On the Boomerang Uniformity of some Permutation Polynomials

Marco Calderini and Irene Villa

University of Bergen (Norway) - Selmer center

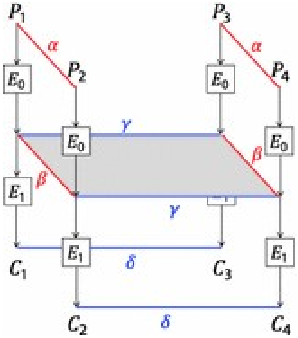
BFA 2019

Boomerang attack

- introduced in 1999 by Wagner [1]
- $\sim$ extension of differential attack
- used when it is not possible to find a high-probability trail for the entire cipher
- based on the idea of combining differential properties of smallest parts of the cipher

Classical Boomerang attack: $E = E_1 \circ E_0$

$$Pr[E_0(x) + E_0(x + \alpha) = \beta] = p \qquad Pr[E_1(x) + E_1(x + \gamma) = \delta] = q$$

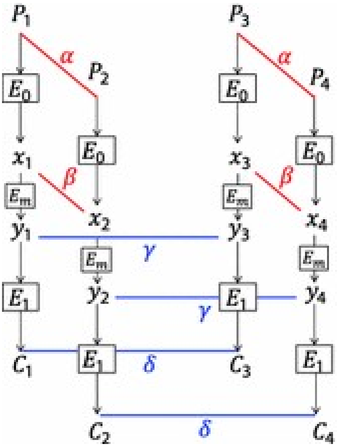


$$Pr[E^{-1}(E(x) \oplus \delta) \oplus E^{-1}(E(x \oplus \alpha) \oplus \delta) = \alpha] = p^2 \cdot q^2 \qquad (1)$$

attack: distinguisher with a data complexity corresponding to $(pq)^{-2}$ adaptive chosen plaintexts/ciphertexts
(pointed out that independences assumption used in (1) may fail)

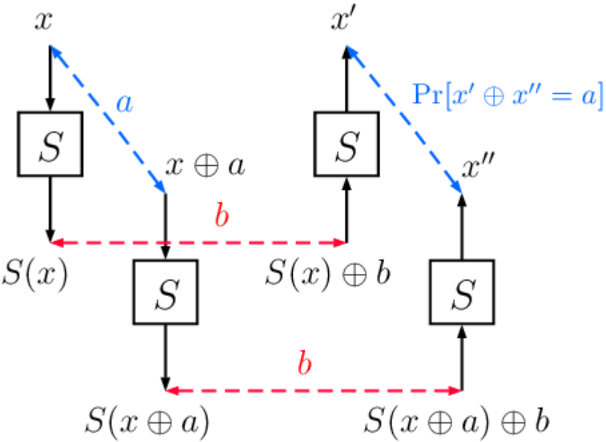
Sandwich attack: $E = E_1 \circ E_m \circ E_0$

E_m simple transformation (Sbox)

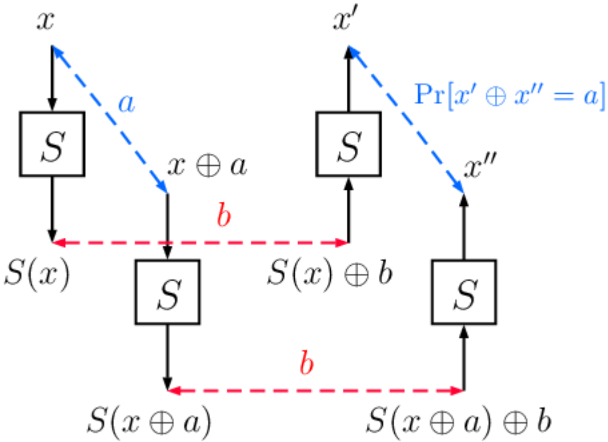


$$Pr[E_m^{-1}(E_m(x) \oplus \gamma) \oplus E_m^{-1}(E_m(x \oplus \beta) \oplus \gamma) = \beta]$$

it plays a key role when estimating the complexity of boomerang attacks and their generalizations



$$S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a$$



$$S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a$$

$$Pr[S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a]$$

Difference Distribution Table DDT

$$DDT(a,b) = \delta_S(a,b) = \sharp\{x : S(x \oplus a) \oplus S(x) = b\}$$

Differential uniformity

$$\delta_S = \max_{a \neq 0} DDT(a,b)$$

Boomerang Connectivity Table BCT (introduced in [2])

$$BCT(a,b) = \beta_S(a,b) = \sharp\{x : S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\}$$

