion with multibit shifting. *IEE Proceedings - Computers and Digital Techniques*, 152(4):489-498, July 2005.
66. L. A. Tawalbeh and A. F. Tenca and Ç. K. Koç. A radix-4 design of a scalable modular multiplier with recoding techniques. *IEEE Potentials*, 24(2):16-18, April/May 2005.
67. M. Kim and Ç. K. Koç. A simple attack on a recently introduced hash-based strong-password authentication scheme. *International Journal of Network Security*, 1(2):77-80, September 2005.
68. M. Kim and Ç. K. Koç. A simple attack on a recently introduced hash-based secure user authentication scheme. *International Journal of Computer Science and Network Security*, 6(5B):157-160, May 2006.
69. S. S. Erdem, T. Yanık, and Ç. K. Koç. Polynomial basis multiplication in GF(2^m). *Acta Applicandae Mathematicae*, 93(1-3):33-55, September 2006.
70. M. Kim and Ç. K. Koç. Vulnerabilities in the Adachi-Aoki-Komano-Ohta micropayment scheme. *International Journal of Network Security*, 4(2):235-239, March 2007.
71. O. Acıiçmez, J. P. Seifert, and Ç. K. Koç. Micro-architectural cryptanalysis. *IEEE Security & Privacy*, 5(4):62-64, July/August 2007.
72. M. Kim and Ç. K. Koç. A secure hash-based strong-password authentication protocol using one-time public-key cryptography. *Journal of Information Science and Engineering*, 24(4):1213-1227, July 2008.
73. R. Steinwandt, W. Geiselmann, and Ç. K. Koç. Guest editors' introduction to the special section on special-purpose hardware for cryptography and cryptanalysis. *IEEE Transactions on Computers*, 57(11):1441-1442, November 2008.
74. E. Savaş and Ç. K. Koç. Finite field arithmetic for cryptography. *IEEE Circuits and Systems Magazine*, 10(2):40-56, 2010.
75. Ç. K. Koç. Introduction to the Journal of Cryptographic Engineering. *Journal of Cryptographic Engineering*, 1(1):1-3, March 2011
76. V. Trujillo-Olaya, T. Sherwood, and Ç. K. Koç. Analysis of performance versus security in hardware realizations of small elliptic curves for lightweight applications. *Journal of Cryptographic Engineering*, 2(3):179-188, 2012.
77. D. D. Chen, G. X. Yao, R. C. C. Cheung, D. Pao, and Ç. K. Koç. Parameter space for the architecture of FFT-based Montgomery modular multiplication. *IEEE Transactions on Computers*, 65(1):147-160, January 2016.

78. C. Kızılkale, Ö. Eğecioğlu, and Ç. K. Koç. A matrix decomposition method for optimal normal basis multiplication. *IEEE Transactions on Computers*, 65(11):3239-3250, November 2016.
79. W. Dai, D. D. Chen, R. C. C. Cheung, and Ç. K. Koç. Area-time efficient architecture of FFT-based Montgomery multiplication. *IEEE Transactions on Computers*, 66(3):375-388, March 2017.
80. N. Fern, İ. San, Ç. K. Koç, and K.-T. Cheng. Hiding hardware Trojan communication channels in partially specified SoC bus functionality. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 36(9):1435-1444, September 2017.
81. B. Peccerillo, S. Bartolini, and Ç. K. Koç. Parallel bitsliced AES through PHAST: a single-source high-performance library for multi-cores and GPUs. *Journal of Cryptographic Engineering*, 2018.
82. W. Dai, D. D. Chen, R. C. C. Cheung, and Ç. K. Koç. FFT-based McLaughlin's Montgomery exponentiation without conditional selections. *IEEE Transactions on Computers*, 2018.
83. E. Savaş and Ç. K. Koç. Montgomery inversion. *Journal of Cryptographic Engineering*, 2018.
84. Ç. K. Koç. Algorithms for inversion in p^k. *IEEE Transactions on Computers*, 2018.

