A superclass of self-dual codes and bijective S-boxes[1]

Patrick Solé,
Telecom ParisTech, Paris, France
and
King Abdulaziz University, Jeddah, Saudia Arabia

KIAS, Seoul, South Korea, November 2012

[1] joint work with Claude Carlet, Philippe Gaborit,Jon-Lark Kim

Motivation: differential power analysis

Physical implementation of cryptosystems on devices such as smart cards leaks information.
This information can be used in differential power analysis (DPA), as was shown by Kocher in Crypto 99.
This kind of attack consists in monitoring the power consumption of the physical device and gathering information on the value of variables occurring in the computation.
These attacks can be devastating if proper counter-measures are not included in the implementation.
This kind of attack belongs to the general context of side-channel attacks .

Boolean masking

Boolean masking, a natural countermeasure, consists in a kind of secret-sharing method changing the variable x say into randomized shares

$$m_1, m_2, \cdots, m_{d+1}$$

called masks such that

$$x = m_1 + m_2 + \cdots + m_{d+1}$$

where $+$ is a group operation - in practice, the XOR.
Since the difficulty of performing an attack of order d (involving $d+1$ shares) increases exponentially with d, it was believed until recently that for increasing the resistance to attacks, new masks have to be added, thereby increasing the order of the countermeasure.
This is both costly in terms of hardware and unsecure (masks refreshing operation)!

Leakage squeezing

Now, it is shown by Carlet (Paris 8) and Danger/ Guilley/Maghrebi (ENST) that another option consists in encoding the masks, which is much less costly in memory resources than adding fresh masks. At the order one , this consists in representing x by the ordered pair $(F(m), x + m)$, where F is a a special type of (bijective) *vectorial Boolean function* called Graph Correlation Immune by Carlet, because $(x, F(x))$ is called the graph of the function F.

Graph Correlation Immune Boolean functions

Wanted: Boolean S-boxes - that is,
permutations $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$,
such that, given some integer d as large as possible,
for every pair of vectors $a, b \in \mathbb{F}_2^n$ such that (a, b) is nonzero and has Hamming weight $< d$, the value of the Walsh transform of F at (a, b) is null.

$$\widehat{F}(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x} = 0$$

We call such functions d-GCI, for Graph Correlation Immune.
Question: Can Coding Theory help to construct such functions?

Systematic Codes

An (unrestricted) binary code C of length N is just a set of vectors of $\mathbb{F}_2^N$.
It is systematic if there exists $I \subseteq [n]$ such that the projection of C on I is one to one and the image of C is 2^I.
The set I is then said to be an **Information set** for C.
The generator matrix of a linear $[2n, n]$ code is said to be in **systematic form** if it is blocked as (I, A) with I the identity matrix of order n. If A is circulant then C is said to be **double circulant.**

Self dual Codes

If C is a linear code, its dual $C^\perp$ is understood w.r.t. the standard inner product. The code C is *self dual* if $C = C^\perp$. The *Hamming weight* $w(z)$ of a binary vector z is the number of its nonzero entries. The *weight enumerator* $W_C(x,y)$ of a code C is the homogeneous polynomial defined by

$$W_C(x,y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)}.$$

The code C is *formally self dual* or FSD for short, if its weight enumerator is invariant under the MacWilliams transform, that is

$$W_C(x,y) = W_C\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right).$$

Complementary Information Set Codes

A binary linear code of length $2n$ and dimension n is said to be **Complementary Information Set** (CIS for short) with a partition L, R if there is an information set L whose complement R is also an information set.
Call the partition $[1..n]$, $[n+1..2n]$ the **systematic partition.**
Since the complement of an information set of a linear code is an information set for its dual code, it is clear that systematic self-dual codes are CIS with the systematic partition.
It is also clear that the dual of a CIS code is CIS.
Hence CIS codes are a natural generalization of self-dual codes.

CIS codes and CGI functions

We attach to a vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ the code C_F of length $2n$ defined as

$$C_F = \{(x, F(x)) | \, x \in \mathbb{F}_2^n\}.$$

Note that C_F is CIS iff F is a permutation.
If F is linear then the generator matrix of C_F is of the form (I, A) with A non singular.

Theorem

The permutation $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a d-GCI function of n variables iff the code C_F has dual distance $\geq d$.

