Research Statement

Oğuz Yayla

June, 2019

My main research area is public key cryptography, cryptographic protocols, sequences in cryptography and telecommunication, algebraic coding theory and blockchain. In my research, I mainly use tools and approaches of combinatorics, algebraic function fields, algebraic curves, algebraic number theory and finite fields. Thus my academic work has an interdisciplinary nature.

I am interested in cryptographic problems that can be solved by combinatoric and algebraic tools. For example, in my recent works I have used tools as diverse as Hermitian function fields, difference sets, Diophantine equations, incomplete character sums, fibre products of Kummer covers, Artin-Schreier curves, cyclotomic number fields and cyclotomic cosets. Due to this reason my research topics include cryptography, coding theory, pseudorandom sequences, lattice based cryptosystems, combinatorial designs, algebraic function fields, algebraic/analytic number theory, finite fields, discrete mathematics and design theory.

I have participated as principal investigator and researcher in 8 research projects about cryptography. In addition, I have already published 14 journal papers and 17 publications in the refereed proceedings of conferences, see references below. I will explain each of them shortly in subsequent pages. They are mainly cryptography related papers, but some of them can be also classified in topics algebraic decoding, algebraic curves, combinatorial designs, pseudorandom numbers/sequences and blockchain. My work has appeared in journals in a number of fields, including: Design Codes and Cryptography, Advances in Mathematics of Communications, Mathematics in Computer Science, Discrete Mathematics, Ramanujan Journal, Theoretical Computer Science, Lecture Notes in Computer Science, Turkish Journal of Mathematics, Journal of Mathematical Cryptology.

Below I briefly state current status of my research work.

Cryptography:

I completed master of science and doctorate programs in the Department of Cryptography, METU. Therefore I have comprehensive knowledge of both theory and application in cryptography. I make use of my knowledge and prepare new papers/projects to convey new points onto my colleagues and academia. My main research are is cryptography, thus I have mostly contributed in this area throughout my academic career. While some of my contributions are related with the mathematical theory of cryptography, the others are in the practical points of cryptography. I consider to exploit algebraic geometric and combinatoric approaches further to get new directions and results in cryptography.

I completed MS thesis on elliptic curve cryptography [1] and studied the public key infrastructures (PKI) in a couple of projects during doctorate program [P1,P2,P3]. One of them was a TUBITAK-1007 project on “Research and Development on PKI”. In this project, I did research on DSA and ECDSA cryptosystems and their implementation. Moreover, I did analysis on test parameters of RSA, DSA and ECDSA cryptosystems for their secure implementation. Secondly, I participated in a research project supported by ASELSAN on “Selecting secure elliptic curves and Implementing a signature system based on elliptic curves”, in which I did research on fast

implementation of elliptic curve cryptography. Thirdly, I was a researcher in the project "Security test of RSA cryptosystem parameters", and I looked for the RSA domain parameters for its secure implementation. We also have implemented all kinds of attacks against RSA cryptosystem. In addition, I have published a few papers in peered reviewed conference proceedings complying with the topics of these three projects [2,3,4,5,6,7,8].

After starting assistant professorship in the Hacettepe University, I completed a TUBITAK-1002 project and I am currently working on TUBITAK-3501 project as a principal investigator [P5,P6]. They are about combinatorial designs of difference sets, Hadamard matrices, sequences and boolean functions for cryptography and telecommunication systems. In these projects, my main aim is using design theory tools to obtain "almost perfect" cryptographic functions and spreading codes since it is still now not known how to construct perfect cryptographic functions and codes for all parameters.

In addition, I am participated in two TUBITAK projects on post quantum lattice based cryptography [P7,P8]. Lattice based cryptography is one of the most attractive area in post quantum public key cryptography. In these projects, I have been working on analysis and test methodology of lattice based key encapsulation cryptosystem. Moreover, I have been doing fast CPU/GPU implementation of lattice based cryptosystems. Our preliminary results were presented in conferences, and appeared in their proceedings. [9,10,11]. I have also been doing research on formal analysis of NTRU based post quantum cryptosystems. Formal analysis is a proof method of possible attacks on the system by using some mathematical formalization of the system., that is, it explores the existence of state against security goals. Formal analysis methodology is commonly used in the evaluation systems of cryptographic soft/hardwares.

Algebraic decoding:

A linear code is a vector space over a finite field and the main task in error correcting codes is (1) to design a long code having elements with high minimum weight and (2) to construct a fast decoding method correcting as many as errors. The minimum weight of elements of a code is called the minimum distance.