7.2. Uluslararası Bilimsel Toplantı Bildiri Kitabında Basılan Yayınlar

1. P. Cappello, G. Davidson, A. Gersho, Ç. K. Koç, and V. Somayazulu. A systolic vector quantization processor for real-time speech coding. *Proceedings of the IEEE International Conference on Acoustic, Speech, and Signal Processing*, Vol. 3, pages 2143-2146, Tokyo, Japan, IEEE Press, New York, New York, April 8-11, 1986.
2. Ö. Eğecioğlu, Ç. K. Koç, and A. J. Laub. Prefix algorithms for tridiagonal systems on hypercube multiprocessors. *Proceedings of the Third Conference on Hypercube Concurrent Computers and Applications*, Vol. 2, pages 1539-1545, Pasadena, California, ACM Press, New York, New York, January 19-20, 1988.
3. Ö. Eğecioğlu and Ç. K. Koç. Orthogonal polynomials and least-squares approximation on the hypercube multiprocessor. *Proceedings of the Fourth Conference on Hypercube Concurrent Computers and Applications*, Vol. 1, pages 411-414, Monterey, California, Golden Gate Enterprises, Los Altos, California, March 6-8, 1989.
4. Ç. K. Koç and P. Cappello. Systolic arrays for integer Chinese remaindering. *Proceedings, 9th Symposium on Computer Arithmetic*, M. D. Ercegovac and E. Swartzlander, editors, pages 216-223, Santa Monica, California, IEEE Computer Society Press, Los Alamitos, California, September 6-8, 1989.
5. Ç. K. Koç. A fast algorithm for mixed-radix conversion in residue arithmetic. *Proceedings, 1989 IEEE International Conference on Computer Design: VLSI in Computers and Processors*, pages 18-21, Cambridge, Massachusetts, IEEE Computer Society Press, Los Alamitos, California, October 2-4, 1989.
6. Ö. Eğecioğlu and Ç. K. Koç. Fast modular exponentiation. *Communication, Control, and Signal Processing: Proceedings of 1990 Bilkent International Conference on New Trends in Communication, Control, and Signal Processing*, E. Arıkan, editor, Vol. 1, pages 188-194, Ankara, Turkey, Elsevier, Amsterdam, Netherlands, July 2-5, 1990.

7. Ç. K. Koç and R. M. Piedra. A parallel algorithm for exact solution of linear equations. *Proceedings of International Conference on Parallel Processing*, Vol. III, pages 1-8, St. Charles, Illinois, CRC Press, Boca Raton, Florida, August 12-16, 1991.
8. Ç. K. Koç, A. Güvenç, and B. Bakkaloğlu. Exact solution of linear equations on distributed-memory multiprocessors. *Proceedings of the 14th IMACS World Congress on Computational and Applied Mathematics*, Vol. 3, pages 1339-1341, Atlanta, Georgia, July 11-15, 1994.
9. G. Chen and Ç. K. Koç. A fast algorithm for matrix-valued Nevanlinna-Pick interpolation. *Conference on Approximation Theory VIII, Vol 1: Approximation and Interpolation*, C. K. Chui and L. L. Schumaker, editors, pages 129-136, World Scientific Publishing, 1995.
10. Ç. K. Koç and B. Bakkaloğlu. Halley's method for the matrix sector function. *Proceedings of the 12th European Conference on Circuit Theory and Design*, Vol. 2, pages 901-904, Istanbul, Turkey, August 27-31, 1995.
11. B. Bakkaloğlu and Ç. K. Koç. Parallel matrix sign iterations. *Proceedings of the 33rd Annual Allerton Conference on Communication, Control, and Computing*, pages 440-446, Urbana, Illinois, October 4-6, 1995.
12. Ç. K. Koç and T. Acar. Montgomery multiplication in GF(2^k). *Proceedings of Third Annual Workshop on Selected Areas in Cryptography*, pages 95-106, Queen's University, Kingston, Ontario, Canada, August 15-16, 1996.
13. C. K. Sandalcı, Ç. K. Koç, and S. M. Goodnick. Three dimensional Monte Carlo device simulation with parallel multigrid solver. *Proceedings of Eight SIAM Conference on Parallel Processing for Scientific Computing*, 10 pages, CD-ROM Format, Minneapolis, Minnesota, March 14-17, 1997.
14. Ç. K. Koç and T. Acar. Fast software exponentiation in GF(2^k). *Proceedings, 13th Symposium on Computer Arithmetic*, T. Lang, J.-M. Muller, and N. Takagi, editors, pages 225-231, Asilomar, California, IEEE Computer Society Press, Los Alamitos, California, July 6-9, 1997.
15. Ç. K. Koç and B. Sunar. Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields. *Proceedings of 1998 IEEE International Symposium on Information Theory*, pages 294-294, MIT, Cambridge, Massachusetts, August 16-21, 1998.
16. M. Aydos, E. Savaş, and Ç. K. Koç. Implementing network security protocols based on elliptic curve cryptography. *Proceedings of the Fourth Symposium on Computer Networks*, S. Oktuğ, B. Örencik, E. Harmancı, editors, pages 130-139, Istanbul, Turkey, May 20-21, 1999.
17. A. F. Tenca and Ç. K. Koç. A scalable architecture for Montgomery multiplication. *Cryptographic Hardware and Embedded Systems*, Ç. K. Koç and C. Paar, editors, First International Workshop, Worcester, MA, USA, pages 94-108. Springer, LNCS Nr. 1717, August 12-13, 1999.
18. A. Halbutoğulları and Ç. K. Koç. Mastrovito multiplier for general irreducible polynomials. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, M. Fossorier, H. Imai, S. Lin, and A. Poli, editors, 13th International Symposium, Honolulu, Hawaii, USA, pages 498-507, Springer, LNCS Nr. 1719, November 15-19, 1999.

