Finite Field Functions to Counterattack Linear and Differential Cryptanalysis

Daniel Panario

School of Mathematics and Statistics
Carleton University
daniel@math.carleton.ca

ASCrypto (Advanced School of Cryptography)
Latincrypt 2019 – Santiago (Chile)

Outline

Finite Fields in Cryptography

- Classical cryptosystems and security:
  - Diffie-Hellman, ElGamal, etc;
  - elliptic and hyperelliptic curve cryptosystem; other cryptosystems (Chor-Rivest, McEliece, TCHo, etc);
  - discrete logarithm problem (index calculus method and its variants).
- Ciphers:
  - RC4, WG, etc;
  - AES, RC6, etc.
- Hardware and software arithmetic.
- Pos-quantum cryptography:
  - code-based;
  - multivariate;
  - isogenies.

Definition

Definition. A field $(F, +, \cdot)$ is a set F together with operations $+$ and $\cdot$ such that:

(1) $(F, +)$ is an Abelian group;

(2) $(F \setminus \{0\}, \cdot)$ is an Abelian group;

(3) distributive laws hold, that is, for $a, b, c \in F$, we have

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c, \\ (b + c) \cdot a &= b \cdot a + c \cdot a. \end{aligned}$$

If $\#F$ is finite, then F is a finite field.

Example:

$\mathbb{Z}/(p)$ is a field if and only if p is a prime.

Background on Finite Fields I

- (Existence and Uniqueness) Up to isomorphism, there is exactly one finite field with $q = p^n$ elements, denoted $\mathbb{F}_{p^n} = \mathbb{F}_q$ for all prime p and positive integer n. The characteristic of the finite field $\mathbb{F}_q$ is p.

- In $\mathbb{F}_q$, $a^q = a$ for all $a \in \mathbb{F}_q$.

- (Freshman's Dream) We have that for $0 < i < p$

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i!} \equiv 0 \pmod{p}.$$

  Hence, if $\alpha, \beta \in \mathbb{F}_p$, we have $(\alpha + \beta)^p = \alpha^p + \beta^p$.
  This generalizes to powers p^n.

- The multiplicative group of $\mathbb{F}_q$ is cyclic. The generators of this multiplicative group are primitive elements.

Background on Finite Fields II

- Every subfield of $\mathbb{F}_{q^n}$ is of the form $\mathbb{F}_{q^k}$ for k dividing n.
- The trace of $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is defined as $\mathsf{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$.

  If $q = p$, p prime, then $\mathsf{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ is the absolute trace and is denoted by $\mathsf{Tr}(\alpha)$.
- The extension field $\mathbb{F}_{q^n}$ can be seen as a vector space of dimension n over $\mathbb{F}_q$.
- For $\alpha \in \mathbb{F}_{q^n}$, if $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$, then N is a normal basis, and α is a normal element.

Polynomial Representation I

A monic polynomial over $\mathbb{F}_q$ of degree n is of the form $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{F}_q$ for $0 \leq i < n$.

- We create $\mathbb{F}_{q^n}$ by taking the quotient of $\mathbb{F}_q[x]$ by an irreducible polynomial f of degree n. That is $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(f)$.

Finite field elements are represented by polynomials of degree less than n with coefficients in $\mathbb{F}_q$. Addition is performed term-wise and multiplication is taken $\pmod{f}$.

There are irreducible polynomials of any degree an over any finite field. Since this is the polynomial used in the reduction, in practice, highly sparse irreducible polynomials are preferred.

Over $\mathbb{F}_2$, the most sparse polynomials are trinomials: $x^n + x^k + 1$.

Polynomial Representation II

Trinomials over $\mathbb{F}_2$ do not exist for all degree n. Hence, many studies center on finding the best irreducible polynomials to use in practice.

Theoretically, it has been proved that trinomials in characteristic 2 of degree a multiple of 8 do not exist (Swan, 1962). For those values of n, pentanomials should be used.

Example

In Rijndael most arithmetic is done in $\mathbb{F}_{2^8}$ using the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$ to define the extension. There are theoretical and practical reasons to pick this polynomial...

Practically, polynomials with many zeros on the upper part of the polynomial (higher degrees) seem to behave better.

Differential Cryptanalysis

General Concepts

Around 1992, two cryptanalysis methods were introduced directed to symmetric cryptosystems: differential cryptanalysis (due to Biham and Shamir) and linear cryptanalysis (due to Matsui).

In order to resist these attacks the S-boxes (that are vectorial functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$) used in an iterated block cipher must satisfy some mathematical properties: nonlinearity and differential uniformity, respectively. [1]

The main goal of this talk is to comment on these properties and to show functions that have good nonlinearity and differential uniformity, and hence can be used (or are already used) as S-boxes.

[1] Although we mostly present results for characteristic 2, all concepts can be generalized to any finite field $\mathbb{F}_q$.

Vectorial Functions

We consider functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$, where we assume $n \geq m$. If $m = 1$, then this is a Boolean function. We are specially interested here in functions on $\mathbb{F}_2^n$, that is, when $m = n$.

Vectorial functions and extension fields over finite fields of characteristic two are used in many cryptographic systems. For example, the Advanced Encryption Standard (AES) use these objects for its S-boxes (substitution boxes). The security of the system depends heavily on the properties of the chosen S-boxes.

This substitution should be one-to-one, to ensure invertibility, but the S-box is usually more than a permutation of the bits. Other properties are needed. . . .

