

## Doç.Dr. MURAT CENK

### Kişisel Bilgiler

İş Telefonu: [+90 312 210 5689](tel:+903122105689)

E-posta: [mcenk@metu.edu.tr](mailto:mcenk@metu.edu.tr)

Web: <https://avesis.metu.edu.tr/mcenk>

### Eğitim Bilgileri

Doktora, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi (Dr), Türkiye 2003 - 2009

Yüksek Lisans, Çankaya Üniversitesi, Fen Bilimleri Enstitüsü, Matematik-Bilgisayar (YI) (Tezli), Türkiye 2001 - 2003

Lisans, Orta Doğu Teknik Üniversitesi, Eğitim Fakültesi, Matematik Ve Fen Bilimleri Eğitimi Bölümü, Türkiye 1994 - 2000

### Yaptığı Tezler

Doktora, Results on complexity of multiplication over finite fields, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi (Dr), 2009

Yüksek Lisans, New geometrical aspects of constrained system, Çankaya Üniversitesi, Fen Bilimleri Enstitüsü, Matematik-Bilgisayar (YI) (Tezli), 2003

### Araştırma Alanları

Bilgi Kuramı , Kuantum Haberleşme, Kriptoloji, Kuantum Kriptografi, Sayılar Kuramı

### Yönetilen Tezler

Cenk M., Cryptographic Misuse Detection Tools, Yüksek Lisans, E.SELİN(Öğrenci), 2021

Cenk M., Zero knowledge range proofs and applications on decentralized constructions, Yüksek Lisans, E.GÜNSAY(Öğrenci), 2021

Cenk M., ANALYSIS AND IMPLEMENTATION OF BINARY POLYNOMIAL MULTIPLICATION, Yüksek Lisans, M.ACHIENG(Öğrenci), 2021

CENK M., Kafes tabanlı algoritmaların verimli gerçekleşmesi, Doktora, Y.Alper(Öğrenci), 2020

Onur E., CENK M., A PUF-BASED LIGHTWEIGHT GROUP AUTHENTICATION AND KEY DISTRIBUTION PROTOCOL, Doktora, H.YILDIZ(Öğrenci), 2020

CENK M., Kriptografide yüksek performanslı sayı kuramsal dönüşümler, Doktora, M.Evrin(Öğrenci), 2020

Cenk M., Yayla O., Decentralized secure multiparty computation, Yüksek Lisans, B.TAŞCI(Öğrenci), 2019

CENK M., Kuantum-dayanıklı çok değişkenli iki bilinmeyenli sistemler ve sayısal imzalar, Yüksek Lisans, E.Altundağ(Öğrenci), 2019

CENK M., Özellik tabanlı şifreleme ile güvenli bulut depolama, Yüksek Lisans, C.Tuğb(Öğrenci), 2019

CENK M., Eşleştirme tabanlı şifreleme kullanan kriptografik protokoller üzerine bir araştırma., Yüksek Lisans, Ş.Fetvacı(Öğrenci), 2019

CENK M., Simetrik anahtar temelli kuantum güvenli sayısal imzalar., Yüksek Lisans, Ş.Erbaş(Öğrenci), 2019

CENK M., Efficient implementation of TMVP-based prime field multiplication and its applications to ecc, Doktora, H.KEMAL(Öğrenci), 2019

CENK M., Large sparse matrix-vector multiplication over finite fields, Doktora, C.MANGIR(Öğrenci), 2019

