Analysis, classification and construction of APN Boolean functions

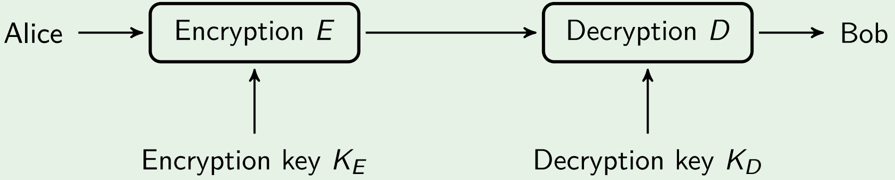
Irene Villa

University of Trento

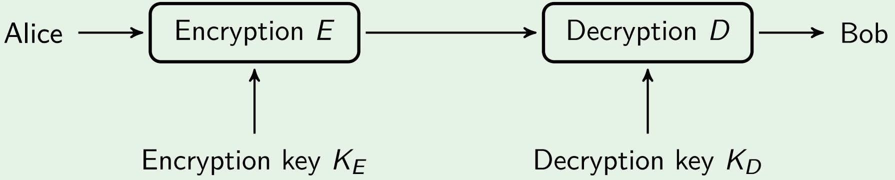
March 25, 2021

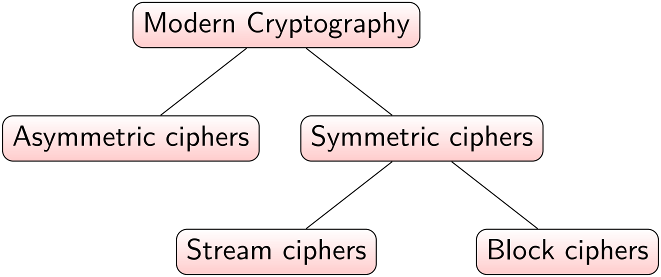
Table of Contents

Cryptography

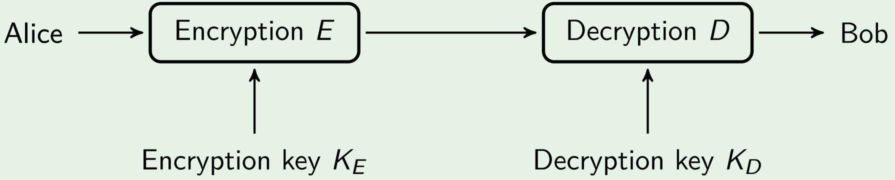


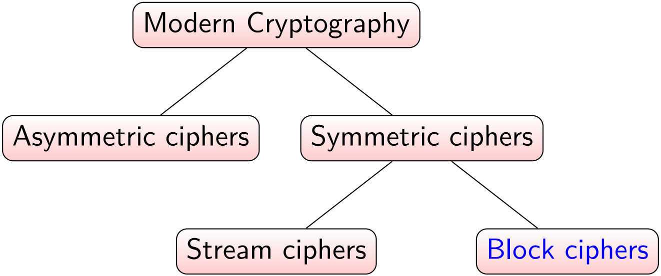
Cryptography





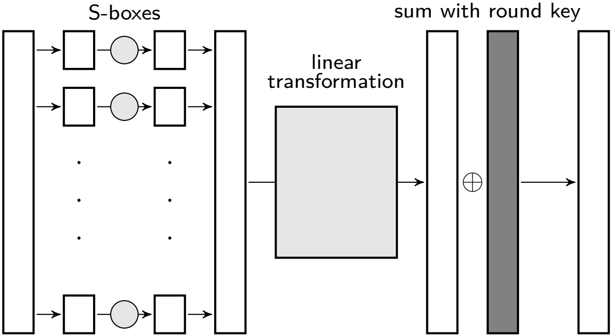
Cryptography



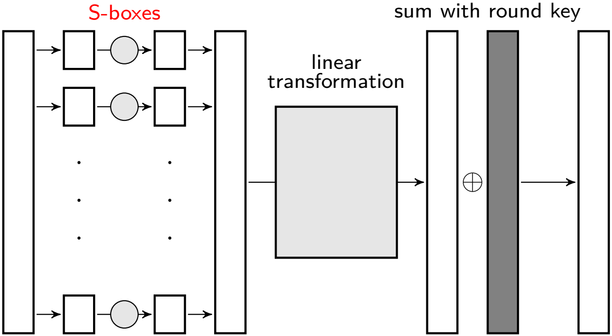


Block ciphers

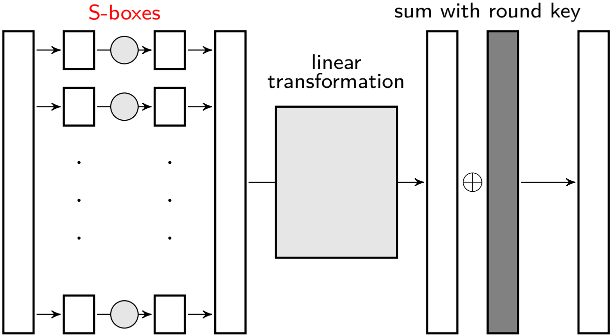
Block ciphers



Block ciphers



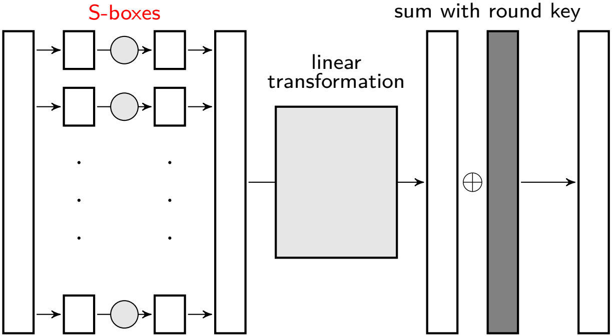
Block ciphers



Substitution box (S-box)

- vectorial Boolean function
- nonlinear
- often invertible
- cryptographic properties

Block ciphers



Substitution box (S-box)

- vectorial Boolean function
- nonlinear
- often invertible
- cryptographic properties

Vectorial Boolean functions

- $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

Vectorial Boolean functions

- $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$
- $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ equivalently $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Vectorial Boolean functions

- $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$
- $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ equivalently $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Vectorial Boolean functions

- $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$
- $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ equivalently $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$
  - F is a permutation if $Im(F) = \mathbb{F}_{2^n}$

Vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Univariate representation of F

$$F(x) = \sum_{i=0}^{2^n-1} b_i x^i, \qquad b_i \in \mathbb{F}_{2^n}$$

Vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Univariate representation of F

$$F(x) = \sum_{i=0}^{2^n-1} b_i x^i, \qquad b_i \in \mathbb{F}_{2^n}$$

- F linear if $F(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$
- F affine if $F =$ linear $+$ constant
- F DO polynomial if $F(x) = \sum_{i,j=0}^{n-1} b_{ij} x^{2^i+2^j}$, $i < j$
- F quadratic if $F =$ DO $+$ affine

Vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Univariate representation of F

$$F(x) = \sum_{i=0}^{2^n-1} b_i x^i, \qquad b_i \in \mathbb{F}_{2^n}$$

- F linear if $F(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$
- F affine if $F =$ linear $+$ constant
- F DO polynomial if $F(x) = \sum_{i,j=0}^{n-1} b_{ij} x^{2^i+2^j}$, $i < j$
- F quadratic if $F =$ DO $+$ affine

