Quadratic APN Polynomials in Few Terms in Small Dimensions

Bo Sun

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity

Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n

Experiment
Construction of Functions
Procedures
Results and Conclusions

Quadratic APN Polynomials in Few Terms in Small Dimensions

Bo Sun

University of Bergen, Norway

The 2nd International Workshop on Boolean Functions and their Applications

July 7, 2017

Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Outline

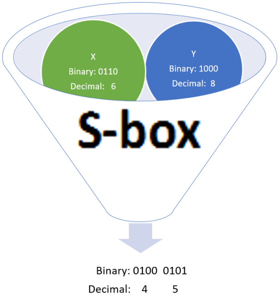
1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

S-boxes

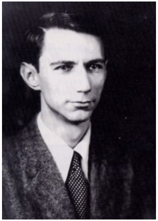
Any S-box substitutes m bits of value from one finite field to other n bits of value from the other finite field, and both sets' characteristic are 2.
S-boxes can be implemented as lookup tables.

Example of lookup table:

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16



Why S-boxes are Critical for Block Ciphers?



Claude E. Shannon (1916-2001)

- Two Properties that a good cryptosystem should have: Confusion and Diffusion
- S-boxes are important because:
  - They are the only nonlinear component in block cipher;
  - They provide confusion to symmetric block cipher;
  - There is strong connection between properties of S-boxes and resistance to many cryptographic attacks.

Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Vectorial Boolean Functions and Attacks

For n and m positive integers

Boolean functions: $f : \mathbb{F}_2^n \to \mathbb{F}_2$

Vectorial Boolean functions: $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

- Linear attacks – Nonlinearity
- Differential attacks – Differential Uniformity
- ...

Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Nonlinearity of Vectorial Boolean Functions

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

Nonlinearity of Vectorial Boolean function: Minimum Hamming distance between all nonzero linear combinations of the boolean functions over $\mathbb{F}_2^n$ and component functions of F.

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Resistance to Linear Attacks

High nonlinearity $N(F)$ is necessary to resist linear attacks.

- Universal upper bound: $N(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$;
- F is bent if $N(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$;
- Bent functions are optimal against linear attacks;
- Bent functions exist iff: n is even and $m \leq n/2$;
- When $n = m$, n is odd, the upper bound is : $N(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$;
- F is Almost Bent(AB) if $N(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$, $n = m$ and n is odd;
- When n = m, n is even, it was conjectured that upper bound is: $N(F) \leq 2^{n-1} - 2^{\frac{n}{2}}$.

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

Quadratic APN Polynomials in Few Terms in Small Dimensions

Bo Sun

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Differential Uniformity of Vectorial Boolean Functions

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is differentially δ-uniform if the equations:

$$F(x+a) - F(x) = b, \qquad \forall a \in \mathbb{F}_2^n \backslash \{0\}, \quad \forall b \in \mathbb{F}_2^m,$$

have at most δ solutions.

Resistance to Differential Attacks

Low differential uniformity is necessary.

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

- F is Perfect Nonlinear(PN) function if it is $2^{(n-m)}$-uniform;
- PN is optimal against differential attack;
  - F is bent iff it is PN;
  - PN is the highest nonlinearity and lowest uniformity
- When $n = m$, F is Almost Perfect Nonlinear(APN) function if it is 2-uniform;
- Every AB function is APN function. The converse is not true.

Optimal Functions on Uniformity and Linearity

Table 1. Optimal Functions on Uniformity and Linearity from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$

Conditions	**Functions' Name with Lowest Uniformity**	**Uniformity**	**Functions' Name with Highest Nonlinearity**	**Nonlinearity**
$m \leqslant n/2$	PN (or bent)	2^{n-m}	bent (or PN)	$2^{n-1} - 2^{\frac{n}{2}-1}$
$n/2 < m < n$	-	$> 2^{n-m}$	-	$\leqslant 2^{n-1} - \frac{1}{2}\left(3 \cdot 2^n - 2 - \frac{2(2^n-1)(2^{n-1}-1)}{(2^m-1)}\right)^{1/2}$
$m = n$, n is odd	APN	2	AB (or maximal nonlinear)	$2^{n-1} - 2^{\frac{n-1}{2}}$
$m = n$, n is even			maximal nonlinear	$\leqslant 2^{n-1} - 2^{\frac{n}{2}}$ (Conjectured as highest)

Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

Quadratic APN Polynomials in Few Terms in Small Dimensions

Bo Sun

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity

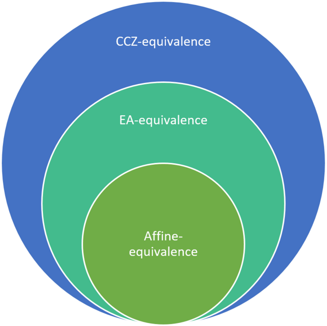
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n

Experiment
Construction of Functions
Procedures
Results and Conclusions

Three Kinds of Equivalences

Equivalent relation which has invariant differential uniformity and nonlinearity, APN-ness:

- Affine Equivalence
- Extended Affine Equivalence(EA-equivalence)
- Carlet-Charpin-Zinoviev equivalence(CCZ-equivalence)



Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

APN Power Functions

Table 2. Known families of APN power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions
Gold	$2^i + 1$	$\gcd(i, n) = 1,\ 1 \leq i < n/2$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1,\ 2 \leq i < n/2$
Welch	$2^m + 3$	$n = 2m + 1$
Niho	$2^m + 2^{\frac{m}{2}} - 1$, m even $2^m + 2^{\frac{3m+1}{2}} - 1$, m odd	$n = 2m + 1$
Inverse	$2^{n-1} - 1$	$n = 2m + 1$
Dobbertin	$2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$	$n = 5m$

Conjecture: Up to CCZ-equivalence, the list is complete.

Quadratic APN Polynomials (I)

Table 3. Known families of quadratic APN polynomials CCZ-inequivalent to power functions on $\mathbb{F}_{2^n}$

N°	Functions	Conditions
1-2	$x^{2^s+1} + \alpha^{2^k-1} x^{2^{ik}+2^{mk+s}}$	$n = pk$, $\gcd(k,p) = \gcd(s,pk) = 1$, $p \in \{3,4\}$, $i = sk \bmod p$, $m = p - i$, $n \geq 12$, α primitive in $\mathbb{F}_{2^n}^*$
3	$x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$	$q = 2^m$, $n = 2m$, $\gcd(i,m) = 1$, $\gcd(2^i+1, q+1) \neq 1$, $cb^q + b \neq 0$, $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $c^{q+1} = 1$
4	$x(x^{2^i} + x^q + cx^{2^i q})$ $+x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$	$q = 2^m$, $n = 2m$, $\gcd(i,m) = 1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^q X + 1$ is irreducible over $\mathbb{F}_{2^n}$

Quadratic APN Polynomials (II)

Table 3. Continued

N°	Functions	Conditions
5	$x^3 + a^{-1}\mathrm{tr}_1^n(a^3x^9)$	$a \neq 0$
6	$x^3 + a^{-1}\mathrm{tr}_3^n(a^3x^9 + a^6x^{18})$	$3 \mid n$, $a \neq 0$
7	$x^3 + a^{-1}\mathrm{tr}_3^n(a^6x^{18} + a^{12}x^{36})$	$3 \mid n$, $a \neq 0$
8-10	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k,3) = \gcd(s,3k) = 1$, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3 \mid (k+s)$, u primitive in $\mathbb{F}_{2^n}^*$
11	$\alpha x^{2^s+1} + \alpha^{2^k}x^{2^{k+s}+2^k} +$ $\beta x^{2^k+1} + \sum_{i=1}^{k-1}\gamma_i x^{2^{k+i}+2^i}$	$n = 2k$, $\gcd(s,k) = 1$, s, k odd, $\beta \notin \mathbb{F}_{2^k}$, $\gamma_i \in \mathbb{F}_{2^k}$, α not a cube

CCZ-inequivalent APN functions (I)