Delsarte's dual distance

If C is a binary code, let B_i denote its distance distribution, that is,

$$B_i = \frac{1}{|C|}|\{(x, y) \in C \times C \mid d(x, y) = i\}|$$

The dual distance distribution $B_i^\perp$ is the MacWilliams transform of the distance distribution, in the sense that

$$D_C^\perp(x, y) = \frac{1}{|C|} D_C(x + y, x - y),$$

where

$$D_C(x, y) = \sum_{i=0}^{n} B_i x^{n-i} y^i,$$

and

$$D_C^\perp(x, y) = \sum_{i=0}^{n} B_i^\perp x^{n-i} y^i.$$

The **dual distance** of C is the smallest $i > 0$ such that $B_i^\perp \neq 0$. When C is linear, it is the minimum distance of $C^\perp$, since $D_C^\perp(x, y) = D_{C^\perp}(x, y)$.

Sketch of proof

The proof follows immediately by the characterization of the dual distance of a code C in terms of characters $\chi_u(C)$

$$\chi_u(C) = \sum_{v \in C} (-1)^{u.v}$$

of C regarded as an element in the group algebra $\mathbb{Q}[\mathbb{F}_2]$.
Essentially, this characterization says that $d^\perp$ if the smallest non zero weight of a $u \in \mathbb{F}_2^n$ such that $\chi_u(C) \neq 0$.
Note that the value of the **Walsh transform** of F at (a, b) is $\chi_u(C)$ for $u = (a, b)$ and $C = C_F$.

Background on $\mathbb{Z}_4$-codes

A $\mathbb{Z}_4$-code of length n is a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$.
Recall that the **Gray map** ϕ from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$ is defined by

$$\phi(0) = 00, \phi(1) = 10, \phi(3) = 01, \phi(2) = 11.$$

This (nonlinear!) map is extended component wise from $\mathbb{Z}_4^n$ to $\mathbb{F}_2^{2n}$.
The **Gray image** $\phi(C)$ of a $\mathbb{Z}_4$-code C is just $\{\phi(c) | \, c \in C\}$.
The Lee distance d_L of C is the Hamming distance of $\phi(C)$.
In general a $\mathbb{Z}_4$-code C is of type $4^k 2^l$ if $C \approx \mathbb{Z}_4^k \mathbb{Z}_2^l$ as additive groups.
A $\mathbb{Z}_4$-code is called **free** if $l = 0$.

Background on $\mathbb{Z}_4$-codes II

An important class of $\mathbb{Z}_4$-codes is that of $QR(p+1)$ where QR stands for **Quadratic Residue codes** and p is a prime congruent to ± 1 modulo 8. They were introduced as **extended cyclic** codes, based on **Hensel lifting** of classical binary quadratic residue codes. Recall that if $n \equiv \pm 1 \pmod 8$, these are cyclic codes of length n and generator g with $x^n + 1 = (x+1)g(x)h(x)$ and

$$g(x) = \prod_{i=\square}(x - \alpha^i),$$

with $\alpha^n = 1$.
Example: $x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$
lifts into
$x^7 - 1 = (x-1)(x^3 + 2x^2 + x - 1)(x^3 - x^2 + 2x - 1)$.

Non linear CIS codes from $\mathbb{Z}_4$−codes

Define a free $\mathbb{Z}_4$-code of length $2n$ with 2^n codewords to be CIS if it contains two disjoint information sets.

Theorem

If $\mathcal{C}$ is a free systematic $\mathbb{Z}_4$-code of length $2n$ with 2^n codewords, then its binary image is a systematic code of the form C_F for some F. Furthermore, $\mathcal{C}$ is CIS with systematic partition if and only if F is one-to-one.

Old Examples I:

Example

Consider the Nordstrom Robinson code in length 16*, a systematic code of distance* 6 *with* 256 *codewords*
twice as many as the best linear code with that length and distance.
It is the Gray image of the octacode , which is free and CIS as self dual.
It therefore can be attached to a 6*-GCI function in* 8 *variables, when the best linear CIS code only gives a* 5*-GCI function.*

Old Examples II:

The octacode is the Hensel lift of the binary QR(7). For larger primes we have

Example

Consider QR24 a self-dual extended cyclic $\mathbb{Z}_4$-code. Its binary image of length 48 *has distance* 12, *which is as good as the best* $[48, 24]$ *binary self-dual code (also a QR code!).*
Consider QR32 a self-dual extended cyclic $\mathbb{Z}_4$-code. Its binary image of length 64 *has distance* 14, *which is better than the best known* $[64, 32]$ *binary code of distance* 12.
Similarly, QR48 has a binary image of distance 18, *when the best binary rate one half code of length* 96 *has distance* 16.

Recent Example:

Example

Recently, Kiermaier and Wassermann have computed the Lee weight enumerator of the Type II $\mathbb{Z}_4$*-code* $QR80$
and its minimum Lee weight $d_L = 26$*.*
Hence its binary image has distance 26*, which is better than the best known* $[160, 80]$ *binary code of distance* 24.

