Construction of Complete Permutation Polynomials

Chunlei Li

joint work with Xiaofang Xu, Xiangyong Zeng
and Tor Helleseth

Selmer Center, University of Bergen

June 17 - 22, 2018
BFA 2018

Outline

Complete Permutation Polynomials

Notation

- $\mathbb{F}_q$ — a finite field with q elements
- I — the identity mapping $I(x) = x$
- F — a polynomial in $\mathbb{F}_q[x]$

Definition

- F is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a bijection $x \mapsto F(x)$ on $\mathbb{F}_q$
- F is called a *complete permutation polynomial* (CPP) if both F and $F + I$ are PPs of $\mathbb{F}_q$
  - also in name of *complete mapping*

Complete Permutation Polynomials

Notation

- $\mathbb{F}_q$ — a finite field with q elements
- I — the identity mapping $I(x) = x$
- F — a polynomial in $\mathbb{F}_q[x]$

Definition

- F is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a bijection $x \mapsto F(x)$ on $\mathbb{F}_q$
- F is called a *complete permutation polynomial* (CPP) if both F and $F + I$ are PPs of $\mathbb{F}_q$
  - also in name of *complete mapping*

Complete Permutation Polynomials

Notation

- $\mathbb{F}_q$ — a finite field with q elements
- I — the identity mapping $I(x) = x$
- F — a polynomial in $\mathbb{F}_q[x]$

Definition

- F is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a bijection $x \mapsto F(x)$ on $\mathbb{F}_q$
- F is called a *complete permutation polynomial* (CPP) if both F and $F + I$ are PPs of $\mathbb{F}_q$
  - also in name of *complete mapping*

Orthomorphisms

CPPs and Orthomorphisms

- F' is an orthomoriphism: F' and $F' - I$ are PPs of $\mathbb{F}_q$
- F is a CPP of $\mathbb{F}_q$ iff. $F + I$ is an orthomoriphism of $\mathbb{F}_q$
- when q is even, CPP = orthomoriphism

Orthomorphisms

CPPs and Orthomorphisms

- F' is an orthomoriphism: F' and $F' - I$ are PPs of $\mathbb{F}_q$
- F is a CPP of $\mathbb{F}_q$ iff. $F + I$ is an orthomoriphism of $\mathbb{F}_q$
- when q is even, CPP = orthomoriphism

Orthomorphisms

CPPs and Orthomorphisms

- F' is an orthomoriphism: F' and $F' - I$ are PPs of $\mathbb{F}_q$
- F is a CPP of $\mathbb{F}_q$ iff. $F + I$ is an orthomoriphism of $\mathbb{F}_q$
- when q is even, CPP = orthomoriphism

Interesting Properties of CPPs

F is a CPP of $\mathbb{F}_q$ <u>iff.</u> one of the followings is a CPP

- $F(x+a)+b$ for any $a, b \in \mathbb{F}_q$
- $aF(a^{-1}x)$ for any $a \neq 0$
- $F^{-1}(x)$

When q is even, if F is a CPP of $\mathbb{F}_q$, then

- F has a single fixed point;
- it is *perfectly balanced* (Mittenthal 1995)

- $F(x)+F(y) \neq x+y$ when $x \neq y$

Interesting Properties of CPPs

F is a CPP of $\mathbb{F}_q$ iff. one of the followings is a CPP

- $F(x+a)+b$ for any $a, b \in \mathbb{F}_q$
- $aF(a^{-1}x)$ for any $a \neq 0$
- $F^{-1}(x)$

When q is even, if F is a CPP of $\mathbb{F}_q$, then

- F has a single fixed point;
- it is *perfectly balanced* (Mittenthal 1995)
  - a permutation of $\mathbb{F}_q$ is *perfectly balanced* if it maps each maximal subgroup of $\langle \mathbb{F}_q, + \rangle$ half into itself, half into its complements;
- $F(x) + F(y) \neq x + y$ when $x \neq y$

Interesting Properties of CPPs

F is a CPP of $\mathbb{F}_q$ <u>iff.</u> one of the followings is a CPP

- $F(x+a)+b$ for any $a, b \in \mathbb{F}_q$
- $aF(a^{-1}x)$ for any $a \neq 0$
- $F^{-1}(x)$

