Constructions of Complete Permutation Polynomials

Xiaofang Xu

Faculty of Mathematics and Statistics, Hubei University

(Joint work with Chunlei Li, Xiangyong Zeng and Tor Helleseth)

The 5th Sino-Korea International Conference on Coding Theory and Related Topics

July 4, 2018

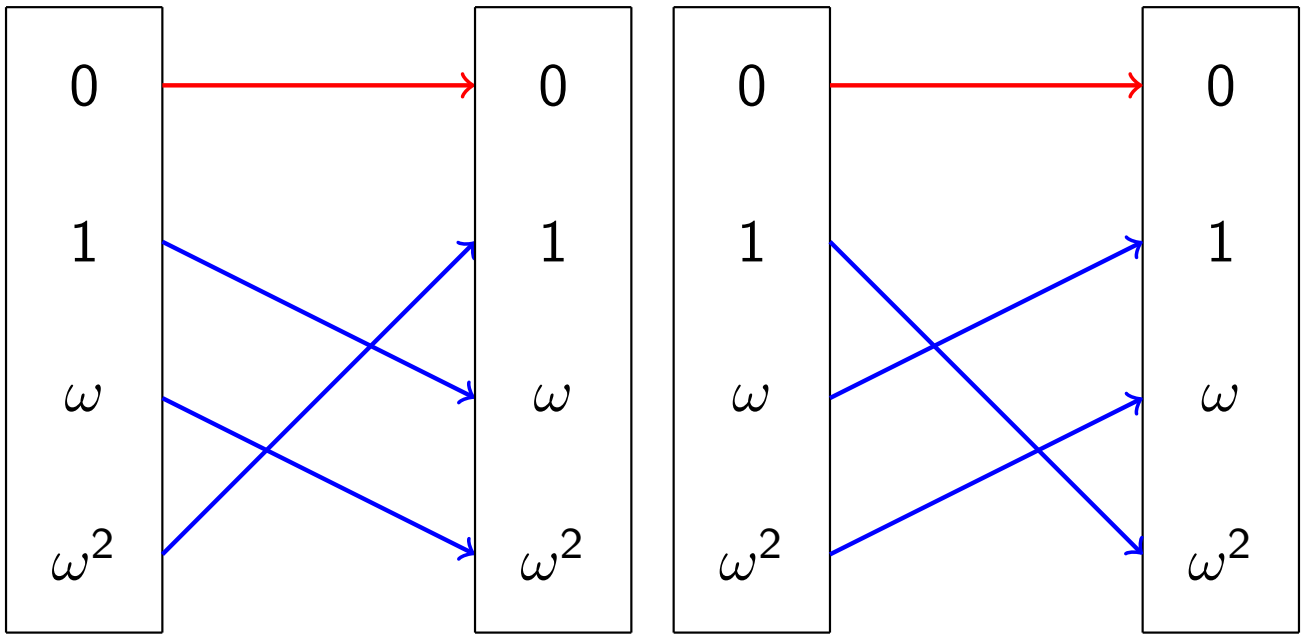
Outline

Outline

PP and CPP

- $\mathbb{F}_q$ is the finite field with q elements where q is a prime power.
- A polynomial $f(x)$ over $\mathbb{F}_q$ is called a *permutation polynomial* (PP) if the induced polynomial function f: $c \mapsto f(c)$ from $\mathbb{F}_q$ to itself permutes $\mathbb{F}_q$.
- A polynomial $f(x)$ over $\mathbb{F}_q$ is called a *complete permutation polynomial* (CPP) if both $f(x)$ and $f(x) + x$ are permutations of $\mathbb{F}_q$.

Example for PP and CPP



$f(x) = \omega x$ $\qquad$ $f(x) + x = \omega^2 x$

- $f(x)$ is a linear CPP of $\mathbb{F}_{2^2}$.

