Generating Graphs Packed With Paths

Philip Vejre¹ Mathias Hall-Andersen² FSE 2019

¹DTU, Akamai Technologies

²PLTC @ University of Copenhagen

Motivation

Linear Cryptanalysis & Graphs

Subgraph Heuristics (for SPN)

Plots & Results

Future Work

Motivation

[BS90]

$\mathbb{P}_{x}[E_{k}(x) + \nabla = E_{k}(x + \Delta)]$

[Mat93]

$$\mathbb{P}_{x}[\langle \alpha, x \rangle = \langle \beta, E_{k}(x) \rangle]$$

[BS90]

$$\mathbb{P}_{x}[E_{k}(x) + \nabla = E_{k}(x + \Delta)]$$

[Mat93]

$$\mathbb{P}_{x}[\langle \alpha, x \rangle = \langle \beta, E_{k}(x) \rangle]$$

[BS90]

$\mathbb{P}_{x}[E_{k}(x) + \nabla = E_{k}(x + \Delta)]$

[Mat93]

$$\mathbb{P}_{\mathbf{x}}[\langle \alpha, \mathbf{x} \rangle = \langle \beta, E_k(\mathbf{x}) \rangle]$$

In this presentation, focus on linear cryptanalysis (differential largely analogous)

[MY92], [Mat93]

$$\mathbb{P}_{x}[\langle \alpha, x \rangle = \langle \beta, E_{k}(x) \rangle]$$

Iterated Ciphers and Trails

$$E_k = E_{k_r}^{(r)} \circ \ldots \circ E_{k_2}^{(2)} \circ E_{k_1}^{(1)}$$

Iterated Ciphers and Trails

$$E_k = E_{k_r}^{(r)} \circ \ldots \circ E_{k_2}^{(2)} \circ E_{k_1}^{(1)}$$
$$U = (\alpha = u_0, \ldots, u_r = \beta)$$

Iterated Ciphers and Trails

$$E_k = E_{k_r}^{(r)} \circ \ldots \circ E_{k_2}^{(2)} \circ E_{k_1}^{(1)}$$
$$U = (\alpha = u_0, \ldots, u_r = \beta)$$
$$C_{(u_i, u_{i+1})}^{k_i}(i) = 2 \cdot \mathbb{P}_{x \in \mathbb{F}^n}[\langle u_i, x \rangle = \langle u_{i+1}, E_{k_i}^{(i)}(x) \rangle] - 1$$

Correlation contribution for linear trail¹:

$$C_U^k = \prod_{i=0}^r C_{(u_i, u_{i+1})}^{k_i}(i)$$

¹under 'Markov cipher assumption'

Correlation contribution for linear trail¹:

$$egin{aligned} \mathcal{C}_U^k &= \prod_{i=0}^r \mathcal{C}_{(u_i,u_{i+1})}^{k_i}(i) \ \mathcal{C}_{lpha,eta}^k &= \sum_{U:(u_0,u_r)=(lpha,eta)} \mathcal{C}_U^k \end{aligned}$$

¹under 'Markov cipher assumption'

$$\forall k : (C_U^k)^2 = (C_U)^2 = \prod_{i=0}^r (C_{(u_i, u_{i+1})}^k(i))^2$$

$$orall k: (C_U^k)^2 = (C_U)^2 = \prod_{i=0}^r (C_{(u_i, u_{i+1})}^k(i))^2 \ \mathbb{E}[(C_{lpha, eta})^2] pprox \sum_{U:(u_0, u_r) = (lpha, eta)} (C_U^k)^2$$

$$orall k: (C_U^k)^2 = (C_U)^2 = \prod_{i=0}^r (C_{(u_i, u_{i+1})}^k(i))^2$$
 $\mathbb{E}[(C_{\alpha, \beta})^2] pprox \sum_{U \in \mathcal{U}, (u_0, u_r) = (\alpha, \beta)} (C_U^k)^2$

$$orall k : (C_U^k)^2 = (C_U)^2 = \prod_{i=0}^r (C_{(u_i, u_{i+1})}^k(i))^2$$

 $\mathbb{E}[(C_{\alpha, \beta})^2] pprox \sum_{U \in \mathcal{U}, (u_0, u_r) = (\alpha, \beta)} (C_U)^2$