Main Idea

The differential attack is based on analyzing how differences in the input of an S-box affect differences in the corresponding outputs. The basic method uses pairs of plaintext related by a constant difference. The attacker then computes the differences of the corresponding ciphertexts, hoping to detect statistical patterns in their distribution.

Let f be an S-box. The method begins by constructing a difference table for f. Let $a \in \mathbb{F}_2^n$ be fixed. For every pair of vectors $x, y \in \mathbb{F}_2^n$ such that $y - x = a$ we compute $f(y) - f(x) = b$ and count the number of times each value of b occurs. We repeat this for every value of $a \in \mathbb{F}_2^n$, so each entry in the table is the number of times b occurs for a given value of a.

From the difference table we select an entry (a, b) such that the pair (a, b) occurs a large number of times. Then, one particular ciphertext difference is expected to be especially frequent and this is used to guess the key.

In order to be resistant to differential cryptanalysis, we should choose our S-boxes such that their difference tables do not have large values.

More precisely, a function f offers high resistance to differential cryptanalysis when the number of solutions to the system

$$\begin{cases} y - x = a, \\ f(y) - f(x) = b, \end{cases}$$

is low for every $a \neq 0, b \in \mathbb{F}_2^n$.

Definition

For fixed $a, b \in \mathbb{F}_2^n$, let $N_f(a,b)$ denote the number of solutions $x \in \mathbb{F}_2^n$ of $f(x+a) - f(x) = b$, where $a, b \in \mathbb{F}_2^n$, and let

$$\Delta_f = \max\{N_f(a,b) \mid a, b \in \mathbb{F}_2^n, a \neq 0\}.$$

Nyberg (1994) defines a mapping f to be differentially k-uniform if $\Delta_f = k$.

If $k = 1$, then f is a perfect nonlinear function (PN).

If $k = 2$, then f is a almost perfect nonlinear function (APN).

These notions can be generalized for vectorial functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$, where $n \geq m$, not necessarily $n = m$.

A function f from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$, where $n \geq m$, is balanced if it is uniformly distributed, that is, f takes each value of $\mathbb{F}_2^m$ exactly 2^{n-m} times. When $n = m$, each value of $\mathbb{F}_2^n$ is taken exactly once.

In general, for $n \geq m$, the function f is PN if and only if all of its derivatives are balanced, that is, if for nonzero $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^m$, $N_f(a, b) = 2^{n-m}$ for any a and any b.

Let $m = 1$. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is PN if and only if for all $a \neq 0$ in $\mathbb{F}_2^n$ and $b \in \mathbb{F}_2$, the number of solutions of $f(x + a) - f(x) = b$ is 2^{n-1}.

PN functions are also called bent functions. They were first introduced in the area of finite geometries as planar functions. They have the property that for every nonzero a, the difference mapping is a permutation in $\mathbb{F}_{p^n}$.

There are many notions related to bent functions including almost bent, hyper bent, self-dual bent, etc.

Bent functions are also related to constructions of objects both in combinatorics and finite geometries including difference sets, strongly regular graphs, association schemes, etc.

Perfect Nonlinear Functions

Two major drawbacks for cryptography is that these optimal functions are not invertible as normally required for S-box functions, and do not exist in characteristic 2.

Proposition. There are no PN permutation.

Proof.
Let f be any PN function. Choose $b = 0$. Since f is PN, for all nonzero a, there must exist a solution to $f(x + a) - f(x) = 0$. Thus, f is not a permutation. $\square$

Example

The function $f(x) = x^2$ defined in a finite field of odd characteristic is PN and not bijective.

Proof.

$$f(x+a) - f(x) = (x+a)^2 - x^2 = 2ax + a^2 = b$$

has exactly one solution since $2a$ is invertible for $a \neq 0$.

This function is not bijective since $f(1) = f(-1)$.

Proposition. There are no perfect nonlinear mappings over fields of characteristic 2.

Proof.
Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be any mapping. If x is a solution to

$$f(x+a) - f(x) = b,$$

then $x + a$ is also a solution, since

$$f((x+a)+a) - f(x+a) = f(x) - f(x+a) = f(x+a) - f(x).$$

Thus, the number of solutions to $f(x+a) - f(x) = b$ is always even. $\square$

Reminder: permutations of low differential uniformity are of interest in cryptography. Indeed, differential and linear cryptanalysis attempt to exploit weaknesses of the uniformity of the functions employed in block ciphers.

As we just saw, when f is defined over $\mathbb{F}_2^n$, solutions come in pairs, and the minimum possible value for Δ_f is two. Hence, over the important characteristic 2 case, APN functions attain this minimum and so are optimally resistant to differential cryptanalysis.

Almost Perfect Nonlinear Functions

The most used APN functions over $\mathbb{F}_2$ are power functions x^d, for some particular values of d, but there are other APN functions.

Monomials are intensively studied, since they usually have a lower implementation cost in hardware. Moreover, their properties regarding differential attacks can be studied more easily. There is also a relation with weight enumerators of some cyclic codes.

When n is odd, in characteristic 2, any APN monomial is a permutation, but not much is known about other APN functions being in general bijective.

Remark: in practice we are generally interested in even extensions of $\mathbb{F}_2 \ldots$.

