Recent developments on APN functions and related topics

Gary McGuire

School of Mathematical Sciences
University College Dublin
Ireland
and
Claude Shannon Institute

September 2009, Brussels

Most modern cryptosystems use S-boxes that are based on Boolean functions.

There are situations (encrypting credit card numbers or social security numbers, for example) where non-binary data is a natural part of the application and one might use non-binary functions in the cryptosystem. The SAFER family of cryptosystems, proposed by Jim Massey, uses non-binary functions.
In fact they use a mixture of binary and non-binary arithmetic to increase the confusion.

Ciphers

Many modern ciphers are (roughly speaking) a series of ROUNDS, where each round consists of an S-box and a P-box.

$$x \longrightarrow \underbrace{S(x) \longrightarrow P(S(x)) \longrightarrow}_{one \quad round} S(P(S(x))) \longrightarrow \cdots$$

The S-box has to satisfy certain criteria to be secure against certain attacks. Some are

Ciphers

Many modern ciphers are (roughly speaking) a series of ROUNDS, where each round consists of an S-box and a P-box.

$$x \longrightarrow \underbrace{S(x) \longrightarrow P(S(x)) \longrightarrow}_{one \quad round} S(P(S(x))) \longrightarrow \cdots$$

The S-box has to satisfy certain criteria to be secure against certain attacks. Some are

1. The PN or APN property provides resistance of the S-box to differential cryptanalysis.
2. High nonlinearity provides resistance of the S-box to linear cryptanalysis
3. The permutation property (i.e. S being invertible) makes it easier to invert (to decrypt).

S-Boxes Criteria

(see M-Alvarez, Proc. NATO workshop)

1. **Balanced.**
2. **Resilience.**
3. **Nonlinearity.**
4. **XOR Table.**
5. **Avalanche.**
6. **Propagation.**
7. **Bit Independence.**
8. **Linear Structures.**
9. **Linear Redundancy.**
10. **Fixed Points.**
11. **Algebraic Degree.**
12. **Degree.**
13. **Algebraic Immunity.**
14. **Cube.**
15. **Branch Number.**

computer environment. Here the data transmitted may often be nonredundant if, for example, they are purely numerical, and an error in a single digit can cause an avalanche of computational errors. Study of the problem has shown that simple error-detecting codes are inadequate for guarding the integrity of computer data against possible tampering by a human expert. What is required is not mere error-detection but cryptographically protected authentication. Surprisingly, this is best achieved by relying on certain principles inherent in the cipher structure itself. Rather than trying to modify the stream concept, let us take a fresh look at the basis of all cryptography: substitution on blocks of message digits.

We shall refer to any cipher that converts n message digits into n cipher digits as a block cipher. For example, a block cipher would be one that turns 00000, standing for a clear-text A, into, say, 11001, the cipher equivalent of A according to some permutation key, exactly as a tableau does. To see how such a binary transformation is performed by an electronic device let us consider a substitution on only three binary digits [*see illustration on preceding page*].

Three binary digits can represent eight items: 2^3 equals eight. The substitution device consists of two switches. The first converts a sequence of three binary digits into its corresponding value to the base eight, thereby energizing any one of eight output lines. These eight lines can be connected to the second switch in any one of 8!, or 40,320, ways. We are at liberty to decide which one of these 40,320 distinct connection patterns, or wire permutations, is to be made between the first switch and the second switch. The role of the second switch is to convert the input, presented as one digit to the base eight, back into a three-digit binary output.

If the substitution device were built to handle a five-digit binary input, it could be used to encipher an alphabet of 32 letters. The number of possible connection patterns between the two switches would then be 32!. That would seem to be an incredibly large number of keys, but the cipher produced must still be regarded as glaringly weak: it could not resist letter-frequency analysis. The weakness is not intrinsic; the device described is mathematically the most general possible. It includes, for any given input-output dimension, any possible reversible cipher that has been or ever could be invented; mathematicians would say it represents the full symmetric group. It is completely "nonsystematic": one permutation connection tells an opponent nothing at all about any other connection. The problem is not intrinsic, then, but is related to size. In spite of the large number of keys, the "catalogue" of possible inputs and outputs is too small: only 32. What is required is a catalogue so large that it is impractical for any opponent to record it. If we had a box with 128 inputs and outputs, for example, an analyst would have to cope with 2^{128} (or more than 10^{38}) possible digit blocks, a number so vast that frequency analysis would no longer be feasible. Unfortunately a substitution device with 128 inputs would also require 2^{128} internal terminals between the first and the second switch, a technological impossibility. This is a fundamental dilemma in cryptography. We know what would be ideal but we cannot achieve the ideal in practice.