Example of linear function

The trace map: $\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$

Differential uniformity

Important cryptographic property related to the differential attack

Differentially δ-uniform

For $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

$$\delta = \max_{a,b \in \mathbb{F}_{2^n} a \neq 0} |\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = b\}|$$

Differential uniformity

Important cryptographic property related to the differential attack

Differentially δ-uniform

For $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

$$\delta = \max_{a,b \in \mathbb{F}_{2^n}\, a \neq 0} \left|\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = b\}\right|$$

F is called almost perfect nonlinear (APN) if $\delta = 2$

Differential uniformity

Equivalence relations

Differential uniformity is invariant under the following equivalence relations

- **linear equivalence** $F \overset{lin}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 linear permutations)
- **affine equivalence** $F \overset{aff}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 affine permutations)
- **EA-equivalence** (extended affine) $F \overset{EA}{\sim} F' + A$ ($F' \overset{aff}{\sim} F$, A affine)
- **CCZ-equivalence** $F \overset{CCZ}{\sim} G$ if $\Gamma_G = \mathcal{L}(\Gamma_F)$
  (Γ_F graph of F, $\mathcal{L}$ affine permutation)

Differential uniformity

Equivalence relations

Differential uniformity is invariant under the following equivalence relations

linear equivalence	$F \overset{lin}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 linear permutations)
affine equivalence	$F \overset{aff}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 affine permutations)
EA-equivalence (extended affine)	$F \overset{EA}{\sim} F' + A$ ($F' \overset{aff}{\sim} F$, A affine)
CCZ-equivalence	$F \overset{CCZ}{\sim} G$ if $\Gamma_G = \mathcal{L}(\Gamma_F)$ (Γ_F graph of F, $\mathcal{L}$ affine permutation)

- $\{$linear eq.$\} \subseteq \{$affine eq.$\} \subseteq \{$EA-eq.$\} \subseteq \{$CCZ-eq.$\}$

Differential uniformity

Equivalence relations

Differential uniformity is invariant under the following equivalence relations

- **linear equivalence** $F \overset{lin}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 linear permutations)
- **affine equivalence** $F \overset{aff}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 affine permutations)
- **EA-equivalence (extended affine)** $F \overset{EA}{\sim} F' + A$ ($F' \overset{aff}{\sim} F$, A affine)
- **CCZ-equivalence** $F \overset{CCZ}{\sim} G$ if $\Gamma_G = \mathcal{L}(\Gamma_F)$ (Γ_F graph of F, $\mathcal{L}$ affine permutation)

- $\{\text{linear eq.}\} \subseteq \{\text{affine eq.}\} \subseteq \{\text{EA-eq.}\} \subseteq \{\text{CCZ-eq.}\}$
- construction methods of optimal functions

Differential uniformity

Equivalence relations

Differential uniformity is invariant under the following equivalence relations

- **linear equivalence** $F \overset{lin}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 linear permutations)
- **affine equivalence** $F \overset{aff}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 affine permutations)
- **EA-equivalence** (extended affine) $F \overset{EA}{\sim} F' + A$ ($F' \overset{aff}{\sim} F$, A affine)
- **CCZ-equivalence** $F \overset{CCZ}{\sim} G$ if $\Gamma_G = \mathcal{L}(\Gamma_F)$ (Γ_F graph of F, $\mathcal{L}$ affine permutation)

- $\{\text{linear eq.}\} \subseteq \{\text{affine eq.}\} \subseteq \{\text{EA-eq.}\} \subseteq \{\text{CCZ-eq.}\}$
- construction methods of optimal functions
- classification of optimal functions

Differential uniformity

Equivalence relations

Differential uniformity is invariant under the following equivalence relations

linear equivalence	$F \overset{lin}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 linear permutations)
affine equivalence	$F \overset{aff}{\sim} A_1 \circ F \circ A_2$ (A_1, A_2 affine permutations)
EA-equivalence (extended affine)	$F \overset{EA}{\sim} F' + A$ ($F' \overset{aff}{\sim} F$, A affine)
CCZ-equivalence	$F \overset{CCZ}{\sim} G$ if $\Gamma_G = \mathcal{L}(\Gamma_F)$ (Γ_F graph of F, $\mathcal{L}$ affine permutation)

- $\{\text{linear eq.}\} \subseteq \{\text{affine eq.}\} \subseteq \{\text{EA-eq.}\} \subseteq \{\text{CCZ-eq.}\}$
- construction methods of optimal functions
- classification of optimal functions
- invariants

On APN functions over $\mathbb{F}_{2^n}$

1994

On APN functions over $\mathbb{F}_{2^n}$

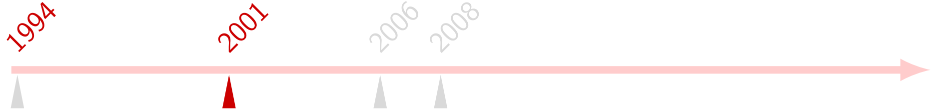
1994

- 6 families of power APN functions

Known APN power functions $F(x) = x^d$ over $\mathbb{F}_{2^n}$

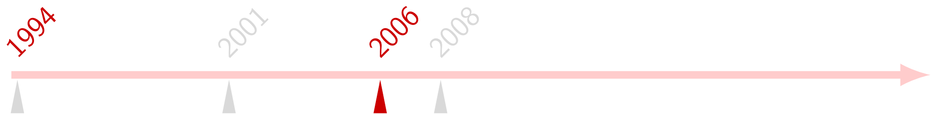
Name	Exponent d	Conditions	Degree
Gold	$2^i + 1$	$\gcd(i, n)$=1	2
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n)$=1	i+1
Welch	$2^t + 3$	$n = 2t + 1$	3
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	$\frac{t+2}{2}$ t+1
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$

On APN functions over $\mathbb{F}_{2^n}$



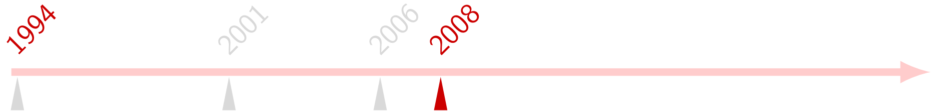
- 6 families of power APN function

On APN functions over $\mathbb{F}_{2^n}$



- 6 families of power APN function

On APN functions over $\mathbb{F}_{2^n}$



- 6 families of power APN function

On APN functions over $\mathbb{F}_{2^n}$

1994 2001 2006 2008

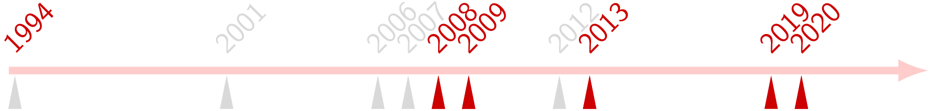
- 6 families of power APN function
- 16 families of quadratic APN functions

Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent fo power functions

N°	APN function over $\mathbb{F}_{2^n}$	Conditions
C1-C2	$x^{2^s+1}+\alpha^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk$, $\gcd(k,3)=\gcd(s,3k)=1$, $p\in\{3,4\}$, $i=sk \mod p$, $m=p-i$, $n\geq 12$, α primitive in $\mathbb{F}_{2^n}^*$
C3	$x^{2^{2i}+2^i}+bx^{q+1}+cx^{q(2^{2i}+2^i)}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $gcd(2^i+1,q+1)\neq 1$, $cb^q+b\neq 0$, $c\notin\{\lambda^{(2^i+1)(q-1)},\lambda\in\mathbb{F}_{2^n}\}$, $c^{q+1}=1$
C4	$x(x^{2^i}+x^q+cx^{2^iq})+$ $x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}$, $s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ is irreducible over $\mathbb{F}_{2^n}$
C5	$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a\neq 0$
C6	$x^3+a^{-1}\mathrm{Tr}_n^3(a^3x^9+a^6x^{18})$	$3\mid n$, $a\neq 0$
C7	$x^3+a^{-1}\mathrm{Tr}_n^3(a^6x^{18}+a^{12}x^{36})$	$3\mid n$, $a\neq 0$
C8-C10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k$, $\gcd(k,3)=\gcd(s,3k)=1$, $v,w\in\mathbb{F}_{2^k}$, $vw\neq 1$, $3\mid(k+s)$, $\mathbb{F}_{2^n}^\star=\langle u\rangle$

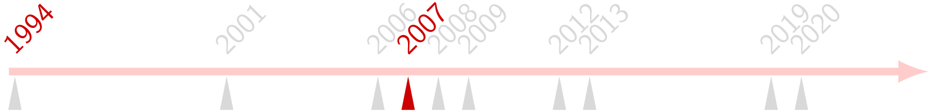
N°	APN function over $\mathbb{F}_{2^n}$	Conditions
C11	$dx^{2^i+1} + d^q x^{q(2^i+1)} +$ $cx^{q+1} + \sum_{s=1}^{m-1} \gamma_s x^{2^s(q+1)}$	$q = 2^m,\ n = 2m,\ \gcd(i, m) = 1,\ i, m$ odd, $c \notin \mathbb{F}_{2^m},\ \gamma_s \in \mathbb{F}_{2^m},\ d$ not a cube
C12	$(x + x^q)^{2^i+1} +$ $u'(ux + u^q x^q)^{(2^i+1)2^j} +$ $u(x + x^q)(ux + u^q x^q)$	$q = 2^m,\ n = 2m,\ m \geq 2$ even, $\gcd(i, m) = 1$ and j even $\mathbb{F}_{2^n}^\star = \langle u \rangle,\ u' \in \mathbb{F}_{2^m}$ not a cube
C13	$ut(x)(x^q + x) + t(x)^{2^{2i}+2^{3i}} +$ $at(x)^{2^{2i}}(x^q + x)^{2^i} + b(x^q + x)^{2^i+1}$	$q = 2^m,\ n = 2m,\ \gcd(i, m) = 1$ $a, b \in \mathbb{F}_{2^m}, u \notin \mathbb{F}_{2^m},\ t(x) = u^q x + x^q u$ and $X^{2^i+1} + aX + b$ has no solution over $\mathbb{F}_{2^m}$
C14	$x^3 + ax^{2^k(2^i+1)}$ $+bx^{3\cdot 2^m} + cx^{2^{n+k}(2^i+1)}$	$n = 2m = 10, (a, b, c) = (\beta, 1, 0), i = 3, k = 2, \mathbb{F}_4^* = \langle \beta \rangle$ $n = 2m, m$ odd, $3 \nmid m, (a, b, c) = (\beta, \beta^2, 1)$, $\mathbb{F}_4^* = \langle \beta \rangle,\ i \in \{m-2, m, 2m-1, (m-2)^{-1} \mod n\}$
C15	$u[t(x)^{2^i+1} + t(x)(x^q + x)^{2^i}$ $+(x^q + x)^{2^i+1}] + t(x)^{2^{2i}+1}$ $+t(x)^{2^{2i}}(x^q + x) + (x^q + x)^{2^{2i}+1}$	$q = 2^m,\ n = 2m,\ \gcd(3i, m) = 1$, $\mathbb{F}_{2^n}^\star = \langle u \rangle,\ t(x) = u^q x + ux^q$
C16	$u[t(x)^{2^i+1} + t(x)(x^q + x)^{2^i}$ $+(x^q + x)^{2^i+1}] + t(x)^{2^{3i}}(x^q + x)$ $+t(x)(x^q + x)^{2^{3i}}$	m odd, $q = 2^m,\ n = 2m,\ \gcd(3i, m) = 1$, $\mathbb{F}_{2^n}^\star = \langle u \rangle,\ t(x) = u^q x + ux^q$

On APN functions over $\mathbb{F}_{2^n}$



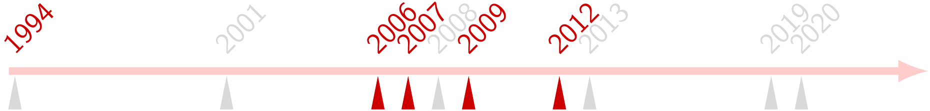
- 6 families of power APN functions
- 16 families of quadratic APN functions

On APN functions over $\mathbb{F}_{2^n}$



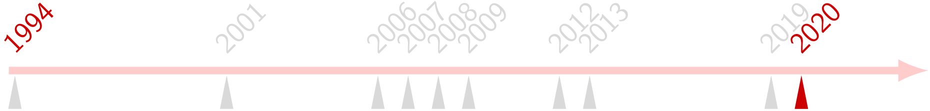
- 6 families of power APN functions
- 16 families of quadratic APN functions
- complete classification of APN functions for $n \leq 5$

On APN functions over $\mathbb{F}_{2^n}$



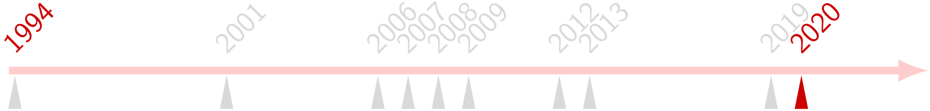
- 6 families of power APN functions
- 16 families of quadratic APN functions
- complete classification of APN functions for $n \leq 5$
- complete classification of quadratic and cubic APN functions for $n = 6$ (13 quadratic and 1 cubic CCZ-classes)

On APN functions over $\mathbb{F}_{2^n}$



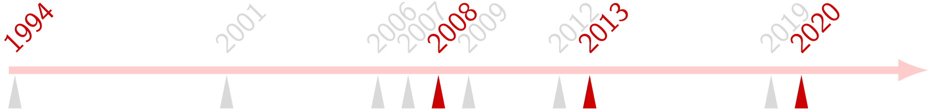
- 6 families of power APN functions
- 16 families of quadratic APN functions
- complete classification of APN functions for $n \leq 5$
- complete classification of quadratic and cubic APN functions for $n = 6$ (13 quadratic and 1 cubic CCZ-classes)
- complete classification of quadratic APN functions for $n = 7$ (488 quadratic CCZ-classes)

On APN functions over $\mathbb{F}_{2^n}$



- 6 families of power APN functions
- 16 families of quadratic APN functions
- complete classification of APN functions for $n \leq 5$
- complete classification of quadratic and cubic APN functions for $n = 6$ (13 quadratic and 1 cubic CCZ-classes)
- complete classification of quadratic APN functions for $n = 7$ (488 quadratic CCZ-classes)
- complete classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for $n = 8, 9$