Table 4. CCZ-inequivalent APN functions on $\mathbb{F}_{2^n}$ from known APN families ($6 \leq n \leq 11$) [Budaghyan, Helleseth, Li, Sun 2017]

n	N°	Functions	Families from Tables 1-2	Relation to [*]
6	6.1	x^3	Gold	Table 5: $N^\circ 1.1$
	6.2	$x^6 + x^9 + a^7 x^{48}$	$N^\circ 3$	5: $N^\circ 1.2$
	6.3	$ax^3 + a^4 x^{24} + x^{17}$	$N^\circ 8$-10	5: $N^\circ 2.3$
7	7.1	x^3	Gold	Table 7 : $N^\circ 1.1$
	7.2	x^5	Gold	7 : $N^\circ 3.1$
	7.3	x^9	Gold	7 : $N^\circ 4.1$
	7.4	x^{13}	Kasami	7 : $N^\circ 5.1$
	7.5	x^{57}	Kasami	7 : $N^\circ 6.1$
	7.6	x^{63}	Inverse	7 : $N^\circ 7.1$
	7.7	$x^3 + \mathrm{tr}_1^7(x^9)$	$N^\circ 5$	7 : $N^\circ 1.2$
8	8.1	x^3	Gold	Table 9 : $N^\circ 1.1$
	8.2	x^9	Gold	9 : $N^\circ 1.2$
	8.3	x^{57}	Kasami	9 : $N^\circ 7.1$
	8.4	$x^3 + x^{17} + a^{48} x^{18} + a^3 x^{33} + ax^{34} + x^{48}$	$N^\circ 4$	9 : $N^\circ 2.1$
	8.5	$x^3 + \mathrm{tr}_1^8(x^9)$	$N^\circ 5$	9 : $N^\circ 1.3$
	8.6	$x^3 + a^{-1}\mathrm{tr}_1^8(a^3 x^9)$	$N^\circ 5$	9 : $N^\circ 1.5$

a: primitive root of $\mathbb{F}_{2^n}$;
[*]: Edel, Y., Pott, A.:"A New Almost Perfect Nonlinear Function Which Is Not Quadratic".

Quadratic APN Polynomials in Few Terms in Small Dimensions

Bo Sun

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonlinearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

CCZ-inequivalent APN functions (II)

Table 4. Continued

n	N°	Functions	Families from Tables 1-2
9	9.1	x^3	Gold
	9.2	x^5	Gold
	9.3	x^{17}	Gold
	9.4	x^{13}	Kasami
	9.5	x^{241}	Kasami
	9.6	x^{19}	Welch
	9.7	x^{255}	Inverse
	9.8	$x^3 + \mathrm{tr}_1^9(x^9)$	$N^\circ 5$
	9.9	$x^3 + \mathrm{tr}_3^9(x^9 + x^{18})$	$N^\circ 6$
	9.10	$x^3 + \mathrm{tr}_3^9(x^{18} + x^{36})$	$N^\circ 7$
10	10.1	x^3	Gold
	10.2	x^9	Gold
	10.3	x^{57}	Kasami
	10.4	x^{339}	Dobbertin
	10.5	$x^6 + x^{33} + a^{31}x^{192}$	$N^\circ 3$
	10.6	$x^{72} + x^{33} + a^{31}x^{258}$	$N^\circ 3$
	10.7	$x^3 + \mathrm{tr}_1^{10}(x^9)$	$N^\circ 5$
	10.8	$x^3 + a^{-1}\mathrm{tr}_1^{10}(a^3x^9)$	$N^\circ 5$

Quadratic APN Polynomials in Few Terms in Small Dimensions

Bo Sun

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

CCZ-inequivalent APN functions (III)

Table 4. Continued

n	N°	Functions	Families from Tables 1-2
11	11.1	x^3	Gold
	11.2	x^5	Gold
	11.3	x^9	Gold
	11.4	x^{17}	Gold
	11.5	x^{33}	Gold
	11.6	x^{13}	Kasami
	11.7	x^{57}	Kasami
	11.8	x^{241}	Kasami
	11.9	x^{993}	Kasami
	11.10	x^{35}	Welch
	11.11	x^{287}	Niho
	11.12	x^{1023}	Inverse
	11.13	$x^3 + \mathrm{tr}_1^{11}(x^9)$	$N^\circ 5$

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

Classification of APN Functions for Small n

Completed

- $n \leqslant 5$: only power APN functions [Brinkmann,Leander 2009]
- $n = 6$, quadratic APN functions (13 classes).