A brief history of CPPs

- CPPs of groups were introduced by Mann [Ann. Math. Stat. 1942];
- A detailed study of CPPs of finite fields was initially carried out by Niederreiter and Robinson [J. Aust. Math. Soc. A, 1982];
- The reduced degree of complete mapping of finite fields with even characteristic was studied by Wan [J. Aust. Math. Soc. A, 1986];

A brief history of CPPs

- Mullen and Niederreiter proved that a Dickson polynomial can be a complete mapping only in some special cases [Cana. Math. Bull. 1987];
- CPPs over $\mathbb{F}_{16}$ were given in [Yuan-Tong-Zhang, LNCS, 2007];
- Monomial CPPs of type $ax^{\frac{q-1}{k}+1}$ were investigated in [Laigle-Chapuy, FFA, 2007; Sarkar-Bhattacharya-Cesmelioglu, LNCS, 2012];

A brief history of CPPs

- By using the technique of polar coordinate representation, monomial CPPs and trinomial CPPs of $\mathbb{F}_{2^n}$ were given in [Tu-Zeng-Hu, FFA, 2014];
- The constructions and proof methods of the above paper triggered a series of investigations on sparse CPPs [Wu-Li-Helleseth-Zhang, FFA, 2014; Xu-Cao, FFA, 2015; Wu-Lin, Discret. Appl. Math. 2015; Bartolia-Giulietti-Zinib, FFA, 2016$\cdots$];
- CPPs were generated by recursive methods in [Muratovic-Pasalic, FFA, 2014; Zha-Hu-Cao, FFA, 2015]

$\cdots\cdots$

The applications of CPPs in cryptography

CPPs have been widely used in cryptography. For examples:

- in the design of nonlinear dynamic substitution device [Mittenthal, Adv.Appl.Math. 1995];
- in the design of Hash functions [Schnorr-Vaudenay, Advances in Cryptology-Eurocrypt'94, 1995; Vaudenay, LNCS, 1994];
- in the Lay-Massey scheme [Vaudenay, Advances in Cryptology-Asiacrypt'99, 1999];
- in block ciphers SMS4 [http://www.oscca.gov.cn/UpFile/20062101642319799O.pdf];
- in stream ciphers Loiss [Feng-Feng-Zhang, et al, LNCS, 2011].

Algebraic degree

Definition 1

Any function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ can be uniquely expressed by a univariate polynomial

$$F(x) = \sum_{i=0}^{p^n-1} b_i x^i \in \mathbb{F}_{p^n}[x]/(x^{p^n} - x)$$

and the algebraic degree of F is defined as

$$\deg(F) = \max_{0 \le i < p^n} \{wt_p(i) : b_i \neq 0\},$$

where $wt_p(s)$ is the p-weight of an integer s, $0 \le s < p^n$, defined as $wt_p(s) = \sum_{i=0}^{n-1} s_i$ by its p-ary expansion $s = \sum_{i=0}^{n-1} s_i p^i$.

For cryptographic applications, it is usually desirable that the PPs in use have high algebraic degree.

The upper bound of algebraic degree of CPPs

- Any CPP of $\mathbb{F}_q$ with $q > 3$ has reduced degree at most $q - 3$ [Niederreiter-Robinson, J. Aust. Math. Soc. A, 1982; Wan, J. Aust. Math. Soc. A, 1986].
- Any CPP of $\mathbb{F}_{p^{kn}}$ with $p^{kn} > 3$ has maximum algebraic degree $kn(p-1) - 1$.

