

Prof. FERRUH ÖZBUDAK

Personal Information

Email: ozbudak@metu.edu.tr

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

International Researcher IDs

ScholarID: io11MRcAAAAJ

ORCID: 0000-0002-1694-9283

Publons / Web Of Science ResearcherID: AAZ-6893-2020

ScopusID: 6603589033

Yoksis Researcher ID: 2212

Education Information

Doctorate, Ihsan Dogramaci Bilkent University, Faculty Of Science, Department Of Mathematics, Turkey 1995 - 1997

Postgraduate, Ihsan Dogramaci Bilkent University, Faculty Of Science, Department Of Mathematics, Turkey 1993 - 1995

Undergraduate, Ihsan Dogramaci Bilkent University, Faculty Of Engineering, Department Of Electrical And Electronics Engineering, Turkey 1988 - 1993

Foreign Languages

English, C1 Advanced

Dissertations

Doctorate, Character sums, algebraic function fields, curves with many rational points and geometric Goppa codes, Bilkent Üniversitesi, Fen Fakültesi, Matematik Bölümü, 1997

Postgraduate, On lower bounds of character sums, Bilkent Üniversitesi, Fen Fakültesi, Matematik Bölümü, 1995

Research Areas

Mathematics, Algebraic Geometry, Field Theory and Polynomials, General Algebraic Systems, Combinatorics, Number Theory, Natural Sciences

Academic and Administrative Experience

Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2007 - Continues

Advising Theses

ÖZBUDAK F., Studies on almost perfect nonlinear functions, Postgraduate, G.BATMAZ(Student), 2022

ÖZBUDAK F., Some studies on CCZ-equivalence of the inverse function, Postgraduate, M.FİDAN(Student), 2021

ÖZBUDAK F., Studies on implementation of some mrd codes, Postgraduate, R.ÖZKERİM(Student), 2021
 ÖZBUDAK F., Some studies on c-differential uniformity of the swapped inverse function, Postgraduate, B.ÜNVER(Student), 2021
 ÖZBUDAK F., Correlation of sequences and quadratic forms, Postgraduate, C.Genişel(Student), 2017
 ÖZBUDAK F., On obtaining regular, weakly regular and non-weakly regular bent functions over finite fields and ring of integers modulo P_m , Doctorate, D.Çelik(Student), 2014
 ÖZBUDAK F., Generalized bent functions with perfect nonlinear functions on arbitrary groups, Postgraduate, E.Sercan(Student), 2012
 ÖZBUDAK F., Drinfeld modular curves with many rational points over finite fields, Doctorate, V.Cam(Student), 2011
 ÖZBUDAK F., On the expected value of the linear complexity of periodic sequences, Postgraduate, Ç.Özakın(Student), 2004

Published journal articles indexed by SCI, SSCI, and AHCI

- I. **On subfield subcodes obtained from restricted evaluation codes**
 Güneri C., ÖZBUDAK F., Sayıcı S.
 Designs, Codes, and Cryptography, vol.92, no.3, pp.667-680, 2024 (SCI-Expanded)
- II. **Further constructions and characterizations of generalized almost perfect nonlinear functions**
 Sălăgean A., ÖZBUDAK F.
 Cryptography and Communications, vol.15, no.6, pp.1117-1127, 2023 (SCI-Expanded)
- III. **Quasi-Cyclic Perfect Codes in Doob Graphs and Special Partitions of Galois Rings**
 Shi M., Li X., Krotov D. S., ÖZBUDAK F.
 IEEE Transactions on Information Theory, vol.69, no.9, pp.5597-5603, 2023 (SCI-Expanded)
- IV. **Complete characterization of some permutation polynomials of the form $xr(1+axs_1(q-1)+bxs_2(q-1))$ over F_{q^2}**
 ÖZBUDAK F., Temür B. G.
 Cryptography and Communications, vol.15, no.4, pp.775-793, 2023 (SCI-Expanded)
- V. **Optimal Binary Linear Complementary Pairs of Codes**
 Choi W., GÜNERİ C., Kim J., ÖZBUDAK F.
 CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.15, no.2, pp.469-486, 2023 (SCI-Expanded)
- VI. **Classification of some quadrinomials over finite fields of odd characteristic**
 Özbudak F., Gulmez Temur B. o. T.
 FINITE FIELDS AND THEIR APPLICATIONS, vol.87, pp.102158, 2023 (SCI-Expanded)
- VII. **On diamond products ensuring irreducibility of the associated composed product**
 İrimağzi C., ÖZBUDAK F.
 Communications in Algebra, vol.51, no.7, pp.3134-3142, 2023 (SCI-Expanded)
- VIII. **EUCLIDEAN POLYNOMIALS FOR CERTAIN ARITHMETIC PROGRESSIONS AND THE MULTIPLICATIVE GROUP OF F_{p^2}**
 Berktav K. I., ÖZBUDAK F.
 QUAESTIONES MATHEMATICAE, vol.46, no.7, pp.1283-1292, 2023 (SCI-Expanded)
- IX. **Boomerang uniformity of power permutations and algebraic curves over F_{2^n}**
 Mesnager S., ÖZBUDAK F.
 Advances in Geometry, vol.23, no.1, pp.107-134, 2023 (SCI-Expanded)
- X. **The c-differential uniformity of the perturbed inverse function via a trace function $\text{Tr}(x^2x+1)$**
 KAYTANCI K., ÖZBUDAK F.
 Periodica Mathematica Hungarica, 2023 (SCI-Expanded)
- XI. **Imprimitive symmetric association schemes of classes 5 and 6 arising from ternary non-weakly regular bent functions**
 ÖZBUDAK F., Pelen R. M.

