Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes

Daniel Augot and Matthieu Finiasz

- Diffusion layers in a block cipher/SPN should:
  - obviously, offer good diffusion,
    → have a large *branch number*,
  - be efficient to evaluate,
    → both in *software* and *hardware* implementations.
  - usually, be linear,
    → simplifies analysis/security proofs.
- MDS matrices offer optimal diffusion:
  - they have the highest possible branch number,
  - but large MDS matrices are slow to evaluate
    → cannot be sparse, no symmetries...

- Recursive MDS matrices come from companion matrices,
  - such that their k-th power is MDS.

$$C = \begin{pmatrix} 0 & 1 & & 0 \\ 0 & & \ddots & \\ 0 & 0 & & 1 \\ c_0 & c_1 & \dots & c_{k-1} \end{pmatrix} \quad \text{and} \quad C^k \text{ is MDS.}$$

- Introduced in LED and Photon: [Guo *et al.* - Crypto 2011] [Guo *et al.* - CHES 2011]
  - compact description,
  - compact hardware implementation,
    - → can be seen as an LFSR, or a generalized Feistel,
  - efficient for well chosen c_i.

- Such matrices can be found through exhaustive search:
  - pick good/efficient values c_i,
  - check if C^k is MDS
    - → all minors (of any size) of C^k should be non-zero.

- [Sajadieh *et al.* - FSE 2012]
  → exhibit intersting 4×4 matrices.
- [Wu *et al.* - SAC 2013]
  → focus on the number of binary XORs.
- [Augot, Finiasz - ISIT 2013]
  → replace symbolic computations with GF operations.

- Such matrices can be found through exhaustive search:
  - pick good/efficient values c_i,
  - check if C^k is MDS
    $\longrightarrow$ all minors (of any size) of C^k should be non-zero.

- Pros: possible to target specific companion matrices.
  - focus more on software or hardware.

- Cons: too expensive for large matrices.
  - for a full layer diffusion in the AES, 2^{128} possiblities.
    $\longrightarrow$ It would be nice to have direct constructions.

Recursive MDS Matrices as Cyclic Codes

Understanding the Matrix Structure

- A companion matrix can be associated to a polynomial:

$$g(X) = X^k + c_{k-1}X^{k-1} + \cdots + c_1 X + c_0$$

- For $k = 3$, for example:

$$C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_0 & c_1 & c_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \multicolumn{3}{c}{X^3 \bmod g(X)} \end{pmatrix}$$

Then:

$$C^2 = \begin{pmatrix} 0 \quad 0 \quad 1 \\ X^3 \bmod g(X) \\ X^4 \bmod g(X) \end{pmatrix}, C^3 = \begin{pmatrix} X^3 \bmod g(X) \\ X^4 \bmod g(X) \\ X^5 \bmod g(X) \end{pmatrix}.$$

Understanding the Matrix Structure

- C^k is MDS iff $G = \left(\ C^k \mid \mathrm{Id}_k\ \right)$ generates an MDS code,
  - → we are looking for MDS codes generated by:

$$G = \left(\begin{array}{c|ccc} X^3 \bmod g(X) & 1 & 0 & 0 \\ X^4 \bmod g(X) & 0 & 1 & 0 \\ X^5 \bmod g(X) & 0 & 0 & 1 \end{array}\right)$$

- Each line of the matrix/codeword is a multiple of $g(X)$
  - → for some $g(X)$, this defines a cyclic code!

Understanding the Matrix Structure

- C^k is MDS iff $G = \left(C^k \mid \mathrm{Id}_k \right)$ generates an MDS code,

  ⟶ we are looking for MDS codes generated by:

$$G = \left(\begin{array}{c|ccc} X^3 \bmod g(X) & 1 & 0 & 0 \\ X^4 \bmod g(X) & 0 & 1 & 0 \\ X^5 \bmod g(X) & 0 & 0 & 1 \end{array} \right)$$

- Each line of the matrix/codeword is a multiple of $g(X)$

  ⟶ for some $g(X)$, this defines a cyclic code!

- A cyclic code is an ideal of $\mathbb{F}_q[X]/(X^n + 1)$:
  - defined by a generator $g(X)$ which divides $X^n + 1$,
  - with dimension $k = n - \deg(g)$,

  ⟶ we need polynomials $g(X)$ defining MDS cyclic codes

BCH Codes

- Computing the minimal distance of a cyclic code is hard
  - for some constructions, lower bounds exist.
- To define a BCH code over F_q:
  - pick β in some extension F_{q^m} of F_q, and integers d, ℓ
  - compute $g(X) = \mathrm{lcm}(\mathrm{Min}_{F_q}(\beta^\ell), \ldots, \mathrm{Min}_{F_q}(\beta^{\ell+d-2}))$
  - $g(X)$ defines a cyclic code of length $n = \mathrm{ord}(\beta)$

    $\longrightarrow$ its minimal distance is $\geq d$

- Computing the minimal distance of a cyclic code is hard
  - for some constructions, lower bounds exist.
- To define a BCH code over F_q:
  - pick β in some extension F_{q^m} of F_q, and integers d, ℓ
  - compute $g(X) = \mathrm{lcm}(\mathrm{Min}_{\mathsf{F}_q}(\beta^\ell), \ldots, \mathrm{Min}_{\mathsf{F}_q}(\beta^{\ell+d-2}))$
  - $g(X)$ defines a cyclic code of length $n = \mathrm{ord}(\beta)$

    $\longrightarrow$ its minimal distance is $\geq d$
- The dimension of the code is $n - \deg(g)$:
  - so, the code is MDS if $\deg(g) = d - 1$

    $\longrightarrow$ the $\beta^{\ell+i}$ need to be “mutual conjugates”.