Power APN functions over $\mathbb{F}_2$

Known classes of power APN functions over $\mathbb{F}_2$:

	Exponents d	Conditions
Gold functions	$2^i + 1$	$\gcd(n, i) = 1$
Kasami functions	$2^{2i} - 2^i + 1$	$\gcd(n, i) = 1$
Welch function	$2^t + 3$	$n = 2t + 1$
Niho function	$2^t + 2^{t/2} - 1$ $2^t + 2^{\frac{3t+1}{2}} - 1$	$n = 2t + 1$, t even $n = 2t + 1$, t odd
Inverse function	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$

Table: Known APN Power Functions x^d on $\mathbb{F}_{2^n}$.

Gold Case

We give the proof of the Gold function due to Nyberg.

We need the following results (more about them later in the talk) that hold for any finite field $\mathbb{F}_q$, $q = p^n$, p prime and n a positive integer:

- A polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial if the map $x \mapsto f(x)$ is a permutation from $\mathbb{F}_q$ to $\mathbb{F}_q$.
- Let $f \in \mathbb{F}_q[x]$. Then $f(x) = x^d$ is a permutation polynomial if and only if $\gcd(d, q-1) = 1$.

Theorem. Let $\gcd(n, i) = s$. Then, the Gold power function over $\mathbb{F}_{2^n}$ defined by $f(x) = x^{2^i+1}$ satisfies $\Delta_f = 2^s$. Moreover, if n/s is odd, then f is a permutation.

Proof (sketch).
In order to determine Δ_f, we count the number of solutions to

$$(x+a)^{2^i+1} + x^{2^i+1} = b, \quad \text{for all } a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}. \tag{1}$$

Since f is defined over $\mathbb{F}_{2^n}$, all solutions come in pairs so suppose that x_1 and x_2 are distinct solutions to the above equation. Then,

$$\begin{aligned} & (x_1+a)^{2^i+1} + x_1^{2^i+1} + (x_2+a)^{2^i+1} + x_2^{2^i+1} = 0 \\ \Leftrightarrow \quad & x_1^{2^i} + x_1 + x_2^{2^i} + x_2 = 0 \\ \Leftrightarrow \quad & (x_1+x_2)^{2^i-1} = 1, \end{aligned}$$

so that $x_1 + x_2 \in \mathbb{F}_{2^s}^*$. From this it can be shown that if x_0 is a solution to (1), the set of all solutions is given by $x_0 + \mathbb{F}_{2^s}^*$, and so there are 2^s solutions. Hence, $\Delta_f = 2^s$.

To prove that f is a permutation, we show that $\gcd(2^i + 1, 2^n - 1) = 1$. We recall the notion of the 2-order of an integer a, which is the highest power of 2 that divides a. Since n/s is odd, the 2-order of s is equal to the 2-order of n, and $\gcd(2i, n) = \gcd(i, n) = s$. Therefore,

$$2^s - 1 = \gcd(2^{2i} - 1, 2^n - 1) = \gcd(2^i - 1, 2^n - 1)\gcd(2^i + 1, 2^n - 1)$$

implies $\gcd(2^i + 1, 2^n - 1) = 1$, and f is a permutation. $\square$

Corollary. If $\gcd(n, i) = 1$, then the Gold power function is APN over $\mathbb{F}_{2^n}$, and an APN permutation if in addition n is odd.

Other important APN functions

The so-called inverse function over $\mathbb{F}_{2^n}$ defined by $f(x) = x^{2^n-2}$ (observe $f(0) = 0$) is APN for n odd.

For even n it has differential uniformity 4 (it takes the values 0, 2 and 4). Indeed, the value 4 is taken once, and so in this sense it is "optimal" among 4-differential functions.

We observe that the S-boxes in AES use the inverse function; AES is defined over $\mathbb{F}_{2^8}$, hence it is a permutation but not APN.

APN permutations take values 0 and 2 the same number of times.

The APN functions 45^x mod 257 and its inverse in $\mathbb{Z}_{256}$ are used in the SAFER cryptosystem by Massey (1993).

Open Problem: find APN permutation in $\mathbb{F}_{2^8}$ (or in $\mathbb{F}_{2^{2n}}$ for $n \geq 4$).

It was conjectured that there are no APN permutations on even extensions of characteristic 2. Hou proved that there are no APN permutations in $\mathbb{F}_{2^4}$.

The first example of an APN permutation in $\mathbb{F}_{2^6}$ was found by Dillon in 2009. Ten years after that is still the only known example of APN permutation in even field extensions of $\mathbb{F}_2$!

Permutation Polynomials and Related Concepts

Definitions and examples

Definition. For q a prime power, let $\mathbb{F}_q$ denote the finite field containing q elements. A polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial (PP) if the function $f : c \to f(c)$ from $\mathbb{F}_q$ into itself induces a permutation. Alternatively, f is a PP if the equation $f(x) = a$ has a unique solution for each $a \in \mathbb{F}_q$.

PPs over finite field $\mathbb{F}_q$ and rings $\mathbb{Z}_n$ have applications in Advanced Encryption Standard (AES), RC6 cipher (Rivest, Robshaw, Sidney and Yin, 1998; Rivest, 2001) among many others ciphers.

RC6 uses the permutation function in $\mathbb{Z}_{2^w}$ ($w = 32$ for the suggested implementation)

$$f(x) = x(2x + 1) \pmod{2^w}.$$

Our security goals are that the data-dependent rotation amount that will be derived from the output of this transformation should depend on all bits of the input word and that the transformation should provide good mixing within the word. The particular choice of this transformation for RC6 is the function f followed by a left rotation by five bit positions. This transformation appears to meet our security goals while taking advantage of simple primitives that are efficiently implemented on most modern processors. Note that f is one-to-one modulo 2^w, and that the high-order bits of f, which determine the rotation amount used, depend heavily on all the bits of x. See "The Security of the RC6 Block Cipher" for more information on these issues.

