Generating Graphs Packed With Paths

Philip Vejre[1] Mathias Hall-Andersen[2]

FSE 2019

[1]DTU, Akamai Technologies

[2]PLTC @ University of Copenhagen

Overview

Motivation

Differential and Linear Distinguishers

[BS90]

$$\mathbb{P}_x[E_k(x) + \nabla = E_k(x + \Delta)]$$

[Mat93]

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

Differential and Linear Distinguishers

[BS90]

$$\mathbb{P}_x[E_k(x) + \nabla = E_k(x + \Delta)]$$

[Mat93]

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

Differential and Linear Distinguishers

[BS90]

$$\mathbb{P}_x[E_k(x) + \nabla = E_k(x + \Delta)]$$

[Mat93]

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

Differential and Linear Distinguishers

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

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

$$U = (\alpha = u_0, \ldots, u_r = \beta)$$

$$C_{(u_i, u_{i+1})}^{k_i}(i) = 2 \cdot \mathbb{P}_{x \in \mathbb{F}^n}[\langle u_i, x \rangle = \langle u_{i+1}, E_{k_i}^{(i)}(x) \rangle] - 1$$

Hull

Correlation contribution for linear trail[1]:

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

[1] under 'Markov cipher assumption'

Hull

Correlation contribution for linear trail[1]:

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

$$C_{\alpha,\beta}^k = \sum_{U:(u_0,u_r)=(\alpha,\beta)} C_U^k$$

[1] under 'Markov cipher assumption'

Hull; Expected Linear Potential

For key-alternating ciphers (key-addition in the field):

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

Hull; Expected Linear Potential

For key-alternating ciphers (key-addition in the field):

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

$$\mathbb{E}[(C_{\alpha,\beta})^2] \approx \sum_{U:(u_0, u_r)=(\alpha,\beta)} (C_U^k)^2$$

Hull; Expected Linear Potential

For key-alternating ciphers (key-addition in the field):

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

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

Hull; Expected Linear Potential

For key-alternating ciphers (key-addition in the field):

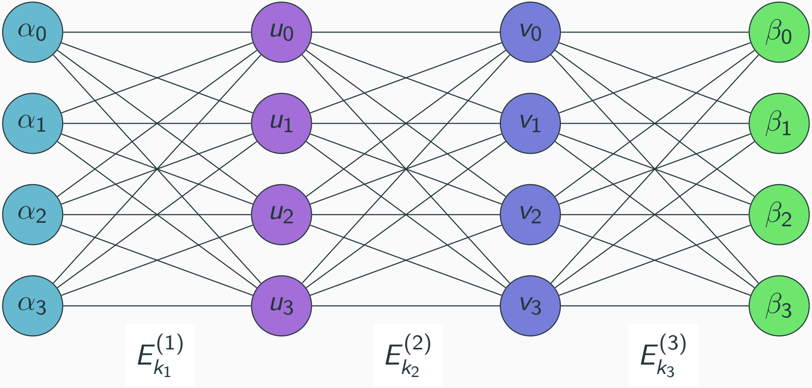
$$\forall k : (C_U^k)^2 = (C_U)^2 = \prod_{i=0}^{r} (C^k_{(u_i, u_{i+1})}(i))^2$$

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

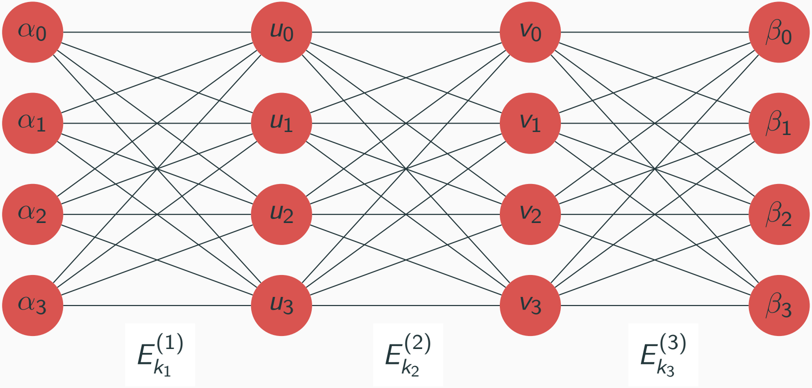
Problem: Current methods usually linear in the number of trails