Constructions techniques for linear CIS codes

It is easy to see that any linear code with generator matrix (I, A) is CIS if A is nonsingular.
Conversely any CIS code can be cast into that form.
If A is circulant with attached polynomial $f \in \mathbb{F}_2[x]$ then A is nonsingular iff $GCD(f, x^n - 1) = 1$.
If A is the adjacency matrix of a Strongly Regular Graph or a Doubly regular Tournament then it satisfies a quadratic equation that allows to give sufficient conditions for regularity.

Combinatorial matrices:

Let A be an integral matrix with 0, 1 valued entries. We shall say that A is the adjacency matrix of a **strongly regular graph** (SRG) of parameters $(n, \kappa, \lambda, \mu)$ if A is symmetric, of order n, verifies $AJ = JA = \kappa J$ and satisfies

$$A^2 = \kappa I + \lambda A + \mu(J - I - A)$$

Alternatively we shall say that A is the adjacency matrix of a **doubly regular tournament** (DRT) of parameters $(n, \kappa, \lambda, \mu)$ if A is skew-symmetric, of order n, verifies $AJ = JA = \kappa J$ and satisfies

$$A^2 = \lambda A + \mu(J - I - A)$$

where I, J are the identity and all-one matrices of order n. DRT are related to skew Hadamard matrices via bordering.

And their codes

In the next result we identify A with its reduction mod 2.

Proposition

Let C be the linear binary code of length $2n$ spanned by the rows of (I, M). With the above notation, C is CIS if A is the adjacency matrix of a

- *SRG of odd order with κ, λ both even and μ odd and if $M = A + I$*
- *DRT of odd order with κ, μ odd and λ even and if $M = A$*
- *SRG of odd order with κ even and λ, μ both odd and if $M = A + J$*
- *DRT of odd order with κ even and λ, μ both odd and if $M = A + J$*

Quadratic Double Circulant codes

Let q be an odd prime power. Let Q be the q by q matrix with zero diagonal and $q_{ij} = 1$ if $j - i$ is a square in $GF(q)$ and zero otherwise.

Corollary

If $q = 8j + 5$ then the span of $(I, Q + I)$ is CIS.
If $q = 8j + 3$ then the span of (I, Q) is CIS.

It is well-known that $q = 4k + 1$ then Q is the adjacency matrix of a SRG with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$.
If $q = 4k + 3$ then Q is the adjacency matrix of a DRT with parameters $(q, \frac{q-1}{2}, \frac{q-3}{4}, \frac{q+1}{4})$.
The result follows by the above Proposition.
The codes obtained in that way are Quadratic Double Circulant codes

Cyclic codes

Denote by C_i the code C shortened at coordinate i
and by $\overline{C}$ the extension of C by an overall parity check.

Proposition

Let C be a cyclic binary code of odd length N, and dimension $\frac{N+1}{2}$. If its generator matrix is in circulant form, both C_1 and C_N are CIS with the systematic partition. If, furthermore, the weight of the generator polynomial is odd, then $\overline{C}$ is CIS with the systematic partition.

Recall that in a cyclic code of dimension k, consecutive k indices form an information set.
The result follows then for C_1 and C_N. In the extended case, the generator matrix of $\overline{C}$ is obtained from that of C by juxtaposing to the right, say, a column of 1's.
It consists then of two juxtaposed triangular, non singular matrices.

Rank conditions for Counter Examples:

Proposition

If a $[2n, n]$ *code* C *has generator matrix* (I, A) *with* $rk(A) < n/2$ *then* C *is* not CIS .

Two different information sets must have more than $n/2$ elements on the left.
Therefore they must intersect non trivially.
We generalize this observation in the next result.

Rank criterion for linear codes

Theorem

Let Σ *denote the set of columns of the generator matrix of a* $[2n, n]$ *linear code* C*.*
C *is CIS iff* $\forall B \subseteq \Sigma,\ rk(B) \geq |B|/2$.

The proof uses **matroid** theory and Edmonds' matroid base packing theorem: A matroid on a set S contain k disjoint bases iff

$$\forall U \subseteq S,\ k(rk(S) - rk(U)) \leq |S \setminus U|.$$

Apply to the matroid of the columns of the generator matrix under linear dependence, with

$$S = \Sigma,\ k = 2,\ rk(\Sigma) = n,\ |\Sigma| = 2n.$$

Dual distance conditions for Counterexamples:

Proposition

If C is a $[2n, n]$ code whose dual has minimum weight 1 then C is not CIS.

If the dual of C has minimum weight 1 then the code C has a zero column and therefore cannot be CIS.

The previous proposition permits to show it is possible for an optimal code not to be CIS.