Problem: Current methods usually linear in the number of trails

Linear Cryptanalysis & Graphs

Multistage Graph



Nodes and Parities



Nodes $\alpha \in \mathbb{F}^n$ represent parities α^* for linear cryptanalysis:

 $\alpha^* : \mathbf{v} \mapsto \langle \mathbf{v}, \alpha \rangle$

Edges and Approximations



 $l(u \to v) = (C_{(u,v)}^k)^2$

Paths and Trails



 $I(v_0 \rightsquigarrow v_r) = \prod_{i=0}^{r-1} I(v_i \rightarrow v_{i+1})$



$$w_{\mathcal{G}_{\mathcal{E}}}(\alpha \diamond \beta) = \sum I(\alpha \rightsquigarrow \beta) = \sum_{v} w_{\mathcal{G}_{\mathcal{E}}}(\alpha \diamond v) \cdot I(v \rightarrow \beta)$$



$$w_{\mathcal{G}_{\mathcal{E}}}(\alpha \diamond \beta) = \sum I(\alpha \rightsquigarrow \beta) = \sum_{v} w_{\mathcal{G}_{\mathcal{E}}}(\alpha \diamond v) \cdot I(v \rightarrow \beta)$$

13



$$w_{\mathcal{G}_{\mathcal{E}}}(\alpha \diamond \beta) = \sum I(\alpha \rightsquigarrow \beta) = \sum_{v} w_{\mathcal{G}_{\mathcal{E}}}(\alpha \diamond v) \cdot I(v \rightarrow \beta)$$

13



$$w_{\mathcal{G}_{\mathcal{E}}}(\alpha \diamond \beta) = \sum I(\alpha \rightsquigarrow \beta) = \sum_{v} w_{\mathcal{G}_{\mathcal{E}}}(\alpha \diamond v) \cdot I(v \rightarrow \beta)$$

The full graph $G_{\mathcal{E}}$ is too large. (exponential in the block-size)

Can we find suitable $\bar{G}_{\mathcal{E}} \subset G_{\mathcal{E}}$, that contains the good trails?

i.e. $\max_{\alpha,\beta} w_{\bar{G}_{\mathcal{E}}}(\alpha \diamond \beta)$ is large.

Subgraph Heuristics (for SPN)

1. Pick disjoint 'families' of edges

- 1. Pick disjoint 'families' of edges
- 2. Prune the families an 'approximate' graph

- 1. Pick disjoint 'families' of edges
- 2. Prune the families an 'approximate' graph
- 3. Expand the families to a full graph

- 1. Pick disjoint 'families' of edges
- 2. Prune the families an 'approximate' graph
- 3. Expand the families to a full graph
- 4. Remove unneeded vertices & edges in resulting graph



$$l(v \to u) = 0$$



Example: 16-bit SPN, with four identical 4-bit S-Boxes.

Example: 16-bit SPN, with four identical 4-bit S-Boxes.

 $C^{2}(0x3, 0xd) = 2^{-2}$ $C^{2}(0x7, 0x4) = 2^{-2}$

Example: 16-bit SPN, with four identical 4-bit S-Boxes.

$$C^2(0x3, 0xd) = 2^{-2}$$

 $C^2(0x7, 0x4) = 2^{-2}$

$$p = (1, 2^{-2}, 1, 2^{-2})$$

Example: 16-bit SPN, with four identical 4-bit S-Boxes.