On APN functions over $\mathbb{F}_{2^n}$



- 6 families of power APN functions
- 16 families of quadratic APN functions
- complete classification of APN functions for $n \leq 5$
- complete classification of quadratic and cubic APN functions for $n = 6$ (13 quadratic and 1 cubic CCZ-classes)
- complete classification of quadratic APN functions for $n = 7$ (488 quadratic CCZ-classes)
- complete classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for $n = 8, 9$
- (not exhaustive) lists of CCZ-inequivalent quadratic APN functions for $n = 8, 9, 10$

APN permutations over $\mathbb{F}_{2^n}$

APN permutations over $\mathbb{F}_{2^n}$

- If n is odd, few functions know (power APN + family (C1) + 2 maps over $\mathbb{F}_{2^9}$)

APN permutations over $\mathbb{F}_{2^n}$

- If n is odd, few functions know (power APN + family (C1) + 2 maps over $\mathbb{F}_{2^9}$)
- If n is even, only one example for $n = 6$ (CCZ-eq. to a quadratic APN function) (2009)

APN permutations over $\mathbb{F}_{2^n}$

- If n is odd, few functions know (power APN + family (C1) + 2 maps over $\mathbb{F}_{2^9}$)
- If n is even, only one example for $n = 6$ (CCZ-eq. to a quadratic APN function) (2009)
- For n even, some non-existence results are known

APN permutations over $\mathbb{F}_{2^n}$

- If n is odd, few functions know (power APN + family (C1) + 2 maps over $\mathbb{F}_{2^9}$)
- If n is even, only one example for $n = 6$ (CCZ-eq. to a quadratic APN function) (2009)
- For n even, some non-existence results are known

The big APN problem

- Construct other APN permutations in even dimension
- Construct an infinite family of APN permutations for even dimensions

Open problems and research interests

- The big APN problem
- Construct other infinite families of APN functions
- Increase the lists of known CCZ-inequivalent APN functions
- Find an equivalence relation more general than CCZ-equivalence
- Provide new CCZ/EA-invariants to help determining the equivalence between functions

Combination of theoretical analysis with computational results

List of papers

1. **Constructing APN functions through isotopic shifts**
   Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert Coulter and I.V., *IEEE Transaction on Information Theory*, vol. 66, no. 8, pp. 5299-5309, 2020.
2. **Generalised isotopic shift construction for APN functions**
   Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert Coulter and I.V., *Designs, Codes and Cryptography*, 2020.
3. **On equivalence between known families of quadratic APN functions**
   Lilya Budaghyan, Marco Calderini and I.V., *Finite Fields and their Applications*, vol. 66, 2020.
4. **Isotopic shift construction for planar functions**
   Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert Coulter and I.V., *2019 IEEE International Symposium on Information Theory (ISIT)*, pp. 2962-2966, 2019.

Planar functions over $\mathbb{F}_{p^n}$

$$\boxed{F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \text{ with } p \text{ prime}}$$

Planar functions over $\mathbb{F}_{p^n}$

$$\boxed{F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \text{ with } p \text{ prime}}$$

- univariate polynomial representation $F(x) = \sum_{i=0}^{p^n-1} b_i x^i,\ b_i \in \mathbb{F}_{p^n}$
- linear, affine, DO and quadratic functions
- differential uniformity

Planar functions over $\mathbb{F}_{p^n}$

$$\boxed{F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \text{ with } p \text{ prime}}$$

- univariate polynomial representation $F(x) = \sum_{i=0}^{p^n-1} b_i x^i,\ b_i \in \mathbb{F}_{p^n}$
- linear, affine, DO and quadratic functions
- differential uniformity

F planar (or differentially 1-uniform)

For any $a \in \mathbb{F}_{p^n}^\star$, $b \in \mathbb{F}_{p^n}$ $F(x+a) - F(x) = b$ has at most one solution.

Planar functions over $\mathbb{F}_{p^n}$

$$\boxed{F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \text{ with } p \text{ prime}}$$

- univariate polynomial representation $F(x) = \sum_{i=0}^{p^n-1} b_i x^i$, $b_i \in \mathbb{F}_{p^n}$
- linear, affine, DO and quadratic functions
- differential uniformity

F planar (or differentially 1-uniform)

For any $a \in \mathbb{F}_{p^n}^{\star}$, $b \in \mathbb{F}_{p^n}$ $F(x+a) - F(x) = b$ has at most one solution.

- linear, affine, EA- and CCZ-equivalence

Isotopic equivalence

- defined for quadratic planar functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
- more general than CCZ-equivalence

Isotopic equivalence

- defined for quadratic planar functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
- more general than CCZ-equivalence

Theorem

For two isotopic equivalent quadratic planar functions F and F' there exists a linear permutation L such that $F' \overset{EA}{\sim} F_L$.

Isotopic equivalence

- defined for quadratic planar functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$
- more general than CCZ-equivalence

Theorem

For two isotopic equivalent quadratic planar functions F and F' there exists a linear permutation L such that $F' \overset{EA}{\sim} F_L$.

The isotopic shift of F by L

$$\boxed{F_L(x) = F(x + L(x)) - F(x) - F(L(x))}$$

In the past years, known families of APN functions have been used to construct planar functions, and vice versa.

Isotopic shift applied to APN maps

In the past years, known families of APN functions have been used to construct planar functions, and vice versa.

$$\boxed{F_L(x) = F(x + L(x)) + F(x) + F(L(x)) \in \mathbb{F}_{2^n}[x]}$$

Isotopic shift applied to APN maps

In the past years, known families of APN functions have been used to construct planar functions, and vice versa.

$$\boxed{F_L(x) = F(x + L(x)) + F(x) + F(L(x)) \in \mathbb{F}_{2^n}[x]}$$

Some properties

- For $F \in \mathbb{F}_{2^n}[x]$ quadratic function and L linear, F_L is APN only if L is a permutation or 2-to-1.
- The isotopic shift does not preserve the differential uniformity.

Isotopic shift of Gold functions

For F a Gold function $F(x) = x^{2^i+1}$,

$$\boxed{F_L(x) = x^{2^i} L(x) + xL(x)^{2^i}}$$

Isotopic shift of Gold functions

For F a Gold function $F(x) = x^{2^i+1}$,

$$\boxed{F_L(x) = x^{2^i} L(x) + xL(x)^{2^i}}$$

When L is a monomial

All such APN maps F_L over $\mathbb{F}_{2^n}$ for $3 \leq n \leq 12$ are affine equivalent to some Gold maps.

$$F_L(x) = x^{2^i} L(x) + x L(x)^{2^i}$$

For $n = km$, $L(x) = \sum_{i=0}^{k-1} b_i x^{2^{im}}$ is a 2^m-polynomial.

Theorem

Characterisation of APN maps F_L over $\mathbb{F}_{2^n}$ with $n = km$, $\gcd(n, i) = 1$ and L a 2^m-polynomial.

$F_L(x) = x^{2^i} L(x) + xL(x)^{2^i}$

For $n = km$, $L(x) = \sum_{i=0}^{k-1} b_i x^{2^{im}}$ is a 2^m-polynomial.

Theorem

Characterisation of APN maps F_L over $\mathbb{F}_{2^n}$ with $n = km$, $\gcd(n, i) = 1$ and L a 2^m-polynomial.