Perhaps one could find a device that is easy to realize for a large number of inputs. One might, for example, build a box with, say, 128 input and 128 output terminals that are connected internally by ordinary wire crossings [*see illustration at left below*]. Such a "permutation box" with $n!$ terminals would have $n!$ possible wire crossings, each of which could be set by a different key. It could be built easily for $n = 128$. Although this provides a usefully large number of keys (128!), we are now faced with a new difficulty. By the use of special trick messages it is possible to read out the complete key to such a system in only $n - 1$ (in this case 127) trials. The trick is to introduce a series of messages containing a single 1 at $n - 1$ positions; the position of the 1 in the output betrays the particular wire crossing used in the box. The flaw in the simple permutation box is again that it is a linear system.

We need a compromise that will at least approximate the features of the general system. We are led to the notion of a product cipher in which two or more ciphers are combined in such a way that the resulting system is stronger than either of the component systems alone. Even before World War I various cumbersome ciphers using several stages of encipherment were studied. The first genuinely successful example was probably the one devised by the Germans that was known as the ADFGVX system. We need only observe here that it coupled "fractionation" with "transposition." By that procedure a message was broken into segments and the segments were transposed. The important fact to note here is that the result of a product cipher is again a block cipher; the goal, of course, is that the cipher behave as much as possible as if it were a general substitution cipher.

Between World War I and World War II interest in product ciphers almost totally disappeared because of the successful development of rotor, or wired-wheel, machines, which belong to the general class of pseudorandom-stream generators. A typical rotor machine has a keyboard resembling that of a typewriter. Each letter is enciphered by the operation of several wheels in succession, the wheels being given a new alignment for each new letter according to an irregular and keyed stepping algorithm. The message is decoded by an identical machine with an identical key setting.

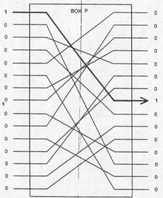
The modern interest in product systems was stimulated by a paper by Claude E. Shannon titled "Communication Theory of Secrecy Systems," published in the *Bell System Technical Journal* in 1949. In a section on practical cipher design Shannon introduced the notion of "mixing transformation," which involved a special way of using products of transformations. In addition to outlining intuitive guides that he believed would lead to strong ciphers, he introduced the concepts of "confusion" and "diffusion." The paper opened up almost unlimited possibilities to invention, design and research.

The manner in which the principles of confusion and diffusion interact to provide cryptographic strength can be described as follows. We have seen that general substitution cannot be realized for large values of n, say $n = 128$, and so we must settle for a substitution scheme of practical size. In the IBM system named Lucifer we have chosen $n = 4$ for the substitution box. Even though 4 may seem to be a small nu ber, it can be quite effective if the su stitution key, or wire-crossing pattern, properly chosen. In Lucifer nonline substitution effectively provides the e ment of confusion.

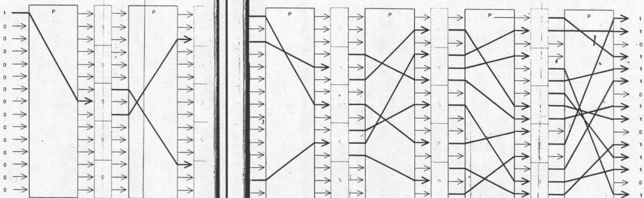
We have also seen that a linear p mutation box is easy to build even $n = 128$. The number of input and o put terminals is simply equal to n. Bei a pure digit-shuffler, a device that me ly moves digits around without alteri the number of 1's in the data, the p mutation box is a natural spreader confusion, that is, it can provide optim diffusion.

In the Lucifer system the input da pass through alternating layers of bo es that we can label P and S. P stan for permutation boxes in which n is large number (64 or 128) and S stan for substitution boxes in which n is sm (4). Whereas either P boxes alone or boxes alone would make a weak syste their strength in combination is cons erable.

One measure of strength is depicted a device in which for simplicity the boxes have $n = 15$ and the S boxes ha $n = 3$ [*see illustration on these t pages*]. If we imagine this sandwich boxes being "tickled" by addressing with a specially selected input, whi might consist of a number made up



PERMUTATION BOX can handle very many terminals but it only shuffles positions of digits. An opponent can learn its wiring by feeding in inputs with single 1's and seeing where 1's come out.