- CENK M., AKYILDIZ E., Homomorphic encryption for data security in cloud computing, Yüksek Lisans, A.WAINAKH(Öğrenci), 2018
- CENK M., Faster residue multiplication modulo 521-bit mersenne prime and application to ecc, Doktora, S.ALI(Öğrenci), 2017
- CENK M., Kriptografide modüler üs alma yöntemleri, Yüksek Lisans, H.Bartu(Öğrenci), 2017
- CENK M., Homomorphic encryption based on the Ring Learning with Errors (RLWE) problem, Yüksek Lisans, İ.KESKİNKURT(Öğrenci), 2017
- CENK M., Modular expoentiation methods in cryptography, Yüksek Lisans, H.BARTU(Öğrenci), 2017
- CENK M., On verifiable internet voting systems, Doktora, K.MUŞ(Öğrenci), 2016
- CENK M., An analysis on efficient polynomial multiplication algorithms for cryptographic purposes, Yüksek Lisans, M.BURHAN(Öğrenci), 2016
- CENK M., Analysis of recent attacks on SSL/TLS protocols, Yüksek Lisans, D.ÖZDEN(Öğrenci), 2016
- CENK M., On the efficient implementation of RSA, Yüksek Lisans, H.KÜBRA(Öğrenci), 2015

## SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

- I. **Faster characteristic three polynomial multiplication and its application to NTRU Prime decapsulation**  
Yeniaras E., CENK M.  
JOURNAL OF CRYPTOGRAPHIC ENGINEERING, 2022 (SCI İndekslerine Giren Dergi)
- II. **Plgakd: A puf-based lightweight group authentication and key distribution protocol**  
YILDIZ H., CENK M., ONUR E.  
IEEE Internet of Things Journal, cilt.8, sa.7, ss.5682-5696, 2021 (SCI İndekslerine Giren Dergi)
- III. **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, cilt.65, sa.8, ss.2477-2490, 2018 (SCI İndekslerine Giren Dergi)
- IV. **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, cilt.90, sa.3, ss.285-294, 2018 (SCI İndekslerine Giren Dergi)
- V. **On the arithmetic complexity of Strassen-like matrix multiplications**  
CENK M., Hasan M. A.  
JOURNAL OF SYMBOLIC COMPUTATION, cilt.80, ss.484-501, 2017 (SCI İndekslerine Giren Dergi)
- VI. **Efficient subquadratic space complexity binary polynomial multipliers based on block recombination**  
Cenk M., Hasan M. A. , Negre C.  
IEEE Transactions on Computers, cilt.63, sa.9, ss.2273-2287, 2014 (SCI İndekslerine Giren Dergi)
- VII. **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, sa.10, ss.2016-2024, 2013 (SCI İndekslerine Giren Dergi)
- VIII. **On the generalisation of special moduli for faster interleaved montgomery modular multiplication**  
AKLEYLEK S., CENK M., ÖZBUDAK F.  
IET INFORMATION SECURITY, cilt.7, sa.3, ss.165-171, 2013 (SCI İndekslerine Giren Dergi)
- IX. **Improved Three-Way Split Formulas for Binary Polynomial and Toeplitz Matrix Vector Products**  
Cenk M., Negre C., Hasan M. A.  
IEEE TRANSACTIONS ON COMPUTERS, cilt.62, sa.7, ss.1345-1361, 2013 (SCI İndekslerine Giren Dergi)
- X. **On the Polynomial Multiplication in Chebyshev Form**  
Akleylek S., Cenk M., ÖZBUDAK F.

IEEE TRANSACTIONS ON COMPUTERS, cilt.61, sa.4, ss.584-587, 2012 (SCI İndekslerine Giren Dergi)

- XI. **Efficient multiplications in  $F(5)^{5n}$  and  $F(7)^{7n}$**   
CENK M., ÖZBUDAK F.  
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, cilt.236, sa.2, ss.177-183, 2011 (SCI İndekslerine Giren Dergi)
- XII. **Multiplication of polynomials modulo  $x(n)$**   
CENK M., ÖZBUDAK F.  
THEORETICAL COMPUTER SCIENCE, cilt.412, sa.29, ss.3451-3462, 2011 (SCI İndekslerine Giren Dergi)
- XIII. **On multiplication in finite fields**  
Cenk M., ÖZBUDAK F.  
JOURNAL OF COMPLEXITY, cilt.26, sa.2, ss.172-186, 2010 (SCI İndekslerine Giren Dergi)
- XIV. **Improved Polynomial Multiplication Formulas over  $F_2$  Using Chinese Remainder Theorem**  
Cenk M., Oezbudak F.  
IEEE TRANSACTIONS ON COMPUTERS, cilt.58, sa.4, ss.572-576, 2009 (SCI İndekslerine Giren Dergi)