Record breakers

We have looked at CIS codes for $2n \leq 130$ by using tables of best linear codes (`www.codetables.de`)
and best self dual codes (Cf. Gaborit Homepage).
The Magma package $BKLC(GF(2), 2n, n))$ provides a code corresponding to the entry in Grassl table.

- The best CIS codes we found are either optimal or best known
- The first length where a non SD optimal CIS code appears is 6: an optimal $[6, 3, 3]$
- The first length where a non FSD optimal CIS code appears is 20 an optimal $[20, 10, 6]$
- The first length where a non CIS BKLC appears is 34 where the $[34, 17, 8]$ has dual distance 1.

Classification

Let $n \geq 2$ be an integer and g_n denote the cardinal of $GL(n,2)$ the general linear group of dimension n over $GF(2)$. It is well-known that

$$g_n = \prod_{j=0}^{n-1} (2^n - 2^j).$$

Proposition

The number e_n of equivalence classes of CIS codes of dimension $n \geq 2$ is at most $g_n/n!$.

The numbers $g_n/n!$ grow very fast: 3, 28, 849, 83328. They count the number of bases of $\mathbb{F}_2^n$ over $\mathbb{F}_2$.
It is easy to see that $e_1 = 1$ and $e_2 = 2$.

Building up Construction I

Proposition (Building up construction)

Suppose that C is a $[2n, n]$ CIS code C with generator matrix $(I_n|A)$, where A has n rows $r_1, \ldots, r_n$. Then for any two vectors $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)^T$ the following matrix G_1 generates a $[2(n+1), n+1]$ CIS code C_1

$$G_1 = \left(\begin{array}{c|cccc|c|c} 1 & 0 & 0 & \cdots & 0 & z_1 & x \\ \hline 0 & 1 & 0 & \cdots & 0 & y_1 & r_1 \\ 0 & 0 & 1 & \cdots & 0 & y_2 & r_2 \\ \vdots & & & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & y_n & r_n \end{array}\right), \tag{1}$$

where c_i's satisfy $x = \sum_{i=1}^{n} c_i r_i$ and $z_1 = 1 + \sum_{i=1}^{n} c_i y_i$.

Building up Construction II

Let us consider a $[6,3,3]$ CIS code C whose generator matrix is given below.

$$G = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right).$$

In order to apply building up construction, we take for example $x = (1,1,1)$ and $y = (1,1,1)^T$. Then $c_1 = c_2 = 0, c_3 = 1$. Hence $z = 0$. In fact, we get the extended Hamming $[8,4,4]$ code whose generator matrix is given below.

$$G_1 = \left(\begin{array}{c|ccc|c|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right).$$

Building up Construction III

The converse is true.

Proposition

Any $[2n, n]$ *CIS code* C *is equivalent to a* $[2n, n]$ *CIS code with the systematic partition which is constructed from a* $[2(n-1), n-1]$ *CIS code by using the preceding Proposition.*

Classification results

The number of CIS codes grows faster than the number of self dual or formally self dual codes.

Table : Classification of all CIS codes of lengths up to 12 in the order of sd, non-sd fsd, and none of them

$2n$	$d = 2$	$d = 3$	$d = 4$	Total #
2	1 (1+0+0)			1
4	2 (1+1+0)			2
6	5 (1+2+2)	1 (0+1+0)		6
8	22 (1+9+12)	4 (0+2+2)	1 (1+0+0)	27
10	156 (2+40+114)	35 (0+9+26)	4 (0+2+2)	195
12	2099 (2+318+1779)	565 (0+87+478)	41 (1+7+33)	2705

Asymptotics

Let δ denote the relative minimum distance of a family of codes. Good self dual codes exist, and counting shows that they are above Varshamov-Gilbert bound that is

$$\delta \geq H^{-1}(1/2) \approx 0.11.$$

The same result can be shown directly for CIS codes without using the fact that self dual codes are a subclass.
Quebbeman has shown by using AG codes over large alphabets and projections over TOB bases that there are self dual codes constructible in polynomial time and with $\delta \approx 0.02$.

Open problems

- Classify CIS codes over other fields and rings
- Can known families of permutation polynomials help?
- QC codes of rate $1/2$ When are they CIS?
- Find good rate $1/2$ free $\mathbb{Z}_4-$codes in the range $48 - -80$
- Are there good long codes of rate $1/2$ that are NOT CIS?
- AG constructions of CIS codes better than AG constructions of SD codes

Conclusion

We have introduced CIS codes a very basic generalization of self dual codes, but still warranting further exploration.
Invariant theory cannot be applied but a mass formula might be possible.
Boolean masking might be the first honest engineering application of self dual codes.