Prof. MURAT CENK

Personal Information

Office Phone: +90 312 210 5689
Email: mcenk@metu.edu.tr
Web: https://avesis.metu.edu.tr/mcenk

International Researcher IDs
ScholarID: wjo_QtgAAAAJ
ORCID: 0000-0003-4941-8734
Publons / Web Of Science ResearcherID: ABA-2432-2020
ScopusID: 6504402955
Yoksis Researcher ID: 220172

Education Information

Doctorate, Middle East Technical University, Institute of Applied Mathematics, Kriptografi (Dr), Turkey 2003 - 2009
Postgraduate, Cankaya University, Institute Of Science, Matematik-Bilgisayar (Yl) (Tezli), Turkey 2001 - 2003
Undergraduate, 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
Postgraduate, New geometrical aspects of constrained system, Çankaya Üniversitesi, Matematik-Bilgisayar (Yl) (Tezli), 2003

Research Areas

Cryptography

Advising Theses

Cenk M., New efficient characteristic three polynomial multiplication algorithms and their applications to NTRU prime, Doctorate, E.YENİARAS(Student), 2022
Cenk M., Efficient multivariate-based ring signature schemes, Doctorate, M.DEMİRCİOĞLU(Student), 2022
Cenk M., Analysis and comparison of fully homomorphic encryption approaches over integers, Postgraduate, C.BOZKURT(Student), 2022
Cenk M., Machine Learning over Encrypted Data With Fully Homomorphic Encyption, Postgraduate, A.KAHYA(Student), 2022
Cenk M., NEW TMVP-BASED MULTIPLICATION ALGORITHMS FOR POLYNOMIAL QUOTIENT RINGS AND APPLICATION TO POST-QUANTUM CRYPTOGRAPHY, Doctorate, İ.KESKİNKURT(Student), 2022
Cenk M., Analyzes of block recombination and lazy interpolation methods and their applications to saber, Postgraduate, B.AKSOY(Student), 2022

Cenk M., Hybrid analysis of TMVP for modular polynomial multiplicationin cryptography, Postgraduate, G.EFE(Student), 2022
Cenk M., Zero knowledge range proofs and applications on decentralized constructions, Postgraduate, E.GÜNSAY(Student), 2021
Cenk M., Cryptographic Misuse Detection Tools, Postgraduate, E.SELİN(Student), 2021
Cenk M., ANALYSIS AND IMPLEMENTATION OF BINARY POLYNOMIAL MULTIPLICATION, Postgraduate, M.ACHIENG(Student), 2021
CENK M., High performance number theoretic transforms in cryptography, Doctorate, M.Evrim(Student), 2020
Onur E., CENK M., A PUF-BASED LIGHTWEIGHT GROUP AUTHENTICATION AND KEY DISTRIBUTION PROTOCOL, Doctorate, H.YILDIZ(Student), 2020
CENK M., Efficient implementation of lattice-based schemes, Doctorate, Y.Alper(Student), 2020
Cenk M., Yayla O., Decentralized secure multiparty computation, Postgraduate, B.TAŞCI(Student), 2019
CENK M., Quantum safe digital signatures from symmetric key primitives, Postgraduate, Ş.Erbaş(Student), 2019
CENK M., Quantum-resistant multivariate quadratic systems and digital signatures, Postgraduate, E.Altundağ(Student), 2019
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., Secure cloud storage with attribute based encryption, Postgraduate, C.Tuğb(Student), 2019
CENK M., A Survey on cryptographic protocols using pairing-based cryptography, Postgraduate, Ş.Fetvacı(Student), 2019
CENK M., AKYILDIZ E., Homomorphic encryption for data security in cloud computing, Postgraduate, A.WAINAKH(Student), 2018
CENK M., Modular exponentiation methods in cryptography, Postgraduate, 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., Modular expoentiation methods in cryptography, Postgraduate, H.BARTU(Student), 2017
CENK M., Homomorphic encryption based on the Ring Learning with Errors (RLWE) problem, Postgraduate, İ.KESKİNKURT(Student), 2017
CENK M., Analysis of recent attacks on SSL/TLS protocols, Postgraduate, D.ÖZDEN(Student), 2016
CENK M., An analysis on efficient polynomial multiplication algorithms for cryptographic purposes, Postgraduate, M.BURHAN(Student), 2016
CENK M., On verifiable internet voting systems, Doctorate, K.MUŞ(Student), 2016
CENK M., On the efficient implementation of RSA, Postgraduate, H.KÜBRA(Student), 2015

Published journal articles indexed by SCI, SSCI, and AHCI

I. **A different base approach for better efficiency on range proofs**
Günsay E., Betin Onur C., CENK M.
Journal of Information Security and Applications, vol.85, 2024 (SCI-Expanded)

II. **A fast NTRU software implementation based on 5-way TMVP**
Yaman Gökce N., Gökce A. B., CENK M.
Journal of Information Security and Applications, vol.81, 2024 (SCI-Expanded)

III. **Faster NTRU on ARM Cortex-M4 With TMVP-Based Multiplication**
Paksoy İ., CENK M.
IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I-REGULAR PAPERS, vol.69, no.10, pp.4083-4092, 2022 (SCI-Expanded)

IV. **Faster characteristic three polynomial multiplication and its application to NTRU Prime decapsulation**
Yeniaras E., CENK M.

