ABSTRACTS

The 2nd International Workshop on

Boolean Functions and their Applications (BFA)

July 3-8, 2017

Sosltrand, Hotel, Os, Norway.

Welcome to the BFA (Boolean Functions and their Applications) workshop 2017 which is held at Os, south of Bergen, Norway. The BFA workshop 2017 at Os is the second in a series of workshops on Boolean functions. The first BFA workshop took place at Rosendal, Norway, from September 2-7, 2014. It is hoped to eventually hold this workshop annually, providing an opportunity for specialists in Boolean functions to share current and ongoing research at picturesque locations within Norway. Each workshop is followed by a dedicated special issue, being the result of a fast reviewing process. For BFA 2017 the issue is scheduled to appear online by the end of 2018 and to be published by the beginning of 2019.

Lilya Budaghyan, Claude Carlet, Tor Helleseth

June 13, 2017

Part I

Abstracts for Invited Talks

Linear and Statistical Independence of Linear Approximations

Kaisa Nyberg

In this talk I will give a survey of independence assumptions in multiple linear cryptanalysis and present strategies how to satisfy them in practical applications. A useful link between linear and statistical independence can be found at http://eprint.iacr.org/2017/432 .

On APN permutations

Marco Calderini

Department of Mathematics, University of Trento, Italy

A Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called differentially δ-uniform if the equation $F(x+a)-F(x)=b$ has at most δ solutions for every nonzero element a of $\mathbb{F}_2^n$ and every b in $\mathbb{F}_2^m$.

In designing block ciphers, bijective Boolean functions defined over $\mathbb{F}_{2^n}$ are usually used as S-boxes. In particular, to thwart differential cryptanalysis we are interested in invertible Boolean functions whose differential uniformity is the smallest possible. Functions which are 2-uniform, also called almost perfect nonlinear (APN), have the smallest possible differential uniformity in the case $n = m$.

Moreover, for software implementation, we are interested in APN permutation defined on a field of even degree. However, up to now only one 6-bit function (up to equivalence) has been shown to be an APN permutation when the dimension is even.

In this talk, we shall attempt to give a survey of results concerning APN permutations. We will discuss properties of APN permutations and of their components. Furthermore, we will examine the open problem of constructing APN permutations in even dimension.

On S-Box Reverse-Engineering: from Cryptanalysis to the Big APN Problem

Léo Perrin*
perrin.leo at gmail.com

DTU Compute, Denmark

S-Boxes are small non-linear functions usually specified via their look-up table used as components by a vast number of cryptographic primitives. The design strategy used to build an S-Box is of crucial importance and is, as such, described by most algorithm designers. However, some designers (such as the NSA and the FSB) do not describe their design rationale and merely give the look-up table necessary to the implementation of their S-Box.

S-Box reverse-engineering is about recovering the design criteria and/or the structure used to build an S-Box given only its look-up table. In this talk, I will discuss recent results on this topic and their surprising application to the big APN problem.

First, it is possible to evaluate the probability that a random S-Box has certain differential or linear properties. If those of a given S-Box are too far from these expected ones, then it can be assumed that it was not picked uniformly at random. This analysis can be applied to the S-Box of the block cipher Skipjack.

Many S-Boxes are built like small block ciphers using e.g. a Feistel structure. Therefore, recovering such structure is equivalent to running a structural attack. I will briefly present two similar such attacks based on a bound on the algebraic degree of Feistel networks and Substitution-Permutation networks.

A powerful tool for decomposing S-Boxes with other structures is the *TU-decomposition*. By identifying linear spaces in the row and column indices of the zeroes in the LAT of an n-bit S-Box, it is possible to decompose it into the composition of two linear permutations and two $n/2$-bit block ciphers. This method can be applied to the S-Box used by the last two Russian standards in symmetric cryptography: the hash function Streebog and the block cipher Kuznyechik.

Surprisingly, the TU-decomposition can also be applied to the only known solution to the big APN problem. The 6-bit APN permutation found by Dillon turns out to have such a decomposition. We used it to generalize this permutation to higher dimensions and called the resulting functions *open butterflies*. We also leveraged the TU-decomposition to identify quadratic functions, called *closed butterflies*, which are CCZ-equivalent to said permutations. We showed that butterflies are, for certain parameters, always differentially 4-uniform. However, we unfortunately proved that no APN butterfly exists that operates on more than 6 bits.

*The content of this talk is based on joint papers with Alex Biryukov, Anne Canteaut, Sébastien Duval, Dmitry Khovratovich and Aleksei Udovenko.

On the possible exponents of APN power functions and their relation with Sidon sets and sum-free sets

Claude Carlet, LAGA, University of Paris 8
Work in common with S. Mesnager and S. Picek

A function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is called APN if, for every nonzero $a \in \mathbb{F}_{2^n}$ and every $b \in \mathbb{F}_{2^n}$, the equation $F(x) + F(x + a) = b$ has at most two solutions. Dobbertin proved that a power function $F(x) = x^d$ over $\mathbb{F}_{2^n}$ can be APN (we shall call such exponent d an APN exponent) only if $gcd(d, 2^n - 1)$ equals 1 if n is odd and 3 if n is even.

We prove more:

Definition *A subset of an additive group $(G, +)$ is called a* Sidon set *if it does not contain elements x, y, z, t, three of which are distinct and such that $x + y = z + t$.*

Definition *A subset S of an additive group $(G, +)$ is called a* sum-free set *if it does not contain elements x, y, z such that $x+y = z$ (i.e. if $S \cap (S+S) = \emptyset$).*

Theorem *For every positive integers n and d and for every integer i such that $0 \leq i \leq n-1$, let $e_i = gcd(d - 2^i, 2^n - 1)$ (viewed as a positive integer, even if $2^i > d$), and let G_{e_i} be the multiplicative subgroup*

$$G_{e_i} = \{x \in \mathbb{F}_{2^n}^*; x^{d-2^i} = 1\} = \{x \in \mathbb{F}_{2^n}^*; x^{e_i} = 1\}$$

of order e_i. If function $F(x) = x^d$ is APN over $\mathbb{F}_{2^n}$, then, for every $i = 0, \ldots, n-1$, G_{e_i} is a Sidon set in the additive group $(\mathbb{F}_{2^n}, +)$ and is also a sum-free set in this same group. Moreover, for every $i \neq j$, if $x \in G_{e_i}$, $y \in G_{e_j}$, $x \neq y$ and $x \neq y^{-1}$, then we have $(x + 1)^{d-2^i} \neq (y + 1)^{d-2^j}$.

We study then those multiplicative subgroups of $\mathbb{F}_{2^n}$ which are Sidon and sum-free and we study if the theorem above can simplify the search of new APN exponents (Canteaut checked that no one exists for $n \leq 26$ and Edel checked the same for $n \leq 34$ and $n = 36, 38, 40, 42$).