JOURNAL OF ALGEBRAIC COMBINATORICS, vol.56, no.3, pp.635-658, 2022 (SCI-Expanded)

- XII. **Additive cyclic complementary dual codes over F_4**
Shi M., Liu N., ÖZBUDAK F., Solé P.
Finite Fields and their Applications, vol.83, 2022 (SCI-Expanded)
- XIII. **Classification of permutation polynomials of the form $x^3g(xq-1)$ of F_{q^2} where $g(x) = x^3 + bx + c$ and $b, c \in F_{q^*}$**
ÖZBUDAK F., Gülmez Temür B.
Designs, Codes, and Cryptography, vol.90, no.7, pp.1537-1556, 2022 (SCI-Expanded)
- XIV. **Construction of self dual codes from graphs**
Fellah N., Guenda K., ÖZBUDAK F., Seneviratne P.
APPLICABLE ALGEBRA IN ENGINEERING COMMUNICATION AND COMPUTING, 2022 (SCI-Expanded)
- XV. **Factorization of some polynomials over finite local commutative rings and applications to certain self-dual and LCD codes**
Koese S., ÖZBUDAK F.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.14, no.4, pp.933-948, 2022 (SCI-Expanded)
- XVI. **Covering Radius of Melas Codes**
Shi M., Helleseth T., Özbudak F., Solé P.
IEEE Transactions on Information Theory, vol.68, no.7, pp.4354-4364, 2022 (SCI-Expanded)
- XVII. **Two or Three Weight Linear Codes from Non-Weakly Regular Bent Functions**
Özbudak F., Pelen R. M.
IEEE Transactions on Information Theory, vol.68, no.5, pp.3014-3027, 2022 (SCI-Expanded)
- XVIII. **Complete b-symbol weight distribution of some irreducible cyclic codes**
Zhu H., Shi M., ÖZBUDAK F.
DESIGNS CODES AND CRYPTOGRAPHY, vol.90, no.5, pp.1113-1125, 2022 (SCI-Expanded)
- XIX. **New constructions of entanglement-assisted quantum codes**
Allahmadi A., AlKenani A., Hijazi R., Muthana N., ÖZBUDAK F., Solé P.
Cryptography and Communications, vol.14, no.1, pp.15-37, 2022 (SCI-Expanded)
- XX. **LCD codes from tridiagonal Toeplitz matrices**
Shi M., ÖZBUDAK F., Xu L., Solé P.
Finite Fields and their Applications, vol.75, 2021 (SCI-Expanded)
- XXI. **CORRELATION DISTRIBUTION OF A SEQUENCE FAMILY GENERALIZING SOME SEQUENCES OF TRACHTENBERG**
ÖZBUDAK F., Tekin E.
ADVANCES IN MATHEMATICS OF COMMUNICATIONS, vol.15, no.4, pp.647-662, 2021 (SCI-Expanded)
- XXII. **Geometric Approach to b-Symbol Hamming Weights of Cyclic Codes**
Shi M., Özbudak F., Solé P.
IEEE Transactions on Information Theory, vol.67, no.6, pp.3735-3751, 2021 (SCI-Expanded)
- XXIII. **New generalized almost perfect nonlinear functions**
ÖZBUDAK F., Salagean A.
FINITE FIELDS AND THEIR APPLICATIONS, vol.70, 2021 (SCI-Expanded)
- XXIV. **On the Parity of Power Permutations**
Comak P., ÖZBUDAK F.
IEEE Access, vol.9, pp.106806-106812, 2021 (SCI-Expanded)
- XXV. **Hermitian Rank Metric Codes and Duality**
La Cruz J. D., Evilla J. R., ÖZBUDAK F.
IEEE ACCESS, vol.9, pp.38479-38487, 2021 (SCI-Expanded)
- XXVI. **Secondary constructions of (non)weakly regular plateaued functions over finite fields**
Mesnager S., ÖZBUDAK F., Sinak A.
TURKISH JOURNAL OF MATHEMATICS, vol.45, pp.2295-2306, 2021 (SCI-Expanded)
- XXVII. **Counting Boolean functions with faster points**