Constructed APN functions over $\mathbb{F}_{2^n}$ for $n = 6, 8, 9, 12, 18$.

- For $n = 9$ $(k = m = 3)$ and $i = 1$, constructed F_L APN and not CCZ-equivalent to any known map (**new**).
- For $n = 8$ $(k = 4,\ m = 2)$ and $i = 3$ constructed $F_L \overset{EA}{\sim} x^9 + \mathrm{Tr}(x^3)$, APN map known since 2006 but not part of any known family (**unclassified**).

$$F_L(x) = x^{2^i}L(x) + xL(x)^{2^i}$$

For $n = km$, $L(x) = \sum_{i=0}^{k-1} b_i x^{2^{im}}$ is a 2^m-polynomial.

Theorem

Characterisation of APN maps F_L over $\mathbb{F}_{2^n}$ with $n = km$, $\gcd(n, i) = 1$ and L a 2^m-polynomial.

Constructed APN functions over $\mathbb{F}_{2^n}$ for $n = 6, 8, 9, 12, 18$.

- For $n = 9$ $(k = m = 3)$ and $i = 1$, constructed F_L APN and not CCZ-equivalent to any known map (**new**).
- For $n = 8$ $(k = 4,\ m = 2)$ and $i = 3$ constructed $F_L \overset{EA}{\sim} x^9 + \mathrm{Tr}(x^3)$, APN map known since 2006 but not part of any known family (**unclassified**).

Conjecture

The Theorem covers APN functions for an infinite number of dimensions n.

The case $n = 6$

The isotopic shift connects any two quadratic APN maps over $\mathbb{F}_{2^6}$

For any $F, G \in \mathbb{F}_{2^6}[x]$ quadratic APN functions there exist L, L' linear maps with L permutation and L' 2-to-1 such that F_L and $F_{L'}$ are EA-equivalent to G.

Isotopic shift with L linear

$$F_L(x) = F(x + L(x)) + F(x) + F(L(x)).$$

When F is a Gold map,

$$F_L(x) = xL(x)^{2^i} + x^{2^i} L(x).$$

Isotopic shift with L linear

$$F_L(x) = F(x + L(x)) + F(x) + F(L(x)).$$

When F is a Gold map,

$$F_L(x) = x L_1(x)^{2^i} + x^{2^i} L_2(x).$$

Isotopic shift with L ~~linear~~ not linear

$$F_L(x) = F(x + L(x)) + F(x) + F(L(x)).$$

When F is a Gold map,

$$F_L(x) = x L_1(x)^{2^i} + x^{2^i} L_2(x).$$

$xL_1(x)^{2^i} + x^{2^i}L_2(x)$ with L_1, L_2 linear

$xL_1(x)^{2^i} + x^{2^i}L_2(x)$ with L_1, L_2 linear

Theorem

Characterisation of APN maps $xL_1(x)^{2^i} + x^{2^i}L_2(x)$ over $\mathbb{F}_{2^n}$ with $n = km$, $\gcd(i, m) = 1$ and L_1, L_2 2^m-polynomials.

$xL_1(x)^{2^i} + x^{2^i}L_2(x)$ with L_1, L_2 linear

Theorem

Characterisation of APN maps $xL_1(x)^{2^i} + x^{2^i}L_2(x)$ over $\mathbb{F}_{2^n}$ with $n = km$, $\gcd(i, m) = 1$ and L_1, L_2 2^m-polynomials.

- For $n = 8$ ($k = 4$, $m = 2$) with L_1, L_2 with coefficients over $\mathbb{F}_{2^4}$ many APN functions constructed (**several unclassified**).
- For $n = 9$ ($k = m = 3$) with L_1, L_2 with coefficients over $\mathbb{F}_{2^3}$ many APN functions constructed (**15 new** and **one unclassified**).

F_L with L not necessarily linear

F_L with L not necessarily linear

Theorem

Over $\mathbb{F}_{2^n}$ with n odd, F any known APN power function (except Dobbertin) there exists a monomial $L(x) = ax^d$ and a Gold map $G(x) = x^{2^i+1}$ such that $G_L \overset{EA}{\sim} F$.

New EA-invariant

New EA-invariant

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

$$S(F) = \{b \in \mathbb{F}_{2^n} : \exists a \in \mathbb{F}_{2^n} \ s.t. \ \mathcal{W}_F(a, b) = 0\}$$

Proposition

Let N_i be the number of $\mathbb{F}_2$-vector subspaces of $\mathbb{F}_{2^n}$ contained in $S(F)$ of dimension i. The values N_i for $i = 0, \ldots, n$ are EA-invariant.

$\mathcal{W}_F(a, b) = \Sigma_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax+bF(x))}$ is the Walsh transform of F in (a, b)

Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

N°	Functions
C1-C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$
C3	$x^{2^{2i}+2^i}+cx^{q+1}+dx^{q(2^{2i}+2^i)}$
C4	$x(x^{2^i}+x^q+cx^{2^iq})+$ $x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$
C5	$x^3+a^{-1}Tr(a^3x^9)$
C6	$x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$
C7	$x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$
C8-C10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$
C11	$dx^{2^i+1}+d^qx^{q(2^i+1)}+$ $cx^{q+1}+\sum_{s=1}^{m-1}\gamma_sx^{2^s(q+1)}$
C17	$L_1(x)^{2^i}x+L_2(x)x^{2^i}$

N°	Functions
C12	$(x+x^q)^{2^i+1}+$ $u'(ux+u^qx^q)^{(2^i+1)2^j}+$ $u(x+x^q)(ux+u^qx^q)$
C13	$(u^{q+1}x+u^2x^q)(x^q+x)+$ $(u^qx+ux^q)^{2^{2i}+2^{3i}}+b(x^q+x)^{2^i+1}+$ $a(u^qx+ux^q)^{2^{2i}}(x^q+x)^{2^i}$
C14	$x^3+ax^{2^k(2^i+1)}+$ $bx^{3\cdot 2^m}+cx^{2^{n+k}(2^i+1)}$
C15	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{2i}+1}+t(x)^{2^{2i}}(x^q+x)+(x^q+x)^{2^{2i}+1}$
C16	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{3i}}(x^q+x)+t(x)(x^q+x)^{2^{3i}}$

Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

N°	Functions
C1-C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$
C3	$x^{2^{2i}+2^i}+cx^{q+1}+dx^{q(2^{2i}+2^i)}$
C4	$x(x^{2^i}+x^q+cx^{2^iq})+$ $x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$
C5	$x^3+a^{-1}Tr(a^3x^9)$
C6	$x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$
C7	$x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$
C8-C10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$
C11	$dx^{2^i+1}+d^qx^{q(2^i+1)}+$ $cx^{q+1}+\sum_{s=1}^{m-1}\gamma_s x^{2^s(q+1)}$
C17	$L_1(x)^{2^i}x+L_2(x)x^{2^i}$

N°	Functions
C12	$(x+x^q)^{2^i+1}+$ $u'(ux+u^qx^q)^{(2^i+1)2^j}+$ $u(x+x^q)(ux+u^qx^q)$
C13	$(u^{q+1}x+u^2x^q)(x^q+x)+$ $(u^qx+ux^q)^{2^{2i}+2^{3i}}+b(x^q+x)^{2^i+1}+$ $a(u^qx+ux^q)^{2^{2i}}(x^q+x)^{2^i}$
C14	$x^3+ax^{2^k(2^i+1)}+$ $bx^{3\cdot 2^m}+cx^{2^{n+k}(2^i+1)}$
C15	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{2i}+1}+t(x)^{2^{2i}}(x^q+x)+(x^q+x)^{2^{2i}+1}$
C16	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{3i}}(x^q+x)+t(x)(x^q+x)^{2^{3i}}$

L. Budaghyan, T. Helleseth, N. Li, B. Sun *Some results on the known classes of quadratic APN functions.* Codes, Cryptology and Information Security - C2SI 2017 (2017).

Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

N°	Functions
C1-C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$
C3	$x^{2^{2i}+2^i}+cx^{q+1}+dx^{q(2^{2i}+2^i)}$
C4	$x(x^{2^i}+x^q+cx^{2^iq})+$ $x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$
C5	$x^3+a^{-1}Tr(a^3x^9)$
C6	$x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$
C7	$x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$
C8-C10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$
C11	$dx^{2^i+1}+d^qx^{q(2^i+1)}+$ $cx^{q+1}+\sum_{s=1}^{m-1}\gamma_s x^{2^s(q+1)}$
C17	$L_1(x)^{2^i}x+L_2(x)x^{2^i}$

N°	Functions
C12	$(x+x^q)^{2^i+1}+$ $u'(ux+u^qx^q)^{(2^i+1)2^j}+$ $u(x+x^q)(ux+u^qx^q)$
C13	$(u^{q+1}x+u^2x^q)(x^q+x)+$ $(u^qx+ux^q)^{2^{2i}+2^{3i}}+b(x^q+x)^{2^i+1}+$ $a(u^qx+ux^q)^{2^{2i}}(x^q+x)^{2^i}$
C14	$x^3+ax^{2^k(2^i+1)}+$ $bx^{3\cdot 2^m}+cx^{2^{n+k}(2^i+1)}$
C15	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{2i}+1}+t(x)^{2^{2i}}(x^q+x)+(x^q+x)^{2^{2i}+1}$
C16	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{3i}}(x^q+x)+t(x)(x^q+x)^{2^{3i}}$

L. Budaghyan, T. Helleseth, N. Li, B. Sun *Some results on the known classes of quadratic APN functions.* Codes, Cryptology and Information Security - C2SI 2017 (2017).

Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

N°	Functions
C1-C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$
C3	$x^{2^{2i}+2^i}+cx^{q+1}+dx^{q(2^{2i}+2^i)}$
C4	$x(x^{2^i}+x^q+cx^{2^iq})+$ $x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$
C5	$x^3+a^{-1}Tr(a^3x^9)$
C6	$x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$
C7	$x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$
C8-C10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$
C11	$dx^{2^i+1}+d^qx^{q(2^i+1)}+$ $cx^{q+1}+\sum_{s=1}^{m-1}\gamma_s x^{2^s(q+1)}$
C17	$L_1(x)^{2^i}x+L_2(x)x^{2^i}$

N°	Functions
C12	$(x+x^q)^{2^i+1}+$ $u'(ux+u^qx^q)^{(2^i+1)2^j}+$ $u(x+x^q)(ux+u^qx^q)$
C13	$(u^{q+1}x+u^2x^q)(x^q+x)+$ $(u^qx+ux^q)^{2^{2i}+2^{3i}}+b(x^q+x)^{2^i+1}+$ $a(u^qx+ux^q)^{2^{2i}}(x^q+x)^{2^i}$
C14	$x^3+ax^{2^k(2^i+1)}+$ $bx^{3\cdot 2^m}+cx^{2^{n+k}(2^i+1)}$
C15	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{2i}+1}+t(x)^{2^{2i}}(x^q+x)+(x^q+x)^{2^{2i}+1}$
C16	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{3i}}(x^q+x)+t(x)(x^q+x)^{2^{3i}}$

L. Budaghyan, T. Helleseth, N. Li, B. Sun *Some results on the known classes of quadratic APN functions.* Codes, Cryptology and Information Security - C2SI 2017 (2017).

APN functions over $\mathbb{F}_{2^n}$:

- (C3)[1] $cx^{2^m+1} + x^{2^{2i}+2^i} + dx^{2^m(2^{2i}+2^i)}$

  with $n = 2m$, $\gcd(i, m) = 1$, $d^{2^m+1} = 1$, $d \notin \{\lambda^{(2^i+1)(2^m+1)} : \lambda \in \mathbb{F}_{2^n}\}$, $dc^{2^m} + c \neq 0$.

- (C11)[2] $cx^{2^m+1} + \sum_{s=1}^{m-1} \gamma_s x^{2^s(2^m+1)} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)}$

  with $n = 2m$, i odd, $\gcd(m, i) = 1$, $c \notin \mathbb{F}_{2^m}$, d not a cube, $\gamma_s \in \mathbb{F}_{2^m}$.

---

[1] L. Budaghyan, C. Carlet *Classes of quadratic APN trinomials and hexanomials and related structures*. IEEE Transaction on Information Theory 54, 5 (2008).

[2] C. Bracken, E. Byrne, N. Markin, G. McGuire *New families of quadratic almost perfect nonlinear trinomials and multinomials*. Finite Fields and their Applications 14, 3 (2008).

[3] X.Y. Duan, Y.L. Deng *Two classes of quadratic crooked functions*. Applied Mechanics and Materials 513 (2014).

APN functions over $\mathbb{F}_{2^n}$:

- (C3)[1] $cx^{2^m+1} + x^{2^{2i}+2^i} + dx^{2^m(2^{2i}+2^i)}$

  with $n = 2m$, $\gcd(i, m) = 1$, $d^{2^m+1} = 1$, $d \notin \{\lambda^{(2^i+1)(2^m+1)} : \lambda \in \mathbb{F}_{2^n}\}$, $dc^{2^m} + c \neq 0$.

- (C3*)[3] $cx^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)} + x^{2^i+2^j} + dx^{2^m(2^i+2^j)}$

  with $n = 2m$, m odd, $i > j$, $\gcd(i-j, m) = 1$, $d^{2^m+1} = 1$, $d \notin \{\lambda^{(2^i+2^j)(2^m-1)} : \lambda \in \mathbb{F}_{2^n}\}$, $dc^{2^m} + c \neq 0$, $d = \gamma_l^{1-2^m}$.

- (C11)[2] $cx^{2^m+1} + \sum_{s=1}^{m-1} \gamma_s x^{2^s(2^m+1)} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)}$

  with $n = 2m$, i odd, $\gcd(m, i) = 1$, $c \notin \mathbb{F}_{2^m}$, d not a cube, $\gamma_s \in \mathbb{F}_{2^m}$.

- (C11*)[3] $cx^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)} + L(dx^{2^i+2^j} + d^{2^m} x^{2^m(2^i+2^j)})$

  with $n = 2m$, m odd, $i > j$, $\gcd(i-j, m) = 1$, $c \notin \mathbb{F}_{2^m}$, $d \notin \{x^{2^i+2^j} : x \in \mathbb{F}_{2^n}\}$, $\gamma_l \in \mathbb{F}_{2^m}$, L linear permutation with coefficients in $\mathbb{F}_{2^m}$.

---

[1] L. Budaghyan, C. Carlet *Classes of quadratic APN trinomials and hexanomials and related structures.* IEEE Transaction on Information Theory 54, 5 (2008).