We also show a new connection between APN exponents and Dickson polynomials.

Symmetric Encryption Scheme Adapted to Fully Homomorphic Encryption Scheme: New Criteria for Boolean functions

Pierrick Meaux

Fully Homomorphic Encryption is a recent powerful cryptographic construction, which enables one to securely compute all functions on encrypted data, and decrypt the result of the function applied to the real data. This construction gives the possibility to securely delegate computation, which is a very important property with the increasing development of Cloud computing. Nevertheless, in current client-server frameworks, the client devices are too restricted to support pure FHE. In order to solve this problem, FHE has to be combined with primitives which incur small computation and communication cost: Symmetric Encryption schemes.

In this talk, we will present a symmetric encryption scheme created for this context: the FLIP family of stream ciphers. This construction has an unusual design: at each clock cycle, the key register is updated by a different, publicly known, wire-cross permutation and then filtered by a Boolean function to produce one key-stream bit. Therefore, the security of the scheme crucially depends on this Boolean function, which should be robust relatively to standard cryptographic criteria and new ones. This lead to study new criteria on Boolean functions, to determine the behavior of functions commonly used in cryptography and to build new functions with good parameters relatively to these criteria.

More precisely, we will talk about "low-cost" Boolean functions adapted to the FHE context; recurrent criteria on Boolean functions obtained by fixing some variables and Boolean criteria on restricted set of inputs.

The presentation will be based on the following works:

1. Maux, Journault, Standaert, Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. Eurocrypt 2016

2. Duval, Lallemand, Rotella. Cryptanalysis of the FLIP Family of Stream Ciphers. Crypto 2016

3. Carlet, Maux, Rotella. Boolean functions with restricted input and their robustness; application to the FLIP cipher. https://eprint.iacr.org/2017/097.pdf

Proving Resistance of a Block Cipher against Invariant Attacks

Anne Canteaut

Joint work with Christof Beierle, Gregor Leander and Yann Rotella

Many lightweight block ciphers apply a very simple key schedule in which the round keys only differ by addition of a round-specific constant. Generally, there is not much theory on how to choose appropriate constants. In fact, several of those schemes were recently broken using invariant attacks, i.e. invariant subspace or nonlinear invariant attacks. This work analyzes the resistance of such ciphers against invariant attacks and reveals the precise mathematical properties that render those attacks applicable. As a first practical consequence, we prove that some ciphers including Prince, Skinny-64 and Mantis7 are not vulnerable to invariant attacks. Also, we show that the invariant factors of the linear layer have a major impact on the resistance against those attacks. Most notably, if the number of invariant factors of the linear layer is small (e.g., if its minimal polynomial has a high degree), we can easily find round constants which guarantee the resistance to all types of invariant attacks, independently of the choice of the S-box layer. We also explain how to construct optimal round constants for a given, but arbitrary, linear layer.

(Generalized) Boolean functions: invariance under some groups of transformations and differential properties

Pante Stănică

Naval Postgraduate School
Department of Applied Mathematics
Monterey, CA 93943–5216, USA; pstanica@nps.edu

July 3-8, 2017

In this talk we will survey some properties of Boolean functions in binary and non-binary (output) characteristic: we concentrate on invariance under some group of transformations and differential properties of the generalized functions, often comparing the binary and non-binary case. Avalanche features, correlation immunity, bentness, etc., will be considered. Constructions, counts will be considered, and open problems will be proposed.

Rank metric codes and related structures

Yue Zhou
yue.zhou.ovgu@gmail.com

College of Science
National University of Defense Technology
Changsha, China

A rank metric code is just a subset of matrices over a (skew) field equipped with the rank metric. There are many interesting mathematical structures which can be interpreted as special types of rank metric codes. In particular, they include the following functions and associated structures which have important applications in cryptography and coding theory:

- Finite semifields or quadratic planar functions,
- Quadratic APN functions and their associated dimensional dual hyperovals,
- Quadratic vectorial bent functions and negabent functions.
- Maximum rank metric codes.

In this talk, I will first introduce some basic properties and the equivalence of rank metric codes. Then we turn to some attractive problems and results of several special types of rank metric codes, including the number of inequivalent maximum rank distance codes, the construction of quadratic vectorial bent-functions and the enumeration of quadratic bent-negabent functions.

Orthogonal group and Boolean functions

Patrick Solé
CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France , sole@enst.fr
(joint work with Minjia Shi and Lin Sok)

Abstract

In this talk, we study orthogonal group over finite fields. We show how to construct self-dual codes and linear complementary dual codes over large finite fields from the elements in the group and explore the connections with the generalized Z_{2^m} self-dual bent functions. We prove existence of optimal LCD codes of some certain lengths over large finite fields. We prove non-existence of the generalized Z_{2^m} regular bent functions in odd variables and classify them in low even variables.

Keywords: Orthogonal matrices, self-dual codes, complementary dual codes, optimal codes, Walsh Hadamard transform, self-dual bent functions, regular bent functions.

Generalized plateaued functions and admissible (plateaued) functions

Sihem Mesnager
Department of Mathematics, University of Paris VIII and Paris XIII LAGA, CNRS, France
(work in common with Chunming Tang and Yanfeng Qi)

Plateaued functions are very important cryptographic functions due to their various desirable cryptographic characteristics. We point out that plateaued functions are more general than bent functions (that is, functions with maximum nonlinearity).
P-ary plateaued functions have attracted recently some attention in the literature and many activities on generalized p-ary functions have been carried out. The aim of the talk is to increase our knowledge on plateaued functions in the general context of generalized p-ary functions. We firstly introduce two new versions of plateaued functions, which we shall call generalized plateaued functions and admissible plateaued functions. The generalized plateaued functions extend the standard notion of plateaued p-ary functions to those whose outputs are in the ring Z_{p^k}. Next, we study the generalized plateaued functions and use admissible plateaued functions to characterize the generalized plateaued functions by means of their components. Finally, we provide for the first time two constructions of generalized plateaued functions. In particular, we generalize a known secondary construction of binary generalized bent functions and derive constructions of binary generalized plateaued functions with different amplitude.

Some recent progress in the applications of Niho exponents

Nian Li

Niho exponent was originally introduced by Niho who investigated the cross-correlation between an m-sequence and its decimation in 1972. Since then, Niho exponents were further studied and had been used in other research topics. In this talk, we will introduce some research problems related to Niho exponents and present some recent developments.

On structural properties of the class of bent functions [1]

Natalia Tokareva

Maximally nonlinear Boolean functions in n variables, where n is even, are called *bent functions*. They form the special mysterious class, $\mathcal{B}_n$, studied from the early sixties in connection with cryptographic applications. Too many problems related to this class are still open. Constructions cover only separate parts of $\mathcal{B}_n$ while the core of it is still hidden from one's eyes.