 $C^{2}(0x3, 0xd) = 2^{-2}$ $C^{2}(0x7, 0x4) = 2^{-2}$

$$p = (1, 2^{-2}, 1, 2^{-2})$$

 $E_{x}(p) = \{(0x0303, 0x0d0d), (0x0307, 0x0d04), \\ (0x0703, 0x040d), (0x0707, 0x0404)\}$

 $E_{x}(p) = \{(0x0303, 0x0d0d), (0x0307, 0x0d04), \\ (0x0703, 0x040d), (0x0707, 0x0404)\}$

 $E_{x_{in}}(p) = \{0x0303, 0x0307, 0x0703, 0x0707\}$ $E_{x_{out}}(p) = \{0x0d0d, 0x0d04, 0x040d, 0x0404\}$



Given a set of S-Box patterns $\mathcal P,$ the graph defined by $\mathcal P \colon$

$$E = \mathsf{Ex}(\mathcal{P}) = \bigcup_{p \in \mathcal{P}} \mathsf{Ex}(p)$$
$$V = \mathsf{Ex}_{in}(\mathcal{P}) \cup \mathsf{Ex}_{out}(\mathcal{P})$$

Let \mathcal{P} be a set of S-Box patterns defining our subgraph.

Let ${\mathcal P}$ be a set of S-Box patterns defining our subgraph.

For intermediate stages:

$$v \notin \mathsf{Ex}_{in}(\mathcal{P}) \cap \mathsf{Ex}_{out}(\mathcal{P}) \implies v \text{ is pruned}$$

Problem: $Ex(\mathcal{P})$ too large to store explicitly $(|Ex(\mathcal{P})| \gg |\mathcal{P}|)$

Problem: $Ex(\mathcal{P})$ too large to store explicitly $(|Ex(\mathcal{P})| \gg |\mathcal{P}|)$

Idea: Can we prune \mathcal{P} before expanding?

Problem: $E_x(\mathcal{P})$ too large to store explicitly $(|E_x(\mathcal{P})| \gg |\mathcal{P}|)$

Idea: Can we prune \mathcal{P} before expanding?

Generate an approximation of $\bar{G}_{\mathcal{E}} = \text{Ex}(\mathcal{P})$, by applying a compression function $g_j : \mathbb{F}^n \to \mathbb{F}^{n/j}$ to every vertex.

$$u o v \in \bar{\mathcal{G}}_{\mathcal{E}} \implies \hat{g}_j(u) o \hat{g}_j(v) \in \hat{g}_j(\bar{\mathcal{G}}_{\mathcal{E}})$$

Iteratively refine the compression:

- 1. Generate a set of patterns \mathcal{P} .
- 2. Pick a j > 1 such that j is a power of two:
 - 2.1 Generate the graph $\hat{g}_j(\bar{G}_{\mathcal{E}})$ from \mathcal{P} and prune.
 - 2.2 Remove dead patterns from \mathcal{P} according to $\hat{g}_j(\bar{G}_{\mathcal{E}})$.
 - 2.3 If j = 2 then stop. Otherwise set j = j/2 and repeat.

Vertex Anchoring







Plots & Results

cryptagraph

https://gitlab.com/psve/cryptagraph

Plots of subgraphs (for small parameters)

PRESENT [BKL⁺07]



GIFT [BPP⁺17]