19. E. Savaş, A. F. Tenca, and Ç. K. Koç. A scalable and unified multiplier architecture for finite fields $GF(p)$ and $GF(2^m)$. *Cryptographic Hardware and Embedded Systems - CHES 2000*, Ç. K. Koç and C. Paar, editors, Second International Workshop, Worcester, MA, USA, pages 277-292. Springer, LNCS Nr. 1965, August 17-18, 2000.
20. M. Aydos, T. Yanık, and Ç. K. Koç. An high-speed ECC-based wireless authentication protocol on an ARM microprocessor. *Proceedings, The 16th Annual Computer Security Applications Conference*, pages 401-409, New Orleans, Louisiana, IEEE Computer Society Press, Los Alamitos, California, December 11-15, 2000.
21. E. Savaş, T. A. Schmidt, and Ç. K. Koç. Generating elliptic curves of known order. *Cryptographic Hardware and Embedded Systems - CHES 2001*, Ç. K. Koç, D. Naccache, and C. Paar, editors, Third International Workshop, Paris, France, pages 142-158. Springer, LNCS Nr. 2162, May 14-16, 2001.
22. A. F. Tenca, G. Todorov, and Ç. K. Koç. High-radix design of a scalable modular multiplier. *Cryptographic Hardware and Embedded Systems - CHES 2001*, Ç. K. Koç, D. Naccache, and C. Paar, editors, Third International Workshop, Paris, France, pages 185-201. Springer, LNCS Nr. 2162, May 14-16, 2001.
23. A. Levi and Ç. K. Koç. Reducing certificate revocation cost using NPKI. *Trusted Information, The New Decade Challenge, IFIP TC11 16th International Conference on Information Security*, pages 51-59, M. Dupuy and P. Paradinas, editors, Kluwer Academic Publishers, Boston, Massachusetts, June 11-13, 2001.
24. A. Levi and Ç. K. Koç. CONSEPP: Convenient and secure electronic payment protocol based on X9.59. *Proceedings, The 17th Annual Computer Security Applications Conference*, pages 286-295, New Orleans, Louisiana, IEEE Computer Society Press, Los Alamitos, California, December 10-14, 2001.
25. A. A.-A. Gutub, A. F. Tenca, and Ç. K. Koç. Scalable VLSI Architecture for GF(p) Montgomery modular inverse computation. *IEEE Computer Society Annual Symposium on VLSI*, pages 53-58, Pittsburgh, Pennsylvania, IEEE Computer Society Press, Los Alamitos, California, April 25-26, 2002.
26. A. A.-A. Gutub, A. F. Tenca, E. Savaş, and Ç. K. Koç. Scalable and unified hardware to compute Montgomery inverse in GF(p) and GF(2^n). *Cryptographic Hardware and Embedded Systems - CHES 2002*, B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, 4th International Workshop, Redwood Shores, CA, USA, pages 484-499. Springer, LNCS Nr. 2523, August 13-15, 2002.
27. E. Savaş and Ç. K. Koç. Architectures for unified field inversion with applications in elliptic curve cryptography. *The 9th IEEE International Conference on Electronics, Circuits and Systems - ICECS 2002*, volume 3, pages 1155-1158, Dubrovnik, Croatia, September 15-18, 2002.
28. C. van Dyke and Ç. K. Koç. On ubiquitous network security and anomaly detection. *2003 Symposium on Applications and Internet (SAINT'03), Workshop 7: Security and Assurance in Ad hoc Networks*, pages 374-378, Orlando, Florida, January 27-31, 2003.
29. F. Rodríguez-Henríquez and Ç. K. Koç. On fully parallel Karatsuba multipliers for GF(2^m). *Proceedings of the International Conference on Computer Science and Technology - CST 2003*, pages 405-410, Acta Press, Cancun, Mexico, May 19-21, 2003.