In this talk we speak about the properties of $\mathcal{B}_n$ at whole considering it as the subset of the corresponding Boolean vector space. We discuss some metrical properties of $\mathcal{B}_n$, aspects related to isometrical mappings of $\mathcal{B}_n$, introduce some new results concerning the problem of decomposition of an arbitrary Boolean function of degree not more than $n/2$ into sum of two bent functions in n variables.

[1]Research was supported by RFBR (project 15-07-01328).

Duality of bent functions in odd characteristic

Alexander Pott

Bent functions defined in characteristic 2 have the property that the dual is, again, a bent function. This is, in general, not true any more in odd characteristic. In my talk, I will discuss recent progress and open problems regarding duality concepts of bent functions, in particular in odd characteristic. The talk is mainly based on papers written jointly with Wilfried Meidl and Ayça Çeşmelioğlu.

«Wavelets transformation and its applications in information security»

Levina Alla,
ITMO University,
Department of Secure Information Technologies,
levina@cit.ifmo.ru

Wavelet transformation has become well known and widely used in many fields of science. The basic concepts of wavelet theory can be found in the works of Daubechies. Many types of wavelets provide quick but very inaccurate compression. My researches based on implementation of wavelet theory in different areas of information security, one of such area is coding theory.

Error detecting codes are widely used for the protection in telecommunication channels, they ensure the reliability and security of devices from soft, hard errors and side channel attacks. The classical approach to providing noise immunity and integrity of information that is processed in computing devices and communication channels is to use linear codes. Linear codes have fast and efficient algorithms for encoding and decoding information, but these codes concentrate their detection and correction abilities in certain error configurations. Robust codes provide protection against any configuration of errors at predetermined probability. This is accomplished by the use of perfect nonlinear and almost perfect nonlinear functions to calculate code redundancy. I present the error-correcting coding scheme using biorthogonal wavelet transform. The wavelet transform is applied in various fields of science. Some wavelet applications clean signals from noise, compress data and execute spectral analysis of signal components. For developed constructions, was build a generator and check matrix that contain the scaling function coefficients of wavelet. Based on linear wavelet codes, was develop robust codes that provide uniform protection against all errors.

An other area of researches is implementation of wavelet theory in construction of Boolean Functions, spline-wavelet function was taken as a parameter of Boolean Function, this scheme can be very useful in the systems where wavelet transformation is already used.

On the periodic sequences with maximal nonlinear complexity

Zhimin Sun, Xiangyong Zeng, **Chunlei Li**, Tor Helleseth

May 10, 2017

Pseudo-random sequences are widely used in secure and reliable communications. In cryptographic applications, security characteristics like randomness and unpredictability of the sequences must be assessed. The linear complexity is henceforth used for assessing the cryptographic strength of binary sequences used in stream ciphers. A more general criterion used to test the randomness property of a sequence is its k-th order complexity. The k-th order complexity of a sequence is the length of the shortest shift register (FSR) with feedback functions having algebraic degree at most k that can generate this sequence. Removal of the restriction on the degree of feedback functions gives the notion of nonlinear complexity, also referred to as the maximum order complexity and the nonlinear span, of a sequence.

Whereas there is a considerable amount of literature on the linear complexity, far less work has been done on the kth-order complexity and the nonlinear complexity due to their intractability. Our recent work contributes to the theory of nonlinear complexity by conducting a comprehensive study of the periodic sequences with maximum nonlinear complexity.

In this talk we characterize the necessary conditions for periodic sequences over an arbitrary field to have the maximum possible nonlinear complexity and introduce a recursive approach to generate all maximum nonlinear complexity sequences. Furthermore, we will give the result of the randomness property of maximum nonlinear complexity sequences by investigating the enumeration and distribution, the balance property, nonlinear complexity of subsequences and the k-error nonlinear complexity of these sequences. It turns out that despite the optimal nonlinear complexity, these sequences do not possess satisfactory randomness property

Boolean functions in quantum computation

Ashley Montanaro

Quantum computers are machines which are designed to use quantum mechanics to solve certain problems more efficiently than any possible computer based only on the laws of classical physics. In this talk I will discuss two connections between the theory of boolean functions and the theory of quantum computation. First, I will describe how certain quantities occurring in the study of quantum circuits can be understood in terms of low-degree polynomials over F_2. Second, I will introduce a noncommutative generalisation of boolean functions which naturally appears when studying quantum algorithms. In each case many interesting, and still open, questions arise.

The talk will be based on two papers:

[1] Quantum circuits and low-degree polynomials over F_2, Journal of Physics A, vol. 50, no. 8, 084002, 2017; arXiv:1607.08473

[2] Quantum boolean functions (with Tobias Osborne), Chicago Journal of Theoretical Computer Science 2010; arXiv:0810.2435

Boolean functions in a Message-Passing, Quantum, and Machine Learning Context

Matthew G. Parker

June 2, 2017

Quadratic Boolean functions have a straightforward mapping to simple graphs and to F_4-additive codes. Such graphs can be used to realise message-passing algorithms for F_4-additive codes. Such structures also model quantum error-correcting codes and quantum contextuality scenarios. It is of further interest to explore such structures in the context of machine learning overlaid with quantum entanglement. This talk will explore these issues.

Part II

Abstracts for Contributed Talks

On the S-boxes Generated via Cellular Automata Rules

Stjepan Picek

In this paper we investigate cellular automata (CA) rules that are used to describe S-boxes with good cryptographic properties. Up to now, CA have been used in several ciphers to define an S-box, but in all those ciphers, the same CA rule is used. This CA rule is known best as the one defining the Keccak transformation. Since there exists no straightforward method for constructing CA rules that define S-boxes of arbitrary size and with good cryptographic properties, we use a special kind of heuristics for that Genetic Programming. Although it is not possible to theoretically prove the efficiency of such a method, our experimental results show that heuristics are able to find a large number of CA rules that define good S-boxes in a relatively easy way. Particularly interesting is the internal encoding of the solutions in the considered heuristics using combinatorial circuits; this makes it easy to approximate a priori the S-box implementation properties like circuit latency (the number of combinatorial gates between input and output) and area (the number of gates). Indeed, when using heuristics of genetic programming type where the obtained solutions are expressed in the tree form, one can easily estimate the latency by just observing the tree depth. Next, we discuss the number of S-boxes obtainable by using only one cellular automata rule and the possible gains from using the switching technique. For the 4 4 size, we explore how many classes and which ones (out of 16 optimal classes) can be obtained with CA rules. In order to do so, we run an exhaustive search since with a single CA rule the search space size equals only 2 16. Subsequently, for the 5 5 size we again conduct an exhaustive search and investigate which AB power functions can be obtained with CA rules. On the other hand, since for 66 and 77 sizes the exhaustive search is not possible, we run heuristics in order to estimate which AB/APN power functions can be constructed. On the basis of those results, we discuss the notion of equivalence and whether CA rules are preserved under various types of affine transformations. We discuss the difference between the global and local CA rules with a special emphasis on a Keccak type rule which results in bijections only for odd dimensions. Moreover, with the increase in the number of variables of an (n, m)- function we can easily see that a number of cryptographic properties degrade if one uses the Keccak rule. For instance, when used in 3 3 S-boxes, both the nonlinearity and differential uniformity equal 2, which is optimal, but if used in 7 7 S-boxes, both of those properties would have a value equal to 32, which is far from optimal. Finally, we investigate what is the necessary number of inputs that needs to be involved in a CA rule in order to obtain optimal values for nonlinearity and differential uniformity.