The algebraic degree of some known CPPs

CPPs	Finite field	Algebraic degree	Literature
Monomial CPPs	$\mathbb{F}_{2^{2n}}$	$\deg \leq n-1$	[Sarkar et al., LNCS, 2012]
Sparse CPPs	$\mathbb{F}_{2^{2n}}$	$\deg \leq 3$	[Tu-Zeng-Hu, FFA, 2014]
Monomial CPPs	$\mathbb{F}_{2^{kn}}$	$\deg \leq k$	[Wu-Li-Helleseth-Zhang, FFA, 2014]
Sparse CPPs	$\mathbb{F}_{2^{2n}}$	$\deg \leq n+1$	[Wu-Lin, Discret. Appl. Math. 2015]
Sparse CPPs	$\mathbb{F}_{3^{2n}}$	$\deg \leq 2n+1$	[Xu-Cao, FFA, 2015]
Monomial CPPs	$\mathbb{F}_{p^{kn}}$	$\deg \leq 4$	[Bassalygo-Zinoviev, FFA, 2015]
Sparse CPPs	$\mathbb{F}_{p^{kn}}$	$\deg \leq n+1$	[Bartolia-Giulietti-Zini, FFA, 2016]
Recursive CPPs	$\mathbb{F}_{p^{kn}}$	$\deg \leq kn$	[Zha-Hu-Cao, FFA, 2015]

Table: The algebraic degree of some known CPPs

Motivation

- A limited number $\dashrightarrow$ known constructions of CPPs.
- The cryptographic properties of CPPs $\dashrightarrow$ not taken into consideration.
- None of the known (infinite) classes of CPPs $\dashrightarrow$ sufficiently high algebraic degree.

Questions

- New approaches $\dashrightarrow$ CPPs?
- Upper bound on the algebraic degree $\dashrightarrow$ CPPs?
- CPPs$\dashrightarrow$ nearly optimal algebraic degree?

Outline

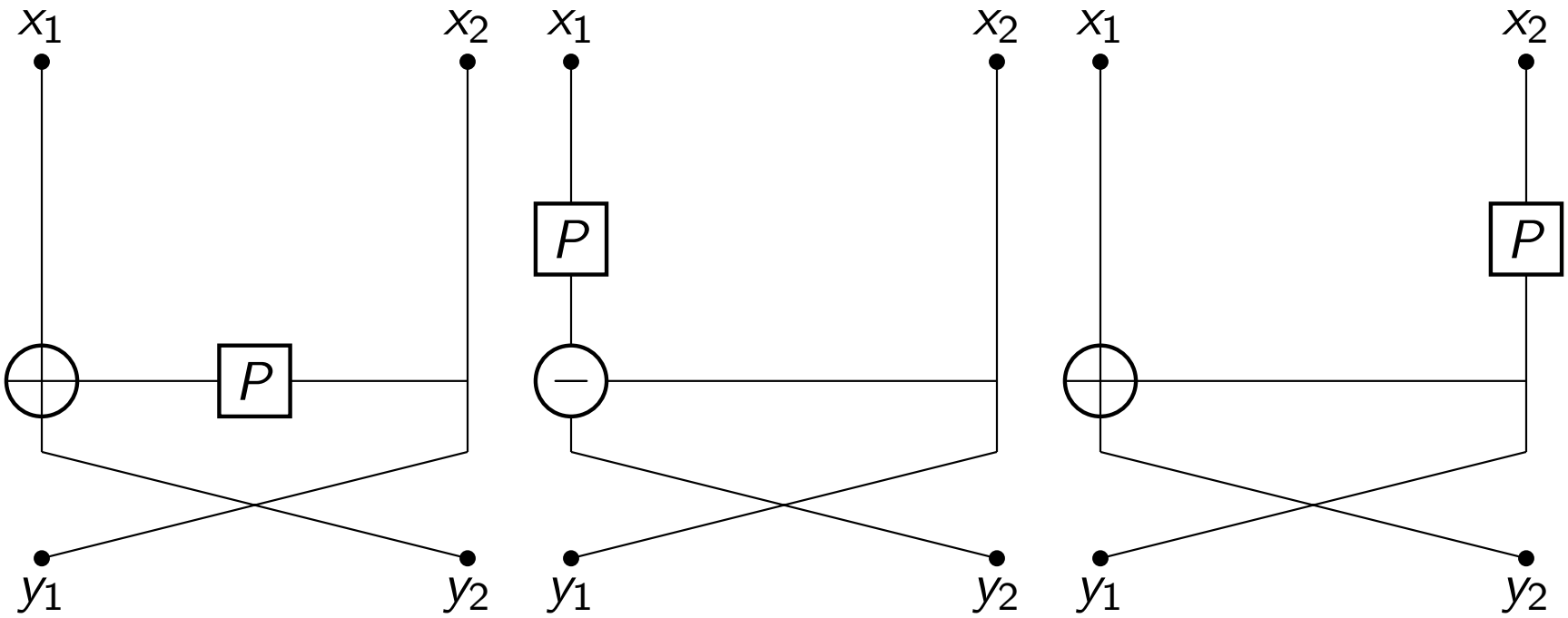
The applications of Feistel and MISTY structures