JOURNAL OF CRYPTOGRAPHIC ENGINEERING, vol.12, no.3, pp.329-348, 2022 (SCI-Expanded)

V. **Plgakd: A puf-based lightweight group authentication and key distribution protocol**
YILDIZ H., CENK M., ONUR E.
IEEE Internet of Things Journal, vol.8, no.7, pp.5682-5696, 2021 (SCI-Expanded)

VI. **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, no.8, pp.2477-2490, 2018 (SCI-Expanded)

VII. **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, no.3, pp.285-294, 2018 (SCI-Expanded)

VIII. **On the arithmetic complexity of Strassen-like matrix multiplications**
CENK M., Hasan M. A.
JOURNAL OF SYMBOLIC COMPUTATION, vol.80, pp.484-501, 2017 (SCI-Expanded)

IX. **Efficient subquadratic space complexity binary polynomial multipliers based on block recombination**
Cenk M., Hasan M. A., Negre C.
IEEE Transactions on Computers, vol.63, no.9, pp.2273-2287, 2014 (SCI-Expanded)

X. **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, no.10, pp.2016-2024, 2013 (SCI-Expanded)

XI. **On the generalisation of special moduli for faster interleaved montgomery modular multiplication**
AKLEYLEK S., CENK M., ÖZBUDAK F.
IET INFORMATION SECURITY, vol.7, no.3, pp.165-171, 2013 (SCI-Expanded)

XII. **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, no.7, pp.1345-1361, 2013 (SCI-Expanded)

XIII. **On the Polynomial Multiplication in Chebyshev Form**
Akleylek S., Cenk M., ÖZBUDAK F.
IEEE TRANSACTIONS ON COMPUTERS, vol.61, no.4, pp.584-587, 2012 (SCI-Expanded)

XIV. **Efficient multiplications in F(5)5n and F(7)7n**
CENK M., ÖZBUDAK F.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.236, no.2, pp.177-183, 2011 (SCI-Expanded)

XV. **Multiplication of polynomials modulo x(n)**
CENK M., ÖZBUDAK F.
THEORETICAL COMPUTER SCIENCE, vol.412, no.29, pp.3451-3462, 2011 (SCI-Expanded)

XVI. **On multiplication in finite fields**
Cenk M., ÖZBUDAK F.
JOURNAL OF COMPLEXITY, vol.26, no.2, pp.172-186, 2010 (SCI-Expanded)

XVII. **Improved Polynomial Multiplication Formulas over F-2 Using Chinese Remainder Theorem**
Cenk M., Oezbudak F.
IEEE TRANSACTIONS ON COMPUTERS, vol.58, no.4, pp.572-576, 2009 (SCI-Expanded)

Articles Published in Other Journals

I. **Cortex-M4 optimizations for {R, M} LWE schemes**
Alkım E., Bilgin Y. A., Cenk M., Gérard F.
IACR Transactions on Cryptographic Hardware and Embedded Systems, vol.2020, no.3, pp.336-357, 2020 (Peer-

Reviewed Journal)

II. **Karatsuba-like formulae and their associated techniques**
CENK M.
JOURNAL OF CRYPTOGRAPHIC ENGINEERING, vol.8, no.3, pp.259-269, 2018 (ESCI)

III. **Efficient Big Integer Multiplication in Cryptography**
İLTER M. B., CENK M.
journal of information security, 2017 (Peer-Reviewed Journal)

IV. **Some new results on binary polynomial multiplication**
CENK M., Hasan M. A.
JOURNAL OF CRYPTOGRAPHIC ENGINEERING, vol.5, no.4, pp.289-303, 2015 (ESCI)

Refereed Congress / Symposium Publications in Proceedings

I. **Improved Polynomial Multiplication Algorithms over Characteristic Three Fields and Applications to NTRU Prime**
Yeniaras E., CENK M.
14th International Conference on Innovative Security Solutions for Information Technology and Communications, SecITC 2021, Virtual, Online, 25 - 26 November 2021, vol.13195 LNCS, pp.125-144

II. **Analysis of Block Recombination and Lazy Interpolation Methods and Their Applications to Saber**
Aksoy B., CENK M.
15th International Conference on Information Security and Cryptography, ISCTURKEY 2022, Ankara, Turkey, 19 - 20 October 2022, pp.61-67

III. **An Improved Range Proof with Base-3 Construction**
GÜNSAY E., Onur C. B., CENK M.
14th International Conference on Security of Information and Networks, SIN 2021, Virtual, Online, United Kingdom, 15 - 17 December 2021

IV. **TMVP-Friendly Primes for Efficient Elliptic Curve Cryptography**
Taskin H. K., Cenk M.
13th International Conference on Information Security and Cryptology, ISCTURKEY 2020, Virtual, Ankara, Turkey, 3 - 04 December 2020, pp.80-87