When q is even, if F is a CPP of $\mathbb{F}_q$, then

- F has a single fixed point;
- it is *perfectly balanced* (Mittenthal 1995)
    - a permutation of $\mathbb{F}_q$ is *perfectly balanced* if it maps each maximal subgroup of $\langle \mathbb{F}_q, + \rangle$ half into itself, half into its complements;
- $F(x) + F(y) \neq x + y$ when $x \neq y$

Interesting Properties of CPPs

F is a CPP of $\mathbb{F}_q$ iff. one of the followings is a CPP

- $F(x+a)+b$ for any $a,b \in \mathbb{F}_q$
- $aF(a^{-1}x)$ for any $a \neq 0$
- $F^{-1}(x)$

When q is even, if F is a CPP of $\mathbb{F}_q$, then

- F has a single fixed point;
- it is *perfectly balanced* (Mittenthal 1995)
  - a permutation of $\mathbb{F}_q$ is *perfectly balanced* if it maps each maximal subgroup of $\langle \mathbb{F}_q, + \rangle$ half into itself, half into its complements;
- $F(x)+F(y) \neq x+y$ when $x \neq y$

Interesting Properties of CPPs

F is a CPP of $\mathbb{F}_q$ <u>iff.</u> one of the followings is a CPP

- $F(x+a)+b$ for any $a, b \in \mathbb{F}_q$
- $aF(a^{-1}x)$ for any $a \neq 0$
- $F^{-1}(x)$

When q is even, if F is a CPP of $\mathbb{F}_q$, then

- F has a single fixed point;
- it is *perfectly balanced* (Mittenthal 1995)
  - a permutation of $\mathbb{F}_q$ is *perfectly balanced* if it maps each maximal subgroup of $\langle \mathbb{F}_q, + \rangle$ half into itself, half into its complements;
- $F(x) + F(y) \neq x + y$ when $x \neq y$

Applications of CPPs

Johnson et al. 1960: mutually orthogonal Latin squares

In cryptography:

- block ciphers: Lay-Massey, SMS4
- stream cipher Loiss
- hash functions SAFER
- pseudo-random generators

Outline

Boolean functions from CPPs

Good Boolean functions from CPPs

$f = (1 + y \cdot x)||(F(y) \cdot x)$ with a CPP F of $\mathbb{F}_{2^m}$

- f is balanced
- $nl(f) \geq 2^{2m} - 2^m$
- f has no nonzero linear structure

Boolean functions from CPPs

A pair of Bent functions from CPPs

- $\varphi_1(x, y) = x \cdot y + G_1(y)$
- $\varphi_2(x, y) = x \cdot F(y) + G_2(y)$

Then φ_1, φ_2 and $\varphi_1 + \varphi_2$ are bent;

Boolean functions from CPPs

Bent-negabent functions from CPPs (Stănică et al. 2012)

For $z = (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, let

- $h(z) = x \cdot y$,
- $s_2(z)$ be the quadratic symmetric function over $\mathbb{F}_{2^{2m}}$ and $s_2(z) = h(A_1(z)) + A_2(z)$,
- $f_F(z) = F(x) \cdot y$ with $\underline{F \text{ being a CPP of } \mathbb{F}_{2^m}}$

then

$$g(z) = f_F(A_1(z)) + s_2(z)$$

is bent-negabent functions and $\deg(g) = \deg(f_F)$.

CPPs of high alg. degree produce bent-negabent func. of high alg. degree (Pasalic 2014)

Constructions of CPPs?

How to construct CPPs of $\mathbb{F}_q$?

- combinatorial method from orthogonal Latin squares
- algebraic investigations on permutations (Niederreiter-Robinson, 1982) $x^{1+\frac{q-1}{k}} + bx$ is a PP of $\mathbb{F}_q$ iff. $(-b)^n \neq 1$ and