## **Diğer Dergilerde Yayınlanan Makaleler**

- I. **Cortex-M4 optimizations for  $\{R, M\}$  LWE schemes**  
Alkm E., Bilgin Y. A. , Cenk M., Gérard F.  
IACR Transactions on Cryptographic Hardware and Embedded Systems, cilt.2020, sa.3, ss.336-357, 2020 (Diğer Kurumların Hakemli Dergileri)
- II. **Karatsuba-like formulae and their associated techniques**  
CENK M.  
JOURNAL OF CRYPTOGRAPHIC ENGINEERING, cilt.8, sa.3, ss.259-269, 2018 (ESCI İndekslerine Giren Dergi)
- III. **Efficient Big Integer Multiplication in Cryptography**  
İLTER M. B. , CENK M.  
journal of information security, 2017 (Diğer Kurumların Hakemli Dergileri)
- IV. **Some new results on binary polynomial multiplication**  
CENK M., Hasan M. A.  
JOURNAL OF CRYPTOGRAPHIC ENGINEERING, cilt.5, sa.4, ss.289-303, 2015 (ESCI İndekslerine Giren Dergi)

## **Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar**

- I. **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, Birleşik Krallık, 15 - 17 Aralık 2021
- II. **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, Türkiye, 3 - 04 Aralık 2020, ss.80-87
- III. **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, Cezayir, 18 - 19 Haziran 2019
- IV. **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, Küba, 2 - 04 Ekim 2019, cilt.11774, ss.237-256

- V. **Data sharing under confidentiality**  
Başer E., Hülagu T., Akyıldız E., Bilgen A., Cenk M., Keskinurt-Paksoy İ., Kestel S. A.  
Ninth IFC Conference , Basel, İsviçre, 30 - 31 Ağustos 2018, ss.1057-1072
- VI. **GUI Based Ring Signature Scheme**  
AKLEYLEK S., Demircioğlu M., CENK M.  
18th Central European Conference on Cryptology (CECC 2018), Smolenice, Slovakya, 6 - 08 Haziran 2018, ss.1-3
- VII. **Speeding up Curve25519 using Toeplitz Matrix-vector Multiplication**  
Taskin H. K. , CENK M.  
5th Workshop on Cryptography and Security in Computing Systems (CS2), Manchester, Birleşik Krallık, 24 Ocak 2018, ss.1-6
- VIII. **How Cryptology Affects Digital Life and Transformation**  
CENK M.  
Digital Transformation, 28 Aralık 2017
- IX. **Efficient Big Integer Multiplication in Cryptography**  
İLTER M. B. , CENK M.  
ISCTurkey, 25 - 26 Ekim 2017
- X. **A New Algorithm for Residue Multiplication Modulo  $2(521)-1$**   
Ali S., CENK M.  
19th International Conference on Information Security and Cryptology (ICISC), Seoul, Güney Kore, 30 Kasım - 02 Aralık 2016, cilt.10157, ss.181-193
- XI. **Efficient Modular Exponentiation Methods for RSA**  
Güner H., CENK M., ÇALIK Ç.  
ISC Turkey 2015, 30 - 31 Ekim 2015
- XII. **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, Kanada, 11 - 12 Ağustos 2011, ss.384-398
- XIII. **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 Aralık 2010
- XIV. **Faster Montgomery modular multiplication without pre-computational phase for some classes of finite fields**  
Akeley S., CENK M., ÖZBUDAK F.  
25th International Symposium on Computer and Information Sciences, ISCIS 2010, London, Birleşik Krallık, 22 - 24 Eylül 2010, ss.405-408
- XV. **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, Amerika Birleşik Devletleri, 8 - 10 Haziran 2009, ss.84-85
- XVI. **Efficient multiplication in  $F-3\ell m$ ,  $m \geq 1$  and  $5 \leq \ell \leq 18$**   
Cenk M., ÖZBUDAK F.  
1st International Conference on Cryptology in Africa, Casablanca, Fas, 11 - 14 Haziran 2008, cilt.5023, ss.406-409
- XVII. **Efficient multiplication in double-struck  $F$  sign  $3\ell m$ ,  $m \geq 1$  and  $5 \leq \ell \leq 18$**   
Cenk M., ÖZBUDAK F.  
1st International Conference on Cryptology in Africa, AFRICACRYPT 2008, Casablanca, Fas, 11 - 14 Haziran 2008, ss.406-414
- XVIII. **Ayrık Logaritma Problemini Kullanan E İmza**  
CENK M., YAYLA O.  
Ulusal Elektronik İmza Sempozyumu, Türkiye, 7 - 08 Aralık 2006, ss.381-386

