Complete mappings over $\mathbb{F}_{2^n}$

Valentin SUDER
(Joint work with Guang GONG and Krystal GUO)

C2 Days, La Bresse.
April 24th 2017

Outline

Definitions

Definition

A mapping $x \mapsto \theta(x)$ acting over a finite abelian group $(G, \cdot)$ is called a **complete mapping** (resp. orthomorphisms) of G if **both**

$x \mapsto \theta(x)$ and $x \mapsto x \cdot \theta(x)$ (resp. $x \mapsto x^{-1} \cdot \theta(x)$) are **bijective** mappings.

In $\mathbb{F}_{p^n}$, we consider **complete mappings** (resp. orthomorphisms) over the additive group. That is, bijective mappings $x \mapsto \theta(x)$ such that $x \mapsto \theta(x) + x$ (resp. $x \mapsto \theta(x) - x$) is also bijective.

Complete mappings and **orthomorphisms** coincide over $\mathbb{F}_{2^n}$.

* complete mappings *a.k.a* complete permutations.

Notations and examples

Vectorial notation:

Let $< 1, z, z^2, \ldots, z^{n-1} >$ be a base of $\mathbb{F}_2^n$ over $\mathbb{F}_2$.
$0 \to 0,\ 1 \to 1,\ z \to 2,\ 1+z \to 3,\ \ldots,\ 1+z+\cdots+z^{n-1} \to 2^n-1.$

Consider the following mapping $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, for $n = 4$:
- as a value table:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(x)$	0	8	13	2	9	6	4	11	12	14	15	3	10	7	5	1

- as a permutation over $\mathbb{S}_{2^n}$ (when f is bijective):
$f = (1\ 8\ 12\ 10\ 15)(2\ 13\ 7\ 11\ 3)(4\ 9\ 14\ 5\ 6)$

- as a polynomial over $\mathbb{F}_{2^n}[x]$:
$f(x) = z^{10}x^{11} + z^{10}x^6 + z^3x$ (if $\mathbb{F}_{2^n}^* =< z >$)

Notations and examples

Vectorial notation:

Let $< 1, z, z^2, \ldots, z^{n-1} >$ be a base of $\mathbb{F}_2^n$ over $\mathbb{F}_2$.
$0 \to 0,\ 1 \to 1,\ z \to 2,\ 1+z \to 3,\ \ldots,\ 1+z+\cdots+z^{n-1} \to 2^n-1.$

Consider the following mapping $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, for $n = 4$:
- as a value table:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(x)$	0	8	13	2	9	6	4	11	12	14	15	3	10	7	5	1
$f(x)+x$	0	9	15	1	13	3	2	12	4	7	5	8	6	10	11	14

- as a permutation over $\mathbb{S}_{2^n}$ (when f is bijective):
$f \quad = (1\ 8\ 12\ 10\ 15)(2\ 13\ 7\ 11\ 3)(4\ 9\ 14\ 5\ 6)$
$f + \mathtt{id} = (1\ 9\ 7\ 12\ 6\ 2\ 15\ 14\ 11\ 8\ 4\ 13\ 10\ 5\ 3)$

- as a polynomial over $\mathbb{F}_{2^n}[x]$:
$f(x) = z^{10}x^{11} + z^{10}x^6 + z^3x$ (if $\mathbb{F}_{2^n}^* =< z >$)

Outline

Orthogonal Latin Squares

Definition

Two Latin Squares are called **orthogonal** if the superposition of them contains all ordered pairs.