- Salagean A., ÖZBUDAK F.
DESIGNS CODES AND CRYPTOGRAPHY, vol.88, no.9, pp.1867-1883, 2020 (SCI-Expanded)
- XXVIII. **Subspace packings: constructions and bounds**
Etzion T., Kurz S., Otal K., ÖZBUDAK F.
DESIGNS CODES AND CRYPTOGRAPHY, vol.88, no.9, pp.1781-1810, 2020 (SCI-Expanded)
- XXIX. **Duals of non-weakly regular bent functions are not weakly regular and generalization to plateaued functions**
ÖZBUDAK F., PELEN R. M.
FINITE FIELDS AND THEIR APPLICATIONS, vol.64, 2020 (SCI-Expanded)
- XXX. **Strongly regular graphs arising from non-weakly regular bent functions**
ÖZBUDAK F., PELEN R. M.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.11, no.6, pp.1297-1306, 2019 (SCI-Expanded)
- XXXI. **A concatenated construction of linear complementary pair of codes**
GÜNERİ C., ÖZBUDAK F., Sacikara E.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.11, no.5, pp.1103-1114, 2019 (SCI-Expanded)
- XXXII. **On q-ary plateaued functions over F_q and their explicit characterizations**
Mesnager S., ÖZBUDAK F., Sinak A., Cohen G.
EUROPEAN JOURNAL OF COMBINATORICS, vol.80, pp.71-81, 2019 (SCI-Expanded)
- XXXIII. **Constructing sequences with high nonlinear complexity using the Weierstrass semigroup of a pair of distinct points of a Hermitian curve**
Geil O., Ozbudak F., Ruano D.
SEMIGROUP FORUM, vol.98, no.3, pp.543-555, 2019 (SCI-Expanded)
- XXXIV. **On affine variety codes from the Klein quartic**
Geil O., ÖZBUDAK F.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.11, no.2, pp.237-257, 2019 (SCI-Expanded)
- XXXV. **Linear codes from weakly regular plateaued functions and their secret sharing schemes**
Mesnager S., ÖZBUDAK F., Sinak A.
DESIGNS CODES AND CRYPTOGRAPHY, vol.87, pp.463-480, 2019 (SCI-Expanded)
- XXXVI. **CYLOTOMIC FUNCTION FIELDS OVER FINITE FIELDS WITH CLASS NUMBER THREE**
Bilhan M., Buyruk D., ÖZBUDAK F.
JOURNAL OF THE KOREAN MATHEMATICAL SOCIETY, vol.56, no.2, pp.559-578, 2019 (SCI-Expanded)
- XXXVII. **SELF-DUALITY OF GENERALIZED TWISTED GABIDULIN CODES**
Otal K., ÖZBUDAK F., Willems W.
ADVANCES IN MATHEMATICS OF COMMUNICATIONS, vol.12, no.4, pp.707-721, 2018 (SCI-Expanded)
- XXXVIII. **On Linear Complementary Pairs of Codes**
CARLET C., Guneri C., ÖZBUDAK F., Ozkaya B., SOLE P.
IEEE TRANSACTIONS ON INFORMATION THEORY, vol.64, no.10, pp.6583-6589, 2018 (SCI-Expanded)
- XXXIX. **New cubic self-dual codes of length 54, 60 and 66**
Comak P., Kim J. L., Ozbudak F.
APPLICABLE ALGEBRA IN ENGINEERING COMMUNICATION AND COMPUTING, vol.29, no.4, pp.303-312, 2018 (SCI-Expanded)
- XL. **On the p-ary (cubic) bent and plateaued (vectorial) functions**
MESNAGER S., ÖZBUDAK F., Sinak A.
DESIGNS CODES AND CRYPTOGRAPHY, vol.86, no.8, pp.1865-1892, 2018 (SCI-Expanded)
- XLI. **Additive cyclic codes over finite commutative chain rings**
Martinez-Moro E., Otal K., ÖZBUDAK F.
DISCRETE MATHEMATICS, vol.341, no.7, pp.1873-1884, 2018 (SCI-Expanded)
- XLII. **Generalized nonbinary sequences with perfect autocorrelation, flexible alphabets and new periods**

BOZTAŞ S., ÖZBUDAK F., TEKİN E.

CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.10, no.3, pp.509-517, 2018 (SCI-Expanded)

XLIII. Explicit Full Correlation Distribution of Sequence Families Using Plateaued Functions

BOZTAŞ S., ÖZBUDAK F., TEKİN E.

IEEE TRANSACTIONS ON INFORMATION THEORY, vol.64, no.4, pp.2858-2875, 2018 (SCI-Expanded)

XLIV. Some new non-additive maximum rank distance codes

Otal K., Ozbudak F.

FINITE FIELDS AND THEIR APPLICATIONS, vol.50, pp.293-303, 2018 (SCI-Expanded)

XLV. A new concatenated type construction for LCD codes and isometry codes

CARLET C., Guneri C., ÖZBUDAK F., SOLÉ P.

DISCRETE MATHEMATICS, vol.341, no.3, pp.830-835, 2018 (SCI-Expanded)

XLVI. A SUPER-SET OF PATTERSON-WIEDEMANN FUNCTIONS: UPPER BOUNDS AND POSSIBLE NONLINEARITIES

Kavut S., MAİTRA S., ÖZBUDAK F.

SIAM JOURNAL ON DISCRETE MATHEMATICS, vol.32, no.1, pp.106-122, 2018 (SCI-Expanded)

XLVII. Cyclic subspace codes via subspace polynomials

Otal K., ÖZBUDAK F.

DESIGNS CODES AND CRYPTOGRAPHY, vol.85, no.2, pp.191-204, 2017 (SCI-Expanded)

XLVIII. Structure and performance of generalized quasi-cyclic codes

Guneri C., ÖZBUDAK F., Ozkaya B., Sacikara E., SEPASDAR Z., SOLÉ P.

FINITE FIELDS AND THEIR APPLICATIONS, vol.47, pp.183-202, 2017 (SCI-Expanded)

XLIX. ON COMPLEMENTARY DUAL ADDITIVE CYCLIC CODES

GÜNERİ C., ÖZBUDAK F., Ozdemir F.

ADVANCES IN MATHEMATICS OF COMMUNICATIONS, vol.11, no.2, pp.353-357, 2017 (SCI-Expanded)

L. Hasse-Weil bound for additive cyclic codes

Guneri C., ÖZBUDAK F., Ozdemir F.

DESIGNS CODES AND CRYPTOGRAPHY, vol.82, pp.249-263, 2017 (SCI-Expanded)

LI. Additive Rank Metric Codes

Otal K., ÖZBUDAK F.

IEEE TRANSACTIONS ON INFORMATION THEORY, vol.63, no.1, pp.164-168, 2017 (SCI-Expanded)

LII. Explicit maximal and minimal curves over finite fields of odd characteristics

ÖZBUDAK F., Saygi Z.