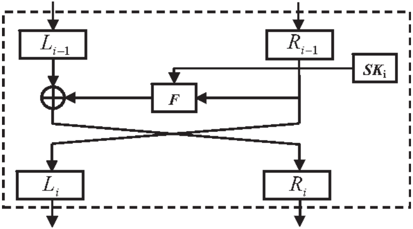
$$\left(\frac{b+w^i}{b+w^j}\right)^{\frac{q-1}{k}} \neq w^{j-i}, \quad \forall 0 \leq i < j < k$$

  where w is the fixed primitive k-th root of unity in $\mathbb{F}_q$

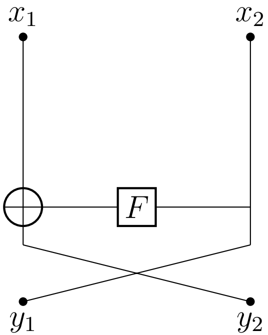
    - a series of works on monomial $b^{-1}x^{\frac{q-1}{k}}$ with $q = q_1^t$ and $k = q_1 - 1$ for $t = 2, 3, 4, 5, 6$

Outline

Feistel Structure

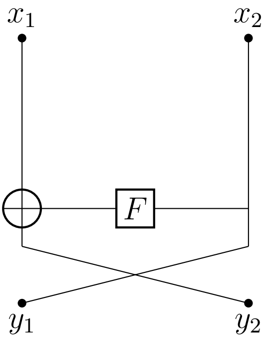


Feistel Structure



balanced Feistel structure without key

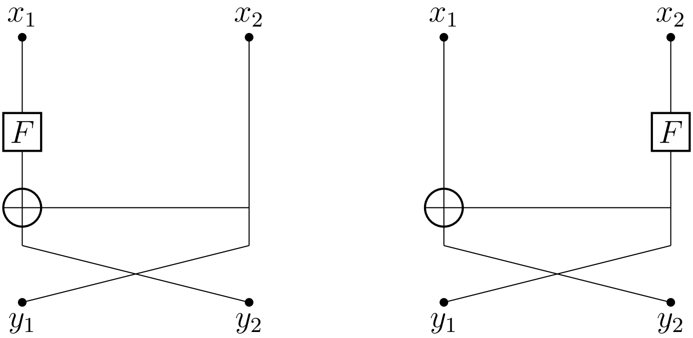
Feistel Structure



balanced Feistel structure without key

- a mapping $\Omega_F : (x_1, x_2) \mapsto (y_1, y_2) = (x_2, x_1 \oplus F(x_2))$

MISTY Structure (unkeyed, balanced)



1-round L-MISTY structure without key

1-round R-MISTY structure without key

- two mappings Φ_F and Ψ_F

Mappings from Feistel/MISTY structure

Feistel/MISTY structures give 3 mappings $\mathbb{F}_q^2 \to \mathbb{F}_q^2$:

$$\begin{array}{ll} \text{Feistel} \Rightarrow: & \Omega_F(x_1, x_2) = (x_2,\ F(x_2) + x_1), \\ \text{L-MISTY} \Rightarrow: & \Phi_F(x_1, x_2) = (x_2,\ F(x_1) + x_2), \\ \text{R-MISTY} \Rightarrow: & \Psi_F(x_1, x_2) = (F(x_2),\ F(x_2) + x_1), \end{array}$$

Interesting properties with these mappings?

- cryptographic properties: nonlinearity, differential uniformity
- mathematical properties: permutation, complete permutation?

Mappings from Feistel/MISTY structure

Feistel/MISTY structures give 3 mappings $\mathbb{F}_q^2 \to \mathbb{F}_q^2$:

$$\begin{array}{ll} \text{Feistel} \Rightarrow: & \Omega_F(x_1, x_2) = (x_2,\ F(x_2) + x_1), \\ \text{L-MISTY} \Rightarrow: & \Phi_F(x_1, x_2) = (x_2,\ F(x_1) + x_2), \\ \text{R-MISTY} \Rightarrow: & \Psi_F(x_1, x_2) = (F(x_2),\ F(x_2) + x_1), \end{array}$$

Interesting properties with these mappings?

- cryptographic properties: nonlinearity, differential uniformity
- mathematical properties: permutation, complete permutation?

Mappings from Feistel/MISTY structure

Feistel/MISTY structures give 3 mappings $\mathbb{F}_q^2 \to \mathbb{F}_q^2$:

$$\begin{array}{ll} \text{Feistel} \Rightarrow: & \Omega_F(x_1, x_2) = (x_2,\ F(x_2) + x_1), \\ \text{L-MISTY} \Rightarrow: & \Phi_F(x_1, x_2) = (x_2,\ F(x_1) + x_2), \\ \text{R-MISTY} \Rightarrow: & \Psi_F(x_1, x_2) = (F(x_2),\ F(x_2) + x_1), \end{array}$$

Interesting properties with these mappings?