Example: for $n = 4$,

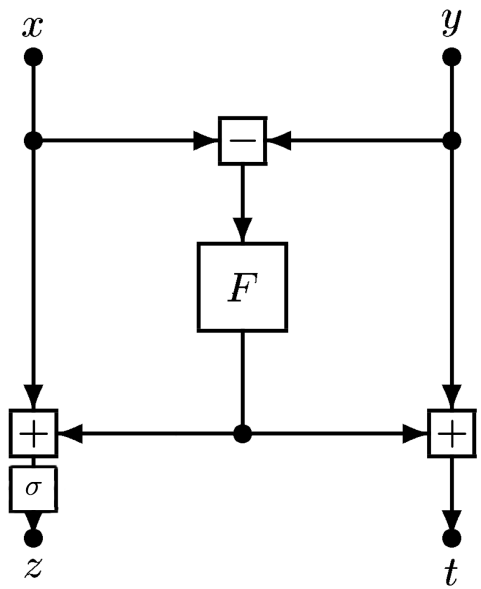
A	B	C	D
C	D	A	B
D	C	B	A
B	A	D	C

A	B	C	D
D	C	B	A
B	A	D	C
C	D	A	B

AA	BB	CC	DD
CD	DC	AB	BA
DB	CA	BD	AC
BC	AD	DA	CB

Cryptographic Applications (I)

Security proof of Lai-Massey schemes



- A 3-round **Feistel** cipher will look random to CP attack if the number of plaintext is $\ll 2^{\frac{m}{4}}$ [Luby-Rackoff'88].
- A similar result for **Lai-Massey** by adding an orthomorphism σ such that:

$$\begin{aligned} z &= \sigma(x + F(x - y)) \\ t &= y + F(x - y). \end{aligned}$$

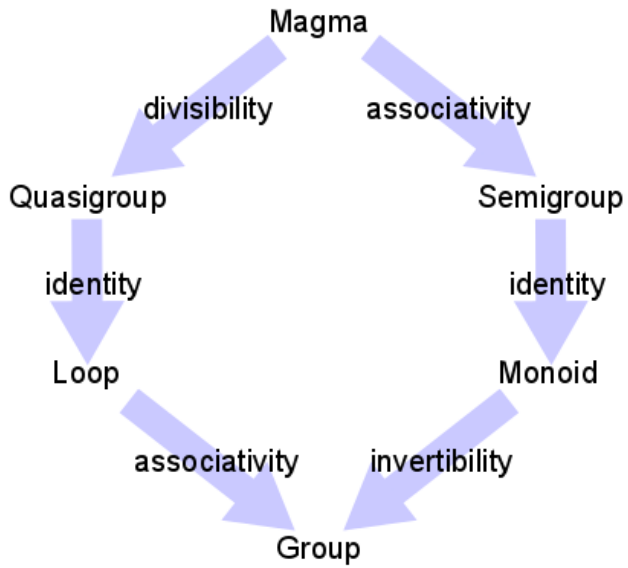
Serge Vaudenay
On the Lai-Massey Scheme,
ASIACRYPT'99, LNCS 1716, 8–19.

Cryptographic Applications (II)

Cryptography with Quasigroups

Quasigroup?

Let $(G, +)$ be a group and F an orthomorphism, then $(G, \star)$, with $x \star y = F(x - y) + y$, is a **quasigroup**.



The **extended Feistel network** over an abelian group $(G, +)$, $F_{a,b,c}$ such that

$$F_{a,b,c}(l, r) = (r + a, l + b + f(r + c)),$$

for $f : G \to G$, is an **orthomorphism**.

$\Rightarrow$ sha3 candidate **NaSha**...

Aleksandra Mileva
Cryptographic Primitives with Quasigroup Transformations,
Mathematica Balkanica 24:3-4 (2010), 207–216.

Check digit systems

EAN, ISBN, IBAN

For $a_0, \ldots, a_{n-2} \in (G, +)$ an abelian group, we can determine the **check digit** $a_{n-1} \in G$ such that:

$$p_0(a_0) + p_1(a_1) + \ldots p_{n-1}(a_{n-1}) = e, \text{ a constant } (\text{usually } 0_G),$$

$p_i : G \to G$ are **bijective functions** (usually $p_i = T^i$ for a certain T).