[2] C. Bracken, E. Byrne, N. Markin, G. McGuire *New families of quadratic almost perfect nonlinear trinomials and multinomials.* Finite Fields and their Applications 14, 3 (2008).

[3] X.Y. Duan, Y.L. Deng *Two classes of quadratic crooked functions.* Applied Mechanics and Materials 513 (2014).

Theorem

The families C3, C3, C11, C11* coincide and they are included in C4. In particular, the hexanomials (C4) admit a representation as pentanomials*

$$H(x) = dx^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + cx^{2^{m+i}+1} + c^{2^m}x^{2^m+2^i},$$

$n = 2m$, $\gcd(m,i) = 1$, $d \notin \mathbb{F}_{2^m}$ *and* $x^{2^i+1} + cx^{2^i} + c^{2^m}x + 1 = 0$ *has no solution* x *such that* $x^{2^m+1} = 1$.

The updated list

Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

N°	Functions	N°	Functions
F1-F2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	F11	$L_1(x)^{2^i}x+L_2(x)x^{2^i}$
F3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+$ $cx^{2^iq+1}+c^qx^{2^i+q}$	F12	$(u^{q+1}x+u^2x^q)(x^q+x)+$ $(u^qx+ux^q)^{2^{2i}+2^{3i}}+b(x^q+x)^{2^i+1}+$ $a(u^qx+ux^q)^{2^{2i}}(x^q+x)^{2^i}$
F4	$x^3+a^{-1}Tr(a^3x^9)$		
F5	$x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$	F13	$x^3+ax^{2^k(2^i+1)}+$ $bx^{3\cdot 2^m}+cx^{2^{n+k}(2^i+1)}$
F6	$x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$		
F7-F9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	F14	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{2i}+1}+t(x)^{2^{2i}}(x^q+x)+(x^q+x)^{2^{2i}+1}$
F10	$(x+x^q)^{2^i+1}+$ $u'(ux+u^qx^q)^{(2^i+1)2^j}+$ $u(x+x^q)(ux+u^qx^q)$	F15	$u[t(x)^{2^i+1}+t(x)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]$ $+t(x)^{2^{3i}}(x^q+x)+t(x)(x^q+x)^{2^{3i}}$

Finite presemifield $\mathcal{S} = (\mathbb{F}_{p^n}, +, \star)$

$\mathcal{S}$ is a ring with left and right distributivity and no zero divisor (not necessarily associative).

Finite presemifield $\mathcal{S} = (\mathbb{F}_{p^n}, +, \star)$

$\mathcal{S}$ is a ring with left and right distributivity and no zero divisor (not necessarily associative).

Isotopic equivalence

$\mathcal{S}_1 = (\mathbb{F}_{p^n}, +, \star)$ and $\mathcal{S}_2 = (\mathbb{F}_{p^n}, +, *)$ are isotopic equivalent if there exist M, N, L linear permutations such that for any $x, y \in \mathbb{F}_{p^n}$

$$T(x \star y) = M(x) * N(y).$$

Finite presemifield $\mathcal{S} = (\mathbb{F}_{p^n}, +, \star)$

$\mathcal{S}$ is a ring with left and right distributivity and no zero divisor (not necessarily associative).

Isotopic equivalence

$\mathcal{S}_1 = (\mathbb{F}_{p^n}, +, \star)$ and $\mathcal{S}_2 = (\mathbb{F}_{p^n}, +, *)$ are isotopic equivalent if there exist M, N, L linear permutations such that for any $x, y \in \mathbb{F}_{p^n}$

$$T(x \star y) = M(x) * N(y).$$

For p odd:

- Given $\mathcal{S}$ commutative, then $F_{\mathcal{S}}(x) = \frac{1}{2} x \star x \in \mathbb{F}_{p^n}[x]$ is planar DO.
- Given $F \in \mathbb{F}_{p^n}[x]$ planar DO polynomial, then $\mathcal{S}_F = (\mathbb{F}_{p^n}, +, \star)$ with $x \star y = F(x+y) - F(x) - F(y)$ is a commutative presemifield.

Quadratic planar functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\mathcal{S}_1 = (\mathbb{F}_{p^n}, +, \star) \arrow[r, dash, "\text{isotopic equivalent}", "T(x \star y) = M(x) * N(y)"'] \arrow[d, leftrightarrow] & \mathcal{S}_2 = (\mathbb{F}_{p^n}, +, *) \arrow[d, leftrightarrow] \\
F_{\mathcal{S}_1} & F_{\mathcal{S}_2}
\end{tikzcd}$$

Quadratic planar functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

$$
\begin{tikzcd}
\mathcal{S}_1 = (\mathbb{F}_{p^n}, +, \star) \arrow[rr, dash, "\text{isotopic equivalent}", "T(x \star y) = M(x) * N(y)"'] \arrow[d, leftrightarrow] & & \mathcal{S}_2 = (\mathbb{F}_{p^n}, +, *) \arrow[d, leftrightarrow] \\
F_{\mathcal{S}_1} & & F_{\mathcal{S}_2}
\end{tikzcd}
$$

- Isotopic equivalence can be extended to planar DO polynomials;
  [F, G isotopic equivalent if $\mathcal{S}_F, \mathcal{S}_G$ isotopic equivalent]
- Isotopic equivalence is more general than CCZ-equivalence;
  [CCZ-equivalence corresponds to $M = N$]
- two planar functions are CCZ-equivalent if and only if they are EA-equivalent.

Isotopic shift of quadratic planar maps over $\mathbb{F}_{p^n}$

$$\boxed{F_L(x) = F(x + L(x)) - F(x) - F(L(x))}$$

- It describes completely (up to EA-equivalence) the isotopic equivalence ($F \overset{isot}{\sim} G \to G \overset{EA}{\sim} F_L$ for some L linear permutation).

Isotopic shift of quadratic planar maps over $\mathbb{F}_{p^n}$

$$\boxed{F_L(x) = F(x + L(x)) - F(x) - F(L(x))}$$

- It describes completely (up to EA-equivalence) the isotopic equivalence ($F \overset{isot}{\sim} G \to G \overset{EA}{\sim} F_L$ for some L linear permutation).
- It can connect planar maps not isotopic equivalent.

$F(x) = x^2$, $L(x) = x^{p^j} \to F_L(x) = 2x^{p^j+1}$ (Albert function)

Isotopic shift of quadratic planar maps over $\mathbb{F}_{p^n}$

$$\boxed{F_L(x) = F(x + L(x)) - F(x) - F(L(x))}$$

- It describes completely (up to EA-equivalence) the isotopic equivalence ($F \overset{isot}{\sim} G \rightarrow G \overset{EA}{\sim} F_L$ for some L linear permutation).
- It can connect planar maps not isotopic equivalent.

$F(x) = x^2$, $L(x) = x^{p^j} \rightarrow F_L(x) = 2x^{p^j+1}$ (Albert function)

- It does not preserve the differential uniformity.

Isotopic shift of quadratic planar maps over $\mathbb{F}_{p^n}$

$$\boxed{F_L(x) = F(x + L(x)) - F(x) - F(L(x))}$$

- It describes completely (up to EA-equivalence) the isotopic equivalence ($F \overset{isot}{\sim} G \rightarrow G \overset{EA}{\sim} F_L$ for some L linear permutation).
- It can connect planar maps not isotopic equivalent.