Linear Cryptanalysis & Graphs

Multistage Graph



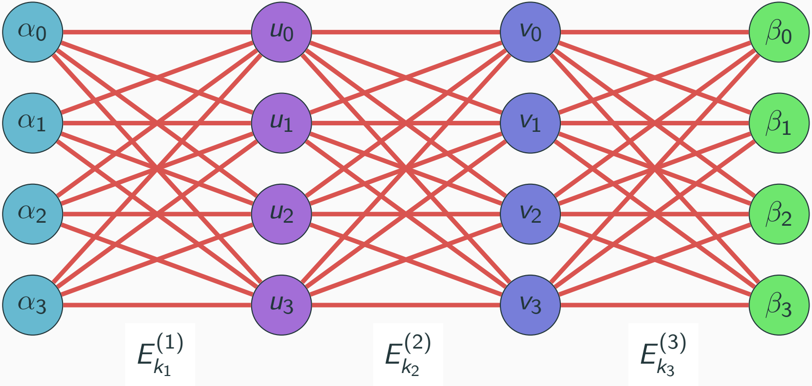
Nodes and Parities



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

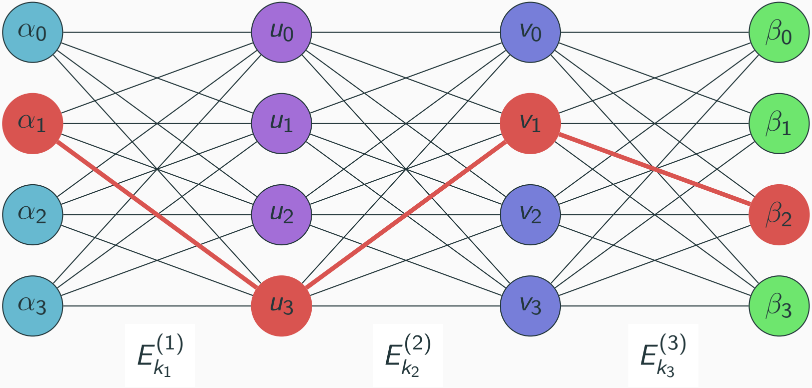
$$\alpha^* : v \mapsto \langle v, \alpha \rangle$$