Boomerang uniformity

$$\beta_S = \max_{a,b \neq 0} BCT(a,b)$$

Known results on the BCT

- [2] $BCT(a,b) \geq DDT(a,b)$,
- [2] if $\delta_S = 2$ then $DDT(a,b) = BCT(a,b)$ for any $a, b \neq 0$,
- [3] Boomerang uniformity is invariant under affine equivalence and inverse, not by EA-eq. and CCZ-eq
- [4] $\beta_F(a,b) = \sharp\left\{(x,y) : \begin{cases} F(x+a) + F(y+a) = b \\ F(x) + F(y) = b \end{cases}\right\}$

  Remark: if (x_0, y_0) is a solution then also $(y_0, x_0), (x_0 + a, y_0 + a), (y_0 + a, x_0 + a)$ are distinct solutions when $x_0 + a \neq y_0$,
- [4] $F(x) = x^d$ then $\beta_F = \max_{b \neq 0} \beta_F(1, b)$
- [4] F quadratic permutation with $\delta_F = \delta$ then $\delta \leq \beta_F \leq \delta(\delta - 1)$

4-uniform DDT Permutations over $\mathbb{F}_{2^n}$

function	expression	conditions
Gold	x^{2^t+1}	$n = 2k,\ k$ odd, $\gcd(n,t)$=2
Kasami	$x^{2^{2t}-2^t+1}$	$n = 2k,\ k$ odd, $\gcd(n,t)$=2
Inverse	x^{-1}	n even
Bracken-Leander	$x^{2^{2t}+2^t+1}$	$n = 4t,\ t$ odd
Bracken-Tan-Tan	$\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{-k}+2^{k+s}}$	some conditions

[3] S the inverse mapping over $\mathbb{F}_{2^n}$ n even

$$\beta_S = \begin{cases} 4, & \text{if} \quad n \equiv 2 \mod 4 \\ 6, & \text{if} \quad n \equiv 0 \mod 4 \end{cases}$$

[3] for $n \equiv 2 \bmod 4$, t even with $\gcd(t,n)$=2, then for $S(x) = x^{2^t+1}$ we have $\delta_S = 4, \beta_S = 4$

[5] for S the Bracken-Tan-Tan function $\beta_S = 4$

Computational results in [4]

Kasami:

Conditions	F	β_F	Conditions	F	β_F
$k=3, t=2$	x^{13}	4	$k=5, t=6$	x^{4033}	44
$k=3, t=4$	x^{241}	4	$k=7, t=2$	x^{13}	24
$k=5, t=2$	x^{13}	44	$k=7, t=4$	x^{241}	16
$k=5, t=4$	x^{241}	44	$k=7, t=6$	x^{4033}	16

Bracken-Leander:

Conditions	F	β_F	Conditions	F	β_F
$k=1$	x^7	4	$k=3$	x^{73}	14

[4] 4-uniform DDT permutations constructed from the inverse

$$F(x)=\begin{cases}1, & \text{if} \quad x=0,\\ 0, & \text{if} \quad x=1,\\ x^{-1}, & \text{otherwise}\end{cases} \qquad \delta_F=\begin{cases}4, & \text{if} \quad n\equiv 2 \bmod 4\\ \leq 6, & \text{otherwise}\end{cases}$$

$$\text{then } \beta_F=\begin{cases}10, & \text{if} \quad n\equiv 0 \bmod 6,\\ 8, & \text{if} \quad n\equiv 3 \bmod 6,\\ 6, & \text{if} \quad n\not\equiv 0 \bmod 3\end{cases}$$