During my PhD thesis I studied decoding of algebraic geometric (AG) codes. They are first proposed by Goppa in 1975. AG codes are important as they break the length barrier of commonly used Reed-Solomon codes. In addition, it was shown in the beginning of 80s that AG codes are asymptotically good codes. In other words there exists a sequence of algebraic curves with codes having high minimum distance. In my thesis, we proposed a new method of decoding AG codes defined over Hermitian curves. Our decoding method is probabilistic but it is shown that we can correct high ratio of errors by high probability. We also utilized solving sparse system of equations to prove our results. We published the results in an international journal [12] and in an international conference [13]. I am still interested in this subject. I look for a way of applying our method to devise a new list decoding algorithm for Hermitian codes.

After completing my PhD thesis, I was participated in TUBITAK-1001 project (PI: Prof. Dr. Ferruh Özbudak) as a postdoctoral researcher [P4]. In this project I did research on fast decoding of interleaved RS-codes and curves with many points for coding theory. In fact, I implemented a search algorithm written in MAGMA for finding curves with many points on a large number of paralel connected computers, and obtained many record breaking results.

It is one of the important tasks to find a family of codes with high minimum distance. It is usually difficult to find out the minimum distance explicitly if the code family is large. We studied the minimum distance of a family of cyclic codes. Cyclic codes are known to be the ideals in a polynomial ring over a finite field. By effective using the cyclotomic coset structure of the finite field elements we proved a lower bound on the minimum distance for a larger family of cyclic codes. This result is accepted by an international journal to be published [14].

Algebraic curves with many points:

Finding number of rational points on a curve is a challenging problem for hundreds of years. Scientist cleverly obtained ingenious methods to count number of rational points on a curve. Today, there are online repositories collecting curves with many points such as http:\\manypoints.org. We studied fibre products of Kummer covers to find explicit examples of algebraic curves with many rational points over finite fields. We discovered new records for certain entries of the repository manypoints.org. In particular, we introduced a new curve with the number of rational points satisfying Ihara bound. We collected the results in a paper that is published in Turkish Journal of Mathematics [15]. I further extended the results for other finite fields and presented them in a national symposium [16]. We further extended these results for new fibre products, and the results are published in the international journal of Advances in Mathematics of Communications [17]. I think that this work will also reveal new examples of curves with many rational points. Besides its self-interest, curves with many points are used in constructing codes having high minimum distance and in obtaining asymptotically good codes. We note that there are other theoretical and practical applications of this topic.

I had the chance of using my knowledge on algebraic curves to prove new results in cryptography. Namely, we proved the existence of Artin-Schreier curves with many points and constructed them explicitly. Then we employed this result to show that certain infinite family of keys are weak in multivariate quadratic public-key cryptosystems. These results are published in Journal of Mathematical Cryptology [18].

Combinatorial designs:

One of the main topics in combinatorics is the design theory. Nowadays I mainly interested in designing difference sets and Hadamard-type matrices. In fact, proving existence or nonexistence of difference sets is my aim in this area. Difference sets are used in designing boolean functions in cryptography, wired communication, wireless communication, sound amplifier, radar, sonar and others. In 2012 we proved certain new nonexistence results of relative difference sets by cultivating their algebraic properties, counting arguments and Diophantine equations. I first presented our results in the international conference of Sequences and Their Applications. Then the paper is published by Lecture Notes in Computer Science [19]. During my postdoctoral period, I made the classification of good sequences in terms of difference set terminology, which was published by Advances in Mathematics of Communications [20]. Recently, we have implemented some good sequences in design of boolean function and communication channel, and presented the results in conferences [21,22,23,24]. I still consider new points in difference sets because of their connection with cryptography, telecommunication theory, algebraic geometry and coding theory.

It is very well known that difference sets with low correlation coefficients are a subclass of generalized Hadamard matrices. In other words, proving new results in generalized Hadamard matrices will lead to new results in difference sets. During my post-doctoral studies at RICAM, Austria, we figured a new analysis method of generalized Hadamard matrices. We exploited the nonexistence of a solution to the Diophantine equation, satisfied by the corresponding generalized Hadamard matrix, in terms of the nonexistence principal ideal decomposition of some numbers over cyclotomic number fields. We have collected the results in a journal paper [25]. Then I have explored this area with my colleagues and published a series of papers [26,27,28]. I should note that using algebraic number theoretical tools to prove new results in combinatorial objects such as generalized Hadamard matrices and applying these result for flourishing new improvements in cryptography and coding theory is very attracting point for me. I will further stay focused on this point and I have a couple of ongoing research [D1,D2,D3,D4].