Edges and Approximations



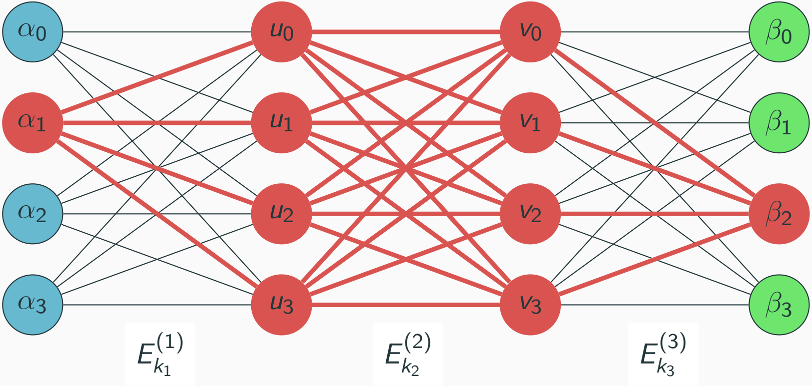
$$I(u \to v) = (C_{(u,v)}^{k})^2$$

Paths and Trails



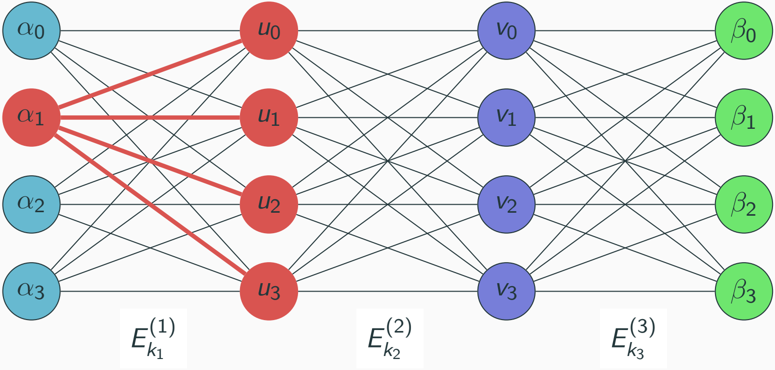
$$l(v_0 \rightsquigarrow v_r) = \prod_{i=0}^{r-1} l(v_i \to v_{i+1})$$

Hulls as Sets of Paths



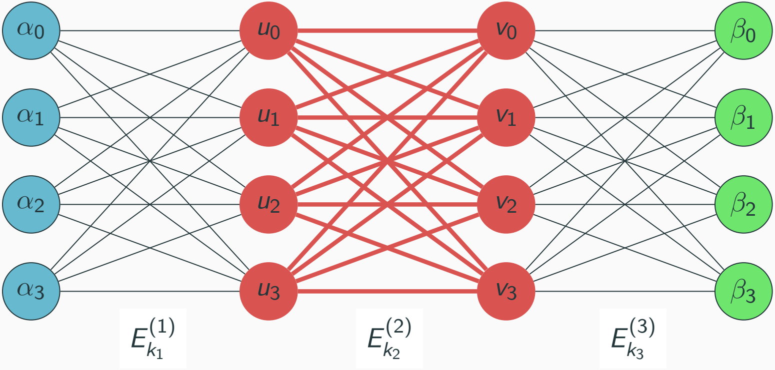
$$w_{G_{\mathcal{E}}}(\alpha \diamond \beta) = \sum l(\alpha \rightsquigarrow \beta) = \sum_{v} w_{G_{\mathcal{E}}}(\alpha \diamond v) \cdot l(v \to \beta)$$

Hulls as Sets of Paths



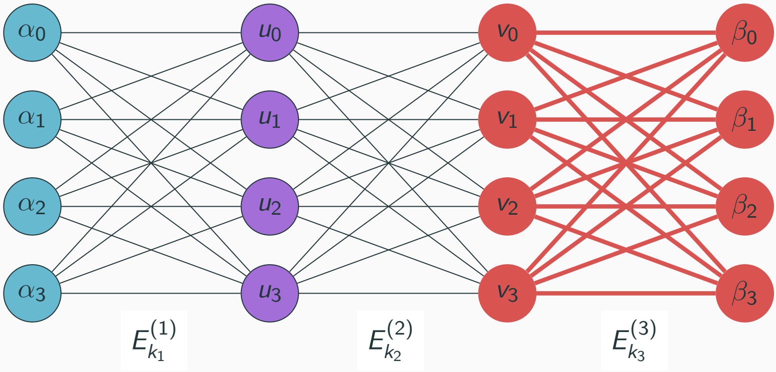
$$w_{G_{\mathcal{E}}}(\alpha \diamond \beta) = \sum l(\alpha \rightsquigarrow \beta) = \sum_{v} w_{G_{\mathcal{E}}}(\alpha \diamond v) \cdot l(v \to \beta)$$

Hulls as Sets of Paths



$$w_{G_\mathcal{E}}(\alpha \diamond \beta) = \sum I(\alpha \rightsquigarrow \beta) = \sum_v w_{G_\mathcal{E}}(\alpha \diamond v) \cdot I(v \to \beta)$$

Hulls as Sets of Paths



$$w_{G_{\mathcal{E}}}(\alpha \diamond \beta) = \sum I(\alpha \rightsquigarrow \beta) = \sum_{v} w_{G_{\mathcal{E}}}(\alpha \diamond v) \cdot I(v \to \beta)$$