PRODUCT-CIPHER SYSTEM combines P boxes and S boxes. The P boxes have a large number of inputs (represented by 15 in the illustration) and the S boxes a number that is manageable for such devices—three in this case. The P boxes shuffle the digits, providing "diffusion." The S boxes provide nonlinear substitution and thus "confusion." In this simplified example the input includes a single 1 and 14 0's. Because the S boxes are nonlinear, they can p tentially increase the number of 1's; meanwhile the P boxes mo the 1's around. The result can be an unpredictable avalanche of 1

20

Definitions

Definition (Perfect Nonlinear function)

Let A, B be finite abelian groups, written additively, of the same cardinality. We say $f : A \longrightarrow B$ is a perfect nonlinear (PN) function iff $f(x+a) - f(x) = b$ has at most one solution for all $a \in A$, $a \neq 0$, and all $b \in B$.

Definition (Perfect Nonlinear function)

Let A, B be finite abelian groups, written additively, of the same cardinality. We say $f : A \rightarrow B$ is a perfect nonlinear (PN) function iff $f(x+a) - f(x) = b$ has at most one solution for all $a \in A$, $a \neq 0$, and all $b \in B$.

The definition implies that $f(x+a) - f(x) = b$ has exactly one solution, or equivalently, the function $f(x+a) - f(x)$ is bijective, or equivalently,

$$f(x+a) - f(x) = f(y+a) - f(y) \implies a = 0 \text{ or } x = y.$$

PN functions are also called planar functions if $A = B = \mathbb{F}_q$.

Definitions

Definition (Perfect Nonlinear function)

Let A, B be finite abelian groups, written additively, of the same cardinality. We say $f : A \rightarrow B$ is a perfect nonlinear (PN) function iff $f(x+a) - f(x) = b$ has at most one solution for all $a \in A$, $a \neq 0$, and all $b \in B$.

The definition implies that $f(x+a) - f(x) = b$ has exactly one solution, or equivalently, the function $f(x+a) - f(x)$ is bijective, or equivalently,

$$f(x+a) - f(x) = f(y+a) - f(y) \implies a = 0 \text{ or } x = y.$$

PN functions are also called planar functions if $A = B = \mathbb{F}_q$.

Example: $f(x) = x^2$ on a finite field of odd characteristic.

PN functions do not exist in characteristic 2, because if x is a solution to $f(x+a) - f(x) = b$ then so is $x + a$ ☹

PN functions do not exist in characteristic 2, because if x is a solution to $f(x+a) - f(x) = b$ then so is $x + a$ ☹
This is why the following definition is made.

Definition (Almost Perfect Nonlinear function)

Let A, B be finite abelian groups, written additively, of the same cardinality. We say $f : A \rightarrow B$ is an almost perfect nonlinear (APN) function iff $f(x+a) - f(x) = b$ has at most two solutions for all $a \in A$, $a \neq 0$ and all $b \in B$.

Example: $f(x) = x^3$ on any finite field.

Permutations

Theorem

PN permutations do not exist.

Proof: Let f be a PN function. Choosing b to be 0, for all nonzero a there must exist a solution to $f(x+a) - f(x) = 0$. Therefore, f cannot be a permutation. □

Permutations

Theorem

PN permutations do not exist.

Proof: Let f be a PN function. Choosing b to be 0, for all nonzero a there must exist a solution to $f(x+a) - f(x) = 0$. Therefore, f cannot be a permutation. $\square$

What about APN permutations? Do they exist?

APN Permutations

It depends on the group.

Big Open Problem: Do APN permutations exist on finite fields $GF(2^n)$ where n is even?
(Remember x^3 is bijective iff n is odd)

APN Permutations

It depends on the group.

Big Open Problem: Do APN permutations exist on finite fields $GF(2^n)$ where n is even?
(Remember x^3 is bijective iff n is odd)

$n = 4$ was checked by exhaustive computer search - none found.

APN Permutations

It depends on the group.

Big Open Problem: Do APN permutations exist on finite fields $GF(2^n)$ where n is even?
(Remember x^3 is bijective iff n is odd)

$n = 4$ was checked by exhaustive computer search - none found.

Recent News:
On July 14, 2009, at the Fq 9 conference, John Dillon announced an APN permutation on $GF(64)$!! (Dillon-Wolfe example)

Alternative Definition of APN

The binary double-error-correcting BCH code is defined by parity check matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^n-2)} \end{bmatrix}$$

Alternative Definition of APN

The binary double-error-correcting BCH code is defined by parity check matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^n-2)} \end{bmatrix}$$

Think of this matrix as having columns labelled by nonzero field elements, and column x has the form

$$\begin{bmatrix} x \\ x^3 \end{bmatrix}.$$

This code is cyclic, has minimum distance 5, dimension $2^n - 1 - 2n$.