30. S. S. Erdem and Ç. K. Koç. A less recursive variant of Karatsuba-Ofman algorithm for multiplying operands of size a power of two. *Proceedings, 16th IEEE Symposium on Computer Arithmetic*, J.-C. Bajard and M. Schulte, editors, pages 28-35, IEEE Computer Society Press, Santiago de Compostela, Spain, June 15-18, 2003.
31. E. Savaş, A. F. Tenca, and Ç. K. Koç. Dual-field multiplier architecture for cryptographic applications. *Thirty-Seventh Asilomar Conference on Signals, Systems, and Computers*, pages 374-378, IEEE Press, Pacific Grove, California, November 9-12, 2003.
32. A. Levi, E. Çetintaş, M. Aydos, Ç. K. Koç, and M. U. Çaglayan. Relay attacks on Bluetooth authentication and solutions. *Computer and Information Sciences - ISCIS 2004*, C. Aykanat et al, editors, 19th International Symposium, Kemer-Antalya, Turkey, pages 278-288, Springer, LNCS Nr. 3280, October 27-29, 2004.
33. L. A. Tawalbeh, A. F. Tenca, S. Park, and Ç. K. Koç. A dual-field modular division algorithm and architecture for application specific hardware. *Thirty-Eighth Asilomar Conference on Signals, Systems, and Computers*, pages 483-487, IEEE Press, Pacific Grove, California, November 7-10, 2004.
34. M. Cihan and Ç. K. Koç. Setting initial secret keys in a mobile adhoc network. *1st International Symposium on Information Technologies - ISIT 2005, Symposium Proceedings*, pages 71-83, Girne, North Cyprus, April 19-21, 2005.
35. L. A. Tawalbeh, A. F. Tenca, S. Park, and Ç. K. Koç. An efficient hardware architecture of a scalable elliptic curve crypto-processor over $GF(2^m)$. *Advanced Signal Processing Algorithms, Architectures, and Implementations XV, Proceedings of SPIE Conference*, F. T. Luk, editor, pages 216-226, Volume 5910, San Diego, California, August 2-4, 2005.
36. O. Acıiçmez, W. Schindler, and Ç. K. Koç. Improving Brumley and Boneh timing attack on unprotected SSL implementations. *Proceedings of 12th ACM Conference on Computer and Communications Security*, C. Meadows and P. Syverson, editors, pages 139-146, Alexandria, Virginia, November 7-11, 2005.
37. O. Acıiçmez and Ç. K. Koç. Trace-driven cache attacks on AES. *8th International Conference on Information and Communications Security, ICISCS 2006*, P. Ning, S. Qing, and N. Li, editors, pages 112-121, Springer, LNCS Nr. 4307, Raleigh, North Carolina, December 4-7, 2006.
38. O. Acıiçmez, W. Schindler, and Ç. K. Koç. Cache based remote timing attack on the AES. *Topics in Cryptology, The Cryptographers' Track at the RSA Conference, CT-RSA 2007*, M. Abe, editor, pages 271-286, Springer, LNCS Nr. 4377, San Francisco, California, February 5-9, 2007.
39. O. Acıiçmez, J. P. Seifert, and Ç. K. Koç. Predicting secret keys via branch prediction. *Topics in Cryptology, The Cryptographers' Track at the RSA Conference, CT-RSA 2007*, M. Abe, editor, pages 225-242, Springer, LNCS Nr. 4377, San Francisco, California, February 5-9, 2007.
40. O. Acıiçmez, Ç. K. Koç, and J. P. Seifert. On the power of simple branch prediction analysis. *ACM Symposium on Information, Computer and Communications Security, ASIACCS 2007*, R. Deng and P. Samarati, editors, pages 312-320, Singapore, March 20-22, 2007.