- The input and output size of a diffusion layer are equal
  - we need a code of dimension k and length $2k$.

$$G = \underbrace{\left(\begin{array}{c|c} \quad C^k \quad & \quad \mathrm{Id}_k \quad \end{array} \right)}_{k \qquad\qquad k} \Big\} k$$

- For a BCH, we need β of order $2k$
  - impossible in a field of characteristic 2,
    $\longrightarrow$ build a longer BCH code, and shorten it.

- The input and output size of a diffusion layer are equal
  - we need a code of dimension k and length $2k$.
- Pick a element β of order $2k + z$
  - use k consecutive powers of β for a $g(X)$ of degree k,
  - shorten the code on its z last positions.

$$G = \left.\underbrace{\begin{pmatrix} X^3 \bmod g(X) \\ X^4 \bmod g(X) \\ X^5 \bmod g(X) \\ X^6 \bmod g(X) \end{pmatrix}}_{k}\underbrace{\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}}_{k+z}\right\} k+z$$

- The input and output size of a diffusion layer are equal
  - we need a code of dimension k and length $2k$.
- Pick a element β of order $2k + z$
  - use k consecutive powers of β for a $g(X)$ of degree k,
  - shorten the code on its z last positions.

$$G' = \left.\begin{pmatrix} \underbrace{\begin{matrix} X^3 \bmod g(X) \\ X^4 \bmod g(X) \\ X^5 \bmod g(X) \\ \\ \end{matrix}}_{k} & \Bigg| & \underbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ & & \end{matrix}}_{k} \end{pmatrix}\right\} k$$

- The input and output size of a diffusion layer are equal
  - we need a code of dimension k and length $2k$.
- Pick a element β of order $2k + z$
  - use k consecutive powers of β for a $g(X)$ of degree k,
  - shorten the code on its z last positions.

- Shortening removes some words from the code:
  - it can only increase its minimal distance,
  - if a code is MDS, shortening it preserves the MDS property.

Direct Constructions

A First Direct Construction

- For a base field of size $q = 2^s$:
  - pick β of order $q+1$
    - $\longrightarrow$ $q+1$ divides q^2-1 so β is always in F_{q^2},
  - appart for $\beta^0 = 1$, $\mathrm{Min}_{\mathsf{F}_q}(\beta^i)$ is always of degree 2
    - $\longrightarrow$ each β^i has a single conjugate $\beta^{qi} = \beta^{-i}$

- For a diffusion layer of k elements of F_q:
  - if k is even, use all the β^i with $i \in \left[\frac{q-k}{2}+1, \frac{q+k}{2}\right]$,
  - if k is odd, use all the β^i with $i \in \left[-\frac{k-1}{2}, \frac{k-1}{2}\right]$.

A First Direct Construction

- For a base field of size $q = 2^s$:
  - pick β of order $q+1$
    - → $q+1$ divides q^2-1 so β is always in F_{q^2},
  - appart for $\beta^0 = 1$, $\mathrm{Min}_{\mathsf{F}_q}(\beta^i)$ is always of degree 2
    - → each β^i has a single conjugate $\beta^{qi} = \beta^{-i}$

- We get a $[q+1, q+1-k, k+1]_q$ MDS BCH code
  - we shorten it on $(q+1-2k)$ positions,
  - we get a $[2k, k, k+1]_q$ MDS code,
    - → gives a $k \times k$ recursive MDS matrix.

Exhaustive Search on BCH Codes

- For a diffusion of k elements of F_q we can search all possible BCH codes in a time polynomial in q and k.

for $z \leftarrow 1$ **to** $(q+1-2k)$, **with** z *odd* **do**
    $\alpha \leftarrow$ primitive $(2k+z)$-th root of unity of F_q
    forall the $\beta = \alpha^i$ **such that** $\mathrm{ord}(\beta) = 2k+z$ **do**
        for $\ell \leftarrow 0$ **to** $(2k+z-2)$ **do**
            $g(X) \leftarrow \prod_{j=0}^{k-1}(X - \beta^{\ell+j})$
            if $g(X) \in \mathsf{F}_q[X]$ **then** *(test if g has its coefficients in F_q)*
                $\mathcal{S} \leftarrow \mathcal{S} \cup \{g(X)\}$
            end
        end
    end
end
return $\mathcal{S}$

What Was Found

- The direct construction gives symmetric solutions:
  - only $\frac{k}{2}$ different coefficients,
  - the inverse diffusion is "the same" as the diffusion,
  - No limit to the diffusion size:
    - → 1024 bits using 128 elements of F_{256},
    - → 2304 bits using 256 elements of F_{512}.

- The exhaustive search gives many solutions:
  - we rediscover many previously found matrices,
  - some are of little interest (complicated coefficients),
  - some are very nice:
    - → $\mathrm{Comp}(1, \alpha^3, \alpha, \alpha^3)^4$ is MDS (for $\alpha^4 + \alpha + 1 = 0$).

What Was Not Found

- All recursive matrices come from shortened cyclic codes:
  - but not all MDS cyclic codes are BCH codes,
    - → we could try to explore other families,
  - most cyclic codes have unknown minimal distance.
- Shortening a code can increase its minimal distance:
  - this is what happens with the Photon matrix,
  - the 4×4 matrix comes from a code of length $2^{24} - 1$:
    - → it has minimal distance 3,
    - → once shortened to a length 8, it grows to 5 (MDS).
- We need to find an explicit construction of such short matrices!