Alternative Definition of APN

The binary double-error-correcting BCH code is defined by parity check matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^n-2)} \end{bmatrix}$$

Think of this matrix as having columns labelled by nonzero field elements, and column x has the form

$$\begin{bmatrix} x \\ x^3 \end{bmatrix}.$$

This code is cyclic, has minimum distance 5, dimension $2^n - 1 - 2n$.

Definition: A function $f : K \longrightarrow K$ is called an APN function if the binary linear code with parity check matrix having columns

$$\begin{bmatrix} x \\ f(x) \end{bmatrix}, \quad x \in K^*$$

has minimum distance 5, and $f(0) = 0$.

Equivalence

An extended APN code has parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} & 0 \\ 1 & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{2^n-2}) & 0 \end{bmatrix}$$

and has minimum distance 6.

Equivalence

An extended APN code has parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} & 0 \\ 1 & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{2^n-2}) & 0 \end{bmatrix}$$

and has minimum distance 6.

Definition: Two APN functions are said to be (CCZ) equivalent if their corresponding extended APN codes are equivalent (as binary codes).

Known APN Functions

Monomial functions: x^d where d is 2^k+1, 4^k-2^k+1, 2^r-2 , $2^{(r-1)/2}+3$, 4^t+2^t-1, $2^{4t}+2^{3t}+2^{2t}+2^t-1$

Non-monomial APN functions: Sporadic examples, Edel Kyureghyan Pott, Browning-Dillon et al, Edel-Pott non-quadratic, Cannon et al.

Infinite families since discovered are:

(due to Budeghyan, Leander, Carlet, Felke, Pott, McGuire, Byrne, Bracken, Markin,...apologies...)

$x^{2^i+1}+ux^{2^{k+i}+2^{k(r-1)}}$ (BCFL) (BCL)

$ux^{2^{-k}+2^{k+s}}+u^{2^k}x^{2^s+1}+vx^{2^{k+s}+2^s}$ (BBMM)

$bx^{2^s+1}+b^{2^k}x^{2^{k+s}+2^k}+cx^{2^k+1}$ (BBMM)

$x^3+\mathrm{Tr}(x^9)$ (BCL)

$u^{2^k}x^{2^{-k}+2^{k+s}}+ux^{2^s+1}+vx^{2^{k+s}+2^s}$ (BBMM)

$u^{2^k}x^{2^{-k}+2^{k+s}}+ux^{2^s+1}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^{k+s}+2^s}$ (BBMM)

General Speculation

Could it be that there are a finite number of sporadic APN functions, and some infinite families ?

General Speculation

The study of APN functions is a Goldilocks story...

There are not too many APNs, not too few APNs, the number is just right!

General Speculation

The study of APN functions is a Goldilocks story...

There are not too many APNs, not too few APNs, the number is just right!

The topic continues to surprise us.

The Equivalence Problem

If you find an APN function, how do you know it is new?
Proving by hand the equivalence (or inequivalence) of two APN functions seems to be very difficult.
We have no good theoretical techniques.
Computing code invariants such as the weight distribution, automorphism group, is not always possible theoretically. Can be done for small n by computer.

The Equivalence Problem

If you find an APN function, how do you know it is new?
Proving by hand the equivalence (or inequivalence) of two APN functions seems to be very difficult.
We have no good theoretical techniques.
Computing code invariants such as the weight distribution, automorphism group, is not always possible theoretically. Can be done for small n by computer.

We have been able to compute the weight distribution for all but one of the infinite families, and they are all the same!

The Equivalence Problem

If you find an APN function, how do you know it is new?
Proving by hand the equivalence (or inequivalence) of two APN functions seems to be very difficult.
We have no good theoretical techniques.
Computing code invariants such as the weight distribution, automorphism group, is not always possible theoretically. Can be done for small n by computer.

We have been able to compute the weight distribution for all but one of the infinite families, and they are all the same!

Results:
Bracken-Byrne-Markin-M (2007): $x^3 + Tr(x^9)$ has same weight distribution as x^3.
Bracken-Byrne-Markin-M (2007): The binomials of Budaghyan, Carlet, Felke, Leander have same weight distribution as x^3.
Bracken-Byrne-Markin-M (2007): The trinomials of BBMM have same weight distribution as x^3.

n=12

$2^{24} \times 2^{24}$ matrices

Family	Function	Delta-Rank
Gold	x^3	7550
Gold	x^{33}	7550
Kasami-Welch	x^{993}	62550
1	$u^{16}x^{768} + ux^{33}$	7816
2	$x^3 + u^7x^{528}$	7822
5	$x^3 + x^{65} + ux^{129} + u^{64}x^{66} + u^3x^{130} + x^{192}$	7550
6	$x^3 + \mathrm{Tr}(x^9)$	7846
7	$u^{16}x^{768} + ux^{33} + u^{290}x^{544}$	7900
8	$u^{16}x^{768} + ux^{33} + x^{257}$	7900
9	$u^{16}x^{768} + ux^{33} + x^{257} + u^{290}x^{544}$	7900

Equivalence Results

First - all the infinite families have been confirmed to be pairwise inequivalent by computer. Not proved by hand generally.