The Feistel and MISTY structures have been used in the design of many block ciphers. For examples:

- in DES algorithm;
- in ZUC algorithm;
- in Lightweight S-Boxes;

  .....

1-round Feistel and MISTY structures



$\Omega_p = (x_2,\ p(x_2) + x_1)$ $\Phi_p = (x_2,\ p(x_1) - x_2)$ $\Psi_p = (p(x_2),\ p(x_2) + x_1)$

1-round Feistel structure 1-round L- MISTY structure 1-round R-MISTY structure

Figure: Balanced Feistel and MISTY structure without round key

CPPs from one-round Feistel and MISTY structions

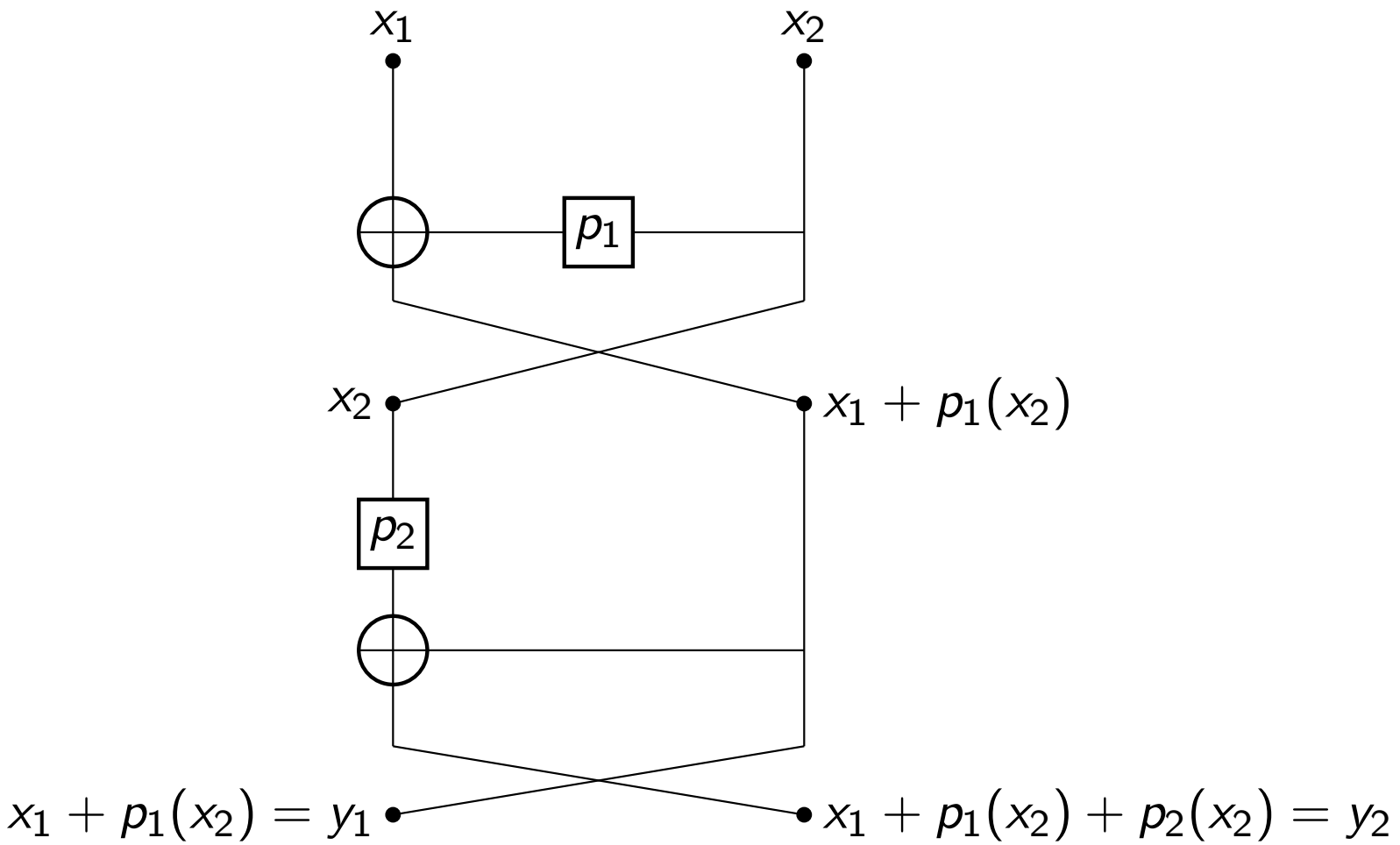
Lemma 1

Let $p(z)$ be a polynomial from $\mathbb{F}_q$ to itself. Let Ω_p, Φ_p and Ψ_p be three mappings from $\mathbb{F}_q^2$ to itself defined by

$$\begin{aligned} \Omega_p(x_1, x_2) &= (x_2,\ p(x_2) + x_1), \\ \Phi_p(x_1, x_2) &= (x_2,\ p(x_1) - x_2), \\ \Psi_p(x_1, x_2) &= (p(x_2),\ p(x_2) + x_1), \end{aligned} \tag{1}$$

where $x = (x_1, x_2) \in \mathbb{F}_q^2$. Then the mappings Ω_p, Φ_p and Ψ_p are CPPs of $\mathbb{F}_q^2$ when $p(z)$ permutes $\mathbb{F}_q$.

Two-round Feistel and MISTY structures



$$\Phi_{p_2} \circ \Omega_{p_1} = \Big(x_1 + p_1(x_2), x_1 + p_1(x_2) + p_2(x_2)\Big)$$

