Perfect Diffusion Primitives for Block Ciphers
–
Building Efficient MDS Matrices

Pascal Junod and Serge Vaudenay

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Selected Areas in Cryptography ’04

University of Waterloo (Canada), August 9, 2004

Perfect Diffusion Primitives for Block Ciphers
–
Building Efficient MDS Matrices

Pascal Junod and Serge Vaudenay

Outline of this talk

- Preliminaries
- MDS Matrices ...
- ... and their Implementation
- Bi-Regular Arrays
- Some New Constructions

Back to Shannon

- Notions of *confusion* and *diffusion* introduced by Shannon in *"Communication Theory of Secrecy Systems" (1949)*
- Confusion: *"The method of confusion is to make the relation between the simple statistics of $E_K(.)$ and the simple description of K a very complex and involved one."*
- Diffusion: *"In the method of diffusion the statistical structure of M which leads to its redudancy is dissipated into long range statistics – i.e., into statistical structure involving long combinations of letters in the cryptogram."*

Confusion

- Notion of confusion nowadays related to the ones of
  - S-Box
  - non-linearity
  - Boolean functions
  - algebraic attacks
- Plenty of academic papers on this subject !

Diffusion : Historical Perspectives

- Less studied in a rigorous (mathematical) way until mid of 90's
- Schnorr-Vaudenay (FSE'93 / EUROCRYPT'94) : introduction of the concept of *multipermutation*
- Vaudenay (FSE'95) : a *linear* multipermutation is equivalent to an MDS code
- Daemen (PhD thesis, 1995): *Wide-Trail Strategy*
  - (Choose "good" S-boxes)
  - "*Design the round transformation in such a way that only trails with many S-boxes occur*."
- Rijmen, Daemen, Preneel, Bossalaers, De Win (FSE'96): design of SHARK whose diffusion layer is based on MDS codes

Multipermutation Nowadays

- Very few MDS codes are known
- Seldom used in practice
- Widely spread building block in symmetric schemes
- Non-linear multipermutation: CS-Cipher
- Linear multipermutation (MDS matrices): AES, Camellia, Twofish, Khazad, FOX, and many, many others !

In this Talk

- Interested in “efficient” linear multipermutations
- Brief recall about MDS matrices and their properties
- Definition of what we mean by “efficient”
- New propositions

Multipermutation: a Definition

Definition (Multipermutation)

A diffusion function f from $\mathcal{K}^p$ to $\mathcal{K}^q$ is a *multipermutation* if for any $x_1, \ldots, x_p \in \mathcal{K}$ and any integer r with $1 \leq r \leq p$, modifying r input values on $f(x_1, \ldots, x_p)$ results in modifying at least $q - r + 1$ output values.

Multipermutation: Another Definition

- **Definition (Multipermutation)**
  A diffusion function f from $\mathcal{K}^p$ to $\mathcal{K}^q$ is a *multipermutation* if the set of all words consisting of $x_1, \ldots, x_p$ concatenated with $f(x_1, \ldots, x_p)$ is a code of $(\#\mathcal{K})^p$ words of length $p + q$ with minimal distance $q + 1$.
- Matches the Singleton bound (hence the link to MDS codes)

Multipermutation: Example

- Representation of the finite field $\mathrm{GF}(2^8)$: polynomials of degree at most seven with coefficients in $\mathrm{GF}(2)$ modulo the irreducible polynomial

$$p(\xi) = \xi^8 + \xi^7 + \xi^6 + \xi^5 + \xi^4 + \xi^3 + 1$$

  - Addition: XOR
  - Multiplication: usual multiplication of polynomials modulo $p(\xi)$
- Consider the following multipermutation on $\mathrm{GF}(2^8)^2$:

$$\mu : \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & \xi \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Why is it a Multipermutation ?

- Because μ is invertible :

$$\begin{pmatrix} 1 & \xi \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \xi^7 + \xi^5 + \xi^3 & \xi^7 + \xi^5 + \xi^3 + 1 \\ \xi^7 + \xi^5 + \xi^3 & \xi^7 + \xi^5 + \xi^3 \end{pmatrix}$$

- Because, when fixing x_1 to a constant c, *both* y_1 and y_2 are permutations of x_2 :

$$\begin{aligned} y_1 &= c \oplus (\xi \cdot x_2) \\ y_2 &= c \oplus x_2 \end{aligned}$$

- Because, when fixing x_2 to a constant c, *both* y_1 and y_2 are permutations of x_1 :

$$\begin{aligned} y_1 &= x_1 \oplus (\xi \cdot c) \\ y_2 &= x_1 \oplus c \end{aligned}$$

Why is it a Multipermutation (2)?