Well known classes of PPs over $\mathbb{F}_q$

Monomials: Monomial x^n is a PP over $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.

Dickson: For $a \neq 0 \in \mathbb{F}_q$, the polynomial

$$D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}$$

is a PP over $\mathbb{F}_q$ if and only if $\gcd(n, q^2-1) = 1$.

Linearized: The polynomial

$$L(x) = \sum_{s=0}^{n-1} a_s x^{q^s} \in \mathbb{F}_{q^n}[x]$$

is a PP in $\mathbb{F}_{q^n}$ if and only if $\det(a_{i-j}^{q^j}) \neq 0$, $0 \leq i, j \leq n-1$.

DO permutation polynomials: A polynomial

$$f(x) = \sum_{i,j=0}^{n-1} a_{i,j} x^{p^j + p^i}$$

is called a Dembowski-Ostrom (DO) polynomial.

DO polynomials cannot be PP in odd characteristic.

Some cases where DO polynomials are PP in characteristic 2 are given by Blokhuis, Coulter, Henderson and O'Keefe (2001).

> *Dembowski-Ostrom polynomials have been used for a cryptographic application in the public key cryptosystem HFE (Patarin, 1996). There the author states that "it seems difficult to choose f (a DO polynomial) such that it is a permutation". It is the purpose of this article to provide some examples of Dembowski-Ostrom permutations. We consider this problem in the purely theoretical spirit of problem P2 of Lidl and Mullen (1988). We do not claim that any of the classes identified in this article could be used to provide a "secure" cryptosystem when implemented in HFE.*

Dickson polynomials

Dickson polynomials generalize monomials: $D_n(x, 0) = x^n$.

The Dickson polynomials with parameter $a = \pm 1$ are related to Fibonacci and Lucas polynomials. For general a, Dickson polynomials over the complex numbers are related to the Chebyshev polynomials T_n:

$$D_n(2xa, a^2) = 2a^n T_n(x).$$

Dickson polynomials have been related to RSA by Muller and Nobauer, and by Lidl and Muller.

For more applications and connections, see the book *Dickson polynomials* by Lidl, Mullen and Turnwald (1993).

PPs and APN functions

Dobbertin (1999) constructed classes of PPs over finite fields of characteristic two and used them to prove conjectures on APN monomials.

Golomb and Moreno (1996) show that PPs are useful in the construction of Costas arrays, which are useful in sonar and radar communications (more later). They gave an equivalent conjecture for Costas arrays in terms of permutation polynomials.

The connection between Costas arrays and APN permutations of integer rings $\mathbb{Z}_n$ is by Drakakis, Gow and McGuire (2009). Composed with discrete logarithms, permutation polynomials of finite fields are used to produce permutations of integer rings $\mathbb{Z}_n$ which generate APN permutations in many cases.

Costas arrays

A Costas array of order n is an $n \times n$ array of dots and blanks which satisfies

- n dots, $n(n-1)$ blanks, with exactly one dot in each row and column; and
- all segments between pairs of dots are different.

Example

$n = 3$:

•		
		•
	•	

	•	
•		
		•

	•	
		•
•		

		•
•		
	•	

A Costas array can be represented by

$f(1)$	$f(2)$	$\cdots$	$f(n)$

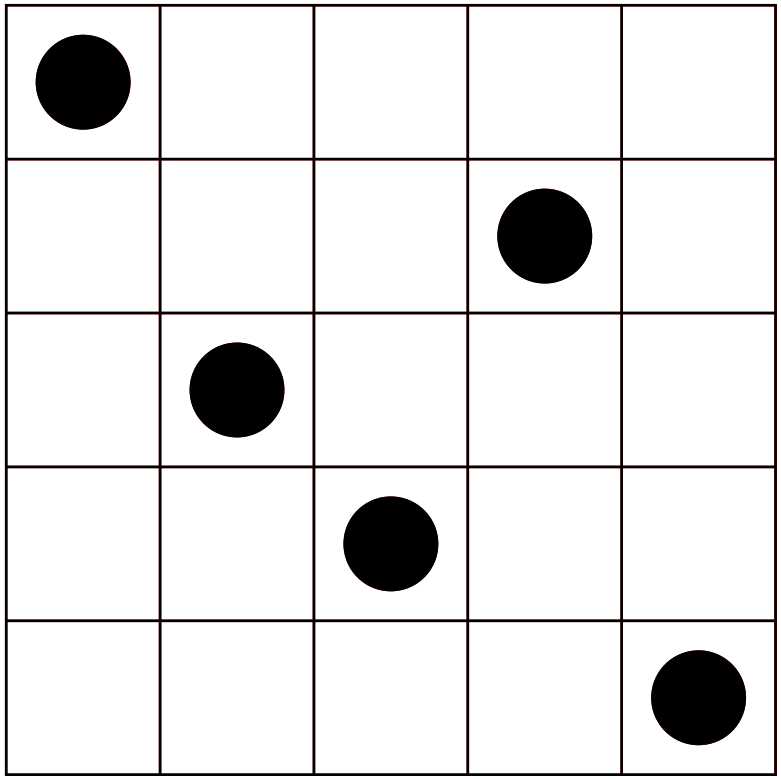
such that $f(j) = i$ if (i, j)-position has a dot, and for $x \neq y$, $k \neq 0$