41. G. Saldamlı and Ç. K. Koç. Spectral modular exponentiation. *Proceedings, 18th IEEE Symposium on Computer Arithmetic*, P. Kornerup and J.-M. Muller, editors, pages 123-130, IEEE Computer Society Press, Montpellier, France, June 25-27, 2007.
42. İ. Yavuz, S. B. Ö. Yalçın, and Ç. K. Koç. FPGA implementation of an elliptic curve cryptosystem over GF(3^m). *2008 International Conference on ReConFigurable Computing and FPGAs*, pages 397-402, IEEE Computer Society Press, Cancun, Mexico, December 3-5, 2008.
43. G. Saldamlı, C. Demirkıran, M. Maguire, C. Minden, J. Topper, A. Troesch, C. Walker, and Ç. K. Koç. Spectral hash. *The First SHA-3 Candidate Conference*, Katholieke Universiteit, Leuven, Belgium, February 25-28, 2009.
44. M. Cenk, Ç. K. Koç, and F. Özbudak. Polynomial multiplication over finite fields using field extensions and interpolation. *Proceedings, 19th IEEE Symposium on Computer Arithmetic*, pages 84-91, IEEE Computer Society Press, Portland, Oregon, June 8-10, 2009.
45. R. C. C. Cheung, Ç. K. Koç, and J. D. Villasenor. An efficient hardware architecture for spectral hash algorithm. *Proceedings, 20th IEEE International Conference on Application-specific Systems, Architectures and Processors*, pages 215-218, IEEE Press, Boston, MA, July 7-9, 2009.
46. L.-W. Kim, J. D. Villasenor, and Ç. K. Koç. A Trojan-resistant system-on-chip bus architecture. *Proceedings of Military Communications Conference (MILCOM)*, pages 1-6, Boston, MA, October 18-21, 2009.
47. G. X. Yao, R. C. C. Cheung, Ç. K. Koç, and K. F. Man. Reconfigurable number theoretic transform architectures for cryptographic applications. *The 2010 International Conference on Field-Programmable Technology (FPT)*, pages 308-311, Beijing, China, December 8-10, 2010.
48. G. Saldamlı, Y.-J. Baek, and Ç. K. Koç. Spectral modular arithmetic for binary extension fields. *The 2011 International Conference on Information and Computer Networks (ICICN)*, pages 323-328, Guiyang, China, January 26-28, 2011.
49. J. Valamehr, T. Huffmire, C. Irvine, R. Kastner, Ç. K. Koç, T. Levin, and T. Sherwood. A qualitative security analysis of a new class of 3-D integrated crypto coprocessors. *Cryptography and Security: From Theory to Applications*, pages 364-382, D. Naccache, editor, LNCS Nr. 6805, Springer, 2012.
50. D. D. Chen, G. X. Yao, Ç. K. Koç, and R. C. C. Cheung. Low complexity and hardware-friendly spectral modular multiplication. *The 2012 International Conference on Field-Programmable Technology (FPT)*, pages 368-375, Seoul, Korea, December 10-12, 2012.
51. Ö. Eğecioğlu and Ç. K. Koç. Reducing the complexity of normal basis multiplication. *International Workshop on the Arithmetic of Finite Fields (WAIFI)*, Springer, LNCS Nr. 9061, pages 61-82, Gebze, Turkey, September 26-28, 2014.
52. N. Fern, İ. San, Ç. K. Koç, and K.-T. Cheng. Hardware Trojans in incompletely specified on-chip bus systems. *Design, Automation and Test in Europe (DATE)*, pages 527-530, Dresden, Germany, March 14-18, 2016.

53. S. Green, İ. Çiçek, and Ç. K. Koç. Continuous-time computational aspects of cyber-physical security. *Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 59-62, Santa Barbara, CA, USA, August 16, 2016.
54. İ. San, N. Fern, Ç. K. Koç, and K.-T. Cheng. Trojans modifying soft-processor instruction sequences embedded in FPGA bitstreams. *26th International Conference on Field-Programmable Logic and Applications (FPL)*, pages 334-337, Lausanne, Switzerland, August 29 - September 2, 2016.
55. S. Green, C. M. Vineyard, and Ç. K. Koç. Impacts of mathematical optimizations on reinforcement learning policy performance. International Joint Conference on Neural Networks (IJCNN), July 8-13, 2018.