## Desteklenen Projeler

CENK M., YILDIZ H., Yükseköğretim Kurumları Destekli Proje, Post-Kuantum Kriptografi Tabanlı Anahtar Paylaşımı, 2021 - Devam Ediyor

Yünüak H. B. , Cenk M., TÜBİTAK Projesi, Kuantum Ertesi Kütüphanesi, 2020 - 2022

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

CENK M., DEMİRCİOĞLU M., BALOĞLU S., TAŞKIN H. K. , YÜNÜAK H. B. , KESKİNKURT PAKSOY İ., Yükseköğretim Kurumları Destekli Proje, Kuantum sonrası kriptografi, 2018 - 2019

Cenk M., Diğer Özel Kurumlarca Desteklenen Proje, Yüksek Performanslı ve Güvenli SSL/TLS Kütüphanesi Geliştirilmesi, 2018 - 2019

Cenk M., Diğer Resmi Kurumlarca Desteklenen Proje, Yeni ve gelecek nesil eliptik eğri tabanlı kriptosistemlerin verimli ve güvenli gerçekleştirilmesi, 2017 - 2019

CENK M., DEMİRCİOĞLU M., MUŞ K., YÜNÜAK H. B. , ALI S., TAŞKIN H. K. , Yükseköğretim Kurumları Destekli Proje, Kriptografik Algoritmaların Hızlı, Verimli ve Güvenli Gerçekleştirimi, 2016 - 2019

CENK M., TÜBİTAK Projesi, Açık Anahtarlı Kriptografi İçin Verimli Algoritmaların Geliştirilmesi Ve Gerçeklenmesi, 2016 - 2018

Doğanaksoy A., Cenk M., Diğer Özel Kurumlarca Desteklenen Proje, İstatistiksel test paketi geliştirilmesi, 2016 - 2017

ÖZBUDAK F., ÇOMAK P., SINAK A., CENK M., OTAL K., Yükseköğretim Kurumları Destekli Proje, Yan Kanal Analizi, Aritmetik Karmaşıklık, Alt Uzay Kodlar, Diziler ve Boole Fonksiyonlar, 2016 - 2016

CENK M., TÜBİTAK Projesi, Aritmetik ve matris problemleri için verimli paralel algoritma geliştirilmesi ve kriptografiye uygulamaları, 2014 - 2016

## Patent

Cenk M., ELEKTRONİK OYLAMA DOĞRULAMA SİSTEMİ, Patent, BÖLÜM B İşlemlerin Uygulanması; Taşıma, Buluşun Tescil No: TR 2016 16657 B , İlk Tescil, 2020

## Atıflar

Toplam Atıf Sayısı (WOS):116

h-indeksi (WOS):6