Assoc. Prof. MURAT CENK

Personal Information

Email: mcenk@metu.edu.tr

Education Information

Doctorate, Middle East Technical University, Institute of Applied Mathematics, Kriptografi (Dr), Turkey 2003 - 2009
Post Graduate, Çankaya Üniversitesi, Fen Bilimleri Enstitüsü, Matematik-Bilgisayar (Yl) (Tezli), Turkey 2001 - 2003
Under Graduate, Middle East Technical University, Faculty of Education, Matematik Ve Fen Bilimleri Eğitimi Bölümü, Turkey 1994 - 2000

Dissertations

Doctorate, Results on complexity of multiplication over finite fields, Middle East Technical University, Institute of Applied Mathematics, Kriptografi (Dr), 2009
Post Graduate, New geometrical aspects of constrained system, Çankaya Üniversitesi, Matematik-Bilgisayar (Yl) (Tezli), 2003

Research Areas

Cryptography, Quantum Cryptography

Academic Titles / Tasks

Assistant Professor, Middle East Technical University, Institute of Applied Mathematics, Kriptografi (Dr), 2014 - Continues

Advising Theses

CENK M., Efficient implementation of TMVP-based prime field multiplication and its applications to ecc, Doctorate, H.KEMAL(Student), 2019
CENK M., Large sparse matrix-vector multiplication over finite fields, Doctorate, C.MANGIR(Student), 2019
CENK M., AKYILDIZ E., Homomorphic encryption for data security in cloud computing, Post Graduate, A.WAINAKH(Student), 2018
CENK M., Homomorphic encryption based on the Ring Learning with Errors (RLWE) problem, Post Graduate, İ.KESKİNKURT(Student), 2017
CENK M., Modular expoentiation methods in cryptography, Post Graduate, H.BARTU(Student), 2017
CENK M., Faster residue multiplication modulo 521-bit mersenne prime and application to ecc, Doctorate, S.ALI(Student), 2017
CENK M., An analysis on efficient polynomial multiplication algorithms for cryptographic purposes, Post Graduate, M.BURHAN(Student), 2016
CENK M., On verifiable internet voting systems, Doctorate, K.MUŞ(Student), 2016
CENK M., Analysis of recent attacks on SSL/TLS protocols, Post Graduate, D.ÖZDEN(Student), 2016

CENK M., On the efficient implementation of RSA, Post Graduate, H.KÜBRA(Student), 2015