- cryptographic properties: nonlinearity, differential uniformity
- mathematical properties: permutation, complete permutation?

PPs from Feistel/MISTY structure

$\Omega_F(x_1, x_2) = (x_2,\ F(x_2) + x_1)$ is a PP of $\mathbb{F}_{q^2}$ for any F:

$$\text{both} \quad \begin{cases} x_2 = \alpha_1 \\ F(x_2) + x_1 = \alpha_2 \end{cases} \quad \text{and} \quad \begin{cases} x_2 = \alpha_1 \\ F(x_2) + x_1 = \alpha_2 \end{cases}$$

have a unqiue solution in $\mathbb{F}_q$

PPs from Feistel/MISTY structure

Observations

Ω_F, Φ_F and Ψ_F are PPs of $\mathbb{F}_q^2$ for any F

Questions

1. Are they also CPPs of $\mathbb{F}_{q^2}$?
2. What are the requirements on F for them to be CPPs?
3. Can we composite these mappings to obtain CPPs?
4. How far can we go?

CPPs from Feistel/MISTY structure

Theorem 1

Ω_F, Φ_F and Ψ_F are CPPs of $\mathbb{F}_{q^2}$ if $F(x)$ is a PP of $\mathbb{F}_q$

Proof. $\Omega_F(x_1, x_2) = (x_2,\ F(x_2) + x_1)$

- Ω_F is a PP for any F
- For $x = (x_1, x_2)$, Ω_F is a CPP if $\Omega_F(x) + x$ is a PP, i.e.,

$$\begin{cases} x_2 + x_1 = \alpha_1 \\ F(x_2) + x_1 + x_2 = \alpha_2 \end{cases}$$

  has a unique solution (x_1, x_2) for any $\alpha_1, \alpha_2 \in \mathbb{F}_q$
- This holds if $F(x_2) = \alpha_1 + \alpha_2$ has a unique solution, i.e., F is a permutation of $\mathbb{F}_q$.

A similar proof for the other two mappings Φ_F, Ψ_F

CPPs from Feistel and MISTY structures

- A PP of $\mathbb{F}_q$ produces CPPs of $\mathbb{F}_q^2$
- PPs are invariant under composition
- CPPs are (generally) not invariant under composition

Question 3

What about the compositions of Ω_F, Φ_F, Ψ_F with F being a PP of $\mathbb{F}_q$?

Outline

CPPs from 2-round Feistel/MISTY

- 3 CPPs Ω_F, Φ_F and Ψ_F from a PP F of $\mathbb{F}_q$
- 9 possible compositions
- more generally, F can be different for each rounds
- PPs F_1 and F_2 PPs of $\mathbb{F}_q$ give

$$\Omega_{F_2} \circ \Omega_{F_1}, \Omega_{F_2} \circ \Phi_{F_1}, \Omega_{F_2} \circ \Psi_{F_1}$$

$$\Phi_{F_2} \circ \Omega_{F_1}, \Phi_{F_2} \circ \Phi_{F_1}, \Phi_{F_2} \circ \Psi_{F_1}$$

$$\Psi_{F_2} \circ \Omega_{F_1}, \Psi_{F_2} \circ \Phi_{F_1}, \Psi_{F_2} \circ \Psi_{F_1}$$

CPPs from 2-round Feistel/MISTY

- 3 CPPs Ω_F, Φ_F and Ψ_F from a PP F of $\mathbb{F}_q$
- 9 possible compositions
- more generally, F can be different for each rounds
- PPs F_1 and F_2 PPs of $\mathbb{F}_q$ give

$$\Omega_{F_2} \circ \Omega_{F_1}, \Omega_{F_2} \circ \Phi_{F_1}, \Omega_{F_2} \circ \Psi_{F_1}$$

$$\Phi_{F_2} \circ \Omega_{F_1}, \Phi_{F_2} \circ \Phi_{F_1}, \Phi_{F_2} \circ \Psi_{F_1}$$

$$\Psi_{F_2} \circ \Omega_{F_1}, \Psi_{F_2} \circ \Phi_{F_1}, \Psi_{F_2} \circ \Psi_{F_1}$$