$$f(x+k) - f(x) \neq f(y+k) - f(y).$$

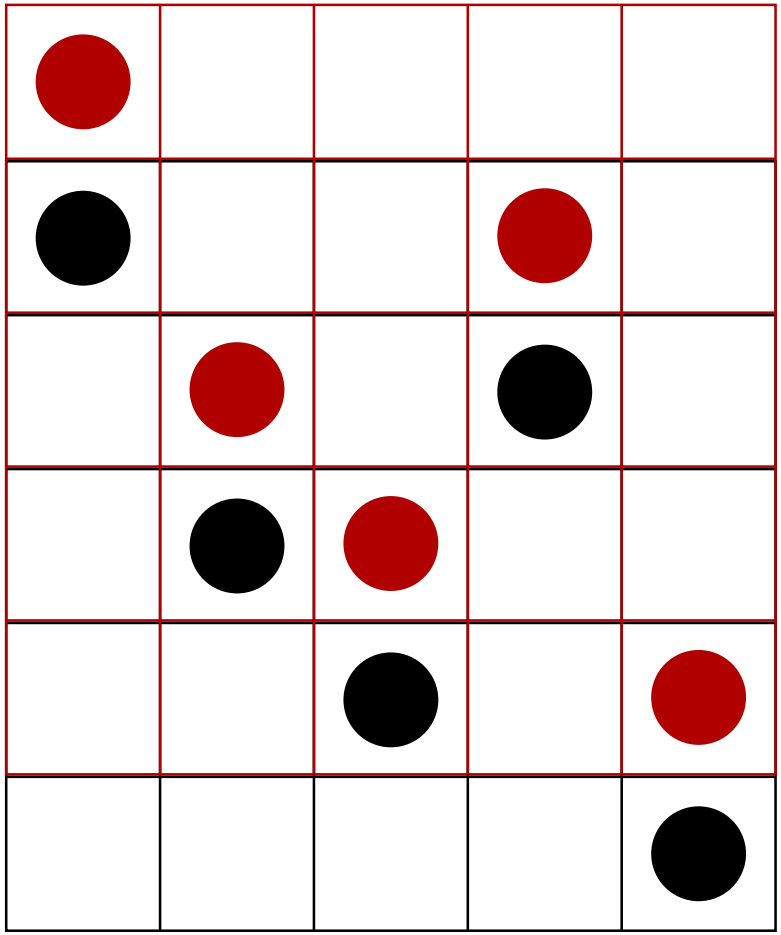
Example

	1	2	3
1	$\cdot$		
2			$\cdot$
3		$\cdot$	
	1	3	2

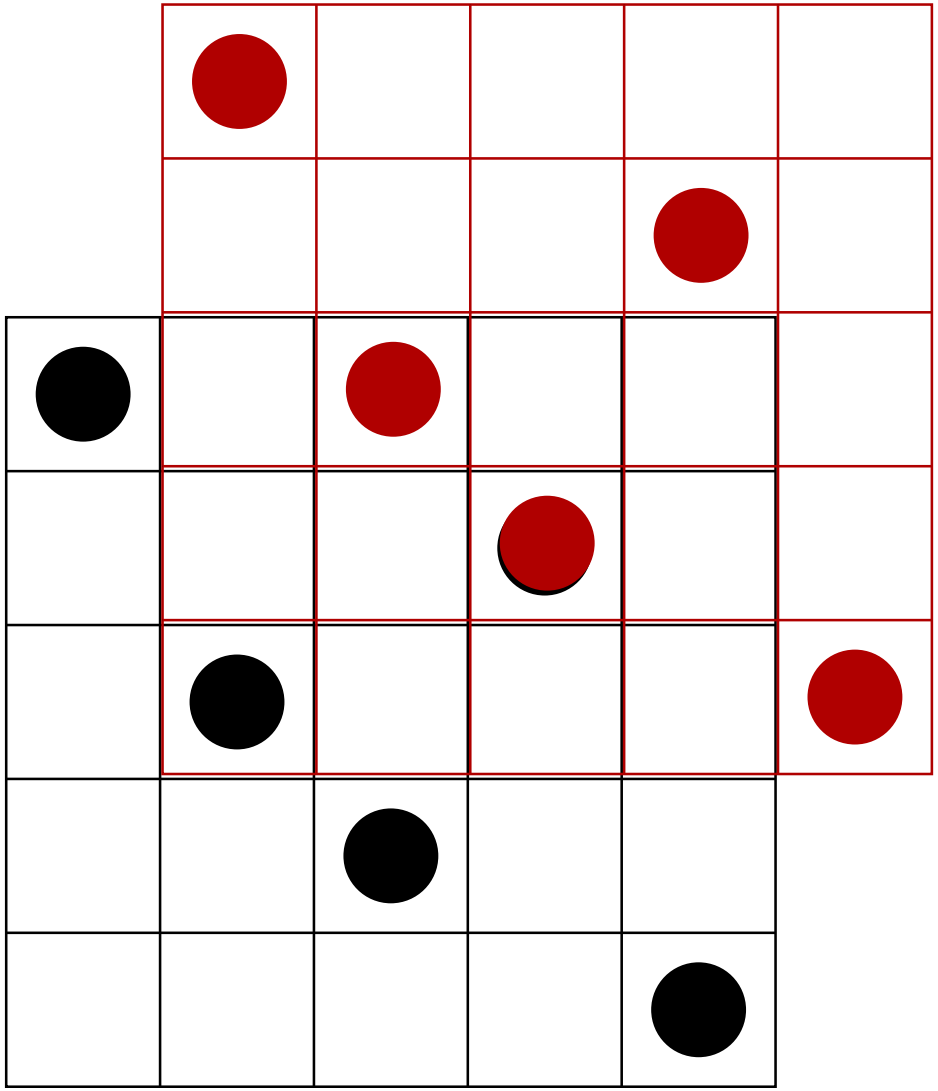
Radar or Sonar Echos



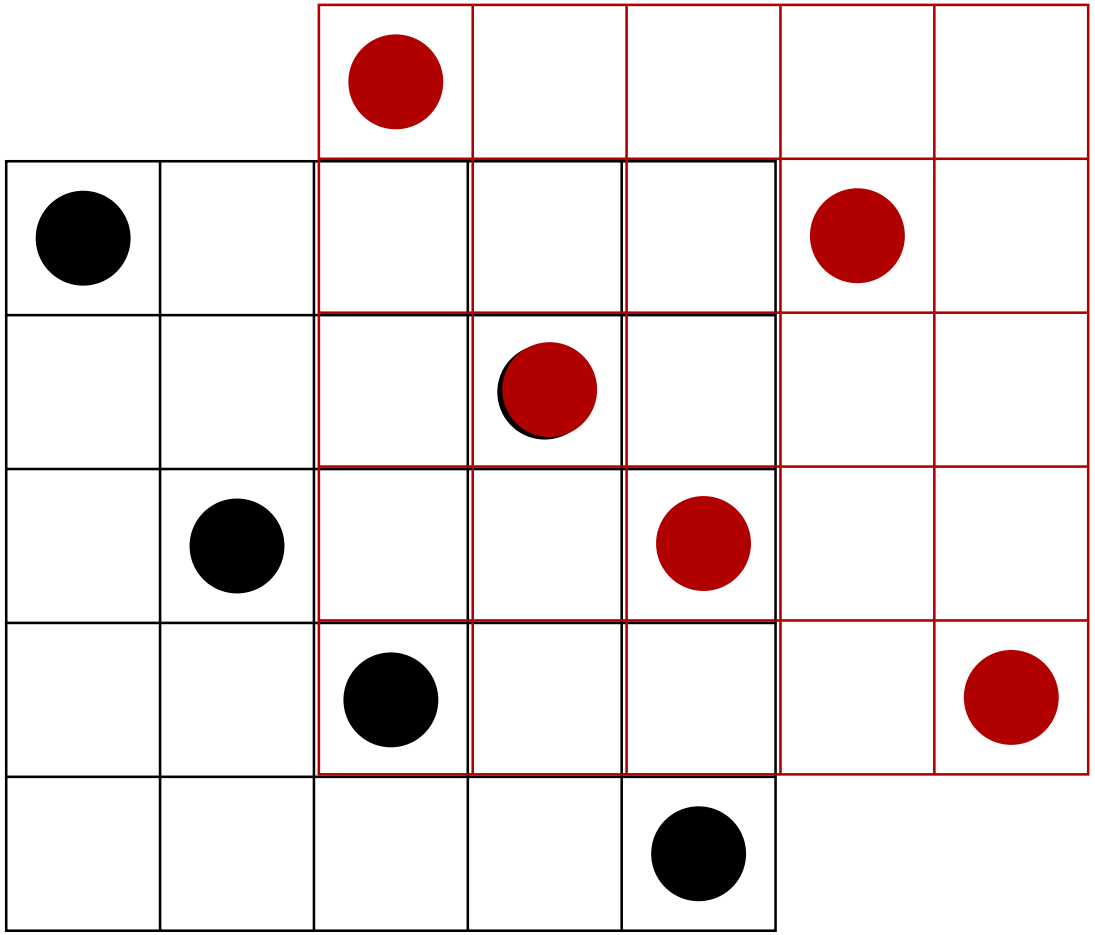
Radar or Sonar Echos



Radar or Sonar Echos



Radar or Sonar Echos



Welch construction

Let p be a prime, $n = p - 1$, α a primitive element in $\mathbb{F}_p$. Then, a_{ij} has a dot iff $\alpha^j = i$. In this case, $f(j) = \alpha^j$, and