Suitable Subgraphs

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)

Overall Method

1. Pick disjoint ‘families’ of edges

Overall Method

1. Pick disjoint ‘families’ of edges
2. Prune the families an ‘approximate’ graph

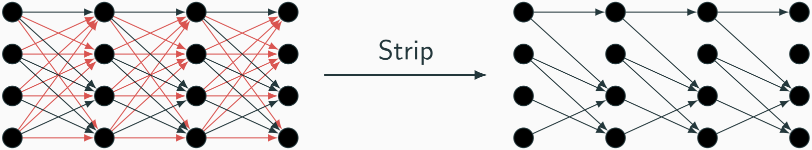
Overall Method

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

Overall Method

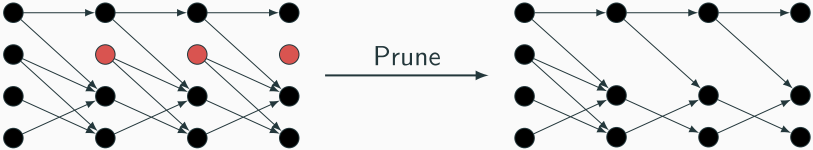
1. Pick disjoint ‘families’ of edges
2. Prune the families an ‘approximate’ graph
3. Expand the families to a full graph
4. Remove unneeded vertices & edges in resulting graph

Pruning



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

Pruning



S-Box Patterns / Families of edges

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

S-Box Patterns / Families of edges

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

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

S-Box Patterns / Families of edges

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

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

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

S-Box Patterns / Families of edges

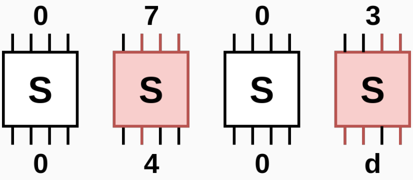
Example: 16-bit SPN, with four identical 4-bit S-Boxes.

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

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

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

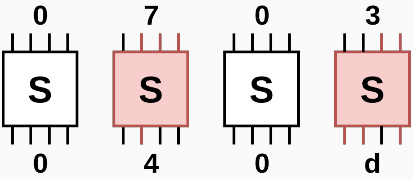
$$\mathrm{Ex}(p) = \{(\texttt{0x0303}, \texttt{0x0d0d}), (\texttt{0x0307}, \texttt{0x0d04}), (\texttt{0x0703}, \texttt{0x040d}), (\texttt{0x0707}, \texttt{0x0404})\}$$



S-Box Patterns / Families of edges

$$\mathsf{Ex}(p) = \{(\texttt{0x0303}, \texttt{0x0d0d}), (\texttt{0x0307}, \texttt{0x0d04}),$$
$$(\texttt{0x0703}, \texttt{0x040d}), (\texttt{0x0707}, \texttt{0x0404})\}$$

$$\mathsf{Ex}_{in}(p) = \{\texttt{0x0303}, \texttt{0x0307}, \texttt{0x0703}, \texttt{0x0707}\}$$
$$\mathsf{Ex}_{out}(p) = \{\texttt{0x0d0d}, \texttt{0x0d04}, \texttt{0x040d}, \texttt{0x0404}\}$$



Graph Defined By S-Box Pattern Set

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

$$E = \mathrm{Ex}(\mathcal{P}) = \bigcup_{p \in \mathcal{P}} \mathrm{Ex}(p)$$

$$V = \mathrm{Ex}_{in}(\mathcal{P}) \ \cup \ \mathrm{Ex}_{out}(\mathcal{P})$$

Graph Defined By S-Box Pattern Set

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

Graph Defined By S-Box Pattern Set

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

For intermediate stages:

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

Graph Compression

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

Graph Compression

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

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

Graph Compression

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

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

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

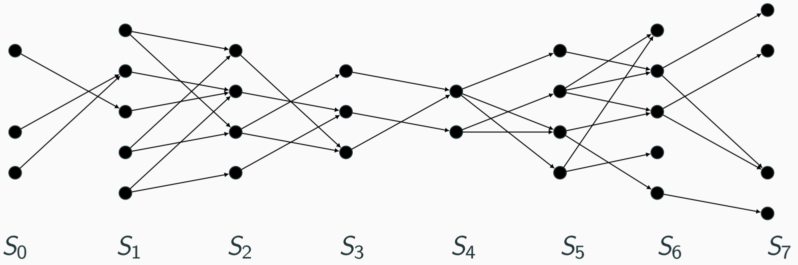
$$u \to v \in \bar{G}_{\mathcal{E}} \implies \hat{g}_j(u) \to \hat{g}_j(v) \in \hat{g}_j(\bar{G}_{\mathcal{E}})$$

Graph Compression

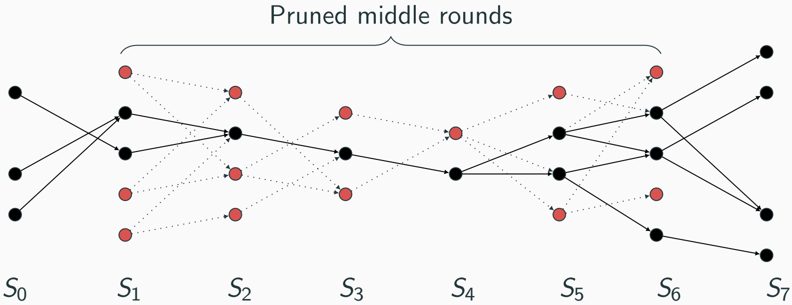
Iteratively refine the compression:

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.