A **codeword** is then a sequence $a_0\, a_1\, \ldots\, a_n$ verifying this equation. We can **detect**:

- **Single errors** : iff T is bijective;
- **adjacent transpositions**: iff $T - \mathrm{id}$ is bijective;
- **Twin errors**: iff $T + \mathrm{id}$ is bijective;
- **Jump transposition**: iff $T \circ T - \mathrm{id}$ is bijective;
- **Jump twin errors**: iff $T \circ T + \mathrm{id}$ is bijective;

Outline

Generalities

Theorem*

Let $f(x) \in \mathbb{F}_{2^n}[x]$ be a complete permutation mapping. Then so are the mappings:

1. $f(x+a)+b$, for all $a, b \in \mathbb{F}_{2^n}$
2. $af(a^{-1}x)$, for all $a \in \mathbb{F}_{2^n}^*$
3. $f^{-1}(x)$

* also true over $\mathbb{F}_{p^n}$.

Proposition

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a complete mapping, then

1. f has **one and only one** fixed point, and
2. f cannot be an involution.

What else?

About **complete** mappings over $\mathbb{F}_{2^n}$:

- Not much is known about the cycle structure
- What is the **proportion** in $\mathbb{S}_{2^n}$? (Some *sort of* trivial lower bounds for the number of cyclotomic complete mappings)
- Most of the **known** classes (in polynomial form...) are either:
  - monomial mappings ($x \mapsto \alpha x^d$)
  - binomial mappings ($x \mapsto \alpha x^d + \beta x^e$)
  - trinomial mappings (very few complete mappings are known)
  - **AND/OR** linear mappings ($x \mapsto \sum_i c_i x^{2^i}$)

Outline

A generalization

From the previous slide:

$$f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \text{ is a complete mapping} \Leftrightarrow f^{-1} \text{ is complete,}$$

can be **generalized** into:

Proposition

The mapping obtained by **inverting** any disjoint cycle of a complete mapping remains complete.

Example: $\mathbb{F}_{16}$

$f = (1\ 8\ 12\ 10\ 15)(2\ 13\ 7\ 11\ 3)(4\ 9\ 14\ 5\ 6)$ is a complete mapping

$(1\ 8\ 12\ 10\ 15)(2\ 3\ 11\ 7\ 13)(4\ 9\ 14\ 5\ 6)$ is complete **too**

$(1\ 8\ 12\ 10\ 15)(2\ 13\ 7\ 11\ 3)(4\ 6\ 5\ 14\ 9)$ is complete **too**

$(1\ 8\ 12\ 10\ 15)(2\ 3\ 11\ 7\ 13)(4\ 6\ 5\ 14\ 9)$ is complete **too**

$\vdots$

A noticeable property

The Idea

Over $\mathbb{F}_{2^n}$,

If $x \mapsto f(x)$ is a **complete mapping**, implying that both $x \mapsto f^{-1}(x)$ and $x \mapsto f(x) + x$ are **complete mappings**.

A noticeable property

The Idea

Over $\mathbb{F}_{2^n}$,

If $x \mapsto f(x)$ is a **complete mapping**, implying that both $x \mapsto f^{-1}(x)$ and $x \mapsto f(x) + x$ are **complete mappings**.

It means that

- $x \mapsto f^{-1}(x) + x$ is a **complete mapping**!
  and so is $x \mapsto (f^{-1}(x) + x)^{-1}$!
  and so is $x \mapsto (f^{-1}(x) + x)^{-1} + x$!
  and so is $x \mapsto ((f^{-1}(x) + x)^{-1} + x)^{-1}$! and so on...

A noticeable property

The Idea

Over $\mathbb{F}_{2^n}$,

If $x \mapsto f(x)$ is a **complete mapping**, implying that both $x \mapsto f^{-1}(x)$ and $x \mapsto f(x) + x$ are **complete mappings**.

It means that

- $x \mapsto f^{-1}(x) + x$ is a **complete mapping**!
  and so is $x \mapsto (f^{-1}(x) + x)^{-1}$!
  and so is $x \mapsto (f^{-1}(x) + x)^{-1} + x$!
  and so is $x \mapsto ((f^{-1}(x) + x)^{-1} + x)^{-1}$! and so on...
- $x \mapsto (f(x) + x)^{-1}$ is a **complete mapping**!
  and so is $x \mapsto (f(x) + x)^{-1} + x$!
  and so is $x \mapsto (f(x) + x)^{-1} + x)^{-1}$! and so on ...