Pseudorandom numbers/sequences:

The Weil bound is very useful tool coming from analytic number theory to devise some bounds on measures and properties of pseudorandom numbers/generators/sequences. A family of sequences with good properties is one of the ultimate aims in pseudorandomness theory. We recently obtained a relation between the cross-correlation measure and the family complexity of family of sequences. Then we presented some families of sequences with good cross-correlation measure and good family complexity by using bounds on incomplete sums of quadratic characters over finite fields [29], and studied their applications in cryptography [30]. Moreover, we improved the number of boxes on a finite field, and so obtained better complexity bounds on some sequences. This result was published by journal of Discrete Mathematics [31]. I have ongoing research on this direction, draft/submitted papers [D5,D6].

Blockchain:

Blockchain is a technology of recording transactions on a ledger uniquely without any need of a trusted third party. In fact, blockchain is a decentralized, distributed, consensus method for exchanging of a kind of goods without an authority. I have been working on this topic since two years. I have been supervising a thesis on Digital Signatures in Blockchain, and co-supervising a thesis on Secure Multiparty Computation by Blockchain. We plan to present our results in conferences [D7,D8].

Research Projects:

[P1] Researcher, TÜBİTAK 1007 Project - METU, Ankara.

Research and development on public key infrastructure

07/2006 - 07/2008

[P2] Researcher, ASELSAN - METU, Ankara.

Selecting secure elliptic curves and Implementing a signature system based on elliptic curves

10/2006 - 03/2008

[P3] Researcher, TÜRKTRUST - METU, Ankara.

Security test of RSA cryptosystem parameters

05/2013 - 06/2013

[P4] Post-Doctoral Researcher, TÜBİTAK 1001-Project - METU, Ankara.

Algebraic curves and their applications in cryptography and coding theory

09/2011 - 04/2013

[P5] Principal Investigator, TÜBİTAK 1002-Project - Hacettepe Uni., Ankara.

Generation of New γ-Butson-Hadamard Matrices and their Cryptographic Applications

05/2016 - 05/2017

[P6] Principal Investigator, TÜBİTAK 3501-Project - Hacettepe Uni., Ankara.

Sequences and Their Applications to Cryptography and Coding Theory

04/2017 - 04/2020

[P7] Researcher, TÜBİTAK 1003-Project - Hacettepe Uni., Ankara.

Design of Lattice Based Cryptosystems and their Analysis

04/2018 - 04/2020

[P8] Researcher, TÜBİTAK-GNSF Turkey-Georgia Science Foundations Joint Project - Hacettepe Uni. Ankara.

Formal Analysis of NTRU Based Cryptosystems

02/2019 - 02/2021

Research Papers:

[1] Ersan Akyıldız and Oğuz Yayla. Scalar multiplication on elliptic curves. In II. National Conference on Cryptology Proceedings, pages 114–124. Ankara, 15–17 Dec 2006. URL: http://goo.gl/KfDBKu.

[2] Murat Cenk and Oğuz Yayla. E–imza uygulamaları ve karşılaştırmaları. In Ulusal Elektronik Imza Sempozyumu Proceedings. Ankara, 7–8 Aralık 2006. URL:http://ueimzas.gazi.edu.tr/pdf/poster/38.pdf.

[3] Oğuz Yayla. DSA sisteminin çalıstırılması ve test edilmesi. In II. International Conference on Information Security and Cryptology Proceedings, pages 290–297. Ankara, 13–14 Dec 2007. URL: http://iscturkey.org/iscold/ISCTURKEY2007/papers/43.pdf.

[4] Oğuz Yayla. Kriptografik modüllerin güvenlik gereksinimleri. In III. International Conference on Information Security and Cryptology Proceedings, pages 253–256. Ankara, 25–27 Dec 2008. URL: http://iscturkey.org/iscold/ISCTURKEY2008/posters/02.pdf.

[5] Sedat Akleylek and Oğuz Yayla. PKI–lite: A PKI system with limited resources. In II. International Conference on Information Security and Cryptology Proceedings, pages 59–62. Ankara, 13–14 Dec 2007. URL: http://iscturkey.org/iscold/ISCTURKEY2007/papers/05.pdf.

[6] Hakan Özadam and Oğuz Yayla. On algebraic attacks using Gröbner basis. In II. International Conference on Information Security and Cryptology Proceedings, pages 312–318. Ankara, 13–14 Dec 2007. URL: http://iscturkey.org/2010/2008/2007/pdf/poster/6.pdf.