Articles Published in Journals That Entered SCI, SSCI and AHCI Indexes

- **Faster Residue Multiplication Modulo 521-bit Mersenne Prime and an Application to ECC**
  Ali S., CENK M.
  IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I-REGULAR PAPERS, vol.65, pp.2477-2490, 2018 (Journal Indexed in SCI)
- **New Efficient Algorithms for Multiplication Over Fields of Characteristic Three**
  CENK M., Zadeh F. H. , Hasan M. A.
  JOURNAL OF SIGNAL PROCESSING SYSTEMS FOR SIGNAL IMAGE AND VIDEO TECHNOLOGY, vol.90, pp.285-294, 2018 (Journal Indexed in SCI)
- **On the arithmetic complexity of Strassen-like matrix multiplications**
  CENK M., Hasan M. A.
  JOURNAL OF SYMBOLIC COMPUTATION, vol.80, pp.484-501, 2017 (Journal Indexed in SCI)
- **Efficient subquadratic space complexity binary polynomial multipliers based on block recombination**
  Cenk M., Hasan M. A. , Negre C.
  IEEE Transactions on Computers, vol.63, pp.2273-2287, 2014 (Journal Indexed in SCI)
- **A New Representation of Elements of Binary Fields with Subquadratic Space Complexity Multiplication of Polynomials**
  ÖZBUDAK F., AKLEYLEK S., Cenk M.
  IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS COMMUNICATIONS AND COMPUTER SCIENCES, pp.2016-2024, 2013 (Journal Indexed in SCI)
- **On the generalisation of special moduli for faster interleaved montgomery modular multiplication**
  AKLEYLEK S., CENK M., ÖZBUDAK F.
  IET INFORMATION SECURITY, vol.7, pp.165-171, 2013 (Journal Indexed in SCI)
- **Improved Three-Way Split Formulas for Binary Polynomial and Toeplitz Matrix Vector Products**
  Cenk M., Negre C., Hasan M. A.
  IEEE TRANSACTIONS ON COMPUTERS, vol.62, pp.1345-1361, 2013 (Journal Indexed in SCI)
- **On the Polynomial Multiplication in Chebyshev Form**
  Akleylek S., Cenk M., ÖZBUDAK F.
  IEEE TRANSACTIONS ON COMPUTERS, vol.61, pp.584-587, 2012 (Journal Indexed in SCI)
- **Efficient multiplications in F(5)5n and F(7)7n**
  CENK M., ÖZBUDAK F.
  JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.236, pp.177-183, 2011 (Journal Indexed in SCI)
- **Multiplication of polynomials modulo x(n)**
  CENK M., ÖZBUDAK F.
  THEORETICAL COMPUTER SCIENCE, vol.412, pp.3451-3462, 2011 (Journal Indexed in SCI)
- **On multiplication in finite fields**
  Cenk M., ÖZBUDAK F.
  JOURNAL OF COMPLEXITY, vol.26, pp.172-186, 2010 (Journal Indexed in SCI)
- **Improved Polynomial Multiplication Formulas over F-2 Using Chinese Remainder Theorem**
  Cenk M., Oezbudak F.
  IEEE TRANSACTIONS ON COMPUTERS, vol.58, pp.572-576, 2009 (Journal Indexed in SCI)

Articles Published in Other Journals

- **Karatsuba-like formulae and their associated techniques**
  CENK M.

- JOURNAL OF CRYPTOGRAPHIC ENGINEERING, vol.8, pp.259-269, 2018 (Journal Indexed in ESCI)
- **Some new results on binary polynomial multiplication**
  CENK M., Hasan M. A.
  JOURNAL OF CRYPTOGRAPHIC ENGINEERING, vol.5, pp.289-303, 2015 (Journal Indexed in ESCI)

Refereed Congress / Symposium Publications in Proceedings

- **Compact and Simple RLWE Based Key Encapsulation Mechanism**
  Alkim E., Bilgin Y. A. , CENK M.
  6th International Conference on Cryptology and Information Security in Latin America (LATINCRYPT), Santiago de Cuba, Cuba, 2 - 04 October 2019, vol.11774, pp.237-256
- **Efficient multiplication in F-3lm, m >= 1 and 5 <= l <= 18**
  Cenk M., ÖZBUDAK F.
  1st International Conference on Cryptology in Africa, Casablanca, Morocco, 11 - 14 June 2008, vol.5023, pp.406-409

Supported Projects

CENK M., DEMİRCİOĞLU M., BALOĞLU S., TAŞKIN H. K. , YÜNÜAK H. B. , KESKİNKURT PAKSOY İ., Project Supported by Higher Education Institutions, Kuantum sonrası kriptografi, 2018 - 2019
CENK M., DEMİRCİOĞLU M., MUŞ K., YÜNÜAK H. B. , ALI S., TAŞKIN H. K. , Project Supported by Higher Education Institutions, Kriptografik Algoritmaların Hızlı, Verimli ve Güvenli Gerçekleştirimi, 2016 - 2019
ÖZBUDAK F., ÇOMAK P., SINAK A., CENK M., OTAL K., Project Supported by Higher Education Institutions, Yan Kanal Analizi, Aritmetik Karmaşıklık, Alt Uzay Kodlar, Diziler ve Boole Fonksiyonlar, 2016 - 2016

Citations

Total Citations (WOS):96
h-index (WOS):5