FINITE FIELDS AND THEIR APPLICATIONS, vol.42, pp.81-92, 2016 (SCI-Expanded)

LIII. A minimum distance bound for quasi-nD-cyclic codes

ÖZBUDAK F., Ozkaya B.

FINITE FIELDS AND THEIR APPLICATIONS, vol.41, pp.193-222, 2016 (SCI-Expanded)

LIV. Switchings of semifield multiplications

Hou X., ÖZBUDAK F., ZHOU Y.

DESIGNS CODES AND CRYPTOGRAPHY, vol.80, no.2, pp.217-239, 2016 (SCI-Expanded)

LV. EXPLICIT CONSTRUCTIONS OF SOME NON-GABIDULIN LINEAR MAXIMUM RANK DISTANCE CODES

Otal K., Ozbudak F.

ADVANCES IN MATHEMATICS OF COMMUNICATIONS, vol.10, no.3, pp.589-600, 2016 (SCI-Expanded)

LVI. Further results on rational points of the curve $y(qn) - y = \gamma x^{qh+1} - \alpha$ over F_{q^m}

Cosgun A., ÖZBUDAK F., SAYGI Z.

DESIGNS CODES AND CRYPTOGRAPHY, vol.79, no.3, pp.423-441, 2016 (SCI-Expanded)

LVII. FURTHER RESULTS ON FIBRE PRODUCTS OF KUMMER COVERS AND CURVES WITH MANY POINTS OVER FINITE FIELDS

ÖZBUDAK F., Temur B. G., YAYLA O.

ADVANCES IN MATHEMATICS OF COMMUNICATIONS, vol.10, no.1, pp.151-162, 2016 (SCI-Expanded)

LVIII. Classification of function fields with class number three

BİLHAN M., Buyruk D., ÖZBUDAK F.

JOURNAL OF PURE AND APPLIED ALGEBRA, vol.219, no.11, pp.5097-5116, 2015 (SCI-Expanded)

- LIX. **A construction of weakly and non-weakly regular bent functions over the ring of integers modulo**
ÇELİK D., ÖZBUDAK F.
APPLICABLE ALGEBRA IN ENGINEERING COMMUNICATION AND COMPUTING, vol.26, no.6, pp.543-554, 2015 (SCI-Expanded)
- LX. **On some bounds on the minimum distance of cyclic codes over finite fields**
ÖZBUDAK F., TUTDERE S., YAYLA O.
Designs, Codes, and Cryptography, vol.76, no.2, pp.173-178, 2015 (SCI-Expanded)
- LXI. **On the exact number of solutions of certain linearized equations**
ÖZBUDAK F., SAYGI Z.
DESIGNS CODES AND CRYPTOGRAPHY, vol.73, no.2, pp.457-468, 2014 (SCI-Expanded)
- LXII. **ON THE NUMBER OF QUADRATIC FORMS HAVING CODIMENSION 2 RADICALS IN CHARACTERISTIC 2 GIVING MAXIMAL/MINIMAL CURVES**
ÖZBUDAK F., SAYGI Z.
COMMUNICATIONS IN ALGEBRA, vol.42, no.9, pp.3795-3810, 2014 (SCI-Expanded)
- LXIII. **Uniqueness of F - q -quadratic perfect nonlinear maps from F - q^3 to F - $q(2)$**
Oezbudak F., POTT A.
FINITE FIELDS AND THEIR APPLICATIONS, vol.29, pp.49-88, 2014 (SCI-Expanded)
- LXIV. **Hybrid classes of balanced Boolean functions with good cryptographic properties**
Khan M. A., ÖZBUDAK F.
INFORMATION SCIENCES, vol.273, pp.319-328, 2014 (SCI-Expanded)
- LXV. **On the arithmetic operations over finite fields of characteristic three with low complexity**
AKLEYLEK S., ÖZBUDAK F., ÖZEL C. S.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.259, pp.546-554, 2014 (SCI-Expanded)
- LXVI. **Finite number of fibre products of Kummer covers and curves with many points over finite fields**
ÖZBUDAK F., GÜLMEZ TEMÜR B.
DESIGNS CODES AND CRYPTOGRAPHY, vol.70, no.3, pp.385-404, 2014 (SCI-Expanded)
- LXVII. **Improved probabilistic decoding of interleaved Reed-Solomon codes and folded Hermitian codes**
ÖZBUDAK F., Yayla O.
THEORETICAL COMPUTER SCIENCE, vol.520, pp.111-123, 2014 (SCI-Expanded)
- LXVIII. **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)
- LXIX. **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)
- LXX. **The Concatenated Structure of Quasi-Cyclic Codes and an Improvement of Jensen's Bound**
Güneri C., ÖZBUDAK F.
IEEE TRANSACTIONS ON INFORMATION THEORY, vol.59, no.2, pp.979-985, 2013 (SCI-Expanded)
- LXXI. **An exhaustive computer search for finding new curves with many points among fibre products of two Kummer covers over F_5 and F_7**
ÖZBUDAK F., GÜLMEZ TEMÜR B., Yayla O.
TURKISH JOURNAL OF MATHEMATICS, vol.37, no.6, pp.908-913, 2013 (SCI-Expanded)
- LXXII. **Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes**
Lopez-Permouth S. R., Ozadam H., ÖZBUDAK F., SZABO S.
FINITE FIELDS AND THEIR APPLICATIONS, vol.19, no.1, pp.16-38, 2013 (SCI-Expanded)
- LXXIII. **Planarity of products of two linearized polynomials**
KYUREGHYAN G., ÖZBUDAK F.