Open

- Many unclassified quadratic APN polynomials for $6 < n \leqslant 12$ [Dillon et all 2006, Edel and Pott 2009; Yu et all 2013].
- One known example of quadratic APN function (with n = 6) with non-Gold like nonlinearity [Dillon et al 2006].
- One known example of APN polynomial CCZ-ineq. to quadratics and to power functions (n=6) [Leander et al 2008; Edel and Pott 2009].
- One known example of APN permutations for n even (with n = 6, CCZ-eq. to quadratics!) [Dillon et al 2009].

Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

Quadratic APN Polynomials in Few Terms in Small Dimensions

Bo Sun

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonlinearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Trinomials

Quadratic Trinomial Functions

$F = x^{2^{i_1}+1} + x^{2^{j_2}(2^{i_2}+1)} + x^{2^{j_3}(2^{i_3}+1)}$, on $\mathbb{F}_{2^n}$ to itself. n is from 6 to 11.

Conditions for efficiency:

- if n is even: $i_1 \leqslant i_2, i_3 \leqslant \frac{n}{2}$;
  if n is odd: $i_1 \leqslant i_2, i_3 \leqslant \frac{n-1}{2}$;
- $0 \leqslant j_2, j_3 \leqslant n-1$;
- $2^{i_1} + 1 < 2^{j_2}(2^{i_2} + 1) \mod (2^n - 1) < 2^{j_3}(2^{i_3} + 1) \mod (2^n - 1)$;

Quadrinomials, Pentanomials, Hexanomials

With similar conditions as trinomial, on $\mathbb{F}_{2^n}$ to itself, $6 \leqslant n \leqslant 11$:

Quadratic Quadrinomials

$$F = x^{2^{i_1}+1} + x^{2^{j_2}(2^{i_2}+1)} + x^{2^{j_3}(2^{i_3}+1)} + x^{2^{j_4}(2^{i_4}+1)};$$

Quadratic Pentanomials

$$F = x^{2^{i_1}+1} + x^{2^{j_2}(2^{i_2}+1)} + x^{2^{j_3}(2^{i_3}+1)} + x^{2^{j_4}(2^{i_4}+1)} + x^{2^{j_5}(2^{i_5}+1)};$$

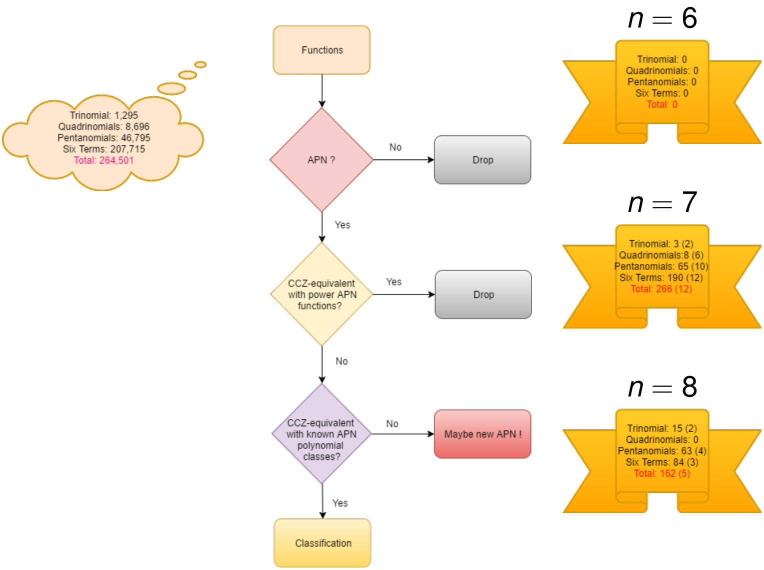
Quadratic Hexanomials

$$F = x^{2^{i_1}+1} + x^{2^{j_2}(2^{i_2}+1)} + x^{2^{j_3}(2^{i_3}+1)} + x^{2^{j_4}(2^{i_4}+1)} + x^{2^{j_5}(2^{i_5}+1)} + x^{2^{j_6}(2^{i_6}+1)}.$$

Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

Procedures, $n = 6, 7, 8$

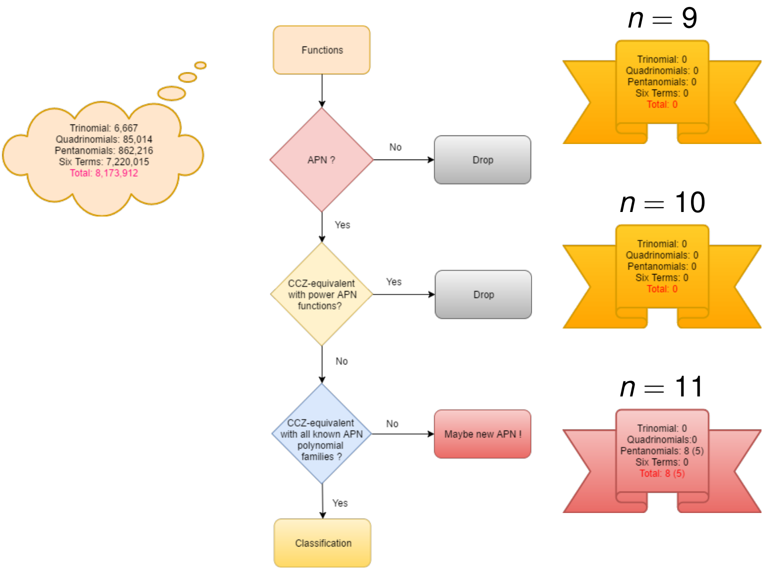


General Background
- Cryptosystems and S-boxes
- Vectorial Boolean Functions and Attacks
- Nonlinearity
- Differential Uniformity

Equivalences between Vectorial Boolean Functions
- Three Equivalences
- Infinite Families of APN Functions
- Classification of APN Functions for Small n

Experiment
- Construction of Functions
- Procedures
- Results and Conclusions

Procedures, $n = 9, 10, 11$



Outline

1. General Background
   - Cryptosystems and S-boxes
   - Vectorial Boolean Functions and Attacks
   - Nonliearity
   - Differential Uniformity
2. Equivalences between Vectorial Boolean Functions
   - Three Equivalences
   - Infinite Families of APN Functions
   - Classification of APN Functions for Small n
3. Experiment
   - Construction of Functions
   - Procedures
   - Results and Conclusions

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonliearity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Result (I)

Table 5. A number of APN polynomials (up to CCZ-equivalence) which are not CCZ-equivalent to power functions.

n	Number of Terms	Number of Polynomials
6	3 – 6	–
7	3	2
	4	6
	5	10
	6	12
8	3	2
	4	–
	5	4
	6	3
9, 10	3 – 6	–
11	3	–
	4	–
	5	5
	6	–

Result (II)

Table 6. A number of APN polynomials (up to CCZ-equivalence) which are not CCZ-equivalent to APN polynomials in fewer terms with coefficients in $\mathbb{F}_2$.

n	Number of Terms	Number of Polynomials
6	$3-6$	–
7	3	2
	4	5
	5	4
	6	1
8	3	2
	4	–
	5	2
	6	1
9, 10	$3-6$	–
11	3	–
	4	–
	5	5
	6	–

5 New APN Polynomials on $\mathbb{F}_{2^{11}}$

Table 7. New 5 APN polynomials (up to CCZ-equivalence) on $\mathbb{F}_{2^{11}}$.

Classes NO.	Polynomials
1	$x^{12} + x^{10} + x^9 + x^5 + x^3$ $x^{1536} + x^{1026} + x^{514} + x^{513} + x^3$
2	$x^{258} + x^{257} + x^{18} + x^{17} + x^3$
3	$x^{96} + x^{66} + x^{34} + x^{33} + x^3$ $x^{192} + x^{130} + x^{129} + x^{65} + x^3$
4	$x^{80} + x^{68} + x^{65} + x^{17} + x^5$ $x^{640} + x^{516} + x^{132} + x^{129} + x^5$
5	$x^{260} + x^{257} + x^{36} + x^{33} + x^5$

General Background
Cryptosystems and S-boxes
Vectorial Boolean Functions and Attacks
Nonlieարity
Differential Uniformity
Equivalences between Vectorial Boolean Functions
Three Equivalences
Infinite Families of APN Functions
Classification of APN Functions for Small n
Experiment
Construction of Functions
Procedures
Results and Conclusions

Thank you!