Figure: $\Phi_{p_2} \circ \Omega_{p_1}$ from two-round structure

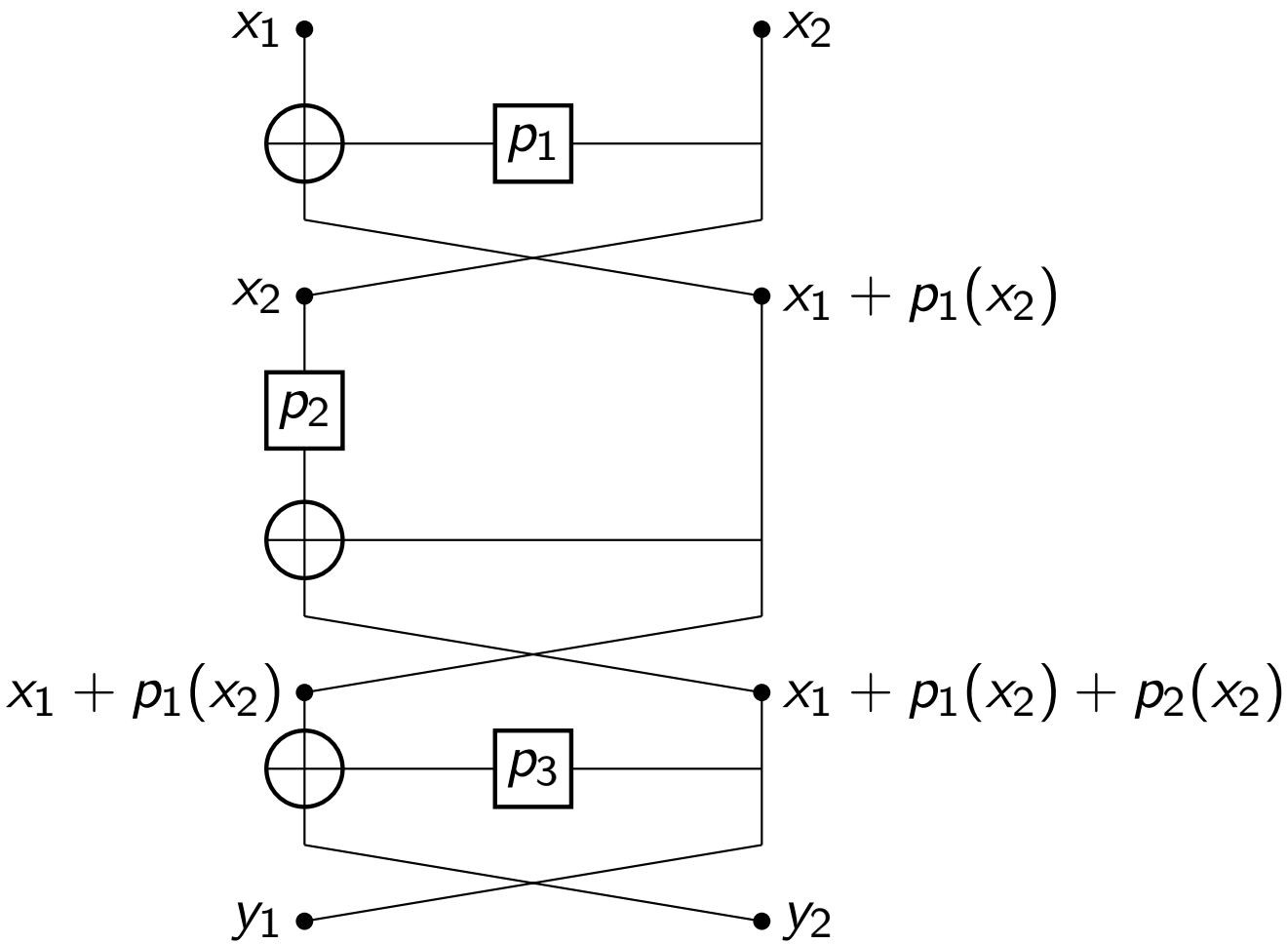
Two-round constructions

Proposition 1

Let $p_1(z), p_2(z)$ be two permutations of $\mathbb{F}_{2^n}$. Then each mapping in $\mathcal{S} = \{\Psi_{p_2} \circ \Omega_{p_1}, \Omega_{p_2} \circ \Phi_{p_1}, \Psi_{p_2} \circ \Phi_{p_1}, \Omega_{p_2} \circ \Omega_{p_1}, \Phi_{p_2} \circ \Omega_{p_1}, \Omega_{p_2} \circ \Psi_{p_1}, \Phi_{p_2} \circ \Psi_{p_1}\}$ is a CPP of $\mathbb{F}_{2^n}^2$.

- $\Phi_{p_2} \circ \Phi_{p_1}$ is a CPP of $\mathbb{F}_{2^n}^2$ if $p_1(z) + p_2(p_1(z) + z + \gamma)$ permutes $\mathbb{F}_{2^n}$ for any $\gamma \in \mathbb{F}_{2^n}$ where $p_1(z)$ and $p_2(z)$ are two permutations of $\mathbb{F}_{2^n}$.
- $\Psi_{p_2} \circ \Psi_{p_1}$ is a CPP of $\mathbb{F}_{2^n}^2$ if $p_1(z) + z + p_2(z + \gamma)$ permutes $\mathbb{F}_{2^n}$ for any $\gamma \in \mathbb{F}_{2^n}$ where $p_1(z)$ and $p_2(z)$ are two permutations of $\mathbb{F}_{2^n}$.