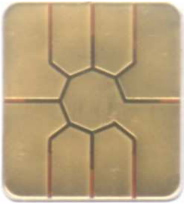
- Because $\det(\mu) \neq 0$ and every sub-determinant of μ is different of 0.

32/64-bit Architectures

- Lot of fast memory (L1 cache)
- Table lookups + XORs:

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1 \times \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \oplus \quad x_2 \times \begin{pmatrix} \xi \\ 1 \end{pmatrix}$$

8-bit Architectures



- Less memory at disposal $\rightarrow$ complete precomputation is impossible!
- The matrix elements value matters !
- Multiplications by 1 are “free” operations
- Possible to precompute the operation “multiplication by a constant c”

Our strategy

- Maximize the number of 1's in the matrix.
- Minimize the number of different constants.
- Two criteria ...
- ... among infinitely many others !
- Corollary (and disclaimer) : it is *always* possible to find an architecture and side constraints such that our strategy leads to poor results.
- One of the constraints we did **not** consider: inverse of a matrix must be "efficient" as well.

Results

- Definition of the concept of “bi-regular array”
- Find the minimal amounts of 1’s and of different coefficients for bi-regular arrays
- Sequence of constructive proofs $\longrightarrow$ matrix skeletons
- Examples of matrices

Bi-Regular Arrays

- A 2×2 array with entries in $\mathcal{K}$ is *bi-regular* if at least one row **and** one column have two different entries.

1	1
1	2

1	1
ξ	ξ

- A $q \times p$ array with entries in $\mathcal{K}$ is *bi-regular* if all 2×2 sub-arrays are bi-regular.
- An MDS matrix must be a bi-regular array ...
- ... but the converse is not true !

From Bi-Regular Arrays to MDS Matrices

- Construct a bi-regular array with large number of 1's and small number of different coefficients.
- Find a suitable set of coefficients (if possible).

Highest Possible Number of 1’s

Summary of our results

	2	3	4	5	6	7	8
2	3	4	5	6	7	8	9
3	4	6	7	8	9	10	11
4	5	7	9	10	12	13	14
5	6	8	10	12	13	14	17
6	7	9	12	13	16	18	19
7	8	10	13	14	18	21	22
8	9	11	14	17	19	22	24

Lowest Possible Number of Different Coefficients

Summary of our results

	2	3	4	5	6	7	8
2	2	2	2	3	3	3	3
3	2	2	3	3	3	3	2
4	2	3	3	3	4	4	4
5	3	3	3	3	4	4	4
6	3	3	4	4	4	4	5
7	3	3	4	4	4	4	5
8	3	4	4	4	5	5	5

A $(4,4)$-Multipermutation

- Example of "optimal" 4×4-matrix

$$\begin{pmatrix} a & 1 & 1 & 1 \\ 1 & 1 & b & a \\ 1 & a & 1 & b \\ 1 & b & a & 1 \end{pmatrix}$$

- 9 coefficients equal to 1, 3 different values
- Used as diffusive component in the round function of FOX64

A Circulating-Like $(8, 8)$-Multipermutation

- Example of a "non-optimal" 4×4-matrix

$$\begin{pmatrix} f & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & b & c & d & e & f \\ 1 & f & 1 & a & b & c & d & e \\ 1 & e & f & 1 & a & b & c & d \\ 1 & d & e & f & 1 & a & b & c \\ 1 & c & d & e & f & 1 & a & b \\ 1 & b & c & d & e & f & 1 & a \\ 1 & a & b & c & d & e & f & 1 \end{pmatrix}$$

- Used as diffusive component in the round function of FOX128

A $(8,8)$-Multipermutation with Rectangle Patterns

- Example of a "partially optimal" 8×8-matrix

$$\begin{pmatrix} b & a & c & b & d & c & 1 & d \\ b & c & a & d & b & 1 & c & 1 \\ c & b & d & a & 1 & b & 1 & c \\ c & d & b & 1 & a & 1 & b & d \\ d & c & 1 & b & 1 & a & d & b \\ d & 1 & c & 1 & b & d & a & c \\ 1 & d & 1 & c & d & b & c & a \\ 1 & 1 & d & d & c & c & b & b \end{pmatrix}$$

- Optimal number of different coefficients
- Non-optimal number of 1's

Thank You !

See you in 25 minutes for the presentation of

Any Question ?