

Table 1: CCZ-equivalences of Families of APN Polynomials over \mathbb{F}_{2^n} from table 2 ($6 \leq n \leq 11$, u is primitive in $\mathbb{F}_{2^n}^*$)

N°	Functions*	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$	$n = 11$
1	$x^{2^s+1} + u^{2^k-1} x^{2^{ik}+2^{mk+s}}$, $p = 3$	Gold	-	-	-	-	-
2	$x^{2^s+1} + u^{2^k-1} x^{2^{ik}+2^{mk+s}}$, $p = 4$	-	-	-	-	-	-
3	$x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$	New	-	-	-	New I ($i = 1, c = u^{31}, b = 1$) New II ($i = 3, c = u^{31}, b = 1$)	-
4	$x(x^{2^i} + x^q + cx^{2^i q})$ $+x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$	$N^\circ 3$	-	New	-	$N^\circ 3$: Case I ($i = 1, c = u^3, s = u$) $N^\circ 3$: Case II ($i = 3, c = u^3, s = w$)	-
5	$x^3 + a^{-1} \text{tr}_n(a^3 x^9)$	Gold ($a = 1$) $N^\circ 3$ ($a = u$)	New	New I ($a = 1$) New II ($a = u$)	New	New I ($a = 1$) New II ($a = u$)	New
6	$x^3 + a^{-1} \text{tr}_n^3(a^3 x^9 + a^6 x^{18})$	Gold ($a = 1$) $N^\circ 3$ ($a = u$)	-	-	New	-	-
7	$x^3 + a^{-1} \text{tr}_n^3(a^6 x^{18} + a^{12} x^{36})$	Gold ($a = 1$) $N^\circ 3$ ($a = u$)	-	-	New	-	-
8	$ux^{2^s+1} + u^{2^k} x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1} x^{2^s+2^{k+s}}$, $v = 0, w \neq 0$	New	-	-	-	-	-
9	$ux^{2^s+1} + u^{2^k} x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1} x^{2^s+2^{k+s}}$, $v \neq 0, w = 0$	$N^\circ 8$	-	-	-	-	-
10	$ux^{2^s+1} + u^{2^k} x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1} x^{2^s+2^{k+s}}$, $v \neq 0, w \neq 0$	$N^\circ 8$	-	-	-	-	-
11	$(x + x^{2^m})^{2^k+1} +$ $u^{(2^n-1)/(2^m-1)}(ux + u^{2^m} x^{2^m})^{(2^k+1)2^i} +$ $u(x + x^{2^m})(ux + u^{2^m} x^{2^m})$	-	-	New ($i = 2$) $N^\circ 4$ ($i = 0$)	-	-	-

* : For the conditions for each family, please reference table 2;
- : Doesn't exist;
New : CCZ-inequivalent with other infinite families.

Table 2: Known classes of quadratic APN polynomials CCZ-inequivalent to APN monomials over \mathbb{F}_{2^n} (u is primitive in $\mathbb{F}_{2^n}^*$)

No.	Functions	Conditions
1-2 [3]	$x^{2^s+1} + u^{2^k-1}x^{2^{i k}+2^{m k}+s}$	$n = pk, \gcd(k, 3) = \gcd(s, 3k) = 1,$ $p \in \{3, 4\}, i = sk \bmod p, m = p - i,$ $n \geq 12$
3 [2]	$x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$	$q = 2^m, n = 2m, \gcd(i, m) = 1,$ $\gcd(2^i + 1, q + 1) \neq 1, cb^q + b \neq 0,$ $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}, c^{q+1} = 1$
4 [2]	$x(x^{2^i} + x^q + cx^{2^i q})$ $+x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$	$q = 2^m, n = 2m, \gcd(i, m) = 1,$ $c \in \mathbb{F}_{2^n}, s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q,$ $X^{2^i+1} + cX^{2^i} + c^q X + 1$ is irreducible over \mathbb{F}_{2^n}
5 [4, 5]	$x^3 + a^{-1} \text{tr}_n(a^3 x^9)$	$a \neq 0$
6 [5]	$x^3 + a^{-1} \text{tr}_n^3(a^3 x^9 + a^6 x^{18})$	$3 n, a \neq 0$
7 [5]	$x^3 + a^{-1} \text{tr}_n^3(a^6 x^{18} + a^{12} x^{36})$	$3 n, a \neq 0$
8-10 [1]	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$ $(x + x^{2^m})^{2^k+1} +$	$n = 3k, \gcd(k, 3) = \gcd(s, 3k) = 1,$ $v, w \in \mathbb{F}_{2^k}, vw \neq 1,$ $3 (k + s)$
11 [6]	$u^{(2^n-1)/(2^m-1)}(ux + u^{2^m}x^{2^m})^{(2^k+1)2^i} +$ $u(x + x^{2^m})(ux + u^{2^m}x^{2^m})$	$m \geq 2, 2 m, n = 2m,$ $\gcd(k, m) = 1, i$ is even

References

- [1] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and Their Applications*, 14(3):703–714, 2008.
- [2] Lilya Budaghyan and Claude Carlet. Classes of quadratic apn trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.
- [3] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two classes of quadratic apn binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

- [4] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new apn functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.
- [5] Lilya Budaghyan, Claude Carlet, and Gregor Leander. On a construction of quadratic apn functions. In *Information Theory Workshop, 2009. ITW 2009. IEEE*, pages 374–378. IEEE, 2009.
- [6] Yue Zhou and Alexander Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, 2013.