$\alpha^{j+k} - \alpha^j = \alpha^{i+k} - \alpha^i$ implies that either $i = j$ or $k = 0$.

Example: let $p = 7$, $n = 6$, $\alpha = 3$:

					•
	•				
•					
			•		
				•	
		•			
3	2	6	4	5	1

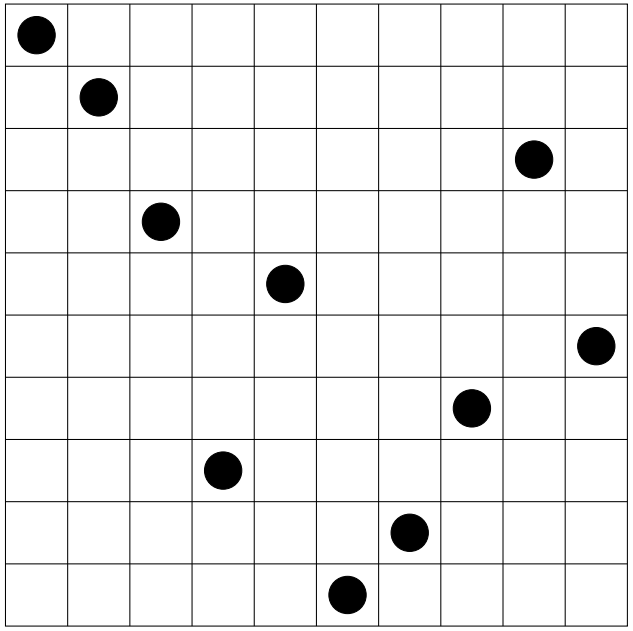
Welch construction of Costas arrays and APN permutations have been related by Drakakis, Gow and McGuire (2009). They construct APN permutations $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$.