- FINITE FIELDS AND THEIR APPLICATIONS, vol.18, no.6, pp.1076-1088, 2012 (SCI-Expanded)
- LXXIV. **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface**
ÖZBUDAK F., Rodríguez-Henríquez F.
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2012 (SCI-Expanded)
- LXXV. **On the Polynomial Multiplication in Chebyshev Form**
Akleyek S., Cenk M., ÖZBUDAK F.
IEEE TRANSACTIONS ON COMPUTERS, vol.61, no.4, pp.584-587, 2012 (SCI-Expanded)
- LXXVI. **Quadratic forms of codimension 2 over finite fields containing F_4 and Artin-Schreier type curves**
ÖZBUDAK F., SAYGI E., Saygi Z.
FINITE FIELDS AND THEIR APPLICATIONS, vol.18, no.2, pp.396-433, 2012 (SCI-Expanded)
- LXXVII. **Modified Redundant Representation for Designing Arithmetic Circuits with Small Complexity**
AKLEYEK S., ÖZBUDAK F.
IEEE TRANSACTIONS ON COMPUTERS, vol.61, no.3, pp.427-432, 2012 (SCI-Expanded)
- LXXVIII. **A new class of quaternary LCZ sequence sets**
ÖZBUDAK F., SAYGI E., SAYGI Z.
DESIGNS CODES AND CRYPTOGRAPHY, vol.62, no.2, pp.189-198, 2012 (SCI-Expanded)
- LXXIX. **A BOUND ON THE MINIMUM DISTANCE OF QUASI-CYCLIC CODES**
Gueneri C., Oezbudak F.
SIAM JOURNAL ON DISCRETE MATHEMATICS, vol.26, no.4, pp.1781-1796, 2012 (SCI-Expanded)
- LXXX. **A relation between quasi-cyclic codes and 2-D cyclic codes**
Guner C., ÖZBUDAK F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.18, no.1, pp.123-132, 2012 (SCI-Expanded)
- LXXXI. **Quadratic forms of codimension 2 over certain finite fields of even characteristic**
ÖZBUDAK F., SAYGI E., Saygi Z.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.3, no.4, pp.241-257, 2011 (SCI-Expanded)
- LXXXII. **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)
- LXXXIII. **Multiplication of polynomials modulo $x(n)$**
CENK M., ÖZBUDAK F.
THEORETICAL COMPUTER SCIENCE, vol.412, no.29, pp.3451-3462, 2011 (SCI-Expanded)
- LXXXIV. **APPROXIMATION OF BOUNDS ON MIXED-LEVEL ORTHOGONAL ARRAYS**
SEZER A. D., ÖZBUDAK F.
ADVANCES IN APPLIED PROBABILITY, vol.43, no.2, pp.399-421, 2011 (SCI-Expanded)
- LXXXV. **A class of authentication codes with secrecy**
ÖZBUDAK E. K., ÖZBUDAK F., SAYGI Z.
DESIGNS CODES AND CRYPTOGRAPHY, vol.59, pp.287-318, 2011 (SCI-Expanded)
- LXXXVI. **Probabilities for absolute irreducibility of multivariate polynomials by the polytope method**
Koyuncu F., ÖZBUDAK F.
TURKISH JOURNAL OF MATHEMATICS, vol.35, no.3, pp.367-373, 2011 (SCI-Expanded)
- LXXXVII. **On Feedback Functions of Maximum Length Nonlinear Feedback Shift Registers**
ÇALIK C., Turan M. S., ÖZBUDAK F.
IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS COMMUNICATIONS AND COMPUTER SCIENCES, no.6, pp.1226-1231, 2010 (SCI-Expanded)
- LXXXVIII. **On multiplication in finite fields**
Cenk M., ÖZBUDAK F.
JOURNAL OF COMPLEXITY, vol.26, no.2, pp.172-186, 2010 (SCI-Expanded)
- LXXXIX. **A NOTE ON NEGACYCLIC AND CYCLIC CODES OF LENGTH $p(s)$ OVER A FINITE FIELD OF**

CHARACTERISTIC p

ÖZADAM H., Ozbudak F.

ADVANCES IN MATHEMATICS OF COMMUNICATIONS, vol.3, no.3, pp.265-271, 2009 (SCI-Expanded)