On APN functions EA-equivalent to permutations

Valeriya Idrisova*

*Sobolev Institute of Mathematics and Novosibirsk State University, Akademgorodok, Novosibirsk, Russia

Abstract

The appearance of the differential cryptanalysis in 1990 made it necessary to search a means to resist this method: the notions of an APN function and a differentially δ-uniform function were proposed by K. Nyberg [2]. A vectorial function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ is called an *APN function* if, for every nonzero a and every b in $\mathbb{F}_2^n$, the equation $F(x) + F(x + a) = b$ has at most two solutions. It is also known that APN functions were investigated starting from 1968 by V. Bashev and B. Egorov in USSR.

One of the most interesting problems in this area is constructing bijective APN functions in even dimensions. There was a conjecture that such functions do not exist, but in 2009 J.F.Dillon et al. [1] presented the first APN permutation for $n = 6$. This permutation was constructed using non-bijective CCZ-equivalent APN function. In this work we investigate special functions EA-equivalent to permutations. More precisely, we consider 2-to-1 APN functions F such that $F + L$ is a permutation for some linear functions L.

Consider the set of all 2-to-1 vectorial Boolean functions. It is easy to prove that for each 2-to-1 function G there exist a function A such that $G + A$ is a permutation and every coordinate Boolean function of A is balanced. This gives an idea that amongst these functions A there can be linear functions since they have balanced coordinate functions. The goal of this work is to find a method how to construct 2-to-1 APN function and search through linear functions L to obtain APN permutations.

An arbitrary 2-to-1 APN function F is 2-to-1 vectorial Boolean function such that all its derivatives $D_a(F)$ are 2-to-1 functions for every nonzero vector a from $\mathbb{F}_2^n$. So, if we consider the vector of values as some sequence of variables $\{\alpha, \beta, \gamma, \epsilon, ...\}$ where each variable occurs twice, we obtain the set of restrictions on this sequence for every nonzero a. For example, if $n = 3$ the sequence of values $\alpha, \alpha, \beta, \gamma, \beta, \epsilon, \gamma, \epsilon$ satisfies all the restrictions, but the sequence $\alpha, \beta, \beta, \alpha, \gamma, \epsilon, \gamma, \epsilon$ does not, since for $a = 010$ and for any values of α and β holds: $F(000) + F(010) = F(001) + F(011) = \alpha + \beta$.

This gives us an algorithm of generating all possible sequences of variables satisfying all the restrictions for every n. The next stage of the method is to assign obtained sequences with some vectors from $\mathbb{F}_2^n$ such that the result still satisfies APN property. In particular, for $n = 3$ is sufficient to use any subset of $\mathbb{F}_2^n$ that is free from any linear subspace of dimension 2.

We found various 2-to-1 APN functions for $n = 3, 5, 6$ such that their sum with some linear functions gives APN permutation. The examples of such function can be found below.

Table 1. An example of 2-to-1 function that gives an APN permutation of $\mathbb{F}_2^5$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F(x)$	0	23	5	21	12	31	0	14	8	17	5	7	17	9	26	7
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$F(x)$	12	15	21	15	8	28	27	9	28	27	22	26	23	22	31	14

Table 2. An example of 2-to-1 function that gives the APN permutation of $\mathbb{F}_2^6$ (Dillon et al.)

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F(x)$	54	52	48	57	14	39	34	0	63	45	45	0	2	33	32	28
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$F(x)$	55	1	6	46	5	46	28	8	37	57	5	19	2	25	48	32
x	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$F(x)$	17	54	58	58	33	1	34	14	51	21	8	29	55	12	30	29
x	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$F(x)$	27	19	21	37	17	40	63	52	40	27	51	12	6	30	39	25

References

[1] Browning K. A., Dillon J. F., McQuistan M. T., Wolfe A. J. An APN permutation in dimension six. (Proc. of the 9th International Conference on Finite Fields and Applications, Dublin, Ireland, July 2009)// Contemporary Mathematics. — 2010. — Vol. 518. — P. 33-42.

[2] Nyberg K. Differentially uniform mappings for cryptography. On almost perfect nonlinear permutations (Proc. of Eurocrypt' 93, Norway, May, 1993) // Lecture Notes in Computer Science. — 1994. — V.765. — P. 55–64.

Investigating the CCZ-Equivalence between Functions with Low Differential Uniformity by Projected Differential Spectrum

Xi Chen, Longjiang Qu and Chao Li

Abstract

Recently, many new constructions of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ were presented. The most famous class was constructed by switching neighbours of the inverse function in the narrow sense. We call them 4-uniform BI permutations for short since they can be regarded as adding a properly chosen Boolean function to the inverse function. C. Carlet et al. presented another construction of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ (4-uniform BCTTL permutations for short), which used the APN property of the inverse function on $\mathbb{F}_{2^{2k-1}}$ [1]. Very recently, J. Peng et al. generalized the switching method and presented a method to construct new differentially 4-uniform permutations from known one by determining the corresponding cycle sets [3]. For simplicity, we call them *PTW differentially 4-uniform permutations*. The size of all aforementioned three classes of differentially 4-uniform permutations grows doubly exponentially when k grows. At Crypto'16, L. Perrin et al. introduced a structure named butterfly, which leads to permutations over $\mathbb{F}_{2^{2k}}$ with differential uniformity at most 4 when k is odd.

It is well known that many cryptographic criteria, such as differential uniformity, nonlinearity, etc, of CCZ-equivalent functions are the same. To prove the CCZ-inequivalence between two functions is mathematically (and also computationally) difficult, unless one can verify that some of their CCZ-equivalent invariants are different. Due to the big cardinality of the aforementioned three classes of differentially 4-uniform permutations, it seems to be quite difficult to prove or to check the CCZ-equivalence between them even for small fields. Very recently, X. Chen et al., introduced a new notion called R-projected differential spectrum to investigate the CCZ-equivalence between functions with low differential uniformity [2].