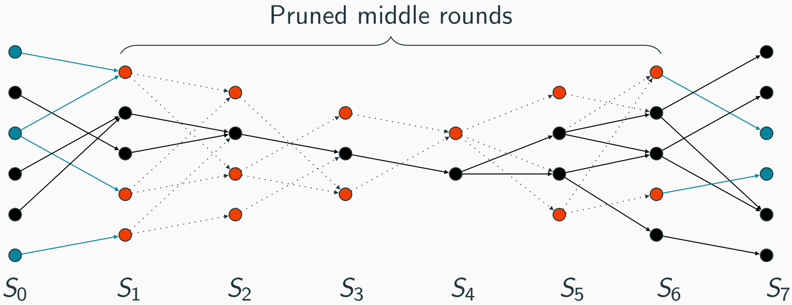
Vertex Anchoring



Vertex Anchoring



Vertex Anchoring



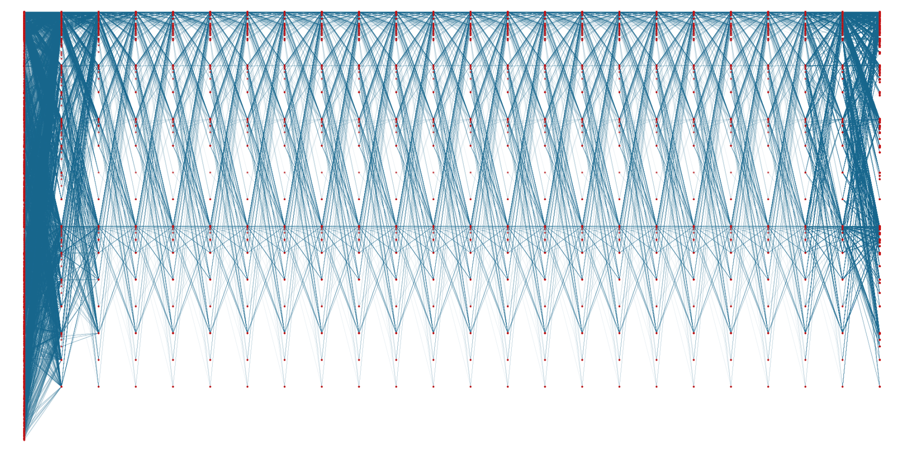
Plots & Results

cryptagraph

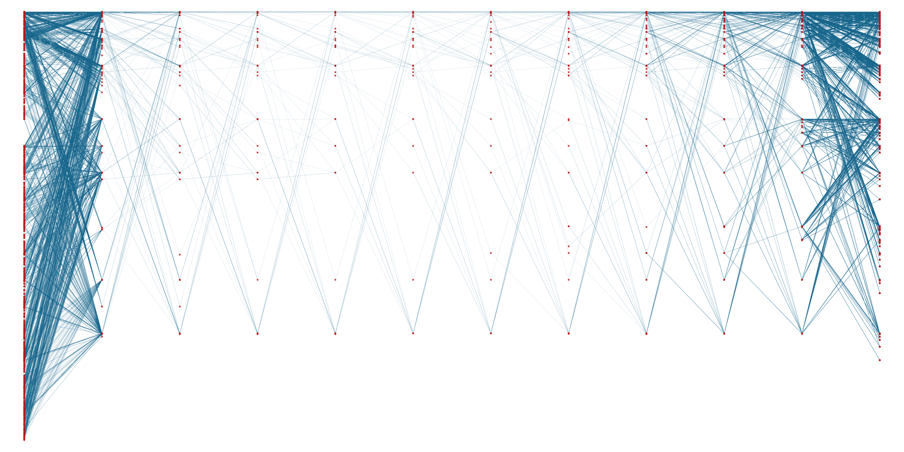
https://gitlab.com/psve/cryptagraph

Plots of subgraphs (for small parameters)

PRESENT [BKL+07]



GIFT [BPP+17]



Linear Results

Cipher (Total rounds, block size)	Rounds	$\lvert\mathcal{A}\rvert$	a	$\lvert\alpha \diamond \beta\rvert$	ELP	T_g	T_s
AES [oST01] (10, 128)	3	$2^{29.9}$	$2^{24.0}$	2^{1}	$2^{-53.36}$	0.0	0.0
	4	$2^{38.8}$	$2^{24.0}$	2^{4}	$2^{-147.88}$	2.5	20.0
EPCBC-48 [YKPH11] (32, 48)	15 † [Bul13]	$2^{26.1}$	–	$2^{31.3}$	$2^{-43.74}$	0.0	0.4
	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
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	$2^{31.8}$	–	$2^{5.1}$	$2^{-55.00}$	0.1	8.0
	12	$2^{32.7}$	–	$2^{3.6}$	$2^{-64.00}$	0.2	41.5
Khazad [BR00] (8, 64)	2	$2^{18.3}$	$2^{25.0}$	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 [GNL11] (12, 64)	5	$2^{30.8}$	$2^{17.0}$	2^{0}	$2^{-46.0}$	0.0	0.0
	6	$2^{39.6}$	$2^{16.9}$	2^{0}	$2^{-66.0}$	0.3	0.0
LED [GPPR11] (32, 64)	4	$2^{24.7}$	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
Midori64 [BBI+15] (16, 64)	6	$2^{44.3}$	–	$2^{19.0}$	$2^{-53.02}$	25.9	0.8
	7	$2^{46.5}$	–	$2^{21.9}$	$2^{-62.88}$	53.1	5.5
present [BKL+07] (31, 64)	23 † [Ohk09]	$2^{31.1}$	–	$2^{55.0}$	$2^{-61.00}$	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
PRIDE [ADK+14] (20, 64)	15	$2^{27.1}$	–	2^{0}	$2^{-58.00}$	0.0	0.0
	16	$2^{37.4}$	–	2^{3}	$2^{-63.99}$	1.8	0.0
PRINCE [BCG+12] (2 · 6, 64)	2 · 3	$2^{18.1}$	–	$2^{2.0}$	$2^{-54.00}$	0.0	0.0
	2 · 4	$2^{38.3}$	–	$2^{6.8}$	$2^{-63.82}$	2.1	0.4
PUFFIN [CHW08] (32, 64)	32	$2^{26.8}$	–	$2^{112.4}$	$2^{-51.90}$	0.0	0.0
QARMA [Ava17] (2 · 8, 64)	2 · 3	$2^{24.8}$	$2^{24.0}$	$2^{5.0}$	$2^{-53.71}$	0.0	0.0
RECTANGLE [ZBL+14] (25, 64)	12 † [ZBL+14]	$2^{31.1}$	–	$2^{15.0}$	$2^{-52.27}$	0.1	21.1
	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
SKINNY-64 [BJK+16] (32, 64)	8	$2^{41.4}$	$2^{23.7}$	$2^{34.4}$	$2^{-50.46}$	0.7	50.7
	9	$2^{41.4}$	$2^{23.9}$	$2^{31.3}$	$2^{-69.83}$	0.4	8.9