Linear Results

Cipher (Total rounds, block size)	Rounds	$ \mathcal{A} $	а	$ \alpha \diamondsuit \beta $	ELP	Tg	Ts
1 NO 5 6Weel (12 100)	3	2 ^{29.9}	224.0	2 ¹	$2^{-53.36}$	0.0	0.0
AES [05101] (10, 128)	4	238.8	$2^{24.0}$	24	$2^{-147.88}$	2.5	20.0
mananci harminal (an in)	15 † [Bul13]	226.1	-	2 ^{31.3}	2-43.74	0.0	0.4
EPUBU-48 [TKPH11] (32, 48)	16 † [Bul13]	$2^{26.1}$	-	234.0	$2^{-46.77}$	0.0	0.4
EDODO os DecDUDI (22. 65)	31	227.6	-	2 ^{63.6}	$2^{-94.47}$	0.0	0.4
ELODO-20 [1KPH11] (32, 90)	32	$2^{27.6}$	-	263.6	$2^{-97.59}$	0.0	0.4
Fly [KG16] (20, 64)	8	2 ^{32.5}	-	2 ^{6.5}	$2^{-54.83}$	0.1	6.0
	9	2 ^{32.5}	-	2 ^{6.1}	2-63.00	0.2	8.8
GIFT-64 [BPP+17] (28, 64)	11	231.8	-	25.1	2-55.00	0.1	8.0
	12	$2^{32.7}$	-	2 ^{3.6}	$2^{-64.00}$	0.2	41.5
Khazad [BR00] (8, 64)	2	218.3	2 ^{25.0}	2 ⁰	$2^{-37.97}$	0.0	0.0
	3	2 ^{30.1}	2 ^{25.0}	2 ⁰	2-68.01	0.2	0.2
KLEIN (CNI 11) (12 64)	5	2 ^{30.8}	2 ^{17.0}	2 ⁰	2-46.0	0.0	0.0
REEIN (GNEII) (12, 04)	6	$2^{39.6}$	$2^{16.9}$	2 ⁰	$2^{-66.0}$	0.3	0.0
LED [GPPR11] (32, 64)	4	224.7	2 ²⁵	2 ²	2-48.68	0.0	0.9
MANTIS ₇ [BJK ⁺ 16] (2 · 8, 64)	2 · 4	2 ^{34.3}	2 ^{24.0}	2 ^{15.0}	2-49.05	0.1	0.0
	6	244.3	-	2 ^{19.0}	2-53.02	25.9	0.8
Midorib4 [BBI+15] (16, 64)	7	246.5	-	$2^{21.9}$	$2^{-62.88}$	53.1	5.5
	23 † [Ohk09]	231.1	-	255.0	$2^{-61.00}$	0.1	6.8
PRESENT [BKL ⁺ 07] (31, 64)	24 † [Ohk09]	$2^{31.1}$	-	257.9	$2^{-63.61}$	0.1	6.9
	25 † [Ohk09]	$2^{31.1}$	-	260.7	$2^{-66.21}$	0.1	6.9
DDIDD [ADK+14] (20, 64)	15	227.1	-	2 ⁰	$2^{-58.00}$	0.0	0.0
PRIDE [ADK ⁺ 14] (20, 64)	16	237.4	-	2 ³	$2^{-63.99}$	1.8	0.0
	2.3	218.1	-	22.0	$2^{-54.00}$	0.0	0.0
PRINCE [BCG ⁺ 12] (2 · 6, 64)	2 · 4	238.3	-	26.8	$2^{-63.82}$	2.1	0.4
PUFFIN [CHW08] (32, 64)	32	2 ^{26.8}	-	2 ^{112.4}	2-51.90	0.0	0.0
QARMA [Aval7] (2 · 8, 64)	2 · 3	2 ^{24.8}	2 ^{24.0}	25.0	2-53.71	0.0	0.0
	12 † [ZBL+14]	231.1	-	215.0	2-52.27	0.1	21.1
RECTANGLE [ZBL+14] (25, 64)	13 † [ZBL+14]	$2^{31.1}$	-	215.9	$2^{-58.14}$	0.1	25.9
	14 † [ZBL+14]	$2^{31.1}$	-	2 ^{18.3}	$2^{-62.98}$	0.1	31.1
	8	241.4	223.7	234.4	2-50.46	0.7	50.7
SKINNY-64 [BJK ⁺ 16] (32, 64)	9	$2^{41.4}$	$2^{23.9}$	$2^{31.3}$	$2^{-69.83}$	0.4	8.9