In this paper, we study the CCZ-equivalence between PTW differentially 4-uniform permutations and other known differentially 4-uniform permutations by selecting different R-projections from [2]. We first introduce an interesting property on PTW differentially 4-uniform permutations. Using this property, we present a necessary condition to check whether a sporadic differentially 4-uniform permutation on small fields is CCZ-inequivalent to any PTW differentially 4-uniform permutations by considering R-projected differential spectrum. As an application, we verified by Magma that any differentially 4-uniform permutations mentioned by L. Perrin et al. [4] with generalised butterfly structure on $\mathbb{F}_{2^6}$ is CCZ-inequivalent to any 4-uniform BI permutations, 4-uniform BCTTL permutations or PTW differentially 4-uniform permutations. By considering the projected differential spectrum on $\mathbb{F}_2^{4k-2}$, we prove a necessary condition and verify that any 4-uniform BCTTL permutations is CCZ-inequivalent to any PTW differentially 4-uniform permutations when $3 \leq k \leq 7$ by Magma.

REFERENCES

[1] C. Carlet, D. Tang, X.H. Tang and Q.Y. Liao, New Construction of Differentially 4-Uniform Bijections. Information Security and Cryptology, Vol. 8567, pp. 22-38, 2014.

[2] X. Chen, L.J. Qu, C. Li and J. Du, A New Method to Investigate the CCZ-Equivalence between Functions with Low Differential Uniformity. Finite Fields and their Applications. Vol. 42, pp. 165-186, 2016.

[3] J. Peng, C. Tan and Q.C. Wang, New secondary construction of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$. International Journal of Computer Mathematics, to appear, DOI: 10.1080/00207160.2016.1227433.

[4] L. Perrin, A. Udovenko, and A. Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. Advances in Cryptology - CRYPTO 2016, Part II, volume 9815 of LNCS, pages 93-122. Springer, 2016.

On Some Properties of Quadratic APN Functions of a Special Form

Irene Villa

University of Bergen
Bergen, Norway
Irene.Villa@uib.no

Abstract

In a recent paper it is shown that functions of the form $L_1(x^3)+L_2(x^9)$, where L_1 and L_2 are linear, are a good source for the construction of new infinite families of Almost Perfect Nonlinear (APN) functions. In the present work we study necessary and sufficient conditions for such functions to be APN and we give some computational results on low dimension cases.

Quadratic APN Polynomials in Few Terms in Small Dimensions

Bo Sun
University of Bergen
Bergen, Norway
Bo.Sun@uib.no

Abstract

We consider quadratic APN polynomials over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$ for $n \leqslant 11$. We computationally determine all such polynomials (up to CCZ-equivalence) containing up to 6 terms. In particular, obtained results are summerized in the table below. These results are from a joint work with Lilya Budaghyan.

Table 1.
Quadratic APN functions over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$ ($6 \leq n \leq 11$)

n	Number of Terms	Number of Polynomials of Type I [*]	Number of Polynomials Type II[**]
6	3-6	–	–
7	3	2	2
	4	6	5
	5	10	4
	6	12	1
8	3	2	2
	4	–	–
	5	4	2
	6	3	1
9,10	3-6	–	–
11	3	–	–
	4	–	–
	5	5	5
	6	–	–

[*]This is a number of APN polynomials (up to CCZ-equivalence) which are not CCZ-equivalent to power functions.
[**]This is a number of APN polynomials (up to CCZ-equivalence) which are not CCZ-equivalent to APN polynomials in fewer terms with coefficients in $\mathbb{F}_2$.

New classes of generalized bent functions

Bimal Mandal, Pantelimon Stănică and Sugata Gangopadhyay
{bimalmandal90, gsugata}@gmail.com, pstanica@nps.edu

Abstract

In 1985, Kumar et al. introduced the concept of generalized bent functions $f : \mathbb{Z}_q^n \longrightarrow \mathbb{Z}_q$, where $q > 1$ is a positive integer and gave constructions for every possible q and n, except for n is odd and $q \equiv 2 \pmod 4$. There has been a flourish of new research into this area, with new constructions being displayed, characterizations, and even connecting them to certain combinatorial objects such as partial difference sets, strongly regular graphs and association schemes. We consider the generalized Boolean functions from $\mathbb{F}_p^{2n}$ to $\mathbb{F}_p$, where p is an odd prime integer, and the set of all n variables generalized Boolean function is denoted by $\mathcal{B}_n^p$. The main contribution of our work can be summarized as follows:

In the first part, we define the subspace sum of $f \in \mathcal{B}_n^p$ with respect to a subspace V of $\mathbb{F}_p^n$

$$\mathcal{S}_V f(x) = \sum_{s \in V} f(x+s) \text{ for all } x \in \mathbb{F}_p^n.$$

Let $V = \langle a \rangle$ be an one dimensional subspace of $\mathbb{F}_p^n$. Then we prove that

$$\mathcal{S}_V f(x) = \underbrace{D_a D_a \dots D_a}_{(p-1)-\text{times}} f(x), \text{ for all } x \in \mathbb{F}_p^n.$$

It is proved that if $f, h \in \mathcal{B}_n^p$ are affine equivalent, then so are $\mathcal{S}_V f$ and $\mathcal{S}_V h$, where V is a subspace of $\mathbb{F}_p^n$. Further, we extend to characteristic $p > 2$ a binary result of Dillon, concerning the vanishing subspace sum of any Maiorana–McFarland bent functions.

For the binary case, Carlet constructed two new classes of bent function by modifying the Maiorana-McFarland bent function. In the second part, we construct two new classes of generalized bent functions, is denoted by $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$. Here $\mathcal{D}_0^p$ is a subclass of $\mathcal{D}^p$ and we observe that if $f \in \mathcal{D}_0^p$ is an n variables Boolean function, then $n \equiv 0 \pmod 4$. We prove that $\mathcal{M}^p$ and $\mathcal{D}_0^p \subseteq \mathcal{D}^p$ are overlapping classes, but in general not included in one another, which is not the case for the binary instance, where $\mathcal{M} \subsetneq \mathcal{D}_0$.

For construction of $\mathcal{C}^p$ bent functions, it is needed to consider a permutation polynomial π on $\mathbb{F}_p^n$ such that $\pi^{-1}(a+L)$ is a flat for any $a \in \mathbb{F}_p^n$, where L is a linear subspace of $\mathbb{F}_p^n$. We investigate these conditions for many classes of permutations and suitable linear subspaces of the dimension less than and equal to 2 for $p = 3$.