- XC. **Joint linear complexity of arbitrary multisequences consisting of linear recurring sequences**
Fu F., Niederreiter H., ÖZBUDAK F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.15, no.4, pp.475-496, 2009 (SCI-Expanded)
- XC1. **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)
- XCII. **Joint linear complexity of multisequences consisting of linear recurring sequences**
Fu F., Niederreiter H., Ozbudak F.
CRYPTOGRAPHY AND COMMUNICATIONS-DISCRETE-STRUCTURES BOOLEAN FUNCTIONS AND SEQUENCES, vol.1, no.1, pp.3-29, 2009 (SCI-Expanded)
- XCIII. **Linear complexity over F_q and over F_{q^m} for linear recurring sequences**
MEIDL W., ÖZBUDAK F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.15, no.1, pp.110-124, 2009 (SCI-Expanded)
- XCIV. **Integral and homothetic indecomposability with applications to irreducibility of polynomials**
Koyuncu F., ÖZBUDAK F.
TURKISH JOURNAL OF MATHEMATICS, vol.33, no.3, pp.283-294, 2009 (SCI-Expanded)
- XCV. **Weil-Serre Type Bounds for Cyclic Codes**
GÜNERİ C., ÖZBUDAK F.
IEEE TRANSACTIONS ON INFORMATION THEORY, vol.54, no.12, pp.5381-5395, 2008 (SCI-Expanded)
- XCVI. **Systematic authentication codes using additive polynomials**
ÖZBUDAK F., Saygi Z.
DESIGNS CODES AND CRYPTOGRAPHY, vol.49, pp.61-77, 2008 (SCI-Expanded)
- XCVII. **Some constructions of (t, m, s) -nets with improved parameters**
Ling S., Ozbudak F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.14, no.3, pp.658-675, 2008 (SCI-Expanded)
- XCVIII. **Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields**
Güneri C., Ozbudak F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.14, no.1, pp.44-58, 2008 (SCI-Expanded)
- XCIX. **Curves related to Coulter's maximal curves**
ÇAKÇAK E., ÖZBUDAK F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.14, no.1, pp.209-220, 2008 (SCI-Expanded)
- C. **Constructions and bounds on linear error-block codes**
LİNG S., Ozbudak F.
DESIGNS CODES AND CRYPTOGRAPHY, vol.45, no.3, pp.297-316, 2007 (SCI-Expanded)
- CI. **Fibre products of Kummer covers and curves with many points**
Oebudak F., Temur B. G.
Applicable Algebra in Engineering, Communications and Computing, vol.18, no.5, pp.433-443, 2007 (SCI-Expanded)
- CII. **Further improvements on asymptotic bounds for codes using distinguished divisors**
Niederreiter H., Ozbudak F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.13, no.3, pp.423-443, 2007 (SCI-Expanded)
- CIII. **Some Artin-Schreier type function fields over finite fields with prescribed genus and number of rational places**
ÇAKÇAK E., Ozbudak F.
JOURNAL OF PURE AND APPLIED ALGEBRA, vol.210, no.1, pp.113-135, 2007 (SCI-Expanded)
- CIV. **Cyclic codes and reducible additive equations**
Güneri C., Ozbudak F.
IEEE TRANSACTIONS ON INFORMATION THEORY, vol.53, no.2, pp.848-853, 2007 (SCI-Expanded)

- CV. **Gilbert Varshamov type bounds for linear codes over finite chain rings**
ÖZBUDAK F., SOLE P.
Advances In Mathematics Of Communications, vol.1, pp.99-109, 2007 (SCI-Expanded)
- CVI. **Some maximal function fields and additive polynomials**
GARCÍA A., ÖZBUDAK F.
COMMUNICATIONS IN ALGEBRA, vol.35, no.5, pp.1553-1566, 2007 (SCI-Expanded)
- CVII. **Low-discrepancy sequences using duality and global function fields**
Niederreiter H., Ozbudak F.
ACTA ARITHMETICA, vol.130, no.1, pp.79-97, 2007 (SCI-Expanded)
- CVIII. **Improved asymptotic bounds for codes using distinguished divisors of global function fields**
Niederreiter H., ÖZBUDAK F.
SIAM JOURNAL ON DISCRETE MATHEMATICS, vol.21, no.4, pp.865-899, 2007 (SCI-Expanded)
- CIX. **Some constructions of systematic authentication codes using Galois rings**
Oezbudak F., Saygi Z.
DESIGNS CODES AND CRYPTOGRAPHY, vol.41, no.3, pp.343-357, 2006 (SCI-Expanded)
- CX. **Aperiodic and odd correlations of some p-ary sequences from Galois rings**
Ling S., Ozbudak F.
IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS COMMUNICATIONS AND COMPUTER SCIENCES, no.9, pp.2258-2263, 2006 (SCI-Expanded)
- CXI. **Improvements on generalized hamming weights of some trace codes**
GÜNERİ C., Ozbudak F.
DESIGNS CODES AND CRYPTOGRAPHY, vol.39, no.2, pp.215-231, 2006 (SCI-Expanded)
- CXII. **An explicit class of codes with good parameters and their duals**
LİNG S., XİNG C., Ozbudak F.
DISCRETE APPLIED MATHEMATICS, vol.154, no.2, pp.346-356, 2006 (SCI-Expanded)
- CXIII. **Improved bounds on Weil sums over Galois rings and homogeneous weights**
Ling S., Ozbudak F.
CODING AND CRYPTOGRAPHY, vol.3969, pp.412-426, 2006 (SCI-Expanded)
- CXIV. **Improved p-ary codes and sequence families from Galois rings of characteristic p(2)**
LİNG S., Ozbudak F.
SIAM JOURNAL ON DISCRETE MATHEMATICS, vol.19, no.4, pp.1011-1028, 2006 (SCI-Expanded)
- CXV. **Number of rational places of subfields of the function field of the Deligne-Lusztig curve of Ree type**
Cakcak E., Ozbudak F.
ACTA ARITHMETICA, vol.120, no.1, pp.79-106, 2005 (SCI-Expanded)
- CXVI. **Elements of prescribed order, prescribed traces and systems of rational functions over finite fields**
Ozbudak F.
DESIGNS CODES AND CRYPTOGRAPHY, vol.34, no.1, pp.35-54, 2005 (SCI-Expanded)
- CXVII. **Improved p-ary codes and sequence families from Galois rings**
Ling S., Ozbudak F.
SEQUENCES AND THEIR APPLICATIONS - SETA 2004, vol.3486, pp.236-242, 2005 (SCI-Expanded)
- CXVIII. **An improvement on the bounds of Weil exponential sums over Galois rings with some applications**
Ling S., Ozbudak F.
IEEE TRANSACTIONS ON INFORMATION THEORY, vol.50, no.10, pp.2529-2539, 2004 (SCI-Expanded)
- CXIX. **Matrix-product constructions of digital nets**
Niederreiter H., Ozbudak F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.10, no.3, pp.464-479, 2004 (SCI-Expanded)
- CXX. **Subfields of the function field of the Deligne-Lusztig curve of Ree type**
ÇAKÇAK E., Ozbudak F.
ACTA ARITHMETICA, vol.115, no.2, pp.133-180, 2004 (SCI-Expanded)
- CXXI. **Constructing linear unequal error protection codes from algebraic curves**
Ozbudak F., STİCHTENOTH H.