7.3. Yazılan Uluslararası Kitaplar

1. Ç. K. Koç and C. Paar, editors. *Cryptographic Hardware and Embedded Systems*. First International Workshop, CHES 1999. Worcester, MA, USA. Springer, LNCS Nr. 1717, August 12-13, 1999.
2. Ç. K. Koç and C. Paar, editors. *Cryptographic Hardware and Embedded Systems*. Second International Workshop, CHES 2000. Worcester, MA, USA. Springer, LNCS Nr. 1965, August 17-18, 2000.
3. Ç. K. Koç, D. Naccache, and C. Paar, editors. *Cryptographic Hardware and Embedded Systems*. Third International Workshop, CHES 2001. Paris, France, Springer, LNCS Nr. 2162, May 14-16, 2001.
4. B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors. *Cryptographic Hardware and Embedded Systems*. 4th International Workshop, CHES 2002. Redwood Shores, CA, USA. Springer, LNCS Nr. 2523, August 13-15, 2002.
5. C. D. Walter, Ç. K. Koç, and C. Paar, editors. *Cryptographic Hardware and Embedded Systems*. 5th International Workshop, CHES 2003. Cologne, Germany, Springer, LNCS Nr. 2779, September 8-10, 2003.
6. J. von zur Gathen, J. L. Imana, and Ç. K. Koç, editors. *Arithmetic of Finite Fields*. 2nd International Workshop, WAIFI 2008. Siena, Italy. Springer, LNCS Nr. 5130, July 6-9, 2008.
7. Ç. K. Koç, S. Mesnager and E. Savaş, editors. *Arithmetic of Finite Fields*. 5th International Workshop, WAIFI 2014. Gebze, Turkey. Springer, LNCS Nr. 9061, September 27-28, 2014.
8. F. Rodríguez-Henríquez, N. A. Saqib, A. Díaz-Perez, and Ç. K. Koç. *Cryptographic Algorithms on Reconfigurable Hardware*. Springer, 2007.
9. Ç. K. Koç. *Cryptographic Engineering*. Springer, 2009.
10. Ç. K. Koç. *Open Problems in Math. and Computational Science*. Springer, 2014.
11. Ç. K. Koç. *Cyber-Physical Systems Security*. Springer, 2018.

7.3. Yazılan Uluslararası Kitaplarda Bölümler

1. Ö. Eğecioğlu, Ç. K. Koç, and A. J. Laub. A recursive doubling algorithm for solution of tridiagonal systems on hypercube multiprocessors. *Parallel Algorithms for Numerical Linear Algebra*, H. A. van der Vorst and P. van Dooren, editors, pages 95-108, North-Holland, Amsterdam, Netherland, 1990.
2. G. Chen and Ç. K. Koç. A fast algorithm for matrix-valued Nevanlinna-Pick interpolation. *Approximation Theory VIII, Vol 1: Approximation and Interpolation*, C. K. Chui and L. L. Schumaker, editors, pages 129-136, World Scientific Publishing, 1995.
3. A. F. Tenca, E. Savaş, and Ç. K. Koç. A design framework for scalable and unified architectures that perform multiplication in $GF(p)$ and $GF(2^m)$. *Embedded Cryptographic Hardware: Methodologies and Architectures*, N. Nedjah and L. de M. Mourelle, editors, pages 68-83, Nova Science Publishers, 2004.
4. L. Tawalbeh and Ç. K. Koç. Efficient elliptic curve cryptographic hardware design for wireless security. *Wireless Security and Cryptography: Specifications and Implementation*, N. Sklavos and X. Zhang, editors, CRC Press, pages 153-175, 2007.
5. S. Contini, Ç. K. Koç, and C. D. Walter. Modular arithmetic. *Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg and S. Jajodia, editors, Second Edition, Part 13, pages 795-798, Springer, August 2011.
6. Ç. K. Koç and C. D. Walter. Montgomery arithmetic. *Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg and S. Jajodia, editors, Second Edition, Part 13, pages 799-803, Springer, August 2011.
7. Ç. K. Koç. About open problems. number generators. *Open Problems in Mathematics and Computational Science*, Ç. K. Koç, editor, pages 1-4, Springer, December 2014.
8. M. Stipčević and Ç. K. Koç. True random number generators. *Open Problems in Mathematics and Computational Science*, Ç. K. Koç, editor, pages 275-315, Springer, December 2014.
9. R. K. Lim, L. R. Petzold, and Ç. K. Koç. Bitsliced high-performance AES-ECB on GPUs. *The New Codebreakers*, P. Y. A. Ryan, D. Naccache, and J.-J. Quisquater, editors, pages 125-133, Springer, LNCS Nr. 9100, 2016.