Generalized bent functions from spreads and their spectra

Wilfried Meidl, Alexander Pott
Otto von Guericke Universiät Magdeburg

Let p be a prime, and let $\zeta_q = e^{\frac{2\pi i}{q}}$. For $a \in \mathbb{Z}_{p^m}$, $u \in \mathbb{F}_p^n$, denote by $\chi_{a,u}(x,y) = \zeta_{p^m}^{ay}\zeta_p^{u\cdot x}$ the characters of the group $\mathbb{F}_p^n \times \mathbb{Z}_{p^m}$ ($u \cdot x$ denotes the conventional dot product). A function f from $\mathbb{F}_p^n$ to the cyclic group $\mathbb{Z}_{p^m}$ is called bent if the character sum

$$\mathcal{H}_f(a,u) = \sum_{x\in\mathbb{F}_p^n} \chi_{a,u}(x,f(x)) = \sum_{x\in\mathbb{F}_p^n} \zeta_{p^m}^{af(x)}\zeta_p^{u\cdot x} \tag{1}$$

has absolute value $p^{n/2}$ for every nonzero $a \in \mathbb{Z}_{p^m}$, and every $u \in \mathbb{F}_p^n$. The graph $(x, f(x))$ of f is a relative difference set in $\mathbb{F}_p^n \times \mathbb{Z}_{p^m}$ with parameters (p^n, p^m, p^n, p^{n-m}) and forbidden subgroup $\mathbb{Z}_{p^m}$. Standard examples of such difference sets are obtained from spreads for every $m \le n/2$.

Recently for the case of $p = 2$, a class of functions that satisfies weaker conditions attracted a lot of attention: Requiring that $|\mathcal{H}_f(a,u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$, but only for $a = 1$ (and hence for all odd a, i.e. exactly for the characters of order 2^{m-1}), yields the so called generalized bent (gbent) functions, which turned out to be essentially a partition of $\mathbb{F}_2^n$ depending on a Boolean bent function.

Though gbent functions are not relative difference set, they inherit some interesting properties. For instance, when n is even, one can see a gbent function written as $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{m-2}a_{m-2}(x) + 2^{m-1}a_{m-1}(x)$ for uniquely determined Boolean functions a_i, as an affine space of bent functions $a_{m-1} + \langle a_0, \ldots, a_{m-2}\rangle$ of dimension $m-1$ with interesting additional properties (if the dimension is smaller, then the function reduces to a function from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^{m'}}$ for some $m' < m$).

In this talk we analyze the construction of gbent functions from (partial) spreads for $p = 2$, which extends some earlier results, and generalize these results to gbent functions from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^m}$ for odd primes p, which are defined in an analog way. We show that there is a large amount of generalized bent functions in dimension $n/2$, the largest dimension that permits relative difference sets, which do not come from bent functions (i.e. from relative difference sets). Even more, using spreads, for any subset $B \subset \{m-1, \ldots, 2\}$ we design functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^m}$ for which $|\sum_{x\in\mathbb{F}_2^n} \chi_{a,u}(x,f(x))| = 2^{n/2}$ for all characters $\chi_{a,u}$ of order 2^t, $t \in B$. For instance, there exist gbent funtions from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^{n/2}}$ (with dimension $n/2$) for which $|\mathcal{H}_f(a,u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$ and $a \in \mathbb{Z}_{2^m}$ except from $a = 2^{n/2-2}, 3\cdot 2^{n/2-2}$. From the character values point of view, such functions can be seen as those gbent functions that are as close as possible to a bent function (without being bent).

Efficient Numerical Approximation of the DMC Channel Capacity

Y. Lu, Z. Tu, D. Zhang

Abstract

This submission work is part of an interdisciplinary project "Walsh Spectrum Analysis and the Cryptographic Applications". The project initiates the study of finding the largest (and/or significantly large) Walsh coefficients and the index positions of an unknown distribution by sampling. This proposed problem is considered suitable for submission to the Nature journal, because it has greatest significance in Cryptography, Communications, Computer science, and Signal Processing and both scientific and engineering communities are believed to benefit from it.

For a few Discrete Memoryless Channels (DMCs) it is known that the capacity can be computed analytically; in general, there is no closed-form solution. This work is concerned with numerical computation of channel capacity for a general DMC. We study both the Blahut-Arimoto algorithm (which gave the first numerical solution historically) and the most recent results [Sutter et al'2014]. For an ϵ-approximation (i.e., the desired absolute accuracy of the approximate solution) of the capacity, the former has the computational complexity $O(MN^2 \log N/\epsilon)$, while the latter has the complexity $O(M^2 N\sqrt{\log N}/\epsilon)$. We will give an efficient algorithm to compute numerically the channel capacity and implement it. Meanwhile, we will study the relation of Renyi's divergence of degree 1/2 and the generalized channel capacity of degree 1/2.

On the Multiplicative Complexity of 6-variable Boolean Functions

Çağdaş Çalık, Meltem Sönmez Turan, René Peralta

National Institute of Standards and Technology, Gaithersburg, MD, USA
{cagdas.calik, meltem.turan, rene.peralta}@nist.gov

Abstract. Multiplicative complexity $C_\wedge(f)$ of a Boolean function is the minimum number of multiplications (AND-$\wedge$ gates) that are sufficient to evaluate the function over the basis (AND, XOR, NOT). Finding the multiplicative complexity of a given function is computationally intractable, even for functions with small number of inputs. Turan et al. [1] showed that n-variable Boolean functions can be implemented with at most $n-1$ AND gates for $n \leq 5$ by utilizing affine equivalence classes. A simple counting argument can be used to show that, for $n \geq 7$, there exists n-variable functions with multiplicative complexity n. However, nobody has yet been able to show that any particular function has this complexity. For $n = 6$, the question remains open.

In this work, we study the multiplicative complexity of 6-variable Boolean functions. The problem of finding the multiplicative complexities of all functions is reduced to finding the multiplicative complexities of 150 357 affine equivalence classes on 6-variables constructed in [2]. The multiplicative complexity of each class is determined by generating all possible circuits for a particular number of AND gates and then identifying which of the classes can be generated by those circuits.

We provide the multiplicative complexity distribution of 6-variable Boolean functions and show that they can be implemented using at most 6 AND gates. Our techniques also enable us to exhibit specific 6-variable functions which have multiplicative complexity 6.

Keywords: Affine equivalence, Boolean functions, Multiplicative complexity

References

1. Meltem Sönmez Turan and René Peralta. The multiplicative complexity of boolean functions on four and five variables. In Thomas Eisenbarth and Erdinç Öztürk, editors, *Lightweight Cryptography for Security and Privacy - Third International Workshop, LightSec 2014, Istanbul, Turkey, September 1-2, 2014, Revised Selected Papers*, volume 8898 of *Lecture Notes in Computer Science*, pages 21–33. Springer, 2014.
2. Joanne Elizabeth Fuller. *Analysis of affine equivalent boolean functions for cryptography.* PhD thesis, Queensland University of Technology, 2003.

Solving polynomial systems over Boolean rings by elimination of variables

Bjørn Møller Greve[1], Håvard Raddum[2] Gunnar Fløystad[3] and Øyvind Ytrehus[2].