[7] Bilal Alam and Oğuz Yayla. Recent attacks against HFE/multi–HFE MQ cryptosystems and connection with Ore's p-polynomial decomposition. In VI. International Conference on Information Security and Cryptology Proceedings, pages 192–198. Ankara, 20–21 Sep 2013. URL: http://iscturkey.org/iscold/ISCTURKEY2013/files/paper93.pdf.

[8] Ersan Akyıldız, Çagdas Çalık, Mert Özarar, Zaliha Tok, and Oğuz Yayla. RSA kriptosistemi parametreleri için güvenlik testi yazılımı. In VI. International Conference on Information Security and Cryptology Proceedings, pages 124–127. Ankara, 20–21 Sep 2013. URL: http://iscturkey.org/iscold/ISCTURKEY2013/files/paper67.pdf.

[9] Damla Acar and Oğuz Yayla Latis tabanlı kriptografi algoritmalarının hız testi. In XI. International Conference on Information Security and Cryptology Proceedings, pages 40--44. Ankara, 17-18 OCTOBER 2018. https://www.iscturkey.org/assets/files/Bildiriler_kitab%C4%B1_2018_3.pdf.

[10] Sibel Kurt and Oğuz Yayla. Kuantum sonrası latis tabanlı anahtar kapsülleme algoritmalarını İncelenmesi. Ankara Matematik Günleri 2018, page~68. Ankara, TOBB ETU, 27-28 Nisan 2018. http://amg2018.etu.edu.tr/documents/AMG2018-bildiri-kitabi.pdf.

[11] Damla Acar and Oğuz Yayla. Latis tabanlı Şifreleme algoritmalarının İncelenmesi. Ankara Matematik Günleri 2018, page~16. Ankara, TOBB ETU, 27-28 Nisan 2018.

http://amg2018.etu.edu.tr/documents/AMG2018-bildiri-kitabi.pdf.

[12] Ferruh Özbudak and Oğuz Yayla. Improved probabilistic decoding of interleaved Reed–Solomon codes and folded Hermitian codes. Theoret. Comput. Sci., 520:111–123, 2014. http://doi.org/10.1016/j.tcs.2013.10.025.

[13] Ferruh Özbudak, Oğuz Yayla. Probabilistic Decoding of RS codes with extended BKY algorithm. International Conference on Applied and Computational Mathematics (ICACM), 3-6 Ekim 2012, Ankara. http://icacm.iam.metu.edu.tr/ocs/index.php/icacm/2012/paper/view/239/155

[14] Ferruh Özbudak, Seher Tutdere, and Oğuz Yayla. On some bounds on the minimum distance of cyclic codes over finite fields. Des. Codes Cryptogr., 76(2):173--178, 2015. http://dx.doi.org/10.1007/s10623-014-9927-7

[15] Ferruh Özbudak, Burcu Gülmez Temür, and Oğuz Yayla. An exhaustive computer search for finding new curves with many points among fibre products of two Kummer covers over F5 and F7. Turkish J. Math., 37(6):908–913, 2013. http://doi.org/10.3906/mat-1206-26.

[16] Oğuz Yayla. GF(11) üzerinde çok noktalı cebirsel egriler. Ankara Matematik Günleri, Ankara,

13 Haziran 2013. http://mcs.cankaya.edu.tr/amg8.

[17] Ferruh Özbudak, Burcu Gümez Temür, and Oğuz Yayla. Further results on fibre products of {K} ummer covers and curves with many points over finite fields. Adv. Math. Commun., 10(1):151--162, 2016. http://dx.doi.org/10.3934/amc.2016.10.151

[18] Bilal Alam, Ferruh Özbudak, and Oğuz Yayla. Classes of weak {D}embowski-{O}strom polynomials for multivariate quadratic cryptosystems. J. Math. Cryptol., 9(1):11--22, 2015. http://dx.doi.org/10.1515/jmc-2013-0019

[19] Ferruh Özbudak, Oğuz Yayla, and C. Cengiz Yıldırım. Nonexistence of certain almost p-ary perfect sequences. In Sequences and their applications—SETA 2012, volume 7280 of Lecture Notes in Comput. Sci., pages 13–24. Springer, Heidelberg, 2012. http://doi.org/10.1007/978-3-642-30615-0_2.