Massey (1993) uses $f(x) = (45^x \bmod 257) \bmod 256$ and its inverse in the SAFER cryptosystem. Drakakis, Gow and McGuire show that the shift $g(x) = (45^x \bmod 257) - 1$ of the above permutation and its inverse are APN permutations in $\mathbb{Z}_{256}$.

Remember: still there are no known APN functions in $\mathbb{F}_{256}$.

Example

$f : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ given by $f(x) = (2^x \bmod 11) - 1$ or
$f = (0)(1)(23768)(4)(59)$ is an APN function in $\mathbb{Z}_{10}$.



Related measures: ambiguity and deficiency

Panario, Sakzad, Stevens and Wang (IEEE-IT, 2011) attempt to understand the injectivity and surjectivity of Δ_f when f is a bijection. How close a bijection f is to be APN?

The deficiency of f is the number of pairs (a, b) such that $\Delta_f(x) = f(x+a) - f(x) = b$ has no solutions. This is a measure of the surjectivity of Δ_f: the lower the deficiency the closer to be surjective.

Moreover, we define the (weighted) ambiguity of f as

$$A(f) = \sum_{0 \le i \le q} n_i(f) \binom{i}{2}.$$

The weighted ambiguity of f measures the total replication of pairs of x and x' such that $f(x+a) - f(x) = f(x'+a) - f(x')$ for some a. This is a measure of the injectivity of the function Δ_f: the lower the ambiguity the closer to be injective.

Related measures: non-balancedness

Let G_1 and G_2 be finite Abelian groups and $f : G_1 \to G_2$. The mean of the (uniform) random variable $|f^{-1}(b)|$ is $|G_1|/|G_2|$; then f is balanced if the random variable is constant. The coalescence, that is the variance of this random variable giving the distribution of the preimage sizes, is

$$\frac{1}{|G_2|} \sum_{b \in G_2} \left(|f^{-1}(b)| - \frac{|G_1|}{|G_2|} \right)^2 .$$

The non-balancedness of f is defined as

$$\mathbb{NB}(f) = \sum_{a \in G_1^*} \sum_{b \in G_2} \left(|\Delta_{f,a}^{-1}(b)| - \frac{|G_1|}{|G_2|} \right)^2 .$$

Non-balancedness is similar to ambiguity; see Fu, Feng, Wang and Carlet (IEEE-IT, 2019). Non-balancedness is used to provide bounds on the nonlinearity of the function; see Carlet and Ding (FFA, 2007).

Related measures: dispersion

The dispersion of a permutation P on the set $\{0, 1, \ldots, p-1\}$ is the cardinality of the set

$$\{(j-i, P(j)-P(i)) \colon 0 \leq i < j \leq p-1\}.$$

Dispersion has been used as a random measure for interleavers in turbo codes; see the book by Heegard and Wicker, 1999.

Dispersion is related to deficiency but deficiency is invariant under extended affine equivalence and dispersion is not; see Çeşmelioğlu, Meidl and Topuzoğlu (JCAM, 2014).

In that paper dispersion is used to provide permutations of given Carlitz rank with prescribed cycle decomposition and dispersion.

Linear Cryptanalysis

General Concepts

Linear cryptanalysis, introduced by Matsui, exploits the relationships between the input x of an S-box f, and the output $f(x)$. Given that the S-boxes are public, one can compute all input-output pairs $(x, f(x))$.

Suppose that there exists a "linear" function (to be defined later) $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ that satisfies $L(x) = f(x)$ for a significant number of inputs x. Then, one can use this approximation, L, to take a guess at the secret key. Thus, functions f that behave like linear functions are not good for use as S-boxes.

We want a measure to quantify how close or far we are from being linear. This measure, to be defined later, is the nonlinearity of the function.

Linearized Polynomials

Let q be a prime power and L a polynomial over $\mathbb{F}_{q^n}$ of the form

$$L(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i},$$

where $\alpha_i \in \mathbb{F}_{q^n}$, then L is a linearized polynomial. Similarly, if $A(x) = L(x) + c$ for some $c \in \mathbb{F}_{q^n}$, then A is an affine polynomial.

Linearized polynomials are indeed linear. . . .

Proposition. If L is a linearized polynomial over $\mathbb{F}_{q^n}$, then L is a linear operator, that is, the following two properties hold

$$L(x+y) = L(x) + L(y),$$
$$L(cx) = cL(x),$$

for all $x,\ y \in \mathbb{F}_{q^n}$ and $c \in \mathbb{F}_q$.

Conversely, if L is a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$ that satisfies the above two properties, then L can be expressed as a linearized polynomial of degree at most $q^n - 1$.