CPPs from 2-round Feistel/MISTY

- 3 CPPs Ω_F, Φ_F and Ψ_F from a PP F of $\mathbb{F}_q$
- 9 possible compositions
- more generally, F can be different for each rounds
- PPs F_1 and F_2 PPs of $\mathbb{F}_q$ give

$$\Omega_{F_2} \circ \Omega_{F_1}, \Omega_{F_2} \circ \Phi_{F_1}, \Omega_{F_2} \circ \Psi_{F_1}$$

$$\Phi_{F_2} \circ \Omega_{F_1}, \Phi_{F_2} \circ \Phi_{F_1}, \Phi_{F_2} \circ \Psi_{F_1}$$

$$\Psi_{F_2} \circ \Omega_{F_1}, \Psi_{F_2} \circ \Phi_{F_1}, \Psi_{F_2} \circ \Psi_{F_1}$$

CPPs from 2-round Feistel/MISTY

- 3 CPPs Ω_F, Φ_F and Ψ_F from a PP F of $\mathbb{F}_q$
- 9 possible compositions
- more generally, F can be different for each rounds
- PPs F_1 and F_2 PPs of $\mathbb{F}_q$ give

$$\Omega_{F_2} \circ \Omega_{F_1}, \Omega_{F_2} \circ \Phi_{F_1}, \Omega_{F_2} \circ \Psi_{F_1}$$

$$\Phi_{F_2} \circ \Omega_{F_1}, \Phi_{F_2} \circ \Phi_{F_1}, \Phi_{F_2} \circ \Psi_{F_1}$$

$$\Psi_{F_2} \circ \Omega_{F_1}, \Psi_{F_2} \circ \Phi_{F_1}, \Psi_{F_2} \circ \Psi_{F_1}$$

- it is clear that the composited mappings are PPs
- what condition make them be CPPs ?
- take $\Omega_{F_2} \circ \Omega_{F_1}$ as a representative

$$(x_1, x_2) \mapsto \Big(F_1(x_2) + x_1, F_2\big(F_1(x_2) + x_1\big) + x_2\Big)$$

- for have a CPP $\Omega_{F_2} \circ \Omega_{F_1}$, we need

$$(x_1, x_2) \mapsto \Big(F_1(x_2), F_2\big(F_1(x_2) + x_1\big)\Big)$$

  be an injective mapping
- it suffices to choose F_1, F_2 to be PPs of $\mathbb{F}_q$

Theorem 2

If F_1, F_2 are PPs of $\mathbb{F}_q$, then

$$\Omega_{F_2} \circ \Omega_{F_1}, \Omega_{F_2} \circ \Phi_{F_1}, \Omega_{F_2} \circ \Psi_{F_1}$$

$$\Phi_{F_2} \circ \Omega_{F_1}, \Phi_{F_2} \circ \Psi_{F_1}$$

$$\Psi_{F_2} \circ \Omega_{F_1}, \Psi_{F_2} \circ \Phi_{F_1},$$

are CPPs of $\mathbb{F}_{q^2}$, respectively.

Remark

- Theorems 1 and 2 are simple, but interesting:
  - starting from any mapping from $\mathbb{F}_q$ to itself
  - by Feistel/MISTY structure, one gets a PP of $\mathbb{F}_q^2$
  - then easily deduces CPPs of the extension fields

$$\mathbb{F}_{q^4}, \mathbb{F}_{q^8}, \cdots, \mathbb{F}_{q^{2^k}}$$

- $\Phi_{F_1} \circ \Phi_{F_2}$, $\Psi_{F_1} \circ \Psi_{F_2}$ are not included in Theorem 2
- F_1, F_2 being PPs of $\mathbb{F}_q$ does not guarantee all compositions of $\Omega_{F_i}, \Phi_{F_i}, \Psi_{F_i}$ are CPPs

Outline

CPPs from 3-round Feistel/MISTY

- three permutations F_i of $\mathbb{F}_q$, $i = 1, 2, 3$
- 3-round compositions produce 27 mappings of $\mathbb{F}_{q^2}$

$$\mathcal{R}_3 \circ \mathcal{R}_2 \circ \mathcal{R}_1, \quad \mathcal{R}_i \in \{\Omega_{F_i}, \Phi_{F_i}, \Psi_{F_i}\}$$