- IEEE TRANSACTIONS ON INFORMATION THEORY, vol.49, no.6, pp.1523-1527, 2003 (SCI-Expanded)
- CXXII. **A note on divisor class groups of degree zero of algebraic function fields over finite fields**
Ozbudak F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.9, no.1, pp.129-133, 2003 (SCI-Expanded)
- CXXIII. **Note on Niederreiter-Xing's propagation rule for linear codes**
Ozbudak F., STİCHTENOTH H.
APPLICABLE ALGEBRA IN ENGINEERING COMMUNICATION AND COMPUTING, vol.13, no.1, pp.53-56, 2002 (SCI-Expanded)
- CXXIV. **Constructions of digital nets using global function fields**
Niederreiter H., Ozbudak F.
ACTA ARITHMETICA, vol.105, no.3, pp.279-302, 2002 (SCI-Expanded)
- CXXV. **On maximal curves and linearized permutation polynomials over finite fields**
ÖZBUDAK F.
Journal of Pure and Applied Algebra, vol.162, no.1, pp.87-102, 2001 (SCI-Expanded)
- CXXVI. **Additive polynomials and primitive roots over finite fields**
Ozbudak F.
COMMUNICATIONS IN ALGEBRA, vol.29, no.3, pp.987-991, 2001 (SCI-Expanded)
- CXXVII. **Constructing codes from algebraic curves**
Ozbudak F., STİCHTENOTH H.
IEEE TRANSACTIONS ON INFORMATION THEORY, vol.45, no.7, pp.2502-2505, 1999 (SCI-Expanded)
- CXXVIII. **Curves with many points and configurations of hyperplanes over finite fields**
Ozbudak F., Stichtenoth H.
FINITE FIELDS AND THEIR APPLICATIONS, vol.5, no.4, pp.436-449, 1999 (SCI-Expanded)
- CXXIX. **Codes on fibre products of some Kummer coverings**
Ozbudak F.
FINITE FIELDS AND THEIR APPLICATIONS, vol.5, no.2, pp.188-205, 1999 (SCI-Expanded)
- CXXX. **Codes on superelliptic curves**
ÖZBUDAK F., Glukhov G.
Turkish Journal of Mathematics, vol.22, no.2, pp.223-234, 1998 (SCI-Expanded)
- CXXXI. **A note on towers of function fields over finite fields**
Ozbudak F., Thomas M.
COMMUNICATIONS IN ALGEBRA, vol.26, no.11, pp.3737-3741, 1998 (SCI-Expanded)
- CXXXII. **On lower bounds for incomplete character sums over finite fields**
Özbudak F.
Finite Fields and their Applications, vol.2, no.2, pp.173-191, 1996 (SCI-Expanded)

Articles Published in Other Journals

- I. **On a class of repeated root monomial like abelian codes**
Martinez Moro E., Özadam H., ÖZBUDAK F., Szabo S.
Journal of Algebra Combinatorics Discrete Structures and Applications, vol.2, pp.75-84, 2015 (Scopus)
- II. **On Verification of Restricted Extended Affine Equivalence of Vectorial Boolean Functions**
ÖZBUDAK F., SINAK A., YAYLA O.
Lecture Notes in Computer Science, vol.9061, pp.137-154, 2015 (Peer-Reviewed Journal)
- III. **Classes of weak Dembowski-Ostrom polynomials for multivariate quadratic cryptosystems**
ALAM B., ÖZBUDAK F., YAYLA O.
Journal of Mathematical Cryptology, vol.9, no.1, pp.11-22, 2015 (Scopus)
- IV. **Characterisation and enumeration of a class of semi bent quadratic Boolean functions**
KOÇAK N., KOÇAK O., ÖZBUDAK F., SAYGI Z.
International Journal of Information and Coding Theory, vol.3, pp.39-57, 2015 (Peer-Reviewed Journal)

V. Fibre products of hyperelliptic curves and geometric Goppa codes

Stepanov S., Özbudak F.

Discrete Mathematics and Applications, vol.7, no.3, pp.223-229, 1997 (Scopus)

Books & Book Chapters

- I. **On two applications of polynomials $x^k - cx - d$ over finite fields and more**
İRİMAĞZI C., ÖZBUDAK F.
in: Arithmetic of Finite Fields, Mesnager Sihem, Zhou Zhengchun, Editor, Springer, Cham, pp.14-32, 2023
- II. **Constructions of Cyclic Subspace Codes and Maximum Rank Distance Codes**
Özbudak F.
in: Network Coding and Subspace Designs, Marcus Greferath, Mario Osvin Pavčević, Natalia Silberstein, María Ángeles Vázquez-Castro, Editor, Springer, London/Berlin, Zürich, pp.43-66, 2018
- III. **Constructive Asymptotic Codes with an Improvement on the Tsfasman-Vlăduț-Zink and Xing Bounds**
NİEDERREITER H., ÖZBUDAK F.
in: Coding Cryptography and Combinatorics, Keqin Feng, Harald Niederreiter, Chaoping Xing, Editor, Birkhäuser Basel, pp.259-275, 2004