The Walsh transform

Let f be an S-box function. In the following, we define the nonlinearity of f, a concrete measure of how far f is from being linear. The functions that achieve the highest possible nonlinearity possess optimal resistance to linear cryptanalysis; they are called almost bent (AB).

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be any function. We start defining the Walsh transform of f that is the function $\lambda_f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{Z}$ defined by

$$\lambda_f(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot f(x)} \in \mathbb{Z},$$

where $x \cdot y = x_1 y_1 + \cdots + x_n y_n$ is the standard inner product.
The Walsh transform is independent of the choice of inner product.

The Walsh transform gives a value between -2^n and 2^n. It measures the correlation between the function f and linear functions $a \cdot x$.

Indeed, the Walsh transform gives a quantitative measure of the distance from f to all linear functions. If $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a nonzero linear function with algebraic normal form

$$f(x_1, \ldots, x_n) = c_1 x_1 + \cdots + c_n x_n,$$

where $c \in \mathbb{F}_2^n$, then there exists $a, b \neq 0$ in $\mathbb{F}_2^n$ such that $a \cdot x + b \cdot f(x) = 0$ for all x. Then, $\lambda_f(a, b) = 2^n$, which is the maximum possible value for $\lambda_f(a', b')$ of all $a', b' \in \mathbb{F}_2^n$.

This leads us to the definition of nonlinearity.

Definition. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be any function. The nonlinearity of f is the value

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{b \neq 0, a \in \mathbb{F}_2^n} |\lambda_f(a, b)|.$$

If $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is linear, then $\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2}2^n = 0$.

We want high nonlinearity.

There is an upper bound on the nonlinearity of a function.

Theorem (Chabaud and Vaudenay, 1995).
The nonlinearity of any function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ satisfies

$$\mathcal{NL}(f) \leq 2^{n-1} - 2^{\frac{n-1}{2}}.$$

We want S-box functions that have nonlinearity closer to this bound.

The functions which have the largest possible nonlinearity offer the greatest resistance to linear cryptanalysis.

Definition. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function such that

$$\mathcal{NL}(f) = 2^{n-1} - 2^{\frac{n-1}{2}}.$$

Then, f is almost bent (AB) or maximally nonlinear.

AB functions exist only for odd n in characteristic 2.

Proposition. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an AB function. Then, n is odd.

Proof. Suppose that $n = 2k$ is even. Then, by definition

$$\begin{aligned}\mathcal{NL}(f) &= 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n, 0 \neq b \in \mathbb{F}_2^n} |\lambda_f(a,b)| \\ &= 2^{n-1} - 2^{\frac{n-1}{2}} = 2^{2k-1} - 2^{\frac{2k-1}{2}},\end{aligned}$$

so that $2^{\frac{2k-1}{2}} = \frac{1}{2} \max_{a \in \mathbb{F}_2^n, 0 \neq b \in \mathbb{F}_2^n} |\lambda_f(a,b)|$. Because $\lambda_f(a,b)$ is an integer, the right hand side of this relation is rational and the left hand side is not, a contradiction. Therefore, n must be odd. □

Since AB functions offer optimal resistance to linear cryptanalysis, and APN functions offer optimal resistance to differential cryptanalysis, it is desirable to have both properties. The following result illustrates that this is possible.

Theorem Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an AB function. Then, f is also APN. Moreover, f is AB if and only if the Walsh spectrum of f is $\Lambda_f = \{0, \pm 2^{\frac{n+1}{2}}\}$.

The Walsh spectrum of f is the set

$$\Lambda_f = \{\lambda_f(a, b) : a, b \in \mathbb{F}_2^n, b \neq 0\}.$$

AB functions on $\mathbb{F}_2^n$, with n odd, provide an optimal resistance to both differential attacks and linear attacks. There exist several classes of AB permutations.

The situation is different for even n: there are APN functions f such that $\mathcal{NL}(f) = 2^{n-1} - 2^{\frac{n}{2}}$. It is conjectured that this is the maximum value.

Example

The inverse function, $f(x) = x^{2^n-2}$, is an APN (not AB) permutation on $\mathbb{F}_2^n$ when n is odd.

For even n, it is a permutation too, but $D_{f,a}$ takes three values, namely 0, 2 and 4 so that $\Delta_f = 4$. This function has the highest degree and satisfies, $\mathcal{NL}(f) = 2^{n-1} - 2^{\frac{n}{2}}$.

The Walsh transform can be defined for a function

$$f : \mathbb{F}_2^n \to \mathbb{F}_2^m, \quad 1 \leq m \leq n.$$

If $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a function, it is possible to define the Walsh transform of f analogously. Instead of using the standard inner product for vectors, we use the absolute trace:

$$\lambda_f(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathsf{Tr}(ax + bF(x))}.$$

Conclusion

- We briefly touch on linear and differential cryptanalysis to then focus on useful functions over finite fields to counterattack them.
- We explain the importance of low differential uniformity.
- We comment on PN and APN functions, permutation polynomials, as well as almost bent functions and other related functions.
- We relate APN to other concepts such as Costas arrays.
- We comment on linearized polynomials and nonlinearity of a function.

Where to read more (shameless advertisement coming)

There has been a lot of research done in these areas in the last 25 years.
The literature is vast but mostly spread in papers.

Where to read more (shameless advertisement coming)

There has been a lot of research done in these areas in the last 25 years.
The literature is vast but mostly spread in papers.