32

Differential Results

Cipher (Total rounds, block size)	Rounds	$ \mathcal{D} $	а	$ \Delta \diamondsuit \nabla $	EDP	$T_{\rm g}$	Ts
A TRUE (CT01) (10, 100)	3	218.7	224.0	2 ⁰	2-54.00	0.0	0.0
AES [05101] (10, 128)	4	$2^{36.9}$	$2^{24.0}$	2 ⁰	$2^{-150.00}$	0.7	0.3
EDGDG (0.00(0)1111 (22, 40)	13	228.4	-	2 ^{21.2}	2-43.86	0.1	13.7
EPCBC-48 [TKPH11] (32, 46)	14	$2^{28.4}$	-	220.4	$2^{-47.65}$	0.1	14.0
	20	232.8	-	216.9	$2^{-92.73}$	1.1	21.6
EPCBC-96 [TKPH11] (32, 90)	21	232.8	-	2 ^{19.9}	$2^{-97.78}$	1.1	22.6
The Breach (an et)	8	2 ^{31.6}	-	2 ^{4.9}	$2^{-55.76}$	0.1	2.6
FL1 [RG10] (20, 04)	9	2 ^{33.2}	-	27.3	$2^{-63.35}$	0.2	17.8
GIFT-64 [BPP ⁺ 17] (28, 64)	12 † [ZDY18]	222.4	-	2 ^{3.3}	$2^{-56.57}$	0.0	0.0
	13	222.4	-	2 ^{3.6}	$2^{-60.42}$	0.0	0.0
Kusan [BB00] (9, 64)	2	2 ^{25.8}	2 ^{24.8}	2 ⁰	$2^{-45.42}$	0.0	0.0
KHAZAD [BRUU] (8, 64)	3	2 ^{25.8}	2 ^{25.0}	2 ⁰	2-81.66	0.0	0.0
KLEIN (GNI 11) (12, 64)	5	2 ^{30.8}	217.0	2 ^{1.0}	$2^{-45.91}$	0.0	0.0
REEN [GNEII] (12, 04)	6	2 ^{39.7}	2 ^{24.0}	2 ^{1.0}	$2^{-69.00}$	0.3	6.4
LED [GPPR11] (32, 64)	4	237.7	2 ^{24.0}	2 ¹	2-49.42	0.5	0.1
		. 37.7		- 10.6	. 47.00		
$\texttt{MANTIS}_7 \; \texttt{[BJK^+16]} \; \texttt{(2\cdot 8, 64)}$	2 · 4	237.7	-	218.0	2-47.98	0.9	0.1
	6	242.2	2 ^{23.9}	2 ^{19.6}	$2^{-52.37}$	1.6	1.0
Midori64 [BBI+15] (16, 64)	7	$2^{42.2}$	2 ^{23.9}	222.8	$2^{-61.22}$	1.0	0.9
	15	2 ^{30.3}	-	227.2	$2^{-58.00}$	0.1	16.2
PRESENT [BKL ⁺ 07] (31, 64)	16 † [Abd12]	2 ^{30.3}	-	2 ^{28.9}	$2^{-61.80}$	0.1	18.0
	17	2 ^{30.3}	-	2 ^{32.9}	$2^{-63.52}$	0.1	18.8
	15	235.9	2 ^{23.6}	25.0	2-58.00	0.5	36.5
PRIDE [ADK 14] (20, 64)	16	235.9	$2^{23.6}$	2 ^{17.4}	$2^{-63.99}$	0.5	44.1
	2 · 3 † [CFG ⁺ 14]	214.0	219	2 ¹	$2^{-55.91}$	0.0	0.0
PRINCE [BCG 12] (2 - 0, 04)	2 · 4	238.7	-	2 ^{9.0}	$2^{-67.32}$	3.0	1.0
	32	226.0	-	2 ^{63.7}	$2^{-59.63}$	0.0	0.0
POPPIN [CHW08] (32, 64)							
04DW4 [A17] (2 9 64)	2 · 3	2 ^{24.8}	2 ^{26.0}	27.3	$2^{-56.47}$	0.1	0.0
uanna [Ava17] (2 · 0, 04)							
	13 † [ZBL+14]	231.1	-	2 ^{15.3}	$2^{-55.64}$	0.1	32.2
RECTANGLE [ZBL+14] (25, 64)	14 † [ZBL+14]	$2^{31.1}$	-	2 ^{15.9}	2-60.64	0.1	41.3
	15 † [ZBL+14]	231.1	-	218.2	2-65.64	0.1	50.2
ON THINK OF IN 1161 (22 64)	8	239.4	224.0	2 ^{31.0}	2-50.72	0.2	15.0
SKINNY-64 [BJK ⁺ 16] (32, 64)	9	241.7	223.8	231.2	$2^{-69.64}$	0.4	6.4