[1] Norwegian Defence Research Establishment (FFI),[2] Simula@UiB and[3] Department of Mathematics, University of Bergen Norway
bjorn-moller.greve@ffi.no, haavardr@simula.no, gunnar.floystad@uib.no, oyvindy@simula.no

We present a new algorithm for eliminating variables from a system of Boolean equations of low degree, while bounding the degree of the resulting polynomials. Our motivation comes from symmetric cryptography, where ciphers can be described as systems of Boolean equations of degree 2 over $GF(2)$. Assume that the plaintext P and the ciphertext C are known, and that the goal is to find the secret key K. Our aim is to find a method to extract the secret key K by solving the equation system produced by the encryption $E_K(P) = C$. In addition to the bits of the unknown K, auxiliary variables need to be introduced to keep the initial equations simple. We attempt to eliminate the auxiliary variables from the set of equations, resulting in some equations containing only variables from K.

The algorithm combines in a novel fashion elements of previously known elimination algorithms, namely the traditional theory of resultants and the theory of Gröbner bases. It is general since it treats any system of quadratic Boolean functions as input and is developed with a focus on bounding the complexity.

For input systems of quadratic and/or cubic Boolean equations, the elimination will never produce polynomials with higher degree than 3. The algorithm's input then consists of two sets F and G of Boolean equations of degree 3 and 2, respectively. In the *resultant and coefficient constraint step* of the algorithm, all monomials containing a particular variable are eliminated, not just single monomials like in the traditional Gröbner basis algorithms. The *hybrid step* of the algorithm removes monomials from the cubic polynomials using the quadratic polynomials as a basis by normalization. This provides a large set of monomials that cannot appear in the cubic sets in the end, and it may squeeze out quadratic polynomials enlarging the elimination sets. We also discuss ways to use the equations that the algorithm produces.

The penalty for lowering the complexity of variable elimination is expansion of the total solution space, which means that the algorithm produces false solutions. Therefore we also present an algorithm for lifting candidate solutions backwards to filter out false solutions to the system. The expansion of the solution space results in a trade-off between complexity and information loss, and we measure this loss during elimination. This approach has the potential to measure the strength of block ciphers.

We apply the algorithm to two small-scale block ciphers. In one case we fail to produce equations of degree only in variables of K, but instead measure how fast information about K is lost during elimination. In the other case we are able to construct such polynomials, and show that the method of re-linearization would break this cipher faster than exhaustive search.

PI is not at least as succinct as MODS

Nikolay Stoyanov Kaleyski

Department of Informatics, University of Bergen, Norway

Given two languages L_1 and L_2 of Boolean sentences, we say that L_1 is at least as succinct as L_2 if there exists a polynomial p such that for every sentence S_2 in L_2 there exists an equivalent sentence S_1 in L_1 with $|S_1| \leq p(|S_2|)$, i.e. whose size is polynomial in the size of S_2 with respect to p.

We show that the language of prime implicates (PI) is not at least as succinct as the language of models (MODS) by constructing a sequence of Boolean functions with "many" prime implicates and "few" models which serves as a counterexample. We prove a lower bound on the number of prime implicates of these functions, and describe how an upper bound and even an exact formula for their number of prime implicates may be derived as well.

On Alltop functions

Fuad Hamidli[1] and Ferruh Özbudak[1,2]

[1] Institute of Applied Mathematics, Middle East Technical University, Turkey
[2] Department of Mathematics, Middle East Technical University, Turkey
fuad_hamidli@yahoo.com,ozbudak@metu.edu.tr

1 Abstract

Let q be a power of an odd prime p and let $\mathbb{F}_q$ be a finite field. A map f is called *planar* on $\mathbb{F}_q$ if for any $a \in \mathbb{F}_q^\star$, the difference map (or derivative of f at a point a) $D_a(x) = f(x+a) - f(x)$ is bijective. The definition of *Alltop function* is that, the difference map at point a in the given field of odd characteristic is itself planar for any $a \in \mathbb{F}_q^\star$. Alltop functions have special importance in cryptography and related areas. For example, they are used to construct mutually unbiased bases (MUB) in quantum information theory. The map $x \mapsto x^3$ is an Alltop function in all finite fields found by Alltop in 1980 which is an optimal function with respect to the known bounds on auto and crosscorrelation. Since then it was shown that these kind of functions do not exist when $p = 3$ (Hall, Rao, Donovan). So far, it has been found that x^{q+2} is also an Alltop function over finite field $\mathbb{F}_{q^2}$ where 3 does not divide $q+1$ and this is EA-inequivalent to x^3 whereas its difference function (derivative), which is planar, is EA-equivalent to x^2 (Hall, Rao, Gagola). It is still an open problem whether there exist another EA-inequivalent Alltop functions or any method to construct new Alltop functions.
In this paper classification of all q-cubic Alltop binomials over $\mathbb{F}_{q^2}$ is given. Specifically, $x^3 + ux^{q+2}$ and $x^3 + ux^{2q+1}$ in $\mathbb{F}_{q^2}$ for $u \in \mathbb{F}_{q^2}^*$ are analyzed and for the former case it is shown that it cannot be Alltop, for the latter case permutation polynomials $L_1(x) = ax + bx^q$ and $L_2(x) = cx + dx^q$ are found that satisfy $L_1 \circ x^3 \circ L_2 = x^3 + ux^{2q+1}$ and $L_1 \circ x^{q+2} \circ L_2 = x^3 + ux^{2q+1}$ for suitable values of u. Moreover, except x^3 and the ones in its equivalence class, it is shown that there is no Alltop cubic q-monomials in $\mathbb{F}_{q^3}$. In addition, new notion "p-ary Alltop functions" are defined from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ and the relation between Alltop functions and p-ary Alltop functions over finite fields is given. Furthermore, by using Maiorana-McFarland construction approach for p-ary bent functions, construction method for p-ary Alltop functions from p-ary bent functions is established.

Keywords: Alltop functions, planar functions, p-ary bent functions

Low-Depth, Low-Size Circuits for Cryptographic Applications

Joan Boyar* Magnus Gausdal Find† René Peralta†

Determining the circuit complexity of a Boolean function is a highly intractable problem. In fact, it is known to be inapproximable even when restricted to linear functions. Here, we report on new techniques for reducing the size and depth of circuits over the basis XOR, AND, NOT (equivalently, arithmetic circuits over $GF(2)$). The techniques have yielded new records for the circuit complexity of Boolean functions of interest to cryptography and coding theory. These include multiplication over $GF(2)$, finite field multiplication, and finite field inversion.

Circuits with few AND gates will naturally have large sections which are purely linear, i.e., contain no AND gates. The size of linear components can be significantly reduced using various heuristics. Boyar and Peralta [1] and Courtois et al. [2] have used this insight to construct circuits much smaller than previously known for a variety of applications. The heuristic both of those papers use is a two-step process which first reduces multiplicative complexity and then optimizes linear components. We present a new heuristic that allows us to simultaneously reduce depth and size of linear circuits.