Three-round Feistel and MISTY structures



$$(y_1, y_2) = \Big(p_2(x_2) + p_1(x_2) + x_1, p_3(p_2(x_2) + p_1(x_2) + x_1) + p_1(x_2) + x_1\Big)$$

$$(y_1, y_2) = \Omega_{p_3} \circ \Phi_{p_2} \circ \Omega_{p_1}(x_1, x_2)$$

Three-round constructions

Theorem 1

Let $p_2(z)$ and $p_3(z) + z$ be two permutations of $\mathbb{F}_{2^n}$. Let $p_1(z)$ be a polynomial over $\mathbb{F}_{2^n}$ such that $p_1(z) + p_2(z)$ is a permutation. Then $\Omega_{p_3} \circ \Phi_{p_2} \circ \Omega_{p_1}$ is a CPP of $\mathbb{F}_{2^n}^2$.

Useful results about $p_1(z) + p_2(z)$

Proposition 2

Let m and k be two odd positive integers with $\gcd(k(k-1), m) = 1$ and let $n = 2m$. Suppose $p_1(z) = uz^{2^k-1}$ for a non-cubic element u in the unit circle $U = \{\lambda \in \mathbb{F}_{2^n} : \lambda^{2^m+1} = 1\}$ and $p_2(z) = z^{(2^{k-1}-1)(2^m-1)+2^k-1}$. Then $p_1(z)$, $p_2(z)$ and $p_1(z) + p_2(z)$ are all permutation polynomials over $\mathbb{F}_{2^n}$.

Proposition 3

Let g_1 and g_2 be polynomials over $\mathbb{F}_q$ with q being a power of 2. Let Φ_{g_1} and Ψ_{g_2} be defined as in (1). If $g_1(z)$ and $g_2(z)$ are CPPs of $\mathbb{F}_q$, then Φ_{g_1}, Ψ_{g_2} and $\Phi_{g_1} + \Psi_{g_2}$ are PPs of $\mathbb{F}_q^2$.

Generalized construction

Theorem 2

Let $p_1(z), p_2(z), p_3(z)$ be polynomials over $\mathbb{F}_{p^n}$ for any prime p. Let F be a function from $\mathbb{F}_{p^n}^2$ to itself given by

$$F(x) = (p_1(-x_2) - x_1 - p_3(\, p_2(\, p_1(-x_2) - x_1) - x_2), p_2(\, p_1(-x_2) - x_1) - x_2)$$

where $x = (x_1, x_2) \in \mathbb{F}_{p^n}^2$.
The polynomial $F(x)$ is a CPP of $\mathbb{F}_{p^n}^2$ if the following two conditions are satisfied:
(1) $p_1(z) - p_3(z + \gamma)$ is a permutation of $\mathbb{F}_{p^n}$ for any $\gamma \in \mathbb{F}_{p^n}$;
(2) $p_2(z)$ is a permutation of $\mathbb{F}_{p^n}$.

The function $F(x)$ is closely related to the mapping Ω_p in Definition 2.

Some trivial examples of $p_1(z)$ and $p_3(z)$

- Let $p_1(z) = p(z) + \sum_{i=0}^{n-1} a_i z^{p^i}$ in $\mathbb{F}_{p^n}[z]$ with a PP $p(z)$ of $\mathbb{F}_{p^n}$.
- Let $p_3(z) = \sum_{i=0}^{n-1} a_i z^{p^i}$.
- $p_1(z) - p_3(z+\gamma) = p(z) - \sum_{i=0}^{n-1} a_i \gamma^{p^i}$ is a PP of $\mathbb{F}_{p^n}$ for any $\gamma \in \mathbb{F}_{p^n}$.