7.4. Ulusal Hakemli Dergilerde Yayınlanan Yayınlar

- Henüz yok

7.5. Ulusal Bilimsel Toplantı Bildiri Kitabında Basılan Yayınlar

- Henüz yok

7.6. Diğer Yayınlar (Patentler)

1. Ç. K. Koç and B. Sunar. Methods and Apparatus for Multiplication in a Galois Field $GF(2^m)$, and Encoders and Decoders using Same. US Patent Nr. 6,343,305. January 29, 2002.
2. Ç. K. Koç and A. F. Tenca. Scalable Methods and Apparatus for Montgomery Multiplication. US Patent Nr. 7,046,800. May 16, 2006.

3. Ç. K. Koç and E. Savaş. Cryptographic Methods and Apparatus using Word-wise Montgomery Multiplication. US Patent Nr. 7,050,579. May 23, 2006.
4. Ç. K. Koç, T. Yanık, and E. Savaş. Methods and Apparatus for Incomplete Modular Arithmetic. US Patent Nr. 7,080,109. July 18, 2006.
5. Ç. K. Koç, A. F. Tenca, and G. Todorov. Methods and Apparatus for Variable Radix Scalable Modular Multiplication. US Patent Nr. 7,174,015. February 6, 2007.
6. Ç. K. Koç, E. Savaş, and A. F. Tenca. Scalable and Unified Multiplication Methods and Apparatus. US Patent Nr. 7,240,204. July 3, 2007.
7. Ç. K. Koç and S. S. Erdem. Multiplication of Multi-precision Numbers having a Size of a Power of Two. US Patent Nr. 7,401,109. July 15, 2008.
8. Ç. K. Koç and S. S. Erdem. Lean multiplication of multi-precision numbers over GF(2^m). US Patent Nr. 7,447,310. November 4, 2008.
9. Ç. K. Koç. Systems and methods for providing security for computer systems. US Patent Nr. 8,090,934. January 3, 2012.
10. G. Hammouri, B. Sunar, Ç. K. Koç, and K. Akdemir. Computing system identifier using software extraction of manufacturing variability. US Patent Nr. 8,694,687, April 8, 2014.
11. Ç. K. Koç and G. Saldamlı. Spectral modular arithmetic method and apparatus. US Patent Nr. 8,719,324. May 6, 2014.
12. G. Hammouri, B. Sunar, and Ç. K. Koç. Mobile phone aided operations system and method. US Patent Nr. 8,842,827. September 23, 2014.
13. M. Hubert, C. Walker, C. Minden, G. Hammouri, and Ç. K. Koç. Systems and methods for authorizing transactions via a digital device. US Patent Nr. 10,013,692. July 3, 2018.

7.6. Diğer Yayınlar (Teknik Raporlar)

14. Ç. K. Koç. High-Speed RSA Implementation. TR 201, RSA Laboratories, November 1994.
15. Ç. K. Koç. RSA Hardware Implementation. TR 801, RSA Laboratories, April 1996.
16. Ç. K. Koç. A Divide-and-Conquer Algorithm for Functions of Triangular Matrices. Technical Report, Electrical Engineering and Computer Science, Oregon State University, June 1996.
17. Ç. K. Koç. Analysis of MMX Technology for Implementing Number-Theoretic Cryptosystems. Technical Report, Intel Corporation, February 1997.
18. Ç. K. Koç and T. Acar. A Methodology for High-Speed Software Implementations of Number-Theoretic Cryptosystems. Technical Report, Electrical Engineering and Computer Science, Oregon State University, May 1997.
19. Ç. K. Koç and A. Halbutoğulları. A Reduction Method for Multiplication in Finite Fields. Technical Report, Electrical Engineering and Computer Science, Oregon State University, August 1998.
20. Ç. K. Koç. Recommended Test Plan for Arithmetic and Cryptographic Operations in DTCP Signing Facility. Technical Report, Intel Corporation, October 1998.

21. E. Savaş and Ç. K. Koç. Efficient Methods for Composite Field Arithmetic. Technical Report, Electrical Engineering and Computer Science, Oregon State University, December 1999.
22. Ç. K. Koç. A Tutorial on p-adic Arithmetic. Technical Report, Electrical Engineering and Computer Science, Oregon State University, April 2002.
23. Ç. K. Koç. Cryptographic Hash Functions. Technical Report, New Technologies Incorporated, November 2002.