Our overall approach uses the observation that one can obtain smaller low-depth circuits by repeatedly optimizing the different linear components of the circuit based on gate-depth information from previous optimizations. We call the resulting heuristic the *See-Saw Method*. The heuristic builds a circuit by repeatedly picking a new pair of wires to XOR. As in Paar's algorithm [3] the target functions, as well as already computed functions, are encoded into a Boolean matrix. However, by keeping track of depth information we are able to avoid XORing gates when doing so would increase the depth beyond precomputed limits. Additionally, a Generalized Paar Operation is introduced which allows cancellation (an XOR operation where at least one variable is present in the linear combinations expressing both inputs to the XOR and thus not in the output). We have elsewhere shown that any heuristic which does not allow cancellation (such as Paar's) will do significantly worse than one that does.

We report new records for size and depth of circuits for the AES S-Box, multiplication in the field $GF(2^8)$, inversion in the field $GF(2^{16})$, and multiplication of polynomials over $GF(2)$.

References

[1] J. Boyar, P. Matthews, and R. Peralta. Logic minimization techniques with applications to cryptology. *J. of Cryptology*, 26(2):280–312, 2013.

[2] N. Courtois, D. Hulme, and T. Mourouzis. Solving circuit optimisation problems in cryptography and cryptanalysis. *IACR Cryptology ePrint Archive*, 2011:475, 2011. Appears in electronic proceedings of 2nd IMA Conference Mathematics in Defense, UK, Swindon, 2011, www.ima.org.uk/_db/_documents/Courtois.pdf.

[3] C. Paar. Optimized arithmetic for Reed-Solomon encoders. In *1997 IEEE International Symposium on Information Theory*, page 250, 1997.

*Dept. of Math. and Comp. Sci., University of Southern Denmark. Partially supported by the Danish Council for Independent Research, Natural Sciences.

†Information Technology Laboratory, NIST

Separable Statistics and Multivariate Linear Cryptanalysis

Stian Fauskanger[1] and Igor Semaev[2]

[1] Norwegian Defence Research Establishment (FFI), PB 25, 2027 Kjeller, Norway
[2] Department of Informatics, University of Bergen, Bergen, Norway

A new extension to linear cryptanalysis is developed here. It is a statistical attack based on a priori computed joint distributions of the encryption algorithm internal bits. We have applied the method to DES, but it should work for other block ciphers as well. Let X_{i-1}, X_i be two 32-bit input-blocks to the i-th encryption round in DES. X_0, X_1 is plain-text and X_{17}, X_{16} is cipher-text 64-bit blocks. We find probability distribution of the 14-bit vector of internal bits, x:

$$x = (X_2[24, 18, 7, 29], X_{15}[16, 15, 14, 13, 12, 11], X_{16}[24, 18, 7, 29]) \ . \tag{1}$$

The exact distribution is hard to compute as it depends on the 56-bit DES key. Under certain statistical assumptions, similar to those used by Matsui in his linear cryptanalysis, a close approximation is found. The approximated distribution of x depends on 7 key-bits. The observation on x depends on plaintext-ciphertext pairs and 39 key-bits from the first and the last round keys. We use the distribution of x in a known-plaintext attack given n plaintext-ciphertext pairs. Logarithmic Likelihood Ratio (LLR) statistic f depends on 45 different key-bits k, besides plaintext-ciphertext pairs, so multivariate linear cryptanalysis of Hermelin et al. won't give any advantage over one-variate linear cryptanalysis. In this case there should be 2^{45} values of the statistic f to range. Therefore, we instead use 10-bit projections of (1):

$$x_{i,j} = (X_2[24, 18, 7, 29], X_{15}[i, j], X_{16}[24, 18, 7, 29]) \tag{2}$$

for $i, j \in \{16, 15, 14, 13, 12, 11\}$, where $i > j$ except $i, j = 16, 11$ for which (2) is uniformly distributed. There are 14 choices of i, j. LLR statistic $f_{i,j}$ for each $x_{i,j}$ depends on 21 different key-bits denoted by $k_{i,j}$. We range the values of $k_{i,j}$ for each i, j separately by the value of $f_{i,j}$. We then combine the values of $k_{i,j}$ to the value of k such that

$$F = \sum_{i,j} c_{ij} f_{i,j} > z \tag{3}$$

for some optimal constants $c_{i,j}$ and threshold z. The main idea of this new approach is to use the separable statistic F instead of LLR statistic f based on the distribution of x. The statistics $f_{i,j}$ are dependent. Nevertheless, as $f_{i,j}$ come from the same (1), we were able to compute the distribution of F in two cases: the value of k is correct and it is incorrect. That enables to evaluate the probability of not missing the correct value of k (success probability) and average number of false candidates for k. All k-candidate are then brute-forced. By symmetry in DES,

$$x' = (X_1[24, 18, 7, 29], X_2[16, 15, 14, 13, 12, 11], X_{15}[24, 18, 7, 29])$$

is similarly distributed as x. As x and x' incorporate different internal bits of the encryption, they are considered independent. So we have two independent identically distributed separable statistics F and F' which involve 28 LLR statistics for 10-bit projections of x and x'. They depend on 54 key-bits combined.

We built a search tree from the LLR values by a gluing type algorithm that goes through the tree to find candidates for 54 out of the 56 key-bits. A 54-bit key candidate is accepted if $F > z$ and $F' > z$ simultaneously. This is brute forced to find the 56-bit DES key.

The complexity of our attack is measured by n (the number of plaintext-ciphertext pairs), the number of nodes visited while traversing the tree, and the number of encryptions to brute force the remaining 2 key-bits for all candidates. For fixed n, we choose the parameter z so that the number of candidates returned from our algorithm is $n/4$. Then n encryptions were performed. Particularly, we fixed $n = 2^{41.8}$ and chose z so that $2^{39.8}$ candidates are expected. The number of encryptions is $2^{41.8}$. The success probability of the attack is the probability that $F > z$ and $F' > z$ for the correct key simultaneously. The success probability is 0.85 (computed theoretically) for our choice of n and z.

We have implemented the method and run an attack on 16-round DES without the final brute force step. The algorithm returned $2^{39.46}$ candidates and the number of visited nodes in the search tree was $2^{45.78}$. The average complexity of visiting one node is 15 bit-xors and 12 small integer additions to compute (3) for F and F' combined. The complexity of doing one DES encryption is 1280 bit-xors. So final complexity of our attack is close to the complexity of $2^{41.8}$ DES encryptions. The goal is to have the final complexity to be less than $2^{41.8}$ encryptions. There is a way to reduce the number of visited nodes. This work is ongoing.