V. **Efficient GeMSS Based Ring Signature Scheme**
Demircioğlu M., AKLEYLEK S., CENK M.
The Second International Workshop on Cryptography and its Applications – 2'IWCA'19, Oran, Algeria, 18 - 19 June 2019

VI. **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

VII. **Data sharing under confidentiality**
Başer E., Hülagu T., Akyıldız E., Bilgen A., Cenk M., Keskinkurt-Paksoy İ., Kestel S. A.
Ninth IFC Conference , Basel, Switzerland, 30 - 31 August 2018, pp.1057-1072

VIII. **GUI Based Ring Signature Scheme**
AKLEYLEK S., Demircioğlu M., CENK M.
18th Central European Conference on Cryptology (CECC 2018), Smolenice, Slovakia, 6 - 08 June 2018, pp.1-3

IX. **Speeding up Curve25519 using Toeplitz Matrix-vector Multiplication**
Taskin H. K., CENK M.
5th Workshop on Cryptography and Security in Computing Systems (CS2), Manchester, United Kingdom, 24 January 2018, pp.1-6

X. **How Cryptology Affects Digital Life and Transformation**
CENK M.

Digital Transformation, 28 December 2017

XI. **Efficient Big Integer Multiplication in Cryptography**
İLTER M. B., CENK M.
ISCTurkey, 25 - 26 October 2017

XII. **A New Algorithm for Residue Multiplication Modulo 2(521)-1**
Ali S., CENK M.
19th International Conference on Information Security and Cryptology (ICISC), Seoul, South Korea, 30 November - 02 December 2016, vol.10157, pp.181-193

XIII. **Efficient Modular Exponentiation Methods for RSA**
Güner H., CENK M., ÇALIK Ç.
ISC Turkey 2015, 30 - 31 October 2015

XIV. **Improved three-way split formulas for binary polynomial multiplication**
Cenk M., Negre C., Hasan M. A.
18th International Conference on Selected Areas in Cryptography, SAC 2011, Toronto, Canada, 11 - 12 August 2011, pp.384-398

XV. **Polynomial Multiplication over Binary Fields Using Charlier Polynomial Representation with Low Space Complexity**
AKLEYLEK S., CENK M., ÖZBUDAK F.
INDOCRYPT 2010 11th International Conference on Cryptology in India, 12 - 15 December 2010

XVI. **Faster Montgomery modular multiplication without pre-computational phase for some classes of finite fields**
Akleylek S., CENK M., ÖZBUDAK F.
25th International Symposium on Computer and Information Sciences, ISCIS 2010, London, United Kingdom, 22 - 24 September 2010, pp.405-408

XVII. **Polynomial Multiplication over Finite Fields using Field Extensions and Interpolation**
Cenk M., KOÇ C. K., ÖZBUDAK F.
19th IEEE Symposium on Computer Arithmetic (ARITH 2009), Oregon, United States Of America, 8 - 10 June 2009, pp.84-85

XVIII. **Efficient multiplication in double-struck F sign3ℓm, m ≥ 1 and 5 ≤ ℓ ≤ 18**
Cenk M., ÖZBUDAK F.
1st International Conference on Cryptology in Africa, AFRICACRYPT 2008, Casablanca, Morocco, 11 - 14 June 2008, pp.406-414

XIX. **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

XX. **Ayrık Logaritma Problemini Kullanan E İmza**
CENK M., YAYLA O.
Ulusal Elektronik İmza Sempozyumu, Turkey, 7 - 08 December 2006, pp.381-386

Supported Projects

CENK M., YILDIZ H., Project Supported by Higher Education Institutions, Post-Kuantum Kriptografi Tabanlı Anahtar Paylaşımı, 2021 - 2023

Yünüak H. B., Cenk M., TUBITAK Project, Post-Quantum Library, 2020 - 2022

Cenk M., Technopark, Kuantum Ertesi Kriptografi, 2018 - 2019

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., Project Supported by Other Private Institutions, Yüksek Performanslı ve Güvenli SSL/TLS Kütüphanesi Geliştirilmesi, 2018 - 2019

Cenk M., Project Supported by Other Official Institutions, Yeni ve gelecek nesil eliptik egri tabanlı kriptosistemlerin verimli ve güvenli gerçeklestirilmesi, 2017 - 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
CENK M., TUBITAK Project, Açık Anahtarlı Kriptografi Için Verimli Algoritmaların Geliştirilmesi Ve Gerçeklenmesi, 2016 - 2018
Doğanaksoy A., Cenk M., Project Supported by Other Private Institutions, İstatistiksel test paketi geliştirilmesi, 2016 - 2017
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
CENK M., TUBITAK Project, Aritmetik ve matris problemleri icin verimli paralel algoritma geliştirilmesi ve kriptografiye uygulamaları, 2014 - 2016

Patent

Cenk M., ELEKTRONİK OYLAMA DOĞRULAMA SİSTEMİ, Patent, CHAPTER B Implementation of Operations; Transport, The Invention Registration Number: TR 2016 16657 B , Standard Registration, 2020

Metrics

Publication: 44
Citation (WoS): 159
Citation (Scopus): 178
H-Index (WoS): 7
H-Index (Scopus): 8