- characterizing the condition on F_i's for each of the 27 composited mappings to be CPP is similar
- 16 out of 27 mappings are manageable
- ... means it's easy to characterize the conditions on F_i's and one could find those F_i's

CPPs from 3-round Feistel/MISTY

Take $\Omega_{F_3} \circ \Phi_{F_2} \circ \Omega_{F_1}$ as a representative

Theorem 3

$\Omega_{F_3} \circ \Phi_{F_2} \circ \Omega_{F_1}$ is a CPP of $\mathbb{F}_{q^2}$ if

- *F_2 and $F_1 + F_2$ are PPs of $\mathbb{F}_q$; and*
- *$F_3(z) + z$ is a PP of $\mathbb{F}_q$*

Proof. The mapping $\Omega_{F_3} \circ \Phi_{F_2} \circ \Omega_{F_1}$ is given by

$$\Big(F_2(x_2)+F_1(x_2)+x_1, F_3(F_2(x_2)+F_1(x_2)+x_1)+F_1(x_2)+x_1\Big)$$

We need to show, for any $(\alpha_1, \alpha_2) \in \mathbb{F}_q^2$, both

$$\begin{cases} F_2(x_2) + F_1(x_2) + x_1 = \alpha_1 \\ F_3(F_2(x_2) + F_1(x_2) + x_1) + F_1(x_2) + x_1 = \alpha_2 \end{cases} \tag{1}$$

and

$$\begin{cases} F_2(x_2) + F_1(x_2) = \alpha_1 \\ F_3(F_2(x_2) + F_1(x_2) + x_1) + F_1(x_2) + x_1 + x_2 = \alpha_2 \end{cases} \tag{2}$$

have a unique solution.

Equations (1) implies

$$\begin{cases} F_2(x_2) + F_1(x_2) + x_1 = \alpha_1 \\ F_3(\alpha_1) + F_1(x_2) + x_1 = \alpha_2 \end{cases}$$

F_2 is a PP of $\mathbb{F}_q$ implies $F_2(x_2) = \alpha_1 + \alpha_2 + F_3(\alpha_1)$ has a unique solution $x_2 \in \mathbb{F}_q$, giving a unique solution $x_1 \in \mathbb{F}_q$

Equation (2) implies

$$\begin{cases} F_2(x_2) + F_1(x_2) = \alpha_1 \\ F_3(\alpha_1 + x_1) + F_1(x_2) + x_1 + x_2 = \alpha_2 \end{cases}$$

$F_1 + F_2$ is a PP of $\mathbb{F}_q$ gives a unique solution $x_2 \in \mathbb{F}_q$

$F_3(z) + z$ is a PP of $\mathbb{F}_q$ gives a unique solution $x_1 \in \mathbb{F}_q$

Equations (1) implies

$$\begin{cases} F_2(x_2) + F_1(x_2) + x_1 = \alpha_1 \\ F_3(\alpha_1) + F_1(x_2) + x_1 = \alpha_2 \end{cases}$$

F_2 is a PP of $\mathbb{F}_q$ implies $F_2(x_2) = \alpha_1 + \alpha_2 + F_3(\alpha_1)$ has a unique solution $x_2 \in \mathbb{F}_q$, giving a unique solution $x_1 \in \mathbb{F}_q$

Equation (2) implies

$$\begin{cases} F_2(x_2) + F_1(x_2) = \alpha_1 \\ F_3(\alpha_1 + x_1) + F_1(x_2) + x_1 + x_2 = \alpha_2 \end{cases}$$

$F_1 + F_2$ is a PP of $\mathbb{F}_q$ gives a unique solution $x_2 \in \mathbb{F}_q$

$F_3(z) + z$ is a PP of $\mathbb{F}_q$ gives a unique solution $x_1 \in \mathbb{F}_q$

CPPs from 3-round Feistel/MISTY(2)

- $\Omega_{F_3} \circ \Phi_{F_2} \circ \Omega_{F_1}$ is a CPP of $\mathbb{F}_{q^2}$ if
  - F_2 and $F_1 + F_2$ are PPs of $\mathbb{F}_q$; and
  - $F_3(z) + z$ is a PP of $\mathbb{F}_q$
- do such F_i's exist or not?
  - F_3 can be easily obtained
  - F_1 and F_2 seems not trivial to find
  - a natural starting point: power functions x^d over $\mathbb{F}_q$

- ax^d is a PP of $\mathbb{F}_q$ iff. $\gcd(d, q-1) = 1$, $a \in \mathbb{F}_q^*$

- for $\gcd(d_i, q-1) = 1$ and $a_i \in \mathbb{F}_q^*$,
  when will $a_1 x^{d_1} + a_2 x^{d_2}$ be a PP of $\mathbb{F}_q$?