A noticeable property

The Idea

Over $\mathbb{F}_{2^n}$,

If $x \mapsto f(x)$ is a **complete mapping**, implying that both $x \mapsto f^{-1}(x)$ and $x \mapsto f(x) + x$ are **complete mappings**.

It means that

- $x \mapsto f^{-1}(x) + x$ is a **complete mapping**!
  and so is $x \mapsto (f^{-1}(x) + x)^{-1}$!
  and so is $x \mapsto (f^{-1}(x) + x)^{-1} + x$!
  and so is $x \mapsto ((f^{-1}(x) + x)^{-1} + x)^{-1}$! and so on...
- $x \mapsto (f(x) + x)^{-1}$ is a **complete mapping**!
  and so is $x \mapsto (f(x) + x)^{-1} + x$!
  and so is $x \mapsto (f(x) + x)^{-1} + x)^{-1}$! and so on ...

WHEN DOES IT STOP?

A noticeable property

More formally

Denote by $\mathbb{O} \subsetneq \mathbb{S}_{2^n}$ the set of all **orthomorphisms** over $\mathbb{F}_{2^n}$.
For any $f \in \mathbb{O}$, there is a group $\mathcal{D}_f$ acting on $\mathbb{O}$ by permutation (with identity $\mathtt{id} : f \mapsto f$) and generated by

$$\iota : f \mapsto f^{-1}$$

$$\tau : f(x) \mapsto f(x) + x, \qquad \text{for any } x \in \mathbb{F}_{2^n}.$$

(for any orthomorphism f, ιf is also one, and so is $\iota\tau f$, and so is $\iota\tau\iota f$, ...)

$\mathcal{D}_f$ is a Coxeter group generated by **two elements** (of order 2)

A noticeable property

More formally

Denote by $\mathbb{O} \subsetneq \mathbb{S}_{2^n}$ the set of all **orthomorphisms** over $\mathbb{F}_{2^n}$.
For any $f \in \mathbb{O}$, there is a group $\mathcal{D}_f$ acting on $\mathbb{O}$ by permutation (with identity $\mathtt{id} : f \mapsto f$) and generated by

$$\iota : f \mapsto f^{-1}$$

$$\tau : f(x) \mapsto f(x) + x, \qquad \text{for any } x \in \mathbb{F}_{2^n}.$$

(for any orthomorphism f, ιf is also one, and so is $\iota\tau f$, and so is $\iota\tau\iota f$, ...)

$\mathcal{D}_f$ is a Coxeter group generated by **two elements** (of order 2)
$\Rightarrow$ it is a **Dihedral** group.

A noticeable property

More formally

Denote by $\mathbb{O} \subsetneq \mathbb{S}_{2^n}$ the set of all **orthomorphisms** over $\mathbb{F}_{2^n}$.
For any $f \in \mathbb{O}$, there is a group $\mathcal{D}_f$ acting on $\mathbb{O}$ by permutation (with identity $\mathtt{id} : f \mapsto f$) and generated by

$$\iota : f \mapsto f^{-1}$$
$$\tau : f(x) \mapsto f(x) + x, \qquad \text{for any } x \in \mathbb{F}_{2^n}.$$

(for any orthomorphism f, ιf is also one, and so is $\iota\tau f$, and so is $\iota\tau\iota f$, ...)

$\mathcal{D}_f$ is a Coxeter group generated by **two elements** (of order 2)
$\Rightarrow$ it is a **Dihedral** group.