[20] Oğuz Yayla. Nearly perfect sequences with arbitrary out-of-phase autocorrelation. Adv. Math. Commun. 10(2):401--411, 2016. http://dx.doi.org/10.3934/amc.2016014

[21] Sibel Kurt and Oğuz Yayla. CDMA sistemleri için yeni mükemmel dizi örnekleri. Şubat 8 - 10, 2017. https://ab.org.tr/ab17/bildiri/124.pdf.

[22] Sibel Kurt and Oğuz Yayla. Küçük otokorelasyonlu neredeyse mükemmel diziler. Ankara Matematik Günleri 2017, page~68. Ankara, Hacettepe Üni., 25-26 MAYIS, 2017. http://www.amg2017.hacettepe.edu.tr/documents/bildiri-ozetleri-kitapcigi.pdf.

[23] Sibel Kurt and Oğuz Yayla. Nearly perfect sequences and cryptographic functions. Workshop on Practical and Theoretical Aspects of Cryptography and Information Security. Tiblisi, Dec 8, 2017. http://www.viam.science.tsu.ge/aminse2017/pdf/book_of_abstracts.pdf.

[24] Ferruh Özbudak, Ahmet Sınak, and Oğuz Yayla. On verification of restricted extended affine equivalence of vectorial {B}oolean functions. Arithmetic of finite fields, volume 9061 of {\em Lecture Notes in Comput. Sci.}, pages 137--154. Springer, Cham, 2015. http://dx.doi.org/10.1007/978-3-319-16277-5_8

[25] Arne Winterhof, O\u{g}uz Yayla, and Volker Ziegler. Non-existence of some nearly perfect sequences, near {B}utson-{H}adamard matrices, and near conference matrices.Math. Comput. Sci., 12(4):465--471, 2018. http://dx.doi.org/10.1007/s11786-018-0383-z

[26] Sibel Kurt and Oğuz Yayla. Near {B}utson-{H}adamard matrices with small off-diagonal entries. 3rd Istanbul Design Theory, Graph Theory and Combinatorics Workshop. İstanbul, June 13 -17, 2016. http://portal.ku.edu.tr/~eyazici/Research/Design2016/abstracts/abstract_kurt.pdf.

[27] Sibel Kurt and O\u{g}uz Yayla. Near {B}utson-{H}adamard matrices and nonlinear {B}oolean functions. Number-theoretic methods in cryptology, volume 10737 of Lecture Notes in Comput. Sci., pages 254--266. Springer, Cham, 2018. http://dx.doi.org/10.1007/978-3-319-76620-1_15

[28] Sibel Kurt and Oguz Yayla. Ideal factorization method and its applications.Mathematics, Informatics, and Their Applications in Natural Sciences and Engineering}, pages 149--160, 2019. http://dx.doi.org/10.1007/978-3-030-10419-1_9

[29] Arne Winterhof and Oğuz Yayla. Family complexity and cross-correlation measure for families of binary sequences. Ramanujan J., 39(3):639--645, 2016. http://dx.doi.org/10.1007/s11139-014-9649-5

[30] Oğuz Yayla. Families of pseudorandom binary sequences with low cross-correlation measure. {BalkanCryptSec} 2014, volume 9024 of Lecture Notes in Comput. Sci., pages 31--39. Springer, 2015. http://dx.doi.org/10.1007/978-3-319-21356-9_3

[31] Laszlo Merai and Oğuz Yayla. Improving results on the pseudorandomness of sequences generated via the additive order of a finite field. Discrete Math., 338(11):2020--2025, 2015. http://dx.doi.org/10.1016/j.disc.2015.04.015

Draft/Submitted papers:

[D1] Büşra Özden and Oğuz Yayla. Almost p-ary sequences. arXiv preprint arXiv:1807.11412v2, 2018.

[D2] Damla Acar and Oğuz Yayla. Power hadamard matrices and codes.

[D3] Sibel Kurt and Oğuz Yayla. Mann test for direct product difference sets.

[D4] Büşra Özden and Oğuz Yayla. Cryptographic functions and bit-error-rate analysis with almost p-ary sequences.

[D5] Yağmur Çakıroglu and Oğuz Yayla. A better lower bound on the family complexity of binary Legendre sequence. arXiv preprint arXiv:1812.06140, 2018.

[D6] Oğuz Yayla. Extended families of binary sequences with high family complexity and low cross correlation measure.

[D7] Fahrettin Yavuzyiğit and Oğuz Yayla. Attribute based signatures in blockchain.

[D8] Murat Cenk, Buse Taşcı and Oğuz Yayla. Secure digital identities via blockchain.