Refereed Congress / Symposium Publications in Proceedings

- I. **On Two Applications of Polynomials $x^k - cx - d$ over Finite Fields and More**
İrimağzı C., ÖZBUDAK F.
9th International Workshop on the Arithmetic of Finite Fields, WAIFI 2022, Chengdu, China, 29 August - 02 September 2022, vol.13638 LNCS, pp.14-32
- II. **New Correlations of m-sequences over the finite field F_4 compatible with a new bijection to Z_4**
Boztas S., ÖZBUDAK F., Tekin E.
10th International Workshop on Signal Design and Its Applications in Communications, IWSDA 2022, Colchester, England, 1 - 05 August 2022
- III. **Counting Boolean Functions with Faster Points**
Salagean A., ÖZBUDAK F.
WCC 2019: The Eleventh International Workshop on Coding and Cryptography, 31 March - 05 April 2019
- IV. **Subspace Packings**
etzion t, kurz s., OTAL K., ÖZBUDAK F.
WCC 2019: The Eleventh International Workshop on Coding and Cryptography, 31 March - 05 April 2019
- V. **On plateaued functions, linear structures and permutation polynomials**
Mesnager S., KAYTANCI K., ÖZBUDAK F.
3rd International Conference on Codes, Cryptology and Information Security, C2SI 2019, Rabat, Morocco, 22 - 24 April 2019, pp.217-235
- VI. **Bounding the Minimum Distance of Affine Variety Codes Using Symbolic Computations of Footprints**
GEİL O., ÖZBUDAK F.
International Castle Meeting on Coding Theory and Applications, ICMCTA 2017, 28 - 31 August 2017, pp.128-138
- VII. **A correction and improvements of some recent results on walsh transforms of gold type and Kasami-Welch type functions**
Coşgun A., ÖZBUDAK F.
6th International Workshop on Arithmetic of Finite Fields, WAIFI 2016, Ghent, Belgium, 13 - 15 July 2016, pp.243-257
- VIII. **A super set of Patterson Wiedemann functions upper bounds and possible nonlinearities**
KAVUT S., Maitra S., ÖZBUDAK F.
International Workshop on the Arithmetic of Finite Fields WAIFI 2016, 13 - 15 July 2016

- IX. **Results on algebraic curves over finite fields with applications incoding theory and cryptography**
ÖZBUDAK F.
Combinatorics 2016, 29 May - 04 June 2016
- X. **Results on characterizations of plateaued functions in arbitrary characteristic**
Mesnager S., ÖZBUDAK F., Sinak A.
2nd International Conference on Cryptography and Information Security in the Balkans, BalkanCryptSec 2015, Koper, Slovenia, 3 - 04 September 2015, vol.9540, pp.17-30
- XI. **Improvement in non-linearity of carlet-feng infinite class of boolean functions**
Khan M. A., ÖZBUDAK F.
11th International Conference on Cryptology and Network Security, CANS 2012, Darmstadt, Germany, 12 - 14 December 2012, pp.280-295
- XII. **Probabilistic Decoding of RS Codes with Extended BKY Algorithm**
YAYLA O., ÖZBUDAK F.
International Conference on Applied and Computational Mathematics, Ankara, Turkey, 3 - 06 October 2012
- XIII. **Nested multipartite secret sharing**
Kaskaloglu K., ÖZBUDAK F.
2011 IEEE International Conference on Computer Science and Automation Engineering, CSAE 2011, Shanghai, China, 10 - 12 June 2011, vol.4, pp.66-73
- XIV. **On Hierarchical Threshold Access Structures**
KAŞKALOĞLU K., ÖZBUDAK F.
Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense), 22 - 23 November 2010
- XV. **Improved bounds on weil sums over galois rings and homogeneous weights**
Ling S., ÖZBUDAK F.
International Workshop on Coding and Cryptography, WCC 2005, Bergen, Norway, 14 - 18 March 2005, pp.412-426
- XVI. **Improved p-ary codes and sequence families from Galois rings**
Ling S., ÖZBUDAK F.
Third International Conference on Sequences and Their Applications - SETA 2004, Seoul, South Korea, 24 - 28 October 2004, vol.3486, pp.236-242
- XVII. **Fibre products of superelliptic curves and codes therefrom**
Stepanov S. A., Ozbudak F.
Proceedings of the 1997 IEEE International Symposium on Information Theory, Ulm, Germany, 29 June - 04 July 1997, pp.413

Supported Projects

ÖZBUDAK F., KIRCALI M., KAYTANCI K., Project Supported by Higher Education Institutions, Dizayn teori kriptografi ve kodlama teorisi konusunda araştırma ve uygulama, 2021 - 2022

ÖZBUDAK F., ÇOMAK P., SINAK A., AYBAK L., OTAL K., Project Supported by Higher Education Institutions, ARC İNŞAALARI VE WEIERSTASS NOKTALARININ KODLAMA TEORİSİNE VE KRİPTOGRAFİYE UYGULAMALARI, 2017 - 2017

ÖZBUDAK F., Muş K., Koçak O., Project Supported by Higher Education Institutions, Algebraic And Combinatorial Methods İn Finite Fields, Coding Theory And Cryptography, 2012 - 2013

ÖZBUDAK F., Project Supported by Higher Education Institutions, Algebraic And Combinatorial Methods İn Finiters Fields, Coding Theory And Cryptography, 2011 - 2011

Activities in Scientific Journals

Advances In Mathematics Of Communications, Committee Member, 2015 - Continues

Metrics

Publication: 205

Citation (WoS): 717

Citation (Scopus): 783

H-Index (WoS): 13

H-Index (Scopus): 13

Non Academic Experience

METU Institute of Applied Mathematics

METU Department of Mathematics

METU Institute of Applied Mathematics

METU Department of Mathematics

METU Department of Mathematics