$F(x) = x^2,\ L(x) = x^{p^j} \rightarrow F_L(x) = 2x^{p^j+1}$ (Albert function)

- It does not preserve the differential uniformity.
- If F_L is planar then L must be a permutation.

Given $F, G \in \mathbb{F}_{p^n}[x]$ quadratic maps, does the existence of a linear isotopic shift connecting F to G ($F_L \overset{EA}{\sim} G$) imply the existence of a linear isotopic shift connecting G to F?

Given $F, G \in \mathbb{F}_{p^n}[x]$ quadratic maps, does the existence of a linear isotopic shift connecting F to G ($F_L \overset{EA}{\sim} G$) imply the existence of a linear isotopic shift connecting G to F?

$$F \xrightarrow{F_L \overset{EA}{\sim} G} G$$

Given $F, G \in \mathbb{F}_{p^n}[x]$ quadratic maps, does the existence of a linear isotopic shift connecting F to G ($F_L \overset{EA}{\sim} G$) imply the existence of a linear isotopic shift connecting G to F?

$$\begin{tikzcd} F \arrow[rr, shift left, "F_L \overset{EA}{\sim} G"] & & G \arrow[ll, shift left, dashed, "? \ G_M \overset{EA}{\sim} F"] \end{tikzcd}$$

Given $F, G \in \mathbb{F}_{p^n}[x]$ quadratic maps, does the existence of a linear isotopic shift connecting F to G ($F_L \overset{EA}{\sim} G$) imply the existence of a linear isotopic shift connecting G to F?

$$
\begin{tikzcd}
F \arrow[r, bend left=0, "F_L \overset{EA}{\sim} G"] & G \arrow[l, dashed, bend left, "? \; G_M \overset{EA}{\sim} F"]
\end{tikzcd}
$$

- YES, if F and G are isotopic equivalent quadratic planar functions

Given $F, G \in \mathbb{F}_{p^n}[x]$ quadratic maps, does the existence of a linear isotopic shift connecting F to G ($F_L \overset{EA}{\sim} G$) imply the existence of a linear isotopic shift connecting G to F?

$$\begin{tikzcd} F \arrow[r, shift left, "F_L \overset{EA}{\sim} G"] & G \arrow[l, dashed, blue, shift left, "? \; G_M \overset{EA}{\sim} F"] \end{tikzcd}$$

- YES, if F and G are isotopic equivalent quadratic planar functions
- NOT ALWAYS in general: let $F(x) = x^2$ and $G(x) = x^{p^j+1}$

Given $F, G \in \mathbb{F}_{p^n}[x]$ quadratic maps, does the existence of a linear isotopic shift connecting F to G ($F_L \overset{EA}{\sim} G$) imply the existence of a linear isotopic shift connecting G to F?

$$
\begin{tikzcd}
F \arrow[r, shift left, "F_L \overset{EA}{\sim} G"] & G \arrow[l, dashed, shift left, "?\ G_M \overset{EA}{\sim} F"]
\end{tikzcd}
$$

- YES, if F and G are isotopic equivalent quadratic planar functions
- NOT ALWAYS in general: let $F(x) = x^2$ and $G(x) = x^{p^j+1}$

YES over $\mathbb{F}_{3^3}, \mathbb{F}_{5^3}, \mathbb{F}_{7^3}$, with $j = 1$

NO over $\mathbb{F}_{3^4}, \mathbb{F}_{3^5}$, with $j = 1, 2$

Given $F, G \in \mathbb{F}_{p^n}[x]$ quadratic maps, does the existence of a linear isotopic shift connecting F to G ($F_L \overset{EA}{\sim} G$) imply the existence of a linear isotopic shift connecting G to F?

$$\begin{tikzcd} F \arrow[r, shift left, "F_L \overset{EA}{\sim} G"] & G \arrow[l, shift left, dashed, "? \; G_M \overset{EA}{\sim} F"] \end{tikzcd}$$

- YES, if F and G are isotopic equivalent quadratic planar functions
- NOT ALWAYS in general: let $F(x) = x^2$ and $G(x) = x^{p^j+1}$

YES over $\mathbb{F}_{3^3}, \mathbb{F}_{5^3}, \mathbb{F}_{7^3}$, with $j = 1$

NO over $\mathbb{F}_{3^4}, \mathbb{F}_{3^5}$, with $j = 1, 2$

The isotopic shift (together with EA-transformation), even when applied to quadratic planar functions, is not an equivalence relation.

Isotopic shift over $\mathbb{F}_{p^n}$

Isotopic shift over $\mathbb{F}_{p^n}$

Proposition ($F(x) = x^2$)

For $n = 3m$ and L a p^m-polynomial with coefficients in $\mathbb{F}_{p^m}$, if $F_L(x) = 2xL(x)$ is planar then it is affine equivalent to x^2 or to x^{p^m+1}.

Isotopic shift over $\mathbb{F}_{p^n}$

Proposition ($F(x) = x^2$)

For $n = 3m$ and L a p^m-polynomial with coefficients in $\mathbb{F}_{p^m}$, if $F_L(x) = 2xL(x)$ is planar then it is affine equivalent to x^2 or to x^{p^m+1}.

Theorem

Characterisation of planar maps $xL_1(x)^{p^i} + x^{p^i}L_2(x)$ over $\mathbb{F}_{p^n}$ with $n = km$, $m/\gcd(m,i)$ odd and L_1, L_2 p^m-polynomials.

Summary

Summary

- APN functions

Summary

- APN functions
  - isotopic shift and generalised isotopic shift
    - powerful construction methods for APN functions
    - the case $\mathbb{F}_{2^6}$

Summary

- APN functions
  - isotopic shift and generalised isotopic shift
    - powerful construction methods for APN functions
    - the case $\mathbb{F}_{2^6}$
  - equivalence among known APN families
    - reduced list of quadratic APN families to pairwise inequivalent ones

Summary

- APN functions
  - isotopic shift and generalised isotopic shift
    - powerful construction methods for APN functions
    - the case $\mathbb{F}_{2^6}$
  - equivalence among known APN families
    - reduced list of quadratic APN families to pairwise inequivalent ones
- planar functions

Summary

- APN functions
  - isotopic shift and generalised isotopic shift
    - powerful construction methods for APN functions
    - the case $\mathbb{F}_{2^6}$
  - equivalence among known APN families
    - reduced list of quadratic APN families to pairwise inequivalent ones
- planar functions
  - isotopic shift and generalised isotopic shift
    - characterisation of isotopic equivalence
    - connection between isotopic inequivalent planar maps

Summary

- APN functions
  - isotopic shift and generalised isotopic shift
    - powerful construction methods for APN functions
    - the case $\mathbb{F}_{2^6}$
  - equivalence among known APN families
    - reduced list of quadratic APN families to pairwise inequivalent ones
- planar functions
  - isotopic shift and generalised isotopic shift
    - characterisation of isotopic equivalence
    - connection between isotopic inequivalent planar maps

Possible future works

- study further the isotopic shift construction over $\mathbb{F}_{2^n}$
  - construct new families of differentially 4-uniform permutations
- study further the isotopic shift construction over $\mathbb{F}_{p^n}$
  - construct new planar families

Thank you for your attention