Table 1: Known infinite families of APN power functions over $\mathbb{F}_{2^n}$

Family	Exponent	Conditions	Algebraic degree	Source
Gold	2^i+1	$\gcd(i,n)=1$	2	[14, 21]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$	[17, 18]
Welch	2^t+3	$n=2t+1$	3	[12]
Niho	$2^t+2^{t/2}-1$, t even $2^t+2^{(3t+1)/2}-1$, t odd	$n=2t+1$	$(t+2)/2$ $t+1$	[11]
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	[1, 21]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$	[13]

Table 2: Known infinite families of quadratic APN polynomials over $\mathbb{F}_{2^n}$ in univariate form

ID	Functions	Conditions	Source
F1-F2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,3)=\gcd(s,3k)=1, p\in\{3,4\}, i=sk \bmod p, m=p-i, n\geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$	[5]
F3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}$	$q=2^m, n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q, X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$	[4]
F4	$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a\neq 0$	[6]
F5	$x^3+a^{-1}\mathrm{Tr}_3^n(a^3x^9+a^6x^{18})$	$3\mid n$, $a\neq 0$	[7]
F6	$x^3+a^{-1}\mathrm{Tr}_3^n(a^6x^{18}+a^{12}x^{36})$	$3\mid n, a\neq 0$	[7]
F7-F9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k, \gcd(k,3)=\gcd(s,3k)=1, v,w\in\mathbb{F}_{2^k}, vw\neq 1, 3\mid(k+s), u$ primitive in $\mathbb{F}_{2^n}^*$	[2]
F10	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n=3m, m$ odd$, L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions of Lemma 8 of [3]	[3]
F11	$x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$	$n=2m=10$, $(a,b,c)=(\beta,0,0)$, $i=3$, $k=2$, β primitive in $\mathbb{F}_{2^2}$ $n=2m$, m odd, $3\nmid m$, $(a,b,c)=(\beta,\beta^2,1)$, β primitive in $\mathbb{F}_{2^2}$, $i\in\{m-2,m,2m-1,(m-2)^{-1} \bmod n\}$ if k is even and $i\in\{m+2,m,(m+2)^{-1} \bmod n\}$ if k is odd	[8]
F12	$a\mathrm{Tr}_m^n(bx^{2^i+1})+a^q\mathrm{Tr}_m^n(cx^{2^s+1})$	$n=2m$, m odd, $q=2^m$, $a\notin\mathbb{F}_q$, $\gcd(i,n)=1$, i,s,b,c satisfy the conditions of Theorem 2	[23]
F13	$L(z)^{2^m+1}+vz^{2^m+1}$	$\gcd(s,m)=1, v\in\mathbb{F}_{2^m}^*, \mu\in\mathbb{F}_{2^{3m}}^*: \mu^{2^{2m}+2^m+1}\neq 1, L(z)=z^{2^{m+s}}+\mu z^{2^s}+z$ permutes $\mathbb{F}_{2^{3m}}$	[20]

Table 3: Known infinite families of quadratic APN polynomials over $\mathbb{F}_{2^{2m}}$ in bivariate form

ID	Functions	Conditions	Source
F14	$(xy, x^{2^k+1} + \alpha y^{(2^k+1)2^i})$	i even, $\gcd(k,m)=1$, m even, α not a cube	[24]
F15	$(xy, x^{2^{2i}+2^{3i}} + ax^{2^{2i}}y^{2^i} + by^{2^i+1})$	$\gcd(i,m)=1$, $a \in \mathbb{F}_2$, $x^{2^i+1}+ax+b$ has no root in $\mathbb{F}_{2^m}$	[22]
F16	$(xy, x^{2^i+1}+x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1})$	$\gcd(i,m)=1$, $(cx^{2^i+1}+bx^{2^i}+1)^{2^{m/2}+1}+x^{2^{m/2}+1}$ has no roots in $\mathbb{F}_{2^m}$	[9]
F17	$(x^{2^i+1} + xy^{2i} + y^{2^i+1}, x^{2^{2i}+1} + x^{2^{2i}}y + y^{2^{2i}+1})$	$\gcd(3i,m)=1$	[15]
F18	$(x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{3i}}y + xy^{2^{3i}})$	$\gcd(3i,m)=1$, m odd	[15]
F19	$(x^3+xy^2+y^3+xy, x^5+x^4y+y^5+xy+x^2y^2)$	$\gcd(3,m)=1$	[20]
F20	$(x^{q+1} + By^{q+1}, x^ry + \frac{a}{B}xy^r)$	$0<k<m$, $q=2^k$, $r=2^{k+m/2}$, $m \equiv 2 \pmod 4$, $\gcd(k,m)=1$, $a \in \mathbb{F}^*_{2^{m/2}}$, $B \in \mathbb{F}_{2^m}$, B not a cube, $B^{q+r} \neq a^{q+1}$	[16]
F21	$(x^{q+1} + xy^q + \alpha y^{q+1}, x^{q^2+1} + \alpha x^{q^2}y + (1+\alpha)^q xy^{q^2} + \alpha y^{q^2+1})$	$k,m>0$, $\gcd(k,m)=1$, $q=2^k$, $\alpha \in \mathbb{F}_{2^m}$, $x^{q+1}+x+\alpha$ has no roots in $\mathbb{F}_{2^m}$	[10]
F22	$(x^3+xy+xy^2+\alpha y^3, x^5+xy+\alpha x^2y^2+\alpha x^4y+(1+\alpha)^2xy^4+\alpha y^5)$	$\alpha \in \mathbb{F}_{2^m}$, $x^3+x+\alpha$ has no roots in $\mathbb{F}_{2^m}$	[10]