Differential Results

Cipher (Total rounds, block size)	Rounds	$\lvert\mathcal{D}\rvert$	a	$\lvert\Delta \diamond \nabla\rvert$	EDP	T_g	T_s
AES [oST01] (10, 128)	3	$2^{18.7}$	$2^{24.0}$	2^{0}	$2^{-54.00}$	0.0	0.0
	4	$2^{36.9}$	$2^{24.0}$	2^{0}	$2^{-150.00}$	0.7	0.3
EPCBC-48 [YKPH11] (32, 48)	13	$2^{28.4}$	–	$2^{21.2}$	$2^{-43.86}$	0.1	13.7
	14	$2^{28.4}$	–	$2^{20.4}$	$2^{-47.65}$	0.1	14.0
EPCBC-96 [YKPH11] (32, 96)	20	$2^{32.8}$	–	$2^{16.9}$	$2^{-92.73}$	1.1	21.6
	21	$2^{32.8}$	–	$2^{19.9}$	$2^{-97.78}$	1.1	22.6
Fly [KG16] (20, 64)	8	$2^{31.6}$	–	$2^{4.9}$	$2^{-55.76}$	0.1	2.6
	9	$2^{33.2}$	–	$2^{7.3}$	$2^{-63.35}$	0.2	17.8
GIFT-64 [BPP+17] (28, 64)	12 † [ZDY18]	$2^{22.4}$	–	$2^{3.3}$	$2^{-56.57}$	0.0	0.0
	13	$2^{22.4}$	–	$2^{3.6}$	$2^{-60.42}$	0.0	0.0
Khazad [BR00] (8, 64)	2	$2^{25.8}$	$2^{24.8}$	2^{0}	$2^{-45.42}$	0.0	0.0
	3	$2^{25.8}$	$2^{25.0}$	2^{0}	$2^{-81.66}$	0.0	0.0
KLEIN [GNL11] (12, 64)	5	$2^{30.8}$	$2^{17.0}$	$2^{1.0}$	$2^{-45.91}$	0.0	0.0
	6	$2^{39.7}$	$2^{24.0}$	$2^{1.0}$	$2^{-69.00}$	0.3	6.4
LED [GPPR11] (32, 64)	4	$2^{37.7}$	$2^{24.0}$	2^{1}	$2^{-49.42}$	0.5	0.1
MANTIS_7 [BJK+16] (2 · 8, 64)	2 · 4	$2^{37.7}$	–	$2^{18.6}$	$2^{-47.98}$	0.9	0.1
Midori64 [BBI+15] (16, 64)	6	$2^{42.2}$	$2^{23.9}$	$2^{19.6}$	$2^{-52.37}$	1.6	1.0
	7	$2^{42.2}$	$2^{23.9}$	$2^{22.8}$	$2^{-61.22}$	1.0	0.9
present [BKL+07] (31, 64)	15	$2^{30.3}$	–	$2^{27.2}$	$2^{-58.00}$	0.1	16.2
	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
PRIDE [ADK+14] (20, 64)	15	$2^{35.9}$	$2^{23.6}$	$2^{5.0}$	$2^{-58.00}$	0.5	36.5
	16	$2^{35.9}$	$2^{23.6}$	$2^{17.4}$	$2^{-63.99}$	0.5	44.1
PRINCE [BCG+12] (2 · 6, 64)	2 · 3 † [CFG+14]	$2^{14.0}$	2^{19}	2^{1}	$2^{-55.91}$	0.0	0.0
	2 · 4	$2^{38.7}$	–	$2^{9.0}$	$2^{-67.32}$	3.0	1.0
PUFFIN [CHW08] (32, 64)	32	$2^{26.0}$	–	$2^{63.7}$	$2^{-59.63}$	0.0	0.0
QARMA [Ava17] (2 · 8, 64)	2 · 3	$2^{24.8}$	$2^{26.0}$	$2^{7.3}$	$2^{-56.47}$	0.1	0.0
RECTANGLE [ZBL+14] (25, 64)	13 † [ZBL+14]	$2^{31.1}$	–	$2^{15.3}$	$2^{-55.64}$	0.1	32.2
	14 † [ZBL+14]	$2^{31.1}$	–	$2^{15.9}$	$2^{-60.64}$	0.1	41.3
	15 † [ZBL+14]	$2^{31.1}$	–	$2^{18.2}$	$2^{-65.64}$	0.1	50.2
SKINNY-64 [BJK+16] (32, 64)	8	$2^{39.4}$	$2^{24.0}$	$2^{31.0}$	$2^{-50.72}$	0.2	15.0
	9	$2^{41.7}$	$2^{23.8}$	$2^{31.2}$	$2^{-69.64}$	0.4	6.4