Cipher (Total rounds, block size)	Rounds	$ \mathcal{A} $	а	$ \alpha \diamondsuit \beta $	ELP	$T_{\rm g}$	$T_{\rm s}$
EDODO 49 04/001111 (22, 49)	15 † [Bul13]	$2^{26.1}$	-	2 ^{31.3}	$2^{-43.74}$	0.0	0.4
ЕРСВС-48 [ткрп11] (32, 48)	16 † [Bul13]	$2^{26.1}$	-	2 ^{34.0}	$2^{-46.77}$	0.0	0.4
EPCBC-96 [YKPH11] (32, 96)	31	$2^{27.6}$	-	2 ^{63.6}	2 ^{-94.47}	0.0	0.4
	32	$2^{27.6}$	-	2 ^{63.6}	$2^{-97.59}$	0.0	0.4
PRESENT [BKL ⁺ 07] (31, 64)	23 † [Ohk09]	2 ^{31.1}	-	255.0	$2^{-61.00}$	0.1	6.8
	24 † [Ohk09]	2 ^{31.1}	-	2 ^{57.9}	$2^{-63.61}$	0.1	6.9
	25 † [Ohk09]	2 ^{31.1}	-	2 ^{60.7}	$2^{-66.21}$	0.1	6.9
	32	2 ^{26.8}	-	2112.4	$2^{-51.90}$	0.0	0.0
	12 † [ZBL+14]	2 ^{31.1}	-	2 ^{15.0}	$2^{-52.27}$	0.1	21.1
RECTANGLE [ZBL ⁺ 14] (25, 64)	13 † [ZBL+14]	$2^{31.1}$	-	2 ^{15.9}	$2^{-58.14}$	0.1	25.9
	14 † [ZBL+14]	$2^{31.1}$	-	2 ^{18.3}	$2^{-62.98}$	0.1	31.1
Cipher(Total rounds, block size)	Rounds	$ \mathcal{D} $	а	$ \Delta\! \diamondsuit\! \nabla $	EDP	$T_{\rm g}$	Ts
Cipher(Total rounds, block size)	Rounds 13	D 2 ^{28.4}	a _	$\frac{ \Delta \diamondsuit \nabla }{2^{21.2}}$	EDP 2 ^{-43.86}	T _g 0.1	<i>T</i> s 13.7
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48)	Rounds 13 14	D 2 ^{28.4} 2 ^{28.4}	a 	$\begin{array}{c} \Delta \diamondsuit \nabla \\ 2^{21.2} \\ 2^{20.4} \end{array}$	EDP 2 ^{-43.86} 2 ^{-47.65}	T _g 0.1 0.1	<i>T</i> _s 13.7 14.0
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48)	Rounds 13 14 20	D 2 ^{28.4} 2 ^{28.4} 2 ^{32.8}	a - -	$\frac{ \Delta \diamondsuit \nabla }{2^{21.2}}$ $\frac{2^{20.4}}{2^{16.9}}$	EDP 2 ^{-43.86} 2 ^{-47.65} 2 ^{-92.73}	T _g 0.1 0.1 1.1	<i>T</i> _s 13.7 14.0 21.6
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48) EPCBC-96 [YKPH11] (32, 96)	Rounds 13 14 20 21	D 2 ^{28.4} 2 ^{28.4} 2 ^{32.8} 2 ^{32.8}	a - - -	$\begin{array}{c} \Delta \diamondsuit \nabla \\ 2^{21.2} \\ 2^{20.4} \\ 2^{16.9} \\ 2^{19.9} \end{array}$	EDP 2 ^{-43.86} 2 ^{-47.65} 2 ^{-92.73} 2 ^{-97.78}	T _g 0.1 0.1 1.1 1.1	<i>T</i> _s 13.7 14.0 21.6 22.6