On the Brecken-Leander function

Consider over $\mathbb{F}_{2^{4k}}$, with k odd and $q = 2^k$, the map

$$F(x) = x^{q^2+q+1}.$$

(proven in [6] that F is a differentially 4-uniform permutation)

We have that

$$\beta_F(1, b) \leq \begin{cases} 12 & \text{if } b \in \mathbb{F}_{q^2} \\ 4 \cdot r + 4 & \text{otherwise} \end{cases}$$

where r is the number of roots not in $\mathbb{F}_{q^2}$ of

$$x^{q+1} \frac{(x^{2q} + x)(x + 1)}{(x^q + x)^2} = b^{q^2} + b.$$

Computationally, we have that

- $\max r = 3$ for $k = 3, 5$ (hence $\beta_F \leq 16$)
- $\max r = 5$ for $k = 7, 9, 11, 13, 15$ (hence $\beta_F \leq 24$)

Computationally, we have that

- max $r = 3$ for $k = 3, 5$ (hence $\beta_F \leq 16$)
- max $r = 5$ for $k = 7, 9, 11, 13, 15$ (hence $\beta_F \leq 24$)

It is possible to verify theoretically that in general $r \leq 5$.

Computationally, we have that

- $\max r = 3$ for $k = 3, 5$ (hence $\beta_F \leq 16$)
- $\max r = 5$ for $k = 7, 9, 11, 13, 15$ (hence $\beta_F \leq 24$)

It is possible to verify theoretically that in general $r \leq 5$.

Theorem

Over $\mathbb{F}_{2^{4k}}$ with k odd, the differentially 4-uniform permutation $F(x) = x^{q^2+q+1}$, where $q = 2^k$, has boomerang uniformity at most 24.

Computationally, we have that

- $\max r = 3$ for $k = 3, 5$ (hence $\beta_F \leq 16$)
- $\max r = 5$ for $k = 7, 9, 11, 13, 15$ (hence $\beta_F \leq 24$)

It is possible to verify theoretically that in general $r \leq 5$.

Theorem

Over $\mathbb{F}_{2^{4k}}$ with k odd, the differentially 4-uniform permutation $F(x) = x^{q^2+q+1}$, where $q = 2^k$, has boomerang uniformity at most 24.

computational results:

$$k = 3 \quad \beta_F = 14, \quad k = 5 \quad \beta_F = 16,$$
$$k = 7 \quad \beta_F = 24, \quad k = 9 \quad \beta_F = 24, \quad k = 11 \quad \beta_F = 24$$

On the inverse modified

Over $\mathbb{F}_{2^n}$ from a cycle $\pi = (\alpha_0, \ldots, \alpha_m)$, with $\alpha_0, \ldots, \alpha_m \in \mathbb{F}_{2^n}$, F is defined as follow

$$F(x) = \pi(x)^{-1} = \begin{cases} \alpha_{i+1}^{-1} & \text{if } x = \alpha_i \\ x^{-1} & \text{if } x \notin \{\alpha_0, \ldots, \alpha_m\} \end{cases}$$

In [7] there are several constructions of such functions that are differentially 4-uniform.

Over $\mathbb{F}_{2^{2k}}$ with $c \neq 0, 1$ such that Tr(c)=Tr(c^{-1})=1 we considered the 4-DDT map from $\pi = (1, c)$

$$F(x) = \begin{cases} c^{-1} & \text{if } x = 1 \\ 1 & \text{if } x = c \\ x^{-1} & \text{otherwise} \end{cases}$$

Over $\mathbb{F}_{2^{2k}}$ with $c \neq 0, 1$ such that Tr(c)=Tr(c^{-1})=1 we considered the 4-DDT map from $\pi = (1, c)$

$$F(x) = \begin{cases} c^{-1} & \text{if } x = 1 \\ 1 & \text{if } x = c \\ x^{-1} & \text{otherwise} \end{cases}$$

Theorem

Over $\mathbb{F}_{2^{2k}}$ the differentially 4-uniform permutation $\pi^{-1}(x)$, with $\pi = (1, c)$ for $c \notin \mathbb{F}_4$ and Tr(c)=Tr(c^{-1})=1, is such that

$$\beta_F = \begin{cases} 10 & \text{if } k \equiv 0 (mod\ 2) \\ 8 & \text{if } k \equiv 1 (mod\ 2) \end{cases}$$

For k odd and $c^2 = c + 1$ we have $\beta_F = 6$.