Cipher(Total rounds, block size)	Rounds	$\lvert\mathcal{A}\rvert$	a	$\lvert\alpha \diamond \beta\rvert$	ELP	T_g	T_s
EPCBC-48 [YKPH11] (32, 48)	15 † [Bul13]	$2^{26.1}$	–	$2^{31.3}$	$2^{-43.74}$	0.0	0.4
	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]	$2^{31.1}$	–	$2^{55.0}$	$2^{-61.00}$	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
PUFFIN [CHW08] (32, 64)	32	$2^{26.8}$	–	$2^{112.4}$	$2^{-51.90}$	0.0	0.0
RECTANGLE [ZBL+14] (25, 64)	12 † [ZBL+14]	$2^{31.1}$	–	$2^{15.0}$	$2^{-52.27}$	0.1	21.1
	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**	$\lvert\mathcal{D}\rvert$	a	$\lvert\Delta \diamond \nabla\rvert$	**EDP**	T_g	T_s
EPCBC-48 [YKPH11] (32, 48)	13	$2^{28.4}$	–	$2^{21.2}$	$2^{-43.86}$	0.1	13.7
	14	$2^{28.4}$	–	$2^{20.4}$	$2^{-47.65}$	0.1	14.0
EPCBC-96 [YKPH11] (32, 96)	20	$2^{32.8}$	–	$2^{16.9}$	$2^{-92.73}$	1.1	21.6
	21	$2^{32.8}$	–	$2^{19.9}$	$2^{-97.78}$	1.1	22.6
PRESENT [BKL+07] (31, 64)	15	$2^{30.3}$	–	$2^{27.2}$	$2^{-58.00}$	0.1	16.2
	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
PUFFIN [CHW08] (32, 64)	32	$2^{26.0}$	–	$2^{63.7}$	$2^{-59.63}$	0.0	0.0
RECTANGLE [ZBL+14] (25, 64)	13 † [ZBL+14]	$2^{31.1}$	–	$2^{15.3}$	$2^{-55.64}$	0.1	32.2
	14 † [ZBL+14]	$2^{31.1}$	–	$2^{15.9}$	$2^{-60.64}$	0.1	41.3
	15 † [ZBL+14]	$2^{31.1}$	–	$2^{18.2}$	$2^{-65.64}$	0.1	50.2

Future Work

Support for ARX ciphers.

Support for ARX ciphers.

Better heuristics for Feistel networks.

cryptagraph

https://gitlab.com/psve/cryptagraph