- in particular, let $a_1 = 1, d_2 = 1$, the problem becomes when $x^d + ax$ is a PP of $\mathbb{F}_q$?

- the known results on monomial CPPs of $\mathbb{F}_q$ can be applied

CPPs from 3-round Feistel/MISTY(3)

How to find a PP of $\mathbb{F}_q$ with the form $ax^{d_1} + x^{d_2}$?

Proposition 1

Suppose

- $q = 2^{2m}$ with an odd integer m
- k is an odd integer with $\gcd(k(k-1), m) = 1$
- a satisfies $a^{2^m+1} = 1$ and $a^{(2^m+1)/3} \neq 1$
- $d_1 = 2^k - 1$
- $d_2 = (2^{k-1} - 1)(2^m - 1) + 2^k - 1$

Then $ax^{d_1} + x^{d_2}$ is a PP of $\mathbb{F}_q$

Sketch of Proof.

- easy to show $\gcd(d_i, q-1) = 1$
- show the exponential sum

$$S(\gamma) = \sum_{x \in \mathbb{F}_q} \chi(\gamma(ax^{d_1} + x^{d_2})) = 0$$

  for all nonzero $\gamma \in \mathbb{F}_q^*$
- write $x = yu$ with $y \in \mathbb{F}_{2^m}^*$ and u in the unit circle U
- the problem can be translated to showing

$$(u + \theta u^{2^k - 1}) + (u + \theta u^{2^k - 1})^{2^m} = 0,$$

  where $\theta = \gamma^{(2^{k-1}-1)(2^m-1)/d_2} a$, has one solution in U
- the fact $\theta \in U$ gives

$$(\theta u^{2^k - 2} + 1)(\theta u^{2^k} + 1) = 0$$

  with $(\theta u^{2^k - 2})^{\frac{(2^m+1)}{3}} \neq 1$. □

CPPs from 3-round Feistel/MISTY(4)

- 27 composited mappings by 3-round Feistel/MISTY
- 16 out of 27 have feasible conditions
- some condition are trivial to satisfy, some are not
- we went through one instance of them
- ... with an interesting condition on F_1 and F_2

Question

Can we find more PPs F_1, F_2 of $\mathbb{F}_q$ such that

- $F_1 + F_2$ is also a PP of $\mathbb{F}_q$?
- particularly for $q = 2^m$ with an odd integer m?

CPPs from Feistel/MISTY

- the Feistel/MISTY structure is just a starting point
- other *structures* are also possible
- it is about construct CPPs of $\mathbb{F}_q$ from its half-field
- the idea can be generalized ...
  - construct CPPs of $\mathbb{F}_q$ from other subfields of $\mathbb{F}_q$
  - construct CPPs of $\mathbb{F}_{p^m}$ for any prime p

Generalized constructions of CPPs (1)

Let $q = p^m$ and F_i's be mapping from $\mathbb{F}_q$ to itself.

Denote $x = (x_1, x_2) \in \mathbb{F}_q^2$. Define $G(x) = (G_1(x), G_2(x)$ with

$$\begin{cases} G_1(x) = F_1(-x_2) - x_1 - F_3(\, F_2(\, F_1(-x_2) - x_1) - x_2) \\ G_2(x) = F_2(\, F_1(-x_2) - x_1) - x_2 \end{cases}$$

Proposition 3

G is a CPP of $\mathbb{F}_q^2$ if

- $F_1(z) - F_3(z + \gamma)$ is a PP of $\mathbb{F}_q$ for any $\gamma \in \mathbb{F}_q$;
- F_2 is a PP of $\mathbb{F}_q$.

Condition 1: $F_1(z) - F_3(z+\gamma)$ is a PP for any $\gamma \in \mathbb{F}_q$

- it seems to be related to planar functions over $\mathbb{F}_q$
- but it is different ...
  - for a planar function F, we only have

$$F(z) - F(z+\gamma)$$

    is a PP of $\mathbb{F}_q$ for any **nonzero** γ
  - F_1 cannot be identical to F_3

How to find F_1 and F_3 satisfying the condition?