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48) EPCBC-96 [YKPH11] (32, 96)	Rounds 13 14 20 21 15	D 2 ^{28.4} 2 ^{32.8} 2 ^{32.8} 2 ^{32.8} 2 ^{30.3}	a 	$\begin{array}{c} \Delta \diamondsuit \nabla \\ 2^{21.2} \\ 2^{20.4} \\ 2^{16.9} \\ 2^{19.9} \\ 2^{27.2} \end{array}$	EDP 2-43.86 2-47.65 2-92.73 2-97.78 2-58.00	T _g 0.1 0.1 1.1 1.1 0.1	<i>T</i> _s 13.7 14.0 21.6 22.6 16.2
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48) EPCBC-96 [YKPH11] (32, 96) PRESENT [BKL ⁺ 07] (31, 64)	Rounds 13 14 20 21 15 16 † [Abd12]	D 2 ^{28.4} 2 ^{28.4} 2 ^{32.8} 2 ^{32.8} 2 ^{30.3} 2 ^{30.3}	a 	$\begin{array}{ \Delta \diamondsuit \nabla \\ 2^{21.2} \\ 2^{20.4} \\ 2^{16.9} \\ 2^{19.9} \\ 2^{27.2} \\ 2^{28.9} \end{array}$	EDP 2-43.86 2-47.65 2-92.73 2-97.78 2-58.00 2-61.80	Tg 0.1 0.1 1.1 1.1 0.1 0.1	Ts 13.7 14.0 21.6 22.6 16.2 18.0
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48) EPCBC-96 [YKPH11] (32, 96) PRESENT [BKL ⁺ 07] (31, 64)	Rounds 13 14 20 21 15 16 † [Abd12] 17	D 2 ^{28.4} 2 ^{32.8} 2 ^{32.8} 2 ^{30.3} 2 ^{30.3} 2 ^{30.3}	a 	$\begin{array}{ \Delta \diamondsuit \nabla \\ 2^{21.2} \\ 2^{20.4} \\ 2^{16.9} \\ 2^{19.9} \\ 2^{27.2} \\ 2^{28.9} \\ 2^{32.9} \end{array}$	EDP 2-43.86 2-47.65 2-92.73 2-97.78 2-58.00 2-61.80 2-63.52	Tg 0.1 0.1 1.1 1.1 0.1 0.1 0.1	Ts 13.7 14.0 21.6 22.6 16.2 18.0 18.8
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48) EPCBC-96 [YKPH11] (32, 96) PRESENT [BKL ⁺ 07] (31, 64) PULEEIN [CLUMOR] (22, 54)	Rounds 13 14 20 21 15 16 † [Abd12] 17 32	D 2 ^{28.4} 2 ^{32.8} 2 ^{30.3} 2 ^{30.3} 2 ^{30.3} 2 ^{30.3} 2 ^{26.0}	a 	$\begin{array}{ \Delta \diamondsuit \nabla } \\ 2^{21.2} \\ 2^{20.4} \\ 2^{16.9} \\ 2^{19.9} \\ 2^{27.2} \\ 2^{28.9} \\ 2^{32.9} \\ 2^{63.7} \end{array}$	EDP 2-43.86 2-47.65 2-92.73 2-97.78 2-58.00 2-61.80 2-63.52 2-59.63	Tg 0.1 0.1 1.1 1.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1	Ts 13.7 14.0 21.6 22.6 16.2 18.0 18.8 0.0