Table 4: Known infinite families of quadratic APN polynomials over $\mathbb{F}_{2^{3m}}$ in trivariate form

ID	Functions	Conditions	Source
F23	$(x^{q+1}+x^qz+yz^q, x^qz+y^{q+1}, xy^q+y^qz+z^{q+1})$	$\gcd(m,7)=1$, $q=2^i$, $\gcd(i,m)=1$ and the bivariate polynomial in [19, Conjecture 6] has no root	[19]
F24	$(x^{q+1}+xy^q+yz^q, xy^q+z^{q+1}, x^qz+y^{q+1}+y^qz)$	$\gcd(m,7)=1$, $q=2^i$, $\gcd(i,m)=1$ and the bivariate polynomial in [19, Conjecture 11] has no root	[19]

References

[1] Thomas Beth and Cunsheng Ding. On almost perfect nonlinear permutations. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 65–76. Springer, 1993.

[2] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 2011.

[3] Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S Coulter, and Irene Villa. Constructing APN functions through isotopic shifts. *IEEE Transactions on Information Theory*, 66(8):5299–5309, 2020.

[4] 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.

[5] 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.

[6] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[7] Lilya Budaghyan, Claude Carlet, and Gregor Leander. On a construction of quadratic APN functions. In *2009 IEEE Information Theory Workshop*, pages 374–378. IEEE, 2009.

[8] Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski. A new family of APN quadrinomials. *IEEE Transactions on Information Theory*, 66(11):7081–7087, 2020.

[9] Marco Calderini, Lilya Budaghyan, and Claude Carlet. On known constructions of APN and AB functions and their relation to each other. *Rad Hrvatske akademije znanosti i umjetnosti: Matematičke znanosti*, (546= 25):79–105, 2021.

[10] Marco Calderini, Kangquan Li, and Irene Villa. Extending two families of bivariate apn functions. *Finite Fields and Their Applications*, 88:102190, 2023.

[11] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): the Niho case. *Information & Computation*, 151(1):57–72, 1999.

[12] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): the Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[13] Hans Dobbertin. Almost perfect nonlinear power functions on GF(2^n): A new case for n divisible by 5. *International Conference on Finite Fields and Applications*, pages 113–121, 2001.

[14] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[15] Faruk Göloğlu. Biprojective almost perfect nonlinear functions. *IEEE Transactions on Information Theory*, 68(7):4750–4760, 2022.

[16] Faruk Göloğlu and Lukas Kölsch. Equivalences of biprojective almost perfect nonlinear functions. *arXiv preprint arXiv:2111.04197*, 2021.

[17] Heeralal Janwa and Richard M Wilson. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 180–194. Springer, 1993.

[18] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes. *Information & Computation*, 18(4):369–394, 1971.

[19] Kangquan Li and Nikolay Kaleyski. Two new infinite families of apn functions in trivariate form. *IEEE Transactions on Information Theory*, 2023.

[20] Kangquan Li, Yue Zhou, Chunlei Li, and Longjiang Qu. Two new families of quadratic APN functions. *IEEE Transactions on Information Theory*, 68(7):4761–4769, 2022.

[21] Kaisa Nyberg. Differentially uniform mappings for cryptography. *Lecture Notes in Computer Science*, 765:55–64, 1994.

[22] Hiroaki Taniguchi. On some quadratic APN functions. *Designs, Codes and Cryptography*, 87(9):1973–1983, 2019.

[23] Lijing Zheng, Haibin Kan, Yanjun Li, Jie Peng, and Deng Tang. Constructing new apn functions through relative trace functions. *IEEE Transactions on Information Theory*, 68(11):7528–7537, 2022.

[24] Yue Zhou and Alexander Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, 2013.