Over $\mathbb{F}_{2^{2k}}$ with k odd $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ we considered the 4-DDT map from $\pi = (0, 1, c)$

$$F(x) = \begin{cases} 1 & \text{if } x = 0 \\ c+1 & \text{if } x = 1 \\ 0 & \text{if } x = c \\ x^{-1} & \text{otherwise} \end{cases}$$

Over $\mathbb{F}_{2^{2k}}$ with k odd $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ we considered the 4-DDT map from $\pi = (0, 1, c)$

$$F(x) = \begin{cases} 1 & \text{if } x = 0 \\ c+1 & \text{if } x = 1 \\ 0 & \text{if } x = c \\ x^{-1} & \text{otherwise} \end{cases}$$

Theorem

Over $\mathbb{F}_{2^{2k}}$, for k odd, the differentially 4-uniform permutation $\pi^{-1}(x)$, with $\pi = (0, 1, c)$ and $c^2 = c + 1$, is such that

$$\beta_F = \begin{cases} 6 & \text{if } k \not\equiv 0 (mod\ 3) \\ 8 & \text{otherwise} \end{cases}$$

Over $\mathbb{F}_{2^{2k}}$ with k odd $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ we considered the 4-DDT map from $\pi = (1, c, c+1)$

$$F(x) = \begin{cases} c+1 & \text{if } x = 1 \\ c & \text{if } x = c \\ 1 & \text{if } x = c+1 \\ x^{-1} & \text{otherwise} \end{cases}$$

Over $\mathbb{F}_{2^{2k}}$ with k odd $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ we considered the 4-DDT map from $\pi = (1, c, c+1)$

$$F(x) = \begin{cases} c+1 & \text{if } x = 1 \\ c & \text{if } x = c \\ 1 & \text{if } x = c+1 \\ x^{-1} & \text{otherwise} \end{cases}$$

Theorem

Over $\mathbb{F}_{2^{2k}}$, for k odd, the differentially 4-uniform permutation $\pi^{-1}(x)$, with $\pi = (1, c, c+1)$ and $c^2 = c+1$, is such that

$$\beta_F = \begin{cases} \leq 6 & \text{if } k \not\equiv 0 (\text{mod } 3) \\ 8 & \text{otherwise} \end{cases}$$

List of references:

[1] D. Wagner. The boomerang attack. In Lars R. Knudsen, editor, *FSE'99*, volume 1636 of *LNCS*, pg 156-170. Springer, Heidelberg, 1999.

[2] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, L. Song. Boomerang connectivity table: a new cryptanalysis tool. In Jesper Buus Nielsen and Vincent Rijmen, ediotrs, *Advances in Cryptology - EUROCRYPT 2018*, pg 683-714, Cham, Springer International Publishing, 2018.

[3] C. Boura, A. Canteaut. On the boomerang uniformity of cryptographic sboxes. *IACR Transactions on Symmetric Cryptology*, 2018(3), pg 290-310, 2018.

[4] K. Li, L. Qu, B. Sun, C. Li. New results about the boomerang uniformity of permutation polynomials. Cryptology ePrint Archive, Report 2019/079, 2019.

[5] S. Mesnager, C. Tang, M. Xiong. On the boomerang uniformity of quadratic permutations over $\mathbb{F}_{2^n}$. Cryptology ePrint Archive, Report 2019/277, 2019.

[6] C. Bracken, G. Leander. A Highly Nonlinear Differentially 4 Uniform Power Mapping That Permutes Fields of Even Degree. Finite Fields and Their Applications 16 pg 231-242, 2009

[7] Y. Li, M. Wang, Y. Yu. Constructing differentially 4-uniform permutations over $GF(2^{2k})$ from the inverse function revisited. Cryptology ePrint Archive, Report 2013/731, 2013.