Theorem

For any $f \in \mathbb{O}$, we have

$$(\iota\tau)^3 f = \mathtt{id}.$$

$$(\iota\tau)^3 f = \mathtt{id}.$$

Proof:
We show that $\iota\tau\iota(f) = \tau\iota\tau(f)$. Since $\tau\iota(f) : x \mapsto f^{-1}(x) + x$, thus $\iota\tau\iota(f) : f^{-1}(x) + x \mapsto x$. We just have to show that $\tau\iota\tau(f) : f^{-1}(x) + x \mapsto x$, or **equivalently**

$$\tau\iota\tau(f^{-1}(x) + x) = x,$$

or **equivalently again**, for $y \in \mathbb{F}_{2^n}$ s.t. $f(y) + y = f^{-1}(x) + x$,

$$y = f^{-1}(x).$$

$$(\iota\tau)^3 f = \mathtt{id}.$$

Proof:
We show that $\iota\tau\iota(f) = \tau\iota\tau(f)$. Since $\tau\iota(f) : x \mapsto f^{-1}(x) + x$, thus $\iota\tau\iota(f) : f^{-1}(x) + x \mapsto x$. We just have to show that $\tau\iota\tau(f) : f^{-1}(x) + x \mapsto x$, or **equivalently**

$$\tau\iota\tau(f^{-1}(x) + x) = x,$$

or **equivalently again**, for $y \in \mathbb{F}_{2^n}$ s.t. $f(y) + y = f^{-1}(x) + x$,

$$y = f^{-1}(x).$$

Corollary

$$\mathtt{ord}(\mathcal{D}_f) = \begin{cases} 2 & \text{if } \iota f = \tau f \\ 6 & \text{otherwise.} \end{cases}$$

Outline

Definitions

Definition

For any $2^n - 1 = k \times d$, the **cyclotomic cosets** of $\mathbb{F}_{2^n}^* =< z >$ are

$$C_i = \left\{ z^{i+kj} \mid j = 0, 1, \ldots, d-1 \right\}, \quad \text{for } i = 0, 1 \ldots, k-1.$$

Definition

For $a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{2^n}$, the **cyclotomic mapping** $f_{a_0,a_1,\ldots,a_{k-1}}$ is:

$$f_{a_0,a_1,\ldots,a_{k-1}}(\zeta) = a_i\zeta, \quad \text{if } \zeta \in C_i, \quad i = 0, 1, \ldots, k-1.$$

Moreover, $f_{a_0,a_1,\ldots,a_{k-1}}(x) \in \mathbb{F}_{2^n}[x]$ is given by

$$f_{a_0,a_1,\ldots,a_{k-1}}(x) = (A_{n-1}x^{(n-1)d} + \cdots + A_1x^d + A_0)x,$$

with

$$A_i = \sum_{j=0}^{k-1} a_j z^{-ijd}.$$

Preliminaries

Lemma

The mapping $f_{a_0,a_1,\ldots,a_{k-1}}$ is bijective over $\mathbb{F}_{2^n}$ **if and only if**

$$a_i C_i \neq a_j C_j, \quad \forall 0 \leq i < j \leq k-1.$$

Theorem

If $|\{a_0, a_1, \ldots, a_{k-1}\}| = 2$, the **number** N of cyclotomic orthomorphisms $f_{a_0,a_1,\ldots,a_{k-1}}$ satisfies:

$$N \geq \frac{(2^n - 1 - k)(2^n - 1 - 2k)}{k^2}.$$

Harald Niederreiter, Arne Winterhof
Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields,
Discrete Mathematics 295 (2005), 161–171.

Example:

$n = 4$, $16 - 1 = 3 \times 5$

Vectorial notation $\rightarrow$ Cyclotomic mapping:

$$\begin{aligned} f = & (1\ 8\ 12\ 10\ 15)(2\ 13\ 7\ 11\ 3)(4\ 9\ 14\ 5\ 6) \\ = & (1\ z^3\ z^6\ z^9\ z^{12})(z\ z^{13}\ z^{10}\ z^7\ z^4)(z^2\ z^{14}\ z^{11}\ z^8\ z^5) \\ = & (z^{0+3j} \mapsto 1 \times z^{0+3j})(z^{1+3j} \mapsto z^{12} \times z^{1+3j})(z^{2+3j} \mapsto z^7 \times z^{2+3j}) \\ = & (1C_0)(z^{12}C_1)(z^7C_2) \end{aligned}$$