Equivalence Results

First - all the infinite families have been confirmed to be pairwise inequivalent by computer. Not proved by hand generally.

Second - we have one recent theoretical result.

Theorem (Bracken-Byrne-M-Nebe)

The APN trinomial functions

$$bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^k+1}$$

are not equivalent to Gold functions.

Proof uses the automorphism groups of both codes.
Now I'll give more details.

Equivalence Results

Conjecture (Edel)

If two quadratic APN functions are CCZ equivalent, then they are EA equivalent.

Equivalence Results

Conjecture (Edel)

If two quadratic APN functions are CCZ equivalent, then they are EA equivalent.

Theorem (Bracken-Byrne-M-Nebe)

True if one of the functions is a Gold function.
In other words, if a quadratic APN function is CCZ equivalent to a Gold function, then it is EA equivalent to that Gold function.

This is proved for some functions "directly" in some papers (e.g. Budaghyan Carlet Leander binomials).
Our proof uses the fact that we know the exact automorphism group of the Gold codes (Berger, and classification of finite simple groups), and any quadratic APN function has the additive group of the field in its automorphism group.

Sketch of Proof:
Let E be the additive group of the field $K = GF(2^n)$.
Show that normalizer of E in $Sym(2^n)$ is $\mathcal{A} = E \cdot GL_n(\mathbb{F}_2)$.
Use (Cannon-Nebe)

Theorem

$\mathcal{A}$ acts on $\{C_f \mid f : K \to K\}$. Functions f and g are EA equivalent functions if and only if the codes C_f and C_g are in the same $\mathcal{A}$-orbit.

Use uniqueness of E as subgroup of

$$\mathcal{G} := Aut(C_g) \cong (K, +) : K^* : Gal(K/\mathbb{F}_2).$$

(g is Gold function)

Equivalence Results

If f and h are CCZ-equivalent, there is $\pi \in Sym(2^n)$ such that $\pi(C_f) = C_h$.
The subgroup $E \leq Aut(C_f)$ is hence conjugated to $\pi E \pi^{-1} \leq Aut(C_h)$.
By uniqueness of E this implies that π normalizes E, and hence $\pi \in Normalizer(E) = \mathcal{A}$.
This means that the two functions are EA-equivalent.

Equivalence Results

More generally

Theorem

Let h be a quadratic APN-function such that $Aut(C_h)$ is isomorphic to a subgroup of $\mathcal{G}$. Then all quadratic APN-functions that are CCZ equivalent to h are indeed EA equivalent to h.

Equivalence Results

More generally

Theorem

Let h be a quadratic APN-function such that $Aut(C_h)$ is isomorphic to a subgroup of $\mathcal{G}$. Then all quadratic APN-functions that are CCZ equivalent to h are indeed EA equivalent to h.

This method will not generalize completely, because there are functions whose automorphism group is not contained in $\mathcal{G}$.

$$h_1 := x^3 + x^5 + u^{62}x^9 + u^3x^{10} + x^{18} + u^3x^{20} + u^3x^{34} + x^{40}$$

Then h_1 is APN on $GF(2^6)$ and $|Aut(C_{h_1})| = 2^6.5$, which is not a divisor of $2^6(2^6 - 1)6$. (Dillon)

The Dillon-Wolfe example is very exciting.
Where did it come from ...

Theorem (Browning-Dillon-Kibler-McQuistan (2007))

The following are equivalent.

$$1.\ f \textit{ is CCZ equivalent to an APN permutation}$$

$$2. C_f^{\perp} \textit{ is an extended double simplex code of dimension 6}$$

So to find an APN permutation we want to write $C_f^{\perp} = W_1 \oplus W_2$ where each W_i is a simplex code.
This paper told us how to find APN permutations...

Classification Result

Call d exceptional if x^d is APN on infinitely many extensions of $\mathbb{F}_2$. (Dillon)

Conjecture: the only exceptional exponents d are Gold and Kasami-Welch.

Building on work of van Lint, Wilson, Janwa, McGuire, Jedlicka, we have a proof:

Theorem (M, Fernando Hernando)

The conjecture is true.

Proof uses Weil bound.