8. Projeler

1. National Science Foundation. *Cyber Physical Systems Security Education Workshop*, Grant: $ 49,350 USD. June 2016.
2. National Science Foundation, *STARSS: Small: Detection of Hardware Trojans Hidden in Unspecified Design Functionality*, Grant: $ 300,000. October 2015.
3. Private Source, *Large-Scale E-voting Algorithms Protocols, User Interfaces, and Machines*. Research Gift: $ 1,700,000. March 2013.
4. National Science Foundation, *SBIR Phase I: Fingerprinting Smart-phones for Strong Authentication*. Grant: $ 150,000. February 2010.
5. Turkish National Science and Engineering Foundation, *Design of a Low-Power, Small-Area Advanced Encryption Standard (AES) Encryption/Decryption Processor*. Grant: $ 400,000. 2008.
6. Pacific Northwest National Laboratories: *Anti-Reverse-Engineering Techniques in Software Development*. Grant: $ 90,000. September 2003 - January 2005.
7. rTrust Technologies, Pasadena, California: *High-Speed Hardware and Software Methods for Elliptic Curve Cryptography*. Grant: $ 1,040,000. October 1998 - 2001.
8. Intel Corporation, Hillsboro, Oregon: *Optimization and Performance Evaluation of Cryptographic Libraries*. Grant: $ 210,564. October 1995 - 1998.
9. National Science Foundation: *Parallelization of Particle Transport Algorithms in Semiconductor Device Physics*. Grant: $ 406,348. June 1994 - December 1998.
10. US Army Research Office: *Robust Hybrid State-Space Self-Tuning Control Using Dual-Rate Sampling*. Grant: $ 160,000. May 1991 - 1993.

9. İdari Görevler

- İstinye Üniversitesi, Mühendislik Fakültesi Dekanı, Ekim 2017den beri

10. Bilimsel Kuruluşlara Üyelikler

- **Kurucu Baş Editör**, *Journal of Cryptographic Engineering*, since 2011. **Kriptografi Mühendisliği alanında en önemli dergi**.
- **Kurucu**, *Workshop on Cryptographic Hardware and Embedded Systems*, since 1999. **Dünyanın ikinci büyük kriptografi konferansı**.
- **Kurucu**, *International Workshop on the Arithmetic of Finite Fields*, since 2007.
- **Kurucu**, *Security Proofs for Embedded Systems Conference*, since 2012.

- **Yardımcı (Associate) Editör**, *International Journal of Foundations of Computer Science*, since 2016.
- **Yardımcı (Associate) Editör**, *IEEE Transactions on Computers*, 2003-2007 and since 2015.
- **Yardımcı (Associate) Editör**, *IEEE Transactions on Mobile Computing*, 2003-2007.
- **Misafir Editör**, *IEEE Transactions on Computers*, Special Section on Engineering of Post-Quantum Cryptography, in progress, 2018.
- **Misafir Editör**, *IEEE Transactions on Computers*, Special Section on Special-Purpose Hardware for Cryptography and Cryptanalysis, Volume 57, Number 11, November 2008.
- **Misafir Editör**, *IEEE Transactions on Computers*, Special Section on Cryptographic Hardware and Embedded Systems, Volume 52, Number 4, April 2003.

11. Ödüller

- Outstanding and Sustained Research Leader, Oregon State University, 2001.
- **IEEE Fellow** for Contributions to Cryptographic Engineering, January 2007.
- En Çok Atif Alan 100 Türk Bilimadamı Arasında
- **Google Scholar Index: 42**

12. Son 2 Yıldaki Lisans ve Lisansüstü Dersleri

Akademik Yıl	Dönem	Dersin Adı	Haftalık Saati		Ögrenci Sayısı
			Teori	Uyg	
2016-2017	Güz	Foundations of Comp Sci	3	2	85
		Projects in Comp Sci	3	1	34
	Kış	Computational Algebra (YL)	4	0	8
		Explorations in Crypto (YL)	3	0	7
	Bahar	Computer Architecture	3	4	108
		Cryptographic Eng (YL)	4	0	16
2015-2016	Güz	Introduction to Comp Sci	3	4	101
		Elliptic Curve Crypto (YL)	4	0	13
	Kış	Prob Solv Computers	3	7	192
		Cryptographic Eng (YL)	4	0	14
		Explorations in Crypto (YL)	3	0	7
	Bahar	Computer Architecture	3	4	108
		Introduction to Comp Sci	3	8	257