Non-trivial examples of $p_1(z)$ and $p_3(z)$ for $p = 2$

Proposition 4

Let $n = 2m$ with an odd positive integer m and $d = 2^k + 1$ with an even positive integer k. Let ω be a primitive root of $\mathbb{F}_{2^2}$, $p_1(z) = z^d$ and $p_3(z) = \omega z^d$. Then $p_1(z) + p_3(z + \gamma)$ for any $\gamma \in \mathbb{F}_{2^n}$ is a permutation of $\mathbb{F}_{2^n}$.

Non-trivial examples of $p_1(z)$ and $p_3(z)$ for $p = 3$

Proposition 5

For a positive odd integer n with $n \geq 3$, if $d \equiv -1 (\mathrm{mod}\, 3)$ and $\gcd(d, 3^{2n} - 1) = 1$, then

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

is a permutation of $\mathbb{F}_{3^n}$, where $D_d(z, 1)$ is the Dickson polynomial.

Corollary

Let n and k be two positive odd integers with $k \leq n - 2$. Let $d = \frac{3^{k+1}+1}{2}$ and $p_1(z) = z^d$, $p_3(z) = -z^d$ be polynomials over $\mathbb{F}_{3^n}$. Then $p_1(z) - p_3(z + \gamma)$ is a permutation of $\mathbb{F}_{3^n}$ for any γ in $\mathbb{F}_{3^n}$.

Outline

The upper bounds on algebraic degree

- Let n be any positive integer.
- Any CPP of $\mathbb{F}_{p^{2n}} \dashrightarrow$ deg $\leq 2n(p-1)-1$.

CPPs	Finite field	Upper bound
Any one-round CPPs	$\mathbb{F}_{2^n}^2$	$n-1$
Any two-round CPPs	$\mathbb{F}_{2^n}^2$	$2n-3$
12 classes of three-round CPPs	$\mathbb{F}_{2^n}^2$	$2n-3$
4 classes of three-round CPPs	$\mathbb{F}_{2^n}^2$	$2n-2$
A class of general CPPs	$\mathbb{F}_{p^n}^2$	$2n(p-1)-3$

Table: The upper bounds of algebraic degree of the proposed CPPs

- The upper bounds are achievable by carefully choosing the polynomials $p_i(z)$, $i = 1, 2, 3$.

Outline

Conclusion

- Feistel and MISTY structures $\dashrightarrow$ CPPs;
- Upper bounds on the algebraic degree $\dashrightarrow$ CPPs;
- CPPs$\dashrightarrow$ nearly optimal algebraic degree.

Xiaofang Xu, Chunlei Li, Xiangyong Zeng, Tor Helleseth, Constructions of complete permutation polynomials, *Designs, Codes and Cryptography*, 2018, DOI 10.1007/s10623-018-0480-7.

Open problems

Open Problem 1

Find polynomials $p_1(z)$, $p_2(z)$ *in* $\mathbb{F}_{p^n}[z]$ *with other forms such that* $p_1(z) - p_2(z+\gamma)$ *is a permutation of* $\mathbb{F}_{p^n}$ *for any* $\gamma \in \mathbb{F}_{p^n}$.

Open Problem 2

For a PP $p(z)$ *in* $\mathbb{F}_{p^n}[z]$, *if* $p(z) - \beta p(z+\gamma)$ *permutes* $\mathbb{F}_{p^n}$ *for any* $\gamma \in \mathbb{F}_{p^n}$ *with* $\beta \in \mathbb{F}_{p^n} \setminus \{0, 1\}$, *do there exist some relationship between* $p(z)$ *and perfect nonlinear functions?*

Open problem 3

Do there exist CPPs with maximum possible algebraic degree constructed from the Feistel structure and/or MISTY structure?

Thanks

Thanks for your attention!