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48) EPCBC-96 [YKPH11] (32, 96) PRESENT [BKL ⁺ 07] (31, 64) PUFFIN [CHW08] (32, 64)	Rounds 13 14 20 21 15 16 † [Abd12] 17 32	D 2 ^{28,4} 2 ^{32,8} 2 ^{32,8} 2 ^{30,3} 2 ^{30,3} 2 ^{30,3} 2 ^{26,0}	a 	$\begin{split} \Delta \diamondsuit \nabla \\ 2^{21.2} \\ 2^{20.4} \\ 2^{16.9} \\ 2^{19.9} \\ 2^{27.2} \\ 2^{28.9} \\ 2^{32.9} \\ 2^{32.9} \\ 2^{63.7} \end{split}$	EDP 2-43.86 2-47.65 2-92.73 2-97.78 2-58.00 2-61.80 2-63.52 2-59.63	Tg 0.1 0.1 1.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1	Ts 13.7 14.0 21.6 22.6 16.2 18.0 18.8 0.0
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48) EPCBC-96 [YKPH11] (32, 96) PRESENT [BKL ⁺ 07] (31, 64) PUFFIN [CHW08] (32, 64)	Rounds 13 14 20 21 15 16 † [Abd12] 17 32 13 † [ZBL+14]	D 2 ^{28.4} 2 ^{32.8} 2 ^{32.8} 2 ^{30.3} 2 ^{30.3} 2 ^{30.3} 2 ^{26.0} 2 ^{21.1}	a 	$\begin{split} \Delta \diamondsuit \nabla \\ 2^{21.2} \\ 2^{20.4} \\ 2^{16.9} \\ 2^{19.9} \\ 2^{27.2} \\ 2^{28.9} \\ 2^{32.9} \\ 2^{63.7} \\ 2^{15.3} \end{split}$	EDP 2-43.86 2-47.65 2-92.73 2-97.78 2-58.00 2-61.80 2-63.52 2-59.63 2-59.64	Tg 0.1 0.1 1.1 1.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1	Ts 13.7 14.0 21.6 22.6 16.2 18.0 18.8 0.0 32.2
Cipher(Total rounds, block size) EPCBC-48 [YKPH11] (32, 48) EPCBC-96 [YKPH11] (32, 96) PRESENT [BKL ⁺ 07] (31, 64) PUFFIN [CHW08] (32, 64) RECTANGLE [ZBL ⁺ 14] (25, 64)	Rounds 13 14 20 21 15 16 † [Abd12] 17 32 13 † [ZBL+14] 14 † [ZBL+14]	D 2 ^{28.4} 2 ^{32.8} 2 ^{30.3} 2 ^{30.3} 2 ^{30.3} 2 ^{26.0} 2 ^{31.1} 2 ^{31.1}	a 	$\begin{split} \Delta \diamondsuit \nabla \\ 2^{21.2} \\ 2^{20.4} \\ 2^{16.9} \\ 2^{19.9} \\ 2^{27.2} \\ 2^{28.9} \\ 2^{32.9} \\ 2^{63.7} \\ 2^{15.3} \\ 2^{15.9} \end{split}$	EDP 2-43.86 2-47.65 2-92.73 2-97.78 2-58.00 2-61.80 2-63.52 2-59.63 2-59.63 2-55.64 2-60.64	Tg 0.1 0.1 1.1 1.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1	Ts 13.7 14.0 21.6 22.6 16.2 18.0 18.8 0.0 32.2 41.3

Future Work

Support for ARX ciphers.

Support for ARX ciphers.

Better heuristics for Feistel networks.

cryptagraph

https://gitlab.com/psve/cryptagraph