A trivial method

- choose a PP F of $\mathbb{F}_q$
- choose F_3 as a linearized polynomial
- take $F_1 = F + F_3$
- $F_1(x) - F_3(x+\gamma) = F(x) + F_3(\gamma)$

How to find F_1 and F_3 satisfying the condition?

Another approach

- start with monomials x^d over $\mathbb{F}_q$
- take $F_1(x) = x^d$ and $F_3(x) = \beta x^d$ with $\beta \neq 1$
- we have

$$F_1(x) - F_3(x+\gamma) = \begin{cases} (1-\beta)x^d, & \text{if } \gamma = 0 \\ \gamma^d[(\frac{x}{\gamma})^d - \beta(\frac{x}{\gamma}+1)^d], & \text{if } \gamma \neq 0 \end{cases}$$

- it suffices to find an integer d s.t. $\gcd(d, q-1) = 1$ and

$$x^d - \beta(x+1)^d$$

  is a PP of $\mathbb{F}_q$
- we consider two cases here: $q = 2^m$ and $q = 3^m$

Case 1: $q = 2^m$

- take $d = 2^k + 1$, $\beta \in \mathbb{F}_{2^k} \setminus \{0,1\}$
- $x^d - \beta(x+1)^d$ becomes

$$x^{2^k+1} + \beta(x+1)^{2^k+1} = (1+\beta)(x + \tfrac{\beta}{1+\beta})^{2^k+1} + \beta$$

- this is a PP of $\mathbb{F}_q$ when $\gcd(2^k+1, 2^m-1) = 1$

Case 2: $q = 3^m$

- take $\beta = -1$
- translate $x^d + (x+1)^d$ to $(x+1)^d + (x-1)^d$
- if $d \equiv -1 \pmod 3$, then

$$(x+1)^d + (x-1)^d = 2D_d(z, 1)$$

  where

$$D_d(z,1) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-1)^i z^{d-2i}$$

  is a Dickson polynomial
- $D_d(z, 1)$ is a PP of $\mathbb{F}_q$ iff. $\gcd(d, q^2 - 1) = 1$
- thus, $d \equiv -1 \pmod 3$ and $\gcd(d, 3^{2m} - 1) = 1$

Generalized constructions of CPPs (2)

- $p_i(z)$ in $\mathbb{F}_q[z]/(z^q - z)$, $i = 1, \cdots, m$
- $G(x)$ be a function from $\mathbb{F}_q^m$ to itself defined by

$$G(x) = (G_1(x), G_2(x), \cdots, G_m(x))$$

with $G_1(x) = p_1(x_m) - x_1$ and

$$G_2(x) = p_2(G_1(x)) - x_1$$
$$\vdots$$
$$G_m(x) = p_m(G_{m-1}) - x_{m-1}$$

Theorem 4

$G(x)$ is a CPP of $\mathbb{F}_q^m$ if $p_i(x)$ is a PP of $\mathbb{F}_q$.

Generalized constructions of CPPs (2)

- $p_i(z)$ in $\mathbb{F}_q[z]/(z^q - z)$, $i = 1, \cdots, m$
- $G(x)$ be a function from $\mathbb{F}_q^m$ to itself defined by

$$G(x) = (G_1(x), G_2(x), \cdots, G_m(x))$$

with $G_1(x) = p_1(x_m) - x_1$ and

$$\begin{aligned} G_2(x) &= p_2(G_1(x)) - x_1 \\ &\vdots \\ G_m(x) &= p_m(G_{m-1}) - x_{m-1} \end{aligned}$$

Theorem 4

$G(x)$ is a CPP of $\mathbb{F}_q^m$ if $p_i(x)$ is a PP of $\mathbb{F}_q$.

Summary

- PPs of small fields can give CPPs of extension fields
  - 1 and 2-round Feistel/MISTY structure
  - 3-round Feistel/MISTY with extra requirements
  - the idea can be extended to general fields and/or more general structure
- other (cryptographic) properties of such CPPs ?
  - differential property, nonlinearity, ...
- deeper connection of properties between such CPPs and their building blocks?

Thanks for your attention!

Questions?