Reminder:

- Cyclotomic cosets

$$C_i = \left\{ z^{i+kj} \mid j = 0, 1, \ldots, d-1 \right\}, \quad \text{for } i = 0, 1 \ldots, k-1.$$

- Cyclotomic mapping

$$f_{a_0, a_1, \ldots, a_{k-1}}(\zeta) = a_i \zeta, \quad \text{if } \zeta \in C_i, \quad i = 0, 1, \ldots, k-1.$$

Outline

General Ideas

$2^n - 1 = kd$

Cyclotomic mappings are just mappings **translating** cosets of subgroups: with $a_i = z^{T_i}$ for any $0 \leq i < k$ and $0 \leq j < d$,

$$f_{a_0,a_1,\ldots,a_{k-1}} : z^{i+kj} \mapsto a_i z^{i+kj} = z^{i+kj+T_i}$$

Theorem

The mapping $f_{a_0,a_1,\ldots,a_{k-1}}$ is **complete** if C_0 is either:

Subfield: $d = 2^m - 1$, for any $1 \leq T_i \leq d$, **OR**

Subgroup: all T_i are equal to $1 \leq T \leq d-1$ or $d - T$.

Subfield: $f(z^{i+kj}) + z^{i+kj} = z^{i+kj}(\underbrace{z^{kT_i} + 1}_{:=z^{u_i} \in \mathbb{F}_{2^m}}) = z^{i+u_i+kj}$

Subgroup: $f(z^{i+kj}) + z^{i+kj} = z^{i+kj}(\underbrace{z^{kT} + 1}_{:=\text{constant}})$

On the number of Cyclotomic complete mappings over $\mathbb{F}_{2^n}$

$2^n - 1 = kd$

The number of **cyclotomic complete mappings** is:

- $(d-1)^k$ when C_0 is a subfield;
- $(d-1)2^{k-1}$ otherwise.

We also have polynomial representation of the cyclotomic complete mappings. Furthermore,

Corollary

For any $\alpha \neq 1 \in \mathbb{F}_{2^n}^*$ of (multiplicative) **order** d and any $\beta = 0$ or of **order**[a] k,

$$f(x) = x(\alpha + \mathtt{Tr}(\beta x^d))$$

defines a **complete mapping** over $\mathbb{F}_{2^n}$.

[a] of any order when C_0 is a subfield.

Regular partitions of $\mathbb{F}_{2^n}^*$

$2^n - 1 = kd$

Definition

Let $d \mid 2^n - 1$, a d-**regular partition** of $\mathbb{F}_{2^n}$ is a collection of k disjoint subsets of d disjoint (non-null) elements such that the sum of all the elements in a subset is 0.

Cyclotomic cosets of $\mathbb{F}_{2^n}^*$ are regular partitions of $\mathbb{F}_{2^n}^*$.

Conjecture: For any d-regular partition of $\mathbb{F}_{2^n}$, there exists at least one **complete mapping** consisting of the k disjoint cycles that form this partition.

Problem:

It's a geometrical problem to find and to enumerate **regular partitions** over a finite field...

Some more conjectures

- $f : z^{i+\frac{2^n-1}{d}j} \mapsto z^{i+\frac{2^n-1}{d}(\sigma_i(j))}$ is complete **if and only if** σ_i's are translations.
- If $f(x)$ is a **cyclotomic complete polynomial** over cosets of a subgroup that is **not** a subfield, then $f(x)+x$ is a one-cycle permutation.
- $\vdots$

Outline

Summary

- We **exposed some** unknown properties of complete mappings/orthomorphisms (inverting a cycle at a time, action of the dihedral group)
- We **provided large** classes of complete mappings. . .
- . . . and we give polynomial representation for some of them.
- A lot of investigation/computation has still to be made.
- Can we find **other** cryptographic applications?