Classification Result

Call d exceptional if x^d is APN on infinitely many extensions of $\mathbb{F}_2$. (Dillon)

Conjecture: the only exceptional exponents d are Gold and Kasami-Welch.

Building on work of van Lint, Wilson, Janwa, McGuire, Jedlicka, we have a proof:

Theorem (M, Fernando Hernando)

The conjecture is true.

Proof uses Weil bound.

Conjecture: The Gold and Kasami-Welch are the only APN functions which are APN on infinitely many extensions of their field of definition.

Definitions

Recall that f is a PN function iff

$$f(x+a) - f(x) = f(y+a) - f(y) \implies a = 0 \text{ or } x = y.$$

Definitions

Definition (Costas permutation)

Let $[n] = \{0, \ldots, n-1\}$, considered as a subset of $\mathbb{Z}$, and let $f : [n] \to [n]$ be a permutation. We say that f is a Costas permutation iff

$$f(i+k) - f(i) = f(j+k) - f(j) \implies k = 0 \text{ or } i = j$$

for all $i, j, k \in [n]$ such that $i + k, j + k \in [n]$.

Note that the implication is not required to hold if one of $i, j, k, i + k, j + k$ is outside the set $[n]$.

Definition (Costas permutation)

Let $[n] = \{0, \ldots, n-1\}$, considered as a subset of $\mathbb{Z}$, and let $f : [n] \to [n]$ be a permutation. We say that f is a Costas permutation iff

$$f(i+k) - f(i) = f(j+k) - f(j) \implies k = 0 \text{ or } i = j$$

for all $i, j, k \in [n]$ such that $i+k, j+k \in [n]$.

Note that the implication is not required to hold if one of $i, j, k, i+k, j+k$ is outside the set $[n]$.

The similarity between this definition and the definition of a PN function motivated the paper
"APN Permutations on $\mathbb{Z}_n$ and Costas Arrays" Konstantinos Drakakis, Rod Gow, Gary McGuire, accepted Discrete Applied Mathematics.

Exponential Welch construction

Let $\mathbb{Z}_p$ be the finite field of prime order p, $p > 2$, and let g be a primitive root of $\mathbb{Z}_p$.

Exponential Welch construction

Let $\mathbb{Z}_p$ be the finite field of prime order p, $p > 2$, and let g be a primitive root of $\mathbb{Z}_p$.
Consider the function $f : \mathbb{Z}_{p-1} \longrightarrow \mathbb{Z}_p$ defined by the formula

$$f(i) = g^i.$$

The values of f lie in $\mathbb{Z}_p \setminus \{0\}$.

Exponential Welch construction

Let $\mathbb{Z}_p$ be the finite field of prime order p, $p > 2$, and let g be a primitive root of $\mathbb{Z}_p$.
Consider the function $f : \mathbb{Z}_{p-1} \longrightarrow \mathbb{Z}_p$ defined by the formula

$$f(i) = g^i.$$

The values of f lie in $\mathbb{Z}_p \setminus \{0\}$.
In order to get a (bijective) function from $[p-1]$ to $[p-1]$, we subtract 1 from the values of f. Denote the resulting function by f again.

Exponential Welch construction

Let $\mathbb{Z}_p$ be the finite field of prime order p, $p > 2$, and let g be a primitive root of $\mathbb{Z}_p$.
Consider the function $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_p$ defined by the formula

$$f(i) = g^i.$$

The values of f lie in $\mathbb{Z}_p \setminus \{0\}$.
In order to get a (bijective) function from $[p-1]$ to $[p-1]$, we subtract 1 from the values of f. Denote the resulting function by f again.Finally, consider f as a function $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$.

Exponential Welch construction

Example

Let $p = 7$, and we will use $g = 3$ as our primitive element, so $f(i) = 3^i$. The sequence 3^i modulo 7, $i = 0, 1, \ldots, 5$, is

$$1, 3, 2, 6, 4, 5.$$

Subtracting 1 gives

$$0, 2, 1, 5, 3, 4$$

which we now consider as elements of $\mathbb{Z}_6$.

The periodic differences $f(i+1) - f(i)$, $i = 0, 1, \ldots, 5$ as *integers* are

$$2, -1, 4, -2, 1, -4.$$

These differences modulo 6 are

$$2, 5, 4, 4, 1, 2.$$

No number appears more than twice, by the APN property.

APN Permutations

Theorem (Drakakis, Gow, M)

Exponential Welch Costas functions are APN permutations on $\mathbb{Z}_{p-1}$.

Choosing $p = 17$ gives an APN permutation on $\mathbb{Z}_{16}$.
($\mathbb{Z}_{16}$ used e.g. in GOST)
Choosing $p = 257$ gives an APN permutation on $\mathbb{Z}_{256}$.
($\mathbb{Z}_{256}$ used e.g. in SAFER)

Nonlinearity

Another requirement of an S-box is that it be resistant to linear cryptanalysis. This requires that the function have a high nonlinearity.

Let $f : A \longrightarrow B$ be a function between finite abelian groups.

We use isomorphisms $\alpha \mapsto \chi_\alpha$ from A to $\hat{A}$ (the group of characters of A) and $\beta \mapsto \psi_\beta$ from B to $\hat{B}$.

Another requirement of an S-box is that it be resistant to linear cryptanalysis. This requires that the function have a high nonlinearity.
Let $f : A \longrightarrow B$ be a function between finite abelian groups.
We use isomorphisms $\alpha \mapsto \chi_\alpha$ from A to $\hat{A}$ (the group of characters of A) and $\beta \mapsto \psi_\beta$ from B to $\hat{B}$.

We define the value of the Fourier transform of f at $\alpha \in A$ and $\beta \in B$ by

$$\hat{f}(\alpha, \beta) = \sum_{a \in A} (\psi_\beta \circ f)(a)\ \chi_\alpha(a) \quad \text{for all } \alpha \in A. \tag{1}$$

Nonlinearity

Another requirement of an S-box is that it be resistant to linear cryptanalysis. This requires that the function have a high nonlinearity.

Let $f : A \longrightarrow B$ be a function between finite abelian groups. We use isomorphisms $\alpha \mapsto \chi_\alpha$ from A to $\hat{A}$ (the group of characters of A) and $\beta \mapsto \psi_\beta$ from B to $\hat{B}$.

We define the value of the Fourier transform of f at $\alpha \in A$ and $\beta \in B$ by

$$\hat{f}(\alpha, \beta) = \sum_{a \in A} (\psi_\beta \circ f)(a)\ \chi_\alpha(a) \quad \text{for all } \alpha \in A. \tag{1}$$

We define the *linearity* of f by

$$\mathbb{L}(f) = \max_{\alpha \in A, \beta \in B^*} |\hat{f}(\alpha, \beta)|. \tag{2}$$

Nonlinearity

In the special but important for us case where $A = B = \mathbb{Z}_m$, the characters are the functions $\chi_j : \mathbb{Z}_m \to \mathbb{C}$, $j \in \mathbb{Z}_m$, where

$$\chi_j(k) = e^{\frac{2\pi ijk}{m}}, \text{ with } k \in \mathbb{Z}_m.$$

It follows then from (1) that

$$\hat{f}(\alpha, \beta) = \sum_{x \in \mathbb{Z}_m} e^{\frac{2\pi i}{m}(\beta f(x) + \alpha x)}. \tag{3}$$

Recall

$$\mathbb{L}(f) = \max_{\alpha \in A, \beta \in B^*} |\hat{f}(\alpha, \beta)|. \tag{4}$$

Nonlinearity

Theorem

If $f : \mathbb{Z}_m \to \mathbb{Z}_m$ *then* $\sqrt{m} \leq \mathbb{L}(f) \leq m$.

(This follows from Parseval's identity.)

We want functions with small linearity (highly nonlinear).

Nonlinearity

Theorem

If $f : \mathbb{Z}_m \to \mathbb{Z}_m$ *then* $\sqrt{m} \leq \mathbb{L}(f) \leq m$.

(This follows from Parseval's identity.)
We want functions with small linearity (highly nonlinear).

Question: what is the linearity of the Exponential Welch Costas permutations?

"On the Nonlinearity of Exponential Welch Costas Functions," Konstantinos Drakakis, Verónica Requena, Gary McGuire, accepted IEEE Transactions Info. Theory.

Nonlinearity of EWC Functions

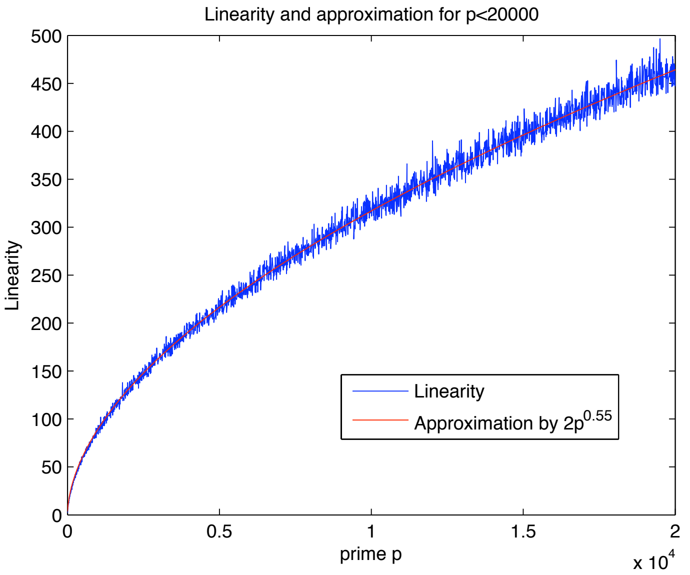
We proved that the linearity is independent of the primitive root.

We computed the linearity of EWC functions for all primes up to 2,000. The results suggest the following conjecture:

Conjecture

A pair (α, β) that maximizes $|\hat{f}(\alpha, \beta)|$ always satisfies the condition that either $\alpha = \frac{n}{2}$ or $\beta = \frac{n}{2}$.

$(n = p - 1)$



This assumes the conjecture.

Nonlinearity of EWC Functions

There are 40 primes less than 50,000 where the maximum occurs at a pair with both $\alpha = \frac{n}{2}$ and $\beta = \frac{n}{2}$, namely 3, 11, 59, 131, 251, 419, 971, 1091, 1811, 1979, 2939, 3251, 4091, 4259, 5099, 6299, 6971, 8291, 8819, 9539, 10139, 10331, 11171, 12011, 12899, 13859, and 19379, 20411, 22571, 23099, 26171, 27011, 28019, 28859, 31379, 31391, 41051, 48179, 48611, 49451

We relate this to the class number $h(-p)$ on the next slide, and this relation potentially implies that the linearity of EWC functions is a rather complicated quantity. Also we have:

Nonlinearity of EWC Functions

There are 40 primes less than 50,000 where the maximum occurs at a pair with both $\alpha = \frac{n}{2}$ and $\beta = \frac{n}{2}$, namely 3, 11, 59, 131, 251, 419, 971, 1091, 1811, 1979, 2939, 3251, 4091, 4259, 5099, 6299, 6971, 8291, 8819, 9539, 10139, 10331, 11171, 12011, 12899, 13859, and 19379, 20411, 22571, 23099, 26171, 27011, 28019, 28859, 31379, 31391, 41051, 48179, 48611, 49451

We relate this to the class number $h(-p)$ on the next slide, and this relation potentially implies that the linearity of EWC functions is a rather complicated quantity. Also we have:

Theorem (Drakakis, Gow, M)

Let f be an EWC function; then, $\hat{f}(\alpha, \beta) = 0$ if $\beta = (p-1)/2$ and α is even.

Nonlinearity of EWC Functions

Theorem (Drakakis, Requena, M)

Let f be an EWC function. Then

$$\left|\hat{f}\left(\frac{p-1}{2},\frac{p-1}{2}\right)\right| = \begin{cases} 0, & \textit{if } p \equiv 1 \bmod 4; \\ 2h(-p), & \textit{if } p \equiv 7 \bmod 8; \\ 6h(-p), & \textit{if } p \equiv 3 \bmod 8. \end{cases}$$

Proof uses a result from Drakakis-Gow-Rickard, "Parity properties of Costas arrays defined via finite fields" In Advances in Mathematics of Communications.

Nonlinearity of EWC Functions

Theorem (Drakakis, Requena, M)

Let f be an EWC function. Then

$$\left|\hat{f}\left(\frac{p-1}{2},\frac{p-1}{2}\right)\right| = \begin{cases} 0, & \text{if } p \equiv 1 \bmod 4; \\ 2h(-p), & \text{if } p \equiv 7 \bmod 8; \\ 6h(-p), & \text{if } p \equiv 3 \bmod 8. \end{cases}$$

Proof uses a result from Drakakis-Gow-Rickard, "Parity properties of Costas arrays defined via finite fields" In Advances in Mathematics of Communications.

This value is the actual nonlinearity for the 40 primes previously mentioned.

Nonlinearity of EWC Functions

So $6h(-p)$ is the actual nonlinearity for the following primes up to 50,000.

3, 11, 59, 131, 251, 419, 971, 1091, 1811, 1979, 2939, 3251, 4091, 4259, 5099, 6299, 6971, 8291, 8819, 9539, 10139, 10331, 11171, 12011, 12899, 13859, 19379, 20411, 22571, 23099, 26171, 27011, 28019, 28859, 31379, 31391, 41051, 48179, 48611, 49451

If you can see a pattern, let me know!
It would be interesting to know if there are infinitely many such primes. Asymptotics of $h(-p)$ compared to $